

Woodytoys

Administration et système réseaux

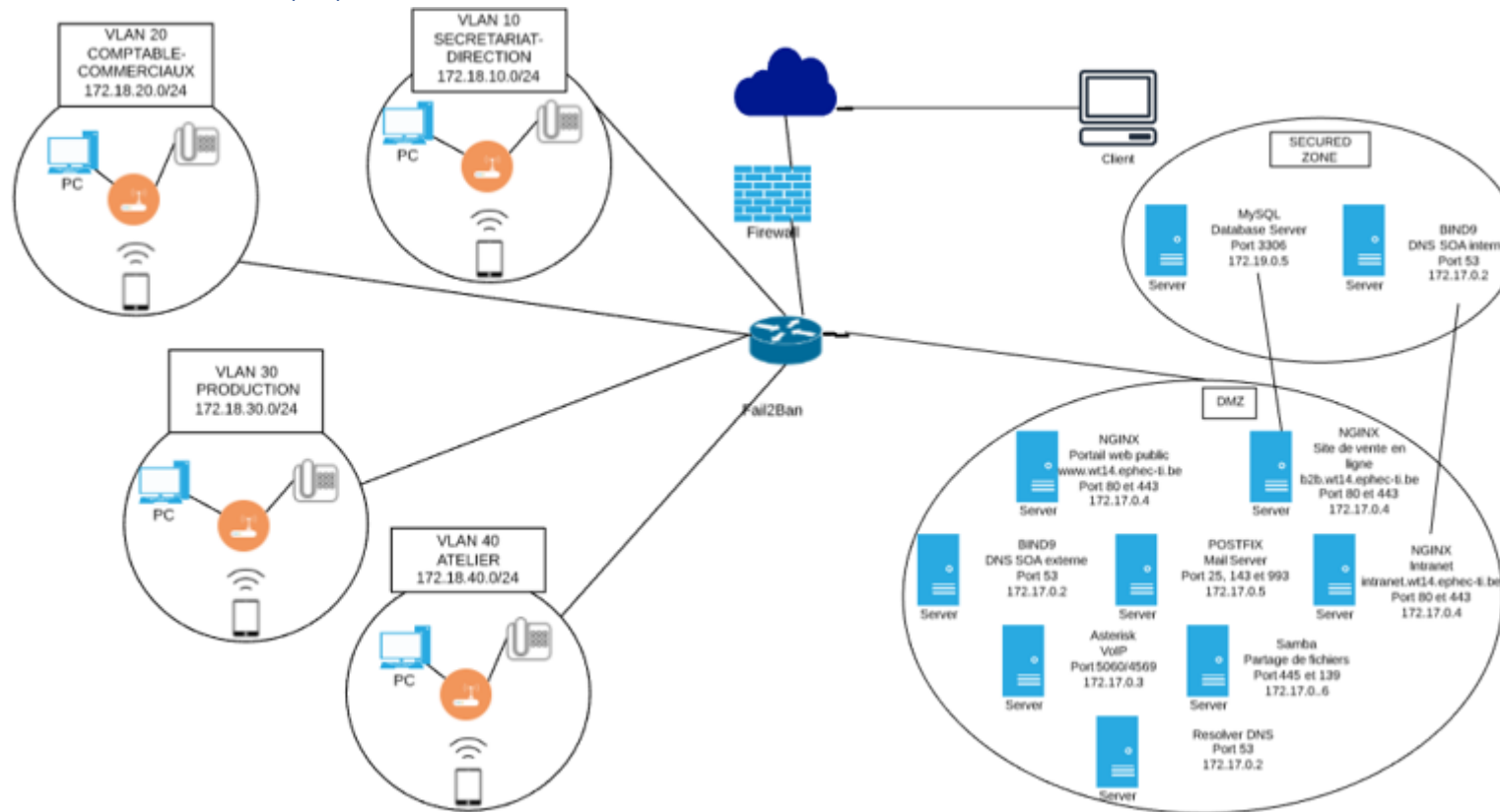
CONDE Ibrahima, LIBER Maxime et VIROUX Nicolas



