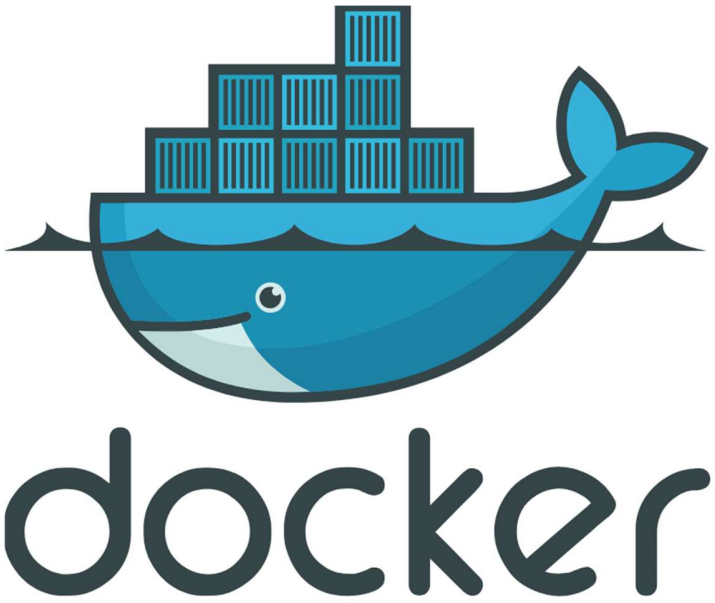
Baugnies Steffi
Bonhomme Jean-Baptiste
Dambois Pierre

2TL1
2016-2017
Groupe 1

L'entreprise WoodyToys
wt1.ephec-ti.be



Les demandes

Le travail qui nous a été demandé est de conceptualiser une architecture de réseau pour votre entreprise (WoodyToys). Cette architecture doit répondre à certaines attentes pour moderniser votre réseau vieillissant.

www.wt1.ephec-ti.be
L'infrastructure doit disposer d'un site web à destination des clients. Ce site est assez simple car il ne s'agit que d'une présentation de l'entreprise et des produits. Le but est évidemment que ce site soit joignable depuis internet pour que les clients potentiels puissent facilement y avoir accès.

b2b.wt1.ephec-ti.be
Un site B2B (business-to-business) nous est également demandé, et celui-ci pour pouvoir gérer les commandes des revendeurs. Celui-ci doit donc être dynamique. Un site dynamique est un site donc le contenu change est fonction de l'interaction avec l'utilisateur. Par exemple pour être capable de gérer un système de recherche et de commande de produits. Il doit également disposer d'une base de données permettant d'enregistrer les divers produits ainsi que les informations sur les différentes commandes et les clients qui les passent.

intranet.wt1.ephec-ti.be
Le dernier site de l'architecture est pour les employés, l'intranet. Les employés doivent disposer d'un ERP (Entreprise Resource Planning) pour l'organisation de l'entreprise. Seuls les employés doivent pouvoir accéder à cet ERP mais ils doivent quand même avoir accès à Internet. Comme les employés se accèderons à un ERP, cet intranet doit également se connecter à une base de données.

Le service mail
Il est également nécessaire pour l'entreprise de disposer d'une boîte mail pour l'ensemble de ses employés. C'est à dire que chaque employé doit avoir une adresse et qu'il faut aussi des adresses de service générique. Chaque employé disposera d'une adresse mail type nom.prenom@<domaine>. Il y aura plusieurs adresses mail de service génériques, une pour le b2b (b2b@<domaine>) et une pour le site principal (contact@<domaine>). Chacune de ces adresses mail doit bien-sûr avoir le même domaine et les mails envoyés aux adresses génériques doivent être redirigées vers l'employé adapté du service en question. Les mails doivent pouvoir être échangés entre les adresses de l'entreprise mais aussi avec n'importe quel adresse mail externe.

Le proxy et reverse proxy
L'infrastructure doit disposer d'un reverse proxy, il s'agit d'une protection pour les serveurs. L'intranet doit, quant à lui, disposer d'un proxy qui a pour but de restreindre l'accès à l'intranet aux employés uniquement dans le cadre du réseau local de l'entreprise. L'intérêt de ces deux dispositifs est de filtrer les connexions entrantes et sortantes, assurant la protection des données de l'entreprise.

