BALMONT Quentin
DUBERNET Virgile
LEITE Mathis

23/11/2023

AP2, Install Architecture Montoutou

Sommaire:

Contexte:

La société MonToutou lancée juste avant la crise sanitaire du Covid19, s'était fixé pour mission d'apporter du bonheur dans les familles en aidant l'adoption des animaux domestiques se trouvant dans les refuges et animalerie. Avec la crise sanitaire, elle a pivoté son activité vers la location d'animaux (en particulier des chiens) pour permettre à ses clients de pouvoir braver les « interdits » des différents confinements.

Ainsi grâce à ses chiens « d'emprunt », les clients de MonToutou peuvent sortir de chez eux pour se promener dans les parcs et forêts de leur voisinage. Pour cela la société s'est appuyée sur un réseau de partenaires (refuges et animaleries) qui s'occupent de la partie logistique animale (prêter et récupérer les chiens, assurer les soins, vendre le matériel nécessaire, ...). MonToutou ne s'occupe que de la partie commerciale (site internet), du support téléphonique des clients et propose via un extranet à ses partenaires les outils de gestion des locations.

La crise sanitaire ayant permis à l'entreprise d'augmenter considérablement son activité, son équipe est passée à 20 personnes avec plus de 50 partenaires. Son dirigeant M. Jean (après une expérience malheureuse de DRH) a décidé d'organiser son informatique qui pour l'instant était faite de bric et de broc. Il veut en particulier s'assurer d'être conforme au RGPD et que son architecture informatique lui garantisse une continuité de service. Pour cela il a fait appel à une E.S.N. (Entreprise de Service Numérique) pour développer son site internet et son extranet partenaire. Ils seront développés sur une technologie basée sur PHP et Mysql.

