

Cahier des charges structure - ACME

Projet “BuFaLo”

Groupe n°1

Benjamin LAMBERT
Linh Chi NGUYEN
Frédéric THEBAULT

Table des matières

Objet du projet	3
Spécifications techniques de l'existant	3
Contexte	3
Problème posé	5
Besoins fonctionnels	6
Préconisations techniques	7
Sécurisation du réseau local de l'entreprise	7
Sécurisation de la base de données et du serveur hébergeant la base de données de l'application	8
Sécurisation de la base de données : chiffrement	8
Vérification de la validité des champs pendant la saisie sous l'application	8
Hachage et salage des mots de passe	8
Monitoring des serveurs	9
Accès à la base de données	9
Sécurisation du serveur	9
Mise en place d'une sauvegarde automatique des données sur un site tiers	10
Utilisation de la solution VEEAM Backup	10
Amélioration de la gestion de parc de machines de la société en automatisant la configuration des machines	10
Monitoring et supervision avec Centreon	11
Déploiement et automatisation des mises à jour avec Ansible.	11
Inventaire (GLPI)	11
Simplification de l'accès à l'application en relation avec la gestion du parc	11
Accès distant sécurisé à l'application	12
Optimisation de l'infrastructure pour supporter la croissance de l'entreprise	12

1) Objet du projet

L'entreprise ACME se trouve dans une situation délicate. En effet, que ce soit au niveau structurel ou en termes de sécurité globale, force est de constater que l'entreprise est vulnérable à bien des égards et il est donc urgent voire vital de prendre d'importantes mesures en vue d'assurer la pérennité voire la survie de l'entreprise. Le présent document érige un constat assez alarmant sur les vulnérabilités recensées au sein de l'entreprise ACME et présente un certain nombre de propositions dans l'optique de moderniser la structure pour pouvoir ainsi envisager l'avenir avec sérénité et ambition.

2) Spécifications techniques de l'existant

a) Contexte

L'entreprise a fait face à plusieurs reprises à des accès non autorisés au réseau et à l'application, et souhaite faire évoluer son système d'informations (SI) afin de sécuriser les outils de travail. Également, avec la croissance de l'entreprise, l'application montre des signes de lenteurs, et des plantages ont eu lieu, entraînant des pertes de données. Enfin, la limitation de l'accès à l'application au réseau local pénalise les commerciaux qui ne peuvent y accéder en mobilité.

L'infrastructure de l'entreprise ACME est la suivante:

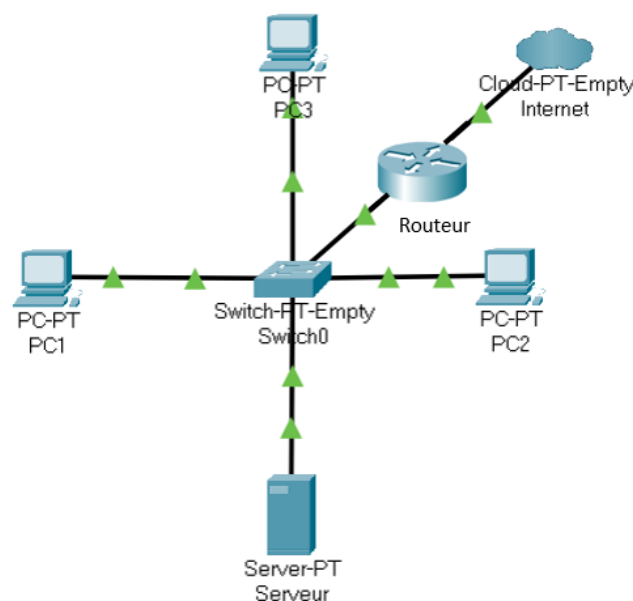


Schéma n°1 - Réseau physique actuel de l'entreprise ACME

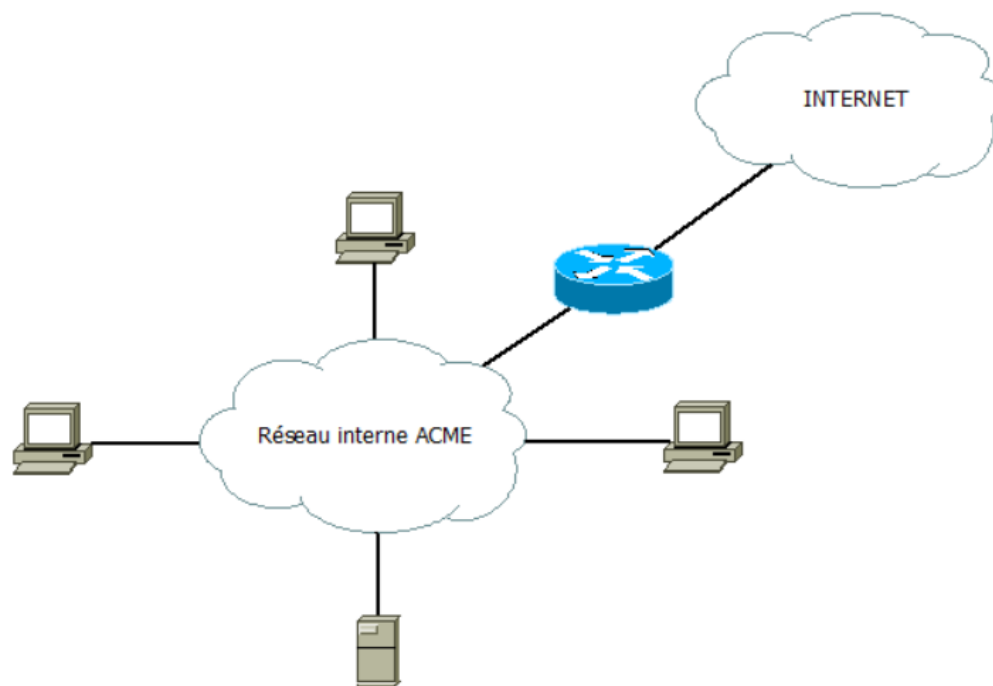


Schéma n°2 - Réseau logique actuel de l'entreprise ACME

Bilan actuel des éléments constitutifs du SI de l'entreprise ACME:

- Postes de travail sous Windows 10, sans configuration spécifique (pas de gestion de parc),
- Serveur sous Ubuntu 12.04 (version ne disposant plus du support de sécurité), hébergeant la base de données de l'application (technologie MySQL, utilisant une version non maintenue). Niveau de puissance en accord avec une machine de puissance moyenne achetée il y a 5 à 8 ans,
- Application CRM développée en Java dans la partie 1.

b) Problème posé

Vulnérabilités au niveau du réseau physique

- Aucun contrôle concernant l'accès à l'unique bâtiment actuel, tout le monde peut rentrer sans s'annoncer à l'accueil. Un individu voulant infiltrer le réseau par l'intérieur ne pourrait rêver mieux comme facilité d'accès.
- L'unique serveur actuel de l'entreprise ACME n'est pas isolé dans une salle dédiée. Tous les employés peuvent y avoir accès même les personnes "invitées" en transit dans l'enceinte de l'entreprise.
- Cet unique serveur signifie aussi que les données de l'entreprise ne sont stockées qu'à un seul endroit. La moindre avarie sur le serveur engendre donc potentiellement une perte partielle, voire totale des données.
- Aucune supervision du parc des machines n'est, à l'heure actuelle, mise en place. Ce qui induit que le moindre incident sur le réseau d'ACME n'est pas suivi et qu'il ne sera détecté que lorsqu'il sera constaté par les équipes de travail donc trop tardivement.
- Aucune redondance d'équipement n'est mise en place. Sur l'unique réseau que compte ACME à l'heure actuelle, le moindre défaut technique d'un équipement entraîne potentiellement la perte ou l'isolement d'une partie, voire la totalité du réseau de l'entreprise (idem pour la connexion au réseau Internet). Il en va de même en cas de coupure de courant.

Vulnérabilités au niveau du réseau logique

- L'entreprise ACME ne compte qu'un seul et unique réseau à l'heure actuelle que se partage l'ensemble des services (administration, production, etc.). Il n'y a pas de séparation des services.
- Entre le réseau interne de l'entreprise et le réseau Internet, il n'y a aucune zone tampon, aucun pare-feu, ce qui rend le réseau de l'entreprise très vulnérable aux attaques extérieures.
- La plupart des logiciels, des OS et des ressources de l'entreprise n'est soit plus maintenue et donc ne reçoit plus de correctifs, soit consomme beaucoup trop d'énergie, ou soit est sans configuration spécifique.

3) Besoins fonctionnels

Après le grand nombre de constats alarmants faits dans la partie précédente, il est donc nécessaire, voire urgent et même vital de consolider la sécurité de l'entreprise ACME. La pérennité de l'entreprise étant en jeu, une levée de fonds sans précédent a été réalisée et a permis de réunir une enveloppe très importante pour la modernisation et le renforcement de la structure ACME. La liste suivante résume les points principaux sur lesquels des directives doivent être prises sans délai et sur lesquels il n'est pas possible de transiger :

- L'optimisation de la structure pour supporter la croissance de l'entreprise,
- La sécurisation de l'accès aux locaux de l'entreprise,
- La sécurisation de l'accès aux serveurs,
- La séparation du réseau interne en fonction des différents services,
- La modernisation des postes, des OS et logiciels utilisés,
- La sécurisation des flux entre le réseau interne et Internet,
- La mise en place d'une gestion du parc de machines,
- La séparation des différents services-clés sur des serveurs différents,
- La mise en place d'un système de sauvegarde pour les données de l'entreprise.