Le service téléphonique
L'entreprise doit également disposer d'un système de téléphonie basée sur IP. C'est à dire un système de téléphonie sur Internet. Chaque département doit être joignable ou être capable de joindre d'autres personnes/départements selon des critères différents. Certains employés doivent être joignable depuis l'extérieur et d'autres seulement depuis l'intérieur de l'entreprise. Certains appels doivent également pouvoir être redirigés à un autre poste. Tous les employés doivent disposer d'une boîte vocale pour les appels en absence.

L'utilisation de ce service sera différente pour tous les départements. Le point commun est qu'ils doivent tous disposer d'une boîte vocale.

- La direction : Le directeur se connectera à son compte grâce à un softphone. Il peut joindre n'importe qui mais n'est pas joignable directement. Les appels passent d'abord par le poste de la secrétaire.
- La secrétaire : Elle peut joindre n'importe qui et est joignable par n'importe qui sur un softphone.
- Les ouvriers : Ils utilisent des postes téléphoniques fixes (des téléphones IP) et peuvent joindre et être appelé par tous les départements internes.
- Le service comptable : Chaque comptable dispose de son propre utilisateur pour le service et s'y connecte via un softphone. Ils peuvent joindre n'importe qui en interne et en externe sauf le directeur. Le service dispose également d'un numéro unique qui permet de joindre le premier comptable disponible. Physiquement, le service comptable sera séparé en 2 bureaux.
- Le service commercial : Les employés de ce service peuvent joindre n'importe qui en interne et en externe sauf le directeur grâce à un softphone et grâce à un GSM pour quand ils sont en déplacement.

Il existe également une deuxième implantation de l'entreprise qui doit être joignable par téléphone depuis la première et inversement.

Le partage de fichiers
Un système de partage de fichiers sera mis en place de manière à pouvoir mettre des ressources en communs entre les différents postes des employés d'un même département. En outre du dossier partagé avec son département, chaque employé pourra également utiliser ce système pour récupérer ses données personnelles quelque soit la machine sur laquelle il se connecte.

Nous avons donc conceptualisé une architecture permettant de mettre en place ces services en répondant à vos demandes. Nous avons également façonné un prototype de démonstration configuré pour pouvoir héberger les services nécessaires.

Les besoins techniques

Les containers
Nous avons décidé, pour ce projet, d'utiliser des containers Docker. Un container est un élément de software permettant le déploiement d'une application à l'intérieur de celui-ci. Chacun des services disponibles dans votre infrastructure se trouve dans un container isolé. L'avantage de ceci est que si une des applications consomme trop de ressources, elle ne bloquera pas pour autant les autres. Grâce à ceci, les éventuels problèmes se rapportant à un des services ne vont pas se propager sur les autres. Chaque container a également son propre espace mémoire ce qui veut dire qu'une application ne peut pas consommer plus de ressource que ce qui lui est alloué. Donc, ne peut pas empêcher l'exécution des autres applications.

Le serveur web
De manière à mettre en place les 3 sites web nécessaires, nous utilisons un serveur web. Le but de celui-ci est de stocker les données du site et de répondre aux requêtes des utilisateurs. C'est sur un serveur web Apache que nous avons décidé d'héberger ces sites.

Nous avons choisi de travailler avec Apache pour sa facilité d'administration, sa fiabilité et sa stabilité. Apache nous permet également d'étendre facilement le réseau si nécessaire dans le futur et de nous adapter facilement à cela. Une alternative aurait été Nginx qui permet un plus grand nombre de connexions simultanées et consomme moins de ressource. Nous n'avons pas opté pour celui-ci car ces caractéristiques ne représentaient pas des critères fondamentaux dans notre cas.

Pour héberger les 3 sites, nous avons décidé d'utiliser le virtual hosting. Cela veut dire qu'au lieu d'avoir un serveur web par site, les 3 se trouvent sur le même serveur. Ceci facilite la gestion et la compréhension de l'infrastructure même si la mise en place demande une étape de réflexion supplémentaire.