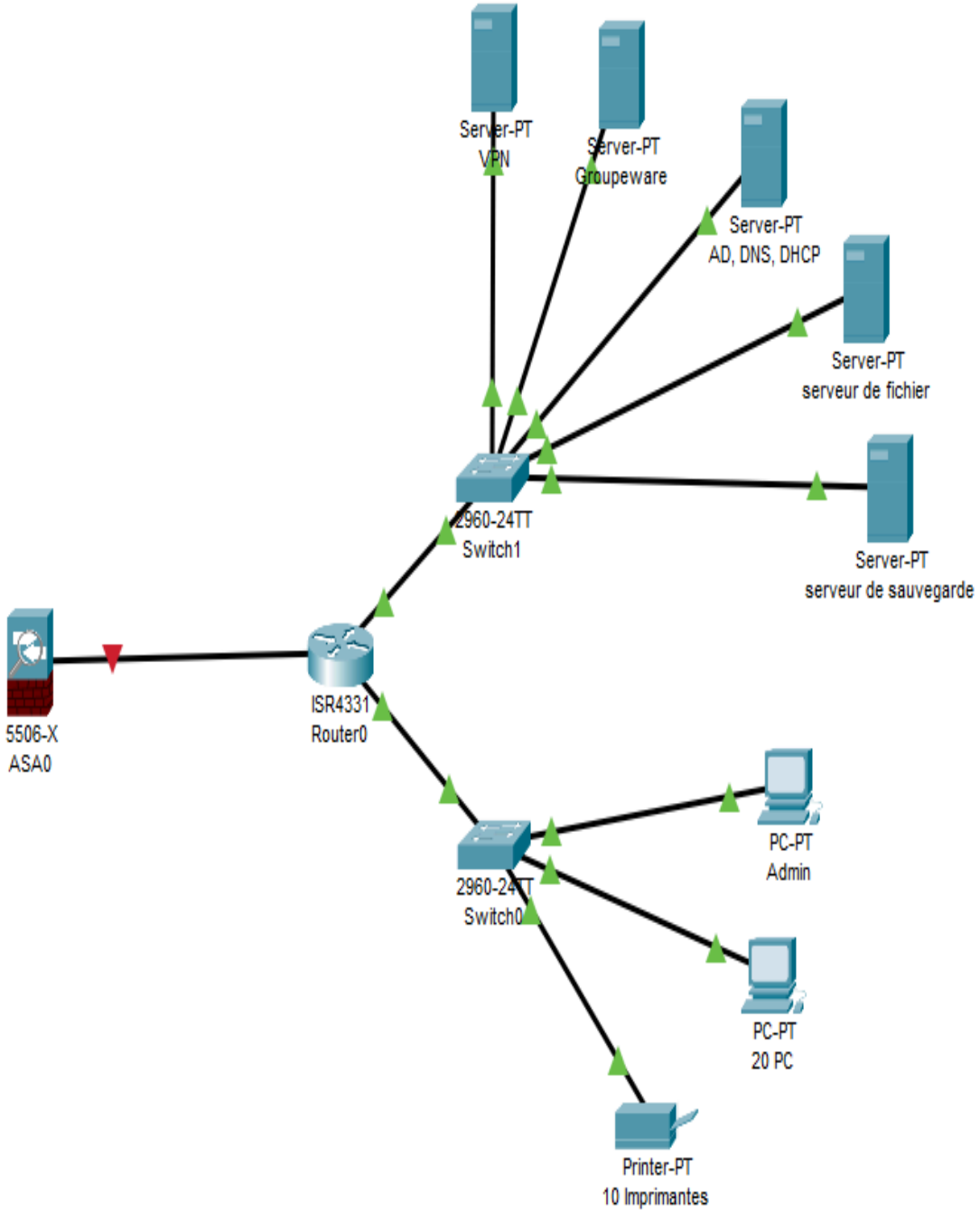
De son côté, M. Jean a décidé d'internaliser son informatique afin de s'assurer de la qualité de son infrastructure et de sa maintenance. Pour cela il décide d'embaucher votre équipe pour mettre en place son service informatique. M. Jean a été « traumatisé » par l'incendie du datacenter d'un grand hébergeur français. Il souhaite donc qu'un maximum de son architecture informatique soit internalisée dans les locaux de l'entreprise. De plus, comme la société est assez nouvelle, il souhaite utiliser un maximum les technologies opensources / gratuites et minimiser l'achat de licence et matériel coûteux.

Infrastructure : (Virgile)

Adressage IP

	Adresse IP	**Masque sous-réseau**	**Passerelle par défaut**
R1 **Fa 0/0 :** **Fa 0/1 :**	 192.168.30.254 192.168.31.254	 255.255.255.0 255.255.255.0	 x x
S1			192.168.30.254
Serveur VPN	192.168.30.20	255.255.255.0	192.168.30.254
Serveur GroupWare	192.168.30.30	255.255.255.0	192.168.30.254
Serveur AD DNS DHCP	192.168.30.40	255.255.255.0	192.168.30.254
Serveur FTP	192.168.30.50	255.255.255.0	192.168.30.254
web	192.168.30.55	255.255.255.0	192.168.30.254
S2			192.168.31.254
10 Imprimantes	192.168.31.20-30	255.255.255.0	192.168.31.254
20 Postes Clients	192.168.31.41-60	255.255.255.0	192.168.31.254

Schéma Réseau :



Notes de service :

L’adressage est tel que tous les serveurs ici présents sont sous un adressage d’IP fixe, de même que les interfaces du routeur (R1), tous les clients présents sur l’interface Fast Ethernet 0/0 sont donc en statique et passent par le switch (S1). Les clients du S2 sont donc attribués au réseau de l’interface Fast Ethernet 0/1, eux sont en adressage dynamique et reçoivent des adresses en fonction des baux attribués par le DHCP présent sur le réseau de S1.