Table des matières

1. Schéma Woodytoys	2
Description du schéma Woodytoys.....	2
2. Schéma prototype	3
Description du schéma prototype	3
3. Difficultés rencontrées	4
4. Justification de l'adressage.....	4
5. Validation de l'infrastructure	4
DNS	4
Web	4
Mail.....	5
VoIP	5
Partage de fichiers.....	5
6. Bilan des missions.....	5
Mission 1 :	5
Mission 2 :	5
Mission 3 :	5
7. Bilan final	6
8. Annexe.....	7
Annexe 1.....	7
Annexe 2.....	8
Annexe 3.....	9
Annexe 4.....	9
Annexe 5.....	10

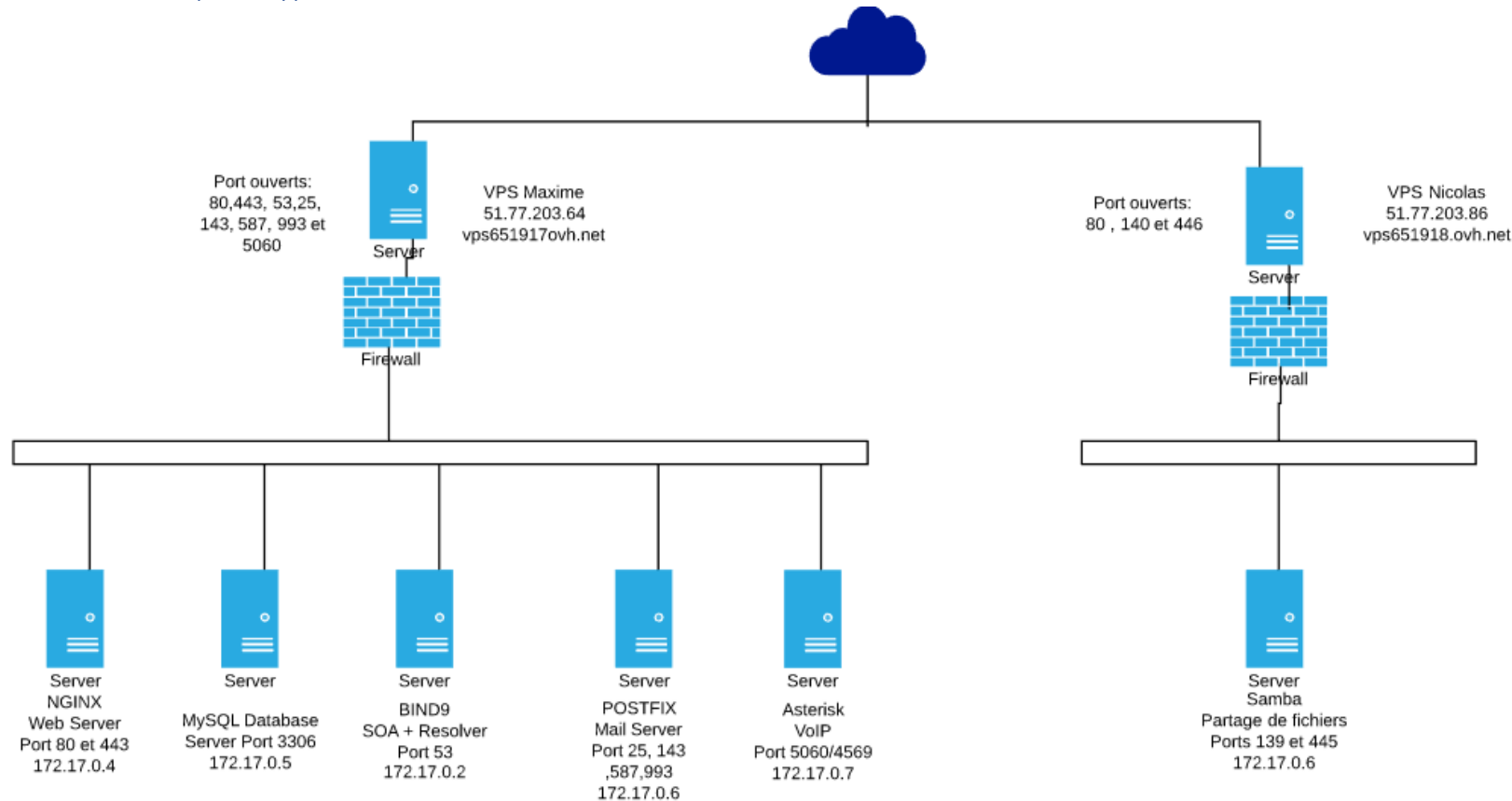
1. Schéma Woodytoys



Description du schéma Woodytoys

Nous avons mis en DMZ tous nos serveurs susceptibles d'être accédés par internet. Cependant, nous avons placé la base de données en dehors de celle-ci car elle ne doit être contactée uniquement par le serveur Web. Nous avons mis en place deux DNS (interne et externe), le serveur interne ne sera accessible qu'aux employés tandis que le serveur externe sera accessible au monde extérieur. A propos de l'adressage, nous avons fait le choix de regrouper certains départements entre eux, ce qui nous a permis de créer 4 VLANs différentes qui possèdent chacune 254 adresses disponibles.

2. Schéma prototype



Description du schéma prototype

Le VPS de Maxime contient presque la totalité des éléments mis à disposition de l'entreprise, nous avons fait ce choix afin de pouvoir effectuer nos tests d'avant déploiement sur les deux autres VPS mis à notre disposition.

Le VPS de Maxime avec l'adresse 51.77.203.64 contient donc les serveurs utiles pour le DNS, le web, le mail et le VoIP. Tandis que celui de Nicolas contient la partie concernant le partage de fichiers.

Sur le schéma vous trouverez les ports ouverts de chaque VPS ainsi que leurs adresses. De plus vous trouverez l'adresses de tous les serveurs utilisés.

3. Difficultés rencontrées