Le système de résolution des adresses
Pour que les visiteurs puissent accéder facilement aux différents sites, nous avons dû mettre en place un système de résolution des adresses, un DNS (Domain Name System). Celui-ci sert à traduire les adresses réelles des sites, c'est à dire les adresses IP des sites, en adresses littérale connue par l'utilisateur et inversement. Les sites sont donc accessibles aux utilisateurs en tapant leurs adresses littérales dans le navigateur (ex : www.wt1.ephec-ti.be)

Pour ce service de traduction d'adresses, nous avons décidé d'utiliser un serveur Bind. Celui-ci est très courant ce qui facilite sa mise en place et sa gestion car beaucoup d'informations sont disponibles à cet effet. De plus, nous avons plus d'expérience avec ce dernier ce qui a grandement facilité sa configuration. Une alternative aurait été NSD mais celui-ci ne répond qu'aux requêtes venant des domaines dont il est responsable alors que Bind peut nous procurer des informations sur n'importe quel domaine.

La base de données
Pour la base de données, nous avons choisi MySQL. Ce système de gestion de bases de données relationnelle (SGBDR) est le plus répandu et est open source contrairement à la plupart de ses concurrents. Étant un système assez léger, il est suffisamment performant pour gérer une petite base de données telle que la vôtre. Il est également assez facile à déployer et à gérer et est très configurable. Il nous semble donc logique d'opter pour cette solution. De plus, une documentation complète est fournie.

Des alternatives auraient été le SGBDR de IBM ou Microsoft SQL server mais ceux-ci, contrairement à MySQL, ne fonctionnent pas sur tous les OS. MySQL est également un des SGBDR les moins limités au niveau de la taille des tables, par exemple.

Le service mail
Pour le serveur mail de l'entreprise, nous avons décidé d'utiliser Postfix pour sa vitesse et sa facilité de maintenance. C'est un MTA (Mail Transfer Agent) assez sécurisé par rapport à d'autres comme par exemple Sendmail. Son but est donc de transférer des messages électroniques entre 2 ordinateurs (ou autre) en utilisant une architecture client-serveur. Il est accompagné d'un serveur Dovecot, c'est un serveur POP/IMAP incluant un MDA (Mail delivery agent), Postfix lui transmet le mail et dovecot le place dans une inbox. On utilisera un MRA(mail retrieval agent) appelé fetchmail, qui permet de transférer les mails depuis le serveur dovecot distant vers la machine locale(IMAP/POP). IMAP et POP sont des protocoles permettant de récupérer les emails. Le serveur mail sera sécurisé avec un filtre anti-spam, spamassassin et d'un anti-virus Clamav.

Nous aurions pu utiliser un autre MTA comme Exim, mais lors de tests de performances, Postfix s'est avéré supérieur même si Exim est plus flexible. La mise en place d'Exim est également plus compliquée. Les utilisateurs utiliseront Thunderbird, un client mail expliqué plus bas.

Le service téléphonique

Pour le système de voix sur IP, nous utilisons Asterisk qui est un software PABX (Private Automatic Branch Exchange). Le but de ce software est de pouvoir y attacher des téléphones physiques ou virtuels. Ces téléphones seront ensuite capables de passer des appels entre eux ainsi que de se connecter à d'autres services téléphoniques. Les avantages d'Asterisk sont premièrement son coût par rapport à un PABX standard et son interopérabilité avec d'autres services. Ce software sauvegarde automatiquement les configurations qu'on lui apporte et est également très stable.

La principale alternative serait d'utiliser FreeSwitch mais ce PABX et plus difficile à configurer. Ceci n'est néanmoins pas la différence principale qui nous a fait choisir Asterisk. Asterisk correspondait, dans ce cas, beaucoup plus pour l'architecture et les caractéristiques désirées. En effet, Asterisk fournit une sorte de structure pour construire des applications de communication alors que FreeSwitch est une plateforme pour ce genre d'application.

Pour les départements qui utilisent un softphone (téléphone virtuel) pour ce service, nous conseillons X-lite. Le dialplan, c'est-à-dire la liste des employés et le plan de numérotation se trouve en annexe.

Pour mettre en commun les serveurs Asterisk des 2 implantations, les serveurs doivent pouvoir communiquer entre eux. Pour faire ceci, nous devons mettre en place un trunk IAX. Ce trunk est une passerelle entre les 2 systèmes et IAX est le protocole qui permet d'établir les sessions entre les différents serveurs.