Le routeur (R1) utilisé est un Cisco qui utilise donc IOS, le fait que le serveur DHCP puisse attribuer des adresses sur un réseau qui n’est pas le sien est rendu possible grâce à un relai DHCP appliqué aux deux interfaces fa0/0 et fa0/1. L’attribution des adresses est donc possible même inter-réseau. L’adressage passe donc par le DHCP sous Windows Serveur et communique avec le switch qui distribue les adresses données.

S1 et S2 sont deux switch qui ne sont pas de niveau 3, ils n’ont donc qu’une passerelle par défaut qui correspond à leurs interfaces du routeur. Les deux réseaux séparés sont le .31 pour les clients (Imprimantes et Ordinateurs Clients), et le .30 pour les serveurs. Grâce au relais DHCP mis en place les clients du réseau .31 ont aussi accès au services du .30, tel que le serveur web, groupware, VPN, etc…

La communication entre les réseaux n’est donc pas un problème, et si d'éventuels problèmes surviennent l’hypothèse à observer en premier serait l’état du relai DHCP qui est un point culminant.

En sortie du réseau sera présent, un pare-feu de chez Fortinet, celui-ci séparant donc l’infrastructure interne de l’accès publique, bloquant donc l’accès d’un côté suite à l’application d’une permission ACL. Le réseau interne aura donc accès à l’extérieur, mais l’inverse ne sera pas possible ou bien réglementé en fonction des indications de l’administrateur réseau qui pourra abaisser le niveau de sécurité en fonction de son souhait et des besoins des utilisateurs.

Mots de Passe et Identifiants : (Groupe)

Serveur FTP :
Identifiant système = Debian
Mot de Passe = aze+123
Identifiant = adminLocal
Mot de passe utilisateur = aze+123
Chemin répertoir = `\\debian\partage`

Windows Serveur :
Identifiant = Administrateur
Mot de Passe= aze+123
Nom de Domaine = ap2.qmiv

VPN :

ID = admin
Mot de passe = aze+123
Mot de passe root = aze+123
Nano pour clés privée/publique = enp0s3

Client Test :
Identifiant = User
Mot de passe = user+123

Nextcloud :
Identifiant = admin
Mot de passe = aze+123

Webserver :
Identifiant = admin
Website mot de passe = aze+123
Mail = aze+123

Procédures:

1/ AD DNS DHCP (Virgile)

Les services Active Directory, DNS et le DHCP tournent sur un seul et unique serveur Windows 2019 avec une licence d'entreprise. Les services sont des rôles attribués qui peuvent être retrouvés dans les différents onglets de la gestion du serveur sur l'interface ou bien directement en ligne de commande Powershell. Il est à savoir que le serveur possède une interface graphique, permettant donc à l'administrateur système de choisir ce qu'il préfère pour effectuer ses tâches.

L'Active Directory est directement relié au groupware car à chaque création de compte utilisateur sur l'AD, il lui est attribué un accès aux différents services de Nextcloud tel que la messagerie, le serveur FTP, etc…

Pour créer un nouvel utilisateur, il faut donc se rendre directement sur le rôle de l'Active Directory sur l'interface graphique du serveur, ou directement via la commande Powershell (cf : New-ADUser).

2/ Serveur FTP (Mathis)

Pour répondre au cahier des charges de l'entreprise nous nous sommes tourné vers Samba qui est un logiciel d'interopérabilité qui implémente le protocole propriétaire SMB/CIFS de Microsoft Windows. Il s'installe sur linux ainsi c'est un logiciel libre et open source permettant de créer un serveur de fichier. Ce serveur est hébergé sur¨debian du fait qu'il soit gratuit, il répond aux besoins.

Pour accéder au partage de fichier, on tape //debian/partage dans l'explorateur de fichier des utilisateurs. Ensuite, il faut rentrer « chef » ou « debian » dans l'utilisateur et « aze+123 » en mot de passe. Comme c'est un protocole SMB, il faut installer sur chaque utilisateur une application qui puisse lire le protocole SMB afin d'accéder au partage de fichier.