Lors du lancement de ce projet et de la mission 1, nous avons émis des problèmes quant à la compréhension du fonctionnement de Docker et ses containers. Afin de résoudre cela, nous nous sommes informés et formés sur le web via des tutoriels et des formations. En plus de cela, nous avons également perdu du temps en ce qui concerne la conception des deux sites dynamiques (b2b et intranet). A la fin de cette mission nous avons aussi eu du mal au niveau du DNS et plus particulièrement avec le fichier de zone.

Lors de la seconde mission, nous avons eu une période creuse car la tâche nous paraissait énorme et nous avons déjà accumulé un peu de retard lors de la première mission. Nous avons émis pas mal de problèmes lors de la conception du Docker File. La discussion lors du cours de 26 mars, nous a permis de découper cette tâche en différentes étapes.

Lors de la troisième mission, nous avons commencé en retard car nous avons pris plus de temps que prévu pour la configuration du mail. Un fois le VoIP commencé, nous avons rencontré des problèmes sur le VPS d'Ibrahima car il ne parvenait pas à faire de mise à jour. Finalement nous avons pris la décision de travailler sur le VPS de Nicolas. Nous avons eu quelques soucis lors de l'utilisation du logiciel X-Lite, au début nous n'arrivions pas à nous entendre.

En plus de cela, lors de la conception du système de partage de fichier. Cela n'a pas été simple car nous avons dû faire énormément de recherches dû au fait que nous n'avons pas vu cette partie en cours. Nous avons dû recommencer plusieurs fois avant d'arriver au résultat attendu.

4. Justification de l'adressage

Les adresses que nous avons utilisées sont les adresses que les containers Docker utilisent.

5. Validation de l'infrastructure

DNS

Nous avons testé notre config de DNS via plusieurs commandes effectuées directement dans le VPS. Voici quelques-unes d'entre elle :

- Dig
- Nslookup
- Nmap

En plus de cela, nous avons utilisé ce site web :

- <https://dnssec-analyzer.verisignlabs.com/>
 - Il nous a servi afin de vérifier les SOA, MX, mail, web. Vous pouvez trouver en annexe (annexe 1 à 4) les résultats obtenus lors de nos tests sur ce site.