Le partage de fichiers

Concernant le partage de fichiers, celui-ci se reposera sur la plateforme Owncloud et les données seront stockées dans une base de données PostgreSQL.

Owncloud offre des services de stockage et de partage de fichiers en ligne. Nous avons préféré utiliser Owncloud plutôt que Samba pour son intuitivité que ce soit au niveau du déploiement côté serveur ou bien de l'expérience utilisateur. En plus d'être utilisable facilement via l'explorateur natif de la plupart des systèmes d'exploitation, il dispose d'une interface en ligne utilisable à condition de disposer d'identifiants et permettant d'accéder aux données en dehors de l'entreprise.

Concernant notre choix pour PostgreSQL, il s'est principalement basé sur le fait que ce système de gestion de base de données est plus fiable que par exemple SQLite (système embarqué dans la configuration de base de OwnCloud) lorsque l'intégrité des données est cruciale, ce qui est le cas ici dans un système de partage de fichiers. De plus, en utilisant une base de données externe, il sera possible de mettre à jour Owncloud aisément sans risquer de perdre les données.

Déploiement, validation et tests

Le serveur web et le système de résolution des adresses
Pour vérifier le bon fonctionnement du serveur Apache, vous pouvez y accéder à l'adresse IP suivante : http://151.80.119.160/, si le serveur est bien configuré, vous devriez tomber sur le site de base.

Pour la partie DNS, entrez les différentes url des différents sites, à savoir :

- www.wt1.ephec-ti.be
- b2b.wt1.ephec-ti.be
- Intranet.wt1.ephec-ti.be : Pour être sûr que ce dernier fonctionne comme prévu il y a deux tests à effectuer. Il faut d'abord tenter de se connecter depuis un ordinateur interne au réseau (le PC d'un employé par exemple). Ceci doit fonctionner. Il faut ensuite essayer de se connecter depuis un ordinateur externe et ceci doit être impossible.

Il faut également vérifier que les différents sites renvoient bien les pages html adéquates. Pour l'instant ces sites ne contiennent que des pages de tests. Néanmoins, l'infrastructure est prête à recevoir les pages créées par vos designers.

On voit également, sur ces pages tests, que l'intranet et le site b2b ont accès à leur base de données.

Le service mail
Il existe de nombreuses façons de vérifier le fonctionnement du service mail, chacune validant un élément des demandes.

On peut, premièrement, entrer en mode console (en ligne de commande) dans le container contenant le service mail. Ici, on peut vérifier que deux employés de l'entreprise peuvent communiquer par mail en utilisant la commande sendmail. Vous n'aurez normalement pas à utiliser cette technique car nous avons mis en place un système plus facile et intuitif à utiliser.

Toujours en ligne de commande et grâce à la commande sendmail, vous pouvez vérifier que l'envoi d'un mail est possible à n'importe quelle adresse extérieure à l'entreprise. La réception d'un mail provenant de n'importe quelle adresse est également possible.

Pour l'utilisation régulière et facilitée, nous avons décidé d'installer Thunderbird, un client mail, sur les ordinateurs et autres machines des employés. Un client mail est un programme qui permet d'accéder aux mails de l'utilisateur et de les gérer. Grâce à celui-ci, vous pouvez tester les différentes fonctionnalités énoncées ci-dessus de manière plus confortable et sans devoir entrer dans le container ou utiliser les lignes de commandes.

Le service téléphonique
Pour le système de VoIP, nous avons installé des softphones sur les ordinateurs de certains employés et sur certains GSM. Ces softphones permettent facilement de se connecter aux utilisateurs que nous avons configuré. Pour cela, il suffit de rentrer dans les paramètres du softphone et d'entrer le nom d'utilisateur, le mot de passe de celui-ci et l'adresse IP du container dans lequel se trouve l'application de VoIP, à savoir 151.80.119.164.

Une fois connecté, pour tester le fonctionnement, on passe des appels aux numéros disponibles dans le plan de numérotation. Les appels doivent aboutir sur les postes correspondants aux numéros appelés.

De l'extérieur, on peut également tenter de contacter le numéro public de l'entreprise, à savoir, contact@wt1.ephec-ti.be. Cet appel doit aboutir sur le poste de la secrétaire.