Sur le serveur, pour voir tout ce qui est stocké dans le serveur de fichier, il suffit d'aller dans le répertoire /srv/partage et il y aura tout dedans.

3/ VPN (Quentin)

Pour relier un client au VPN il suffit d'installer le fichier exécutable depuis leur site web (wireguard.com/install/). Après avoir exécuté l'installation, lancer le client wireguard, une fois sa fenêtre ouverte il faut importer un tunnel dans l'onglet en bas à gauche dans le menu déroulant. Reprendre la configuration de "montoutou-vpn" renseigner l'adresse IP du poste client sur la ligne "Address" dans "[Interface]" puis modifiez les plages d'adresse IP sur la ligne "AllowedIPs" si besoins dans le cadre d'une possible croissance des utilisateurs.

Il reste ensuite à déclarer le client sur le serveur Debian 12 où est installé le VPN wireguard dans le répertoire vpn.conf. Dans ce fichier, à la suite du bloc [Interface], il faut que l'on déclare un bloc [Peer]. Ce bloc [Peer] contient la clé publique du PC Windows 10 (PublicKey) ainsi que l'adresse IP de l'interface de ce PC (AllowedIPs) : le serveur communiquera dans ce tunnel WireGuard uniquement pour contacter le client Windows.

Enfin, il suffit de retourner sur le PC client et d'activer la connexion vers le serveur par le VPN.

4/ Serveur Web et Groupeware

Le serveur WEB est accessible aux utilisateurs du réseau interne et externe grâce à une règle ACL, via l'url : **montoutou-ap .** Le serveur Web tourne sous un serveur Debian 11 pour des soucis de moyen, l'utilisation de Linux revenant moins cher que le fait de payer une autre licence Windows.

Dans un premier temps un serveur LAMP est donc mis en place sur un Debian, ensuite Next Cloud nous servira de Groupware, de même que pour le service de mail intégré nous avons dû mettre en place un serveur IMAP et SMTP, via l'utilisation de dovecot (Fichier de configuration de dovecot : */etc/dovecot/conf.d/).* L'adresse email du compte admin sera : **admin@ap1.qmiv.fr .**

5/ Serveur de Sauvegarde

Le serveur de sauvegarde tourne sur Veam et est récupéré de l'AP1, il ne fait donc que des sauvegardes sur un serveur local, le sien en l'occurrence, présent dans le réseau en .30 il effectue des sauvegardes du dossier partagé par le serveur FTP. Le serveur peut tout à fait exporter ses sauvegardes sur un serveur externe(Méthode 3-2-1), mais cela n'était pas spécialement le but de cet AP.

Conclusion :

Tous les services sont dans la capacité de communiquer entre eux, nous avons pu le tester via différents ping entre les infrastructures. De même que des test ont pu être réalisé tel que se connecter au serveur via un poste client, et afficher la page apache, etc…

Le seul point qui n'a pas été grandement poussé est le firewall et par conséquent l'accès à internet, donc la sortie du réseau interne vers le reste du monde. Qui pour l'instant est simplement bloqué par des ACL sur le routeur Cisco.

Nous avons aussi mis beaucoup de temps à mettre en place le système de relais sur le routeur, nous permettant d'éviter d'utiliser pfSense et donc d'éviter un nouvel intermédiaire. Une raison de plus est que nous nous trouvons plus à l'aise avec le matériel physique et le langage Cisco IOS.

Le serveur FTP fonctionne, c'est-à-dire que le stockage se trouve sur un serveur tournant sur Debian avec Samba. Et depuis un poste client Windows 10 classique, il est possible d'avoir accès à un répertoire seulement en installant des extensions Windows, autrement nous avons un refus du lecteur qui détecte la présence du dossier mais nous refuse l'accès.

En conclusion, la majorité des points ont été abordés, malgré quelques défaillances du système cités précédemment dans cette conclusion.

Le point à améliorer dans cette infrastructure est clairement l'aspect Cybersécurité.