Web

Afin de vérifier la bonne configuration de notre partie Web, nous avons tester l'accès de nos sites web via leurs noms de domaine ainsi que via leurs adresses IPv4 et IPv6.

En plus de cela, nous avons utilisé ce site web :

- <https://www.dareboost.com/fr>
 - Voir résultat en annexe 5

Mail

Nous avons testé la bonne config du mail via l'envoi de courriers électronique entre nos différents utilisateurs. Cependant le test effectué dans l'annexe 3 correspondent aussi pour cette partie. En plus de cela, nous avons utilisé ces deux sites :

- <https://mxtoolbox.com/diagnostic.aspx>
- <https://tools.dnsstuff.com/mstc>

VoIP

La seule chose que nous avons testé pour ce service est la communication entre les différents utilisateurs. Nous avons cherché des sites afin de vérifier cela mais nous n'avons malheureusement rien trouvé.

Partage de fichiers

Afin de voir que les fichiers sont bien envoyés, nous avons créé un fichier sur le VPS, par la suite nous avons lié le VPS avec le conteneur adéquat et nous avons vérifié que le fichier était bien présent.

6. Bilan des missions

Mission 1 :

Ce début de projet a été compliqué car c'est la première fois que nous étions face à une tâche d'une telle ampleur. Cependant nous avons essayé de répartir les tâches entre nous afin d'y voir plus clair. Nous sommes parvenus à atteindre ce que nous nous étions fixé comme objectif malgré quelques soucis que nous allons corriger dès que possible.

Mission 2 :

Cette mission a été compliquée pour notre groupe car nous ne savions pas par quoi commencer. Tout d'abord nous devions corriger et compléter ce qu'il fallait dans la mission 1. Par la suite nous avons un peu bloqué sur le démarrage du mail jusqu'à ce qu'on en parle durant le cours de mardi.

Mission 3 :

Cette mission est celle qui s'est le mieux déroulé car nous avons déjà beaucoup plus de connaissances que pendant les missions précédentes. Nous sommes parvenus à atteindre nos objectifs et avons même pris le temps de mettre en place certains points bonus.

7. Bilan final

Nous avons émis de la difficulté au départ au niveau de la compréhension du fonctionnement de Docker. Cela nous a fait perdre du temps lors de la première mission. Une fois cette étape passée, nous avons su nous organiser pour rattraper notre retard et répartir le travail.

Cependant nous avons encore perdu du temps lors de la création du serveur mail, c'est la mission dans laquelle nous avons rencontrés le plus d'obstacles (pas d'images, les diverses configurations,...).

Après cette étape finie, nous n'avons pas émis trop de problèmes quant à la création de notre serveur VoIP. Mais nous ne sommes pas parvenus à créer une communication avec un autre groupe malgré plusieurs tentatives.

A la fin de ce projet, nous avons encore un peu de temps à consacrer à la partie « partage de fichiers » et après nombreuses recherches nous avons réussi à configurer celle-ci.

En conclusion, nous avons apprécié travailler sur ce projet car nous avons appris énormément de choses.

Nous avons dû faire beaucoup de recherches en plus de ce que l'on avait vu en cours, ce qui nous a poussé à apprendre par nous-mêmes. C'est un domaine dans lequel nous n'avions jamais fait autant de pratique et nous avons aimé travailler sur du « réel ».

Pour finir l'entente dans le groupe s'est bien déroulée et nous avons su nous arranger entre nous pour nous répartir le travail car nous nous connaissons bien et ce n'est pas le premier projet que nous faisons ensemble.