Pour tester le lien avec la deuxième implantation, on passe un appel avec les mêmes numéros qui sont disponibles dans votre implantation mais précédé d'un 1.

Le partage de fichiers
Pour tester le système OwnCloud de partage de fichier, il suffit de se rendre à l'adresse ce celui-ci (http://owncloud.wt1.ephec-ti.be) dans un navigateur quelconque et de disposer d'un identifiant et d'un mot de passe valide. En tapant l'adresse dans le navigateur, si on tombe bien sur le site, le service est présent et fonctionnel. Si en se connectant à un compte on a bien accès à des fichiers, la base de données est fonctionnelle. Il faut également constater qu'en se connectant à différents comptes, on a accès à différents fichiers. Il est également possible de configurer l'accès au cloud par WebDav via l'explorateur natif de son système d'exploitation.

Niveau de déploiement, avancement

Notre solution n'est, à ce jour, pas totalement déployée, nous rencontrons encore quelques problèmes aux niveaux de la configuration des différentes mesures de protections du serveur web, plus principalement le proxy et du côté de la restriction à l'accès de la zone intranet aux employés uniquement. Ces problèmes ne sont pas encore résolus mais nous y travaillons.

Le serveur web
Le serveur Apache répond à toutes les demandes énoncées précédemment sauf la restriction de l'accès à l'intranet. Celui-ci ne devrait pas être accessible depuis internet mais nous rencontrons encore quelques problèmes quant à la mise en œuvre de cette solution.

La base de données
La base de données (MySQL) est déployée avec un script minimaliste pour vérifier son bon fonctionnement, il ne restera plus qu'à transférer les données de l'ancienne base de données vers la nouvelle. Nous avons également fait le lien entre cette base de données et le site B2B. Celui-ci a donc maintenant accès à la base de données qui pourra contenir tous les produits et potentiellement une liste des clients et des commandes. L'intranet a également accès à une base de données différentes qui contiendra les informations relatives à l'organisation de l'entreprise.

Le service mail
Du côté du serveur mail, il est bien installé et les configurations sont optimales pour la plupart. Un filtre anti-spam et un antivirus sont également déployés pour renforcer le degré de sécurité. Les mails peuvent être envoyés et reçus en interne et en externe depuis le serveur.

Le service téléphonique
Pour la VoIP, Asterisk est en place et nous avons configuré les différentes restrictions nécessaires pour l'entreprise. Les différents softphones sont mis en place et la communication entre deux utilisateurs s'effectue. Nous rencontrons néanmoins certains problèmes de configuration notamment au niveau de la boite vocale qui ne fonctionne actuellement pas. Les redirections de certains appels ne fonctionnent pas non plus.

L'entreprise est bien joignable depuis l'adresse contact@wt1.ephec-ti.be qui est traduite par notre système DNS. Le service comptable est bien joignable depuis un numéro unique et chaque poste de l'entreprise possède un numéro fonctionnel.

Le lien avec la deuxième implantation n'est actuellement pas fonctionnel.

Le partage de fichiers
Le système de partage de fichiers est en place, fonctionnel et intégré au DNS. Chaque employé enregistré peut se connecter à son compte personnel et, de là, avoir accès aux fichiers dont il a les permissions. Par exemple, si un des comptables se connecte à son compte, il aura accès aux dossiers sur lesquels les comptables ont les permissions. On constate donc également de notre base de données est fonctionnelle et qu'on a accès à celle-ci depuis notre OwnCloud.

Annexes

Diaplan

Département	Numéros	Restrictions	Postes
Direction	101	- Peut joindre n'importe qui - N'est pas joignable directement, tous les appels vers le directeur passent par le poste de la secrétaire	- Directeur -> 101
Secrétariat	102	- Peut joindre n'importe qui - Est joignable par n'importe qui - Est joignable par de l'extérieur « contact@wt1.ephec-ti.be »	- Secretaire -> 102
Ouvrier	200 -> 299	- Peut joindre tous les départements internes - Est joignable par tous les départements internes	- Ouvrier1 -> 201 - Ouvrier2 -> 202
Comptable	300 -> 399	- Peut joindre tout le monde en interne et en externe sauf le directeur - Se sépare physiquement en 2 bureaux	- Numéro commun -> 300 - Comptable1 -> 301 - Comptable2 -> 302 - Comptable3 -> 303 - Comptable4 -> 304
Commercial	400 -> 499	- Peut joindre tout le monde en interne et en externe sauf le directeur	- Commerce1 -> 401 - Commerce2 -> 402