8. Annexe

Annexe 1

Information à des serveurs de noms faisant autorité















✓	Nameservers déclaré à autorité	Selon l'autorité des serveurs de noms il ya des 1 serveurs de noms pour les wt14.ephec-ti.be domaine: ns1.wt14.ephec-ti.be - 51.77.203.64 Tous les tests individuels ci-dessous qui comportent des serveurs de noms faisant autorité seront fait par interrogation ns1.wt14.ephec-ti.be .
✓	Validité nom Nameservers	Tous les serveurs de noms énumérés à l'autorité pour wt14.ephec-ti.be domaine ont des noms valides.
✓	IP publique pour serveurs	Tous les serveurs de noms énumérés à l'autorité ont IP publique.
✓	Répondre aux serveurs de noms pour de domaine	Tous les serveurs de noms énumérés à l'autorité sont répondre aux questions au sujet wt14.ephec-ti.be de domaine.
⚠	Test de serveurs de noms récursifs pour	Certains de ces serveurs permet des requêtes récursives. Ce n'est pas une bonne mesure car il peut permettre à un empoisonnement DNS: ns1.wt14.ephec-ti.be - Recursive
⚠	TCP test pour serveurs	Pas tous les serveurs de noms requêtes réponse que sujet wt14.ephec-ti.be de domaine autorise les connexions TCP: ns1.wt14.ephec-ti.be - Ne permet pas le protocole TCP
❗	Même les serveurs de noms au TLD et autoritaire	Il ya des différences entre les serveurs énumérés au TLD et ceux fournies par autorité. Voir ci-dessus pour plus de détails.
⚠	Plusieurs serveurs de noms	Il n'ya pas assez serveurs de noms pour ce domaine. Selon RFC2182 article 5, un domaine doit avoir au au moins 3 serveurs de noms et pas plus à 7. Ce domaine a 1 serveurs de noms.
✓	Différents sous-réseaux	Tous les serveurs de noms se trouvent sur différents sous-réseaux. C'est une configuration fiable. Voir ci-dessus pour plus de détails.
✓	Différents numéros AS	Tous les serveurs de noms sont situés sur différents systèmes autonomes. C'est une configuration fiable: ns1.wt14.ephec-ti.be - AS16276
⚠	Version Nameserver logiciels	Certains de ces serveurs de noms révèle leur logiciel version. Bien que la sécurité par l'obscurité est pas la sécurité, c'est une bonne mesure à prendre. En outre, cela peut être une fausse alerte puisque la version peut être falsifiée ou une chaîne personnalisée, voir ci-dessous: ns1.wt14.ephec-ti.be - "9.11.3-1ubuntu1.5-Ubuntu "
✓	Boîteux nameservers	Tous les serveurs de noms, la réponse autoritaire pour le domaine.
✓	Domaine CNAME	Il ne fait aucun enregistrement CNAME pour wt14.ephec-ti.be de domaine. C'est une bonne chose selon RFC1912 2.4 et 10.3 RFC2181.
✓	Serveur de noms CNAME	Il ne fait aucun enregistrement CNAME pour serveurs d' wt14.ephec-ti.be de domaine. C'est une bonne chose selon RFC1912 2.4 et 10.3 RFC2181.

Annexe 2**SOA informations**

	Enregistrement SOA	<p>L'enregistrement SOA, comme des ns1.wt14.ephec-ti.be:</p> <p>Nameserver primaire: ns1.wt14.ephec-ti.be Hostmaster: root.wt14.ephec-ti.be Série: 1 Actualiser: 10800 Réessayer: 15 Expirez: 604800 TTL par défaut: 10800</p>
	Série sur tous les serveurs de noms mêmes	Tous les serveurs de noms ont la même série.
	Primaires même sur tous les serveurs de noms	Tous les serveurs de noms annoncer les mêmes nameserver primaire.
	SOA serveur primaire	Le serveur de noms primaire en fonction de l'enregistrement SOA est pointant correctement à l'un des serveurs de noms énumérés au fait autorisé.
	SOA Hostmaster	Le hostmaster adresse e-mail en fonction de l'enregistrement SOA est valide: class="pagetext-important">root.wt14@ephec-ti.be.
	SOA Serial	Serial est un entier, mais il n'est pas dans le format recommandé. Il est recommandé de format est AAAAMMJJnn, où nn est le numéro de modification en ce jour. Par exemple: 2010092402 signifie que le seconde modification faite le 24 Septembre 2010.
	SOA Refresh	La valeur de rafraîchissement en fonction de l'enregistrement SOA est 10800 secondes. Valeur recommandée en fonction de RIPE.NET  est de 86400 secondes (24 heures).
	SOA Réessayer	La valeur réessayer en fonction de l'enregistrement SOA est 15 secondes qui est trop faible. Valeur recommandée en fonction de RIPE.NET  est 7200 secondes (2 heures).
	Expire SOA	La valeur réessayer en fonction de l'enregistrement SOA est 604800 secondes. Valeur recommandée en fonction de RIPE.NET  est 3600000 secondes (1000 heures).
	SOA Minimum TTL	La valeur minimale TTL fonction enregistrement SOA est 10800 secondes . Valeur recommandée en fonction de RIPE.NET  est 172800 secondes (2 jours).