Schéma réseau physique

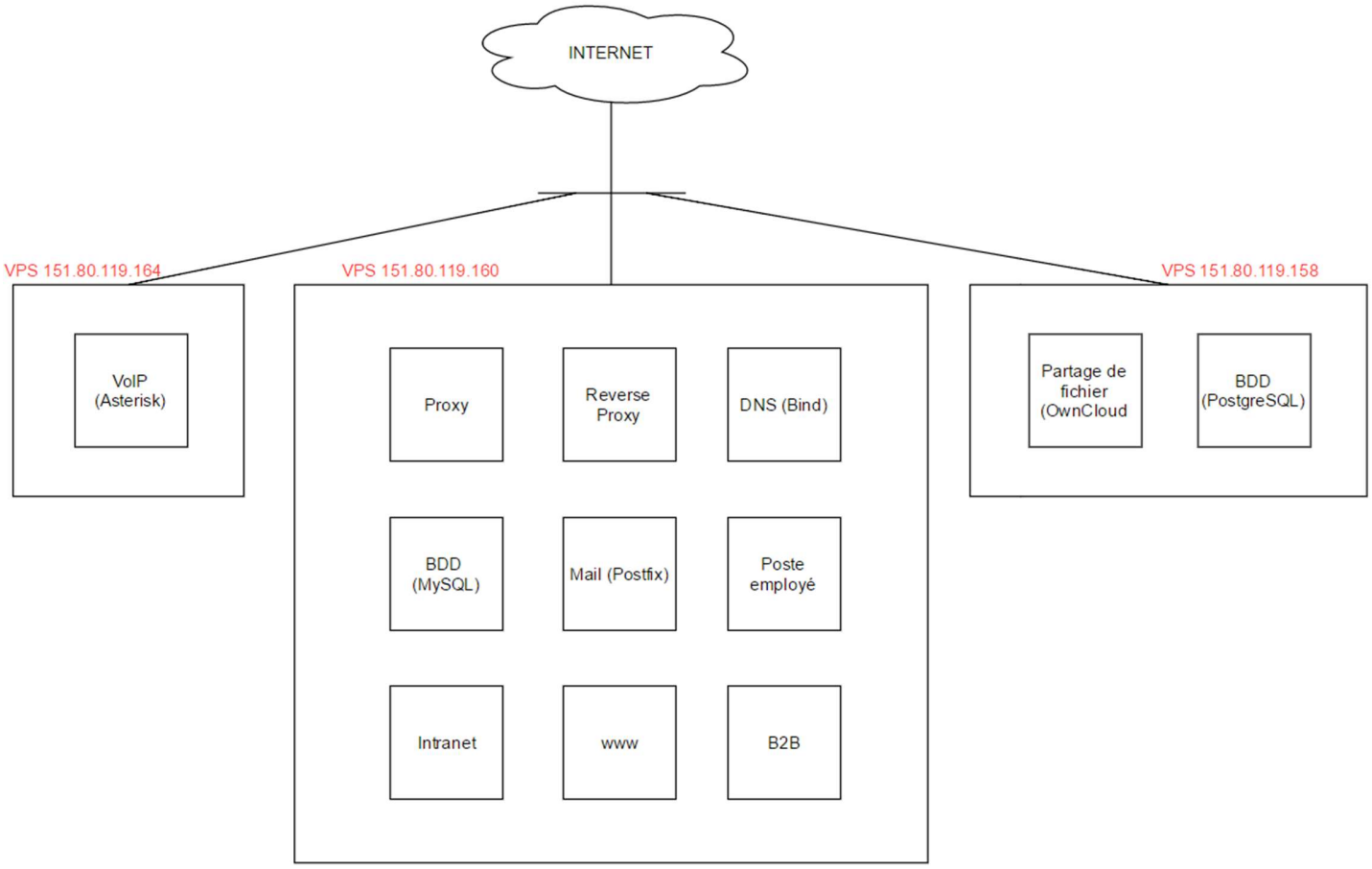


Schéma réseau logique