Annexe 3

Informations MX

	Les enregistrements MX	Selon l' ns1.wt14.ephec-ti.be serveur, wt14.ephec-ti.be de domaine a 1 échangeurs de messagerie: mail.wt14.ephec-ti.be - 51.77.203.64, Prio 10
	MX même sur tous les serveurs de noms	Tous les serveurs de noms rapport du échangeurs même mail.
	MX nom valide	Tous les échangeurs de courrier pour wt14.ephec-ti.be domaine ont des noms valides.
	MX est IP	Aucun des échangeurs de messagerie pour wt14.ephec-ti.be domaine sont fixé comme IP plutôt qu'un nom.
	MX a IP publique	Tous les échangeurs de courrier pour wt14.ephec-ti.be de domaine qui ont des IPs publiques. Voir ci-dessus pour plus de détails.
	IP double emploi avec pour MX	Domaine wt14.ephec-ti.be a MXs trop peu, tester sauter.
	MX a record A	Tous les échangeurs de courrier pour wt14.ephec-ti.be domaine ont des dossiers fixée au A autorité serveurs de noms.
	MX enregistrement CNAME	Aucun des échangeurs de messagerie pour wt14.ephec-ti.be domaine ont CNAME records.
	MX A requête retourne CNAME	Aucun des échangeurs de messagerie pour wt14.ephec-ti.be domaine renvoie enregistrement CNAME lorsqu'il est interrogé pour un enregistrement A.
	PTR record pour MX	Tous les échangeurs de courrier pour wt14.ephec-ti.be domaine ont PTR records: 64.203.77.51.in-addr.arpa - 64.ip-51-77-203.eu
	PTR record pour MX correspond au nom du	Certains d'échangeurs de courrier pour wt14.ephec-ti.be domaine ont des enregistrements PTR qui ne sont pas identiques à leurs noms: mail.wt14.ephec-ti.be - 64.ip-51-77-203.eu
	Nombre de MX	Domaine wt14.ephec-ti.be ont 1 Les enregistrements MX. Ce n'est pas une configuration fiable.
	MX sur différents sous-réseaux	Domaine wt14.ephec-ti.be a MXs trop peu, tester sauter.
	MX sur AS différents	Domaine wt14.ephec-ti.be a MXs trop peu, tester sauter.

Annexe 4

Les détails du système e-mail

	SPF enregistrement	Selon ns1.wt14.ephec-ti.be l'enregistrement SPF pour wt14.ephec-ti.be est: v=spf1 a mx ip4:51.77.203.64 include: _spf.google.com ~all
---	--------------------	--

Les détails du système Web

	WWW A enregistrement	Selon ns1.wt14.ephec-ti.be l'adresse IP de www.wt14.ephec-ti.be est: 51.77.203.64
	WWW enregistrement CNAME	Selon ns1.wt14.ephec-ti.be l'enregistrement CNAME du www.wt14.ephec-ti.be est: web.wt14.ephec-ti.be
	WWW a IP publique	Toutes les adresses IP qui www.wt14.ephec-ti.be décide de sont publiques.
	Le statut du serveur HTTP	Code de retour HTTP lors de l'accès www.wt14.ephec-ti.be est la suivante: 301 Redirect: Moved Permanently Ce code signifie que le service web est en marche mais redirige l'indice de www.wt14.ephec-ti.be .

Annexe 5

Analyse de qualité et performance web

<http://www.wt14.ephec-ti.be>

Rapport généré le 4 juin 2019 09:37:59

 Télécharger le rapport