4) Préconisations techniques

a) Sécurisation du réseau local de l'entreprise

- Mise en place du protocole « Spanning tree » (topologie réseau sans boucle) sur la nouvelle architecture réseau de l'entreprise (LAN n°1 et LAN n°2) pour éviter les tempêtes de diffusion qui paralysent le réseau.
- Mise en place d'un cœur de réseau (double-routeur avec firewall intégré) pour relier les différents LAN de l'entreprise ACME avec un routage en « fail-over ». Ce double-routage permet de basculer sur l'un ou l'autre des routeurs du cœur de réseau quand le premier ne peut plus répondre à ses fonctions momentanément. En cas de panne de l'un d'eux, l'autre prend la relève en totalité et assure la continuité du service. Bien entendu, les liaisons fibrées sur les deux routeurs du cœur de réseau sont isolées les unes des autres pour des raisons de sécurité.
- Isolation du réseau pour les invités : Mise en place d'un réseau physique dédié pour les connexions invitées connecté au cœur de réseau afin d'éviter qu'un invité puisse traverser un LAN de l'entreprise.
- Mise en place d'une zone démilitarisée (DMZ) entre le réseau de l'entreprise ACME et le réseau Internet comme décrite ci-dessous :

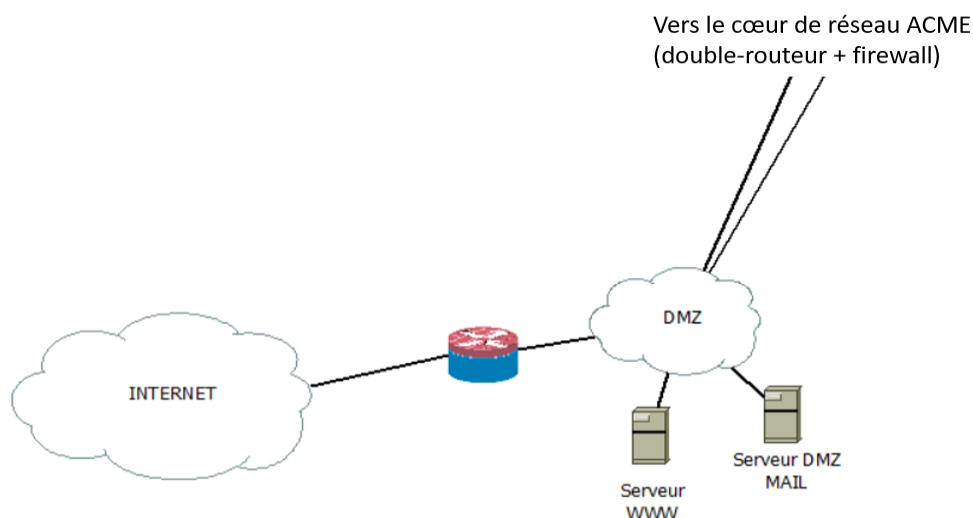


Schéma n°3 - Mise en place d'une zone démilitarisée (DMZ) entre Internet et le réseau ACME

La DMZ se place entre le réseau Internet et le réseau de l'entreprise ACME. Le LAN DMZ est situé entre deux pare-feu qui doivent impérativement être deux pare-feu de constructeurs différents (pour ne pas faciliter les tentatives de piratage). Ainsi, les flux provenant d'Internet traversent un premier pare-feu puis passent directement par le LAN DMZ où ils sont scannés, analysés par l'antivirus (au sein du serveur WWW) avant d'être redirigés vers le second pare-feu (cœur de réseau) pour enfin rentrer dans le réseau d'ACME. Pour les échanges d'e-mails, les flux sont reçus par la DMZ puis sont dirigés vers le serveur DMZ MAIL afin d'être analysés avant d'être envoyés au serveur MAIL de la salle des serveurs d'ACME.

b) Sécurisation de la base de données et du serveur hébergeant la base de données de l'application

Sécurisation de la base de données : chiffrement

Pour ce qui concerne la problématique de sécurisation de la base de données de l'application, le choix a été fait de chiffrer certaines données des clients enregistrées en base (Prénom, Nom, Adresse postale et adresse e-mail). Il pourrait être intéressant dans les évolutions futures de chiffrer d'autres données pour les clients et de chiffrer également les données les plus sensibles des employés.

Sécurisation de l'application : mot de passe oublié

Il est nécessaire de gérer l'action de réinitialisation d'un mot de passe lors de l'accès à l'application CRM par un employé. En cas d'oubli de mot de passe, il est proposé d'ajouter une option de réinitialisation de mot de passe qui serait en lien avec l'adresse e-mail de chaque utilisateur. De cette façon, la procédure de réinitialisation de mot de passe serait envoyée à l'employé pour mener à bien les étapes de la dite procédure.

Vérification de la validité des champs pendant la saisie sous l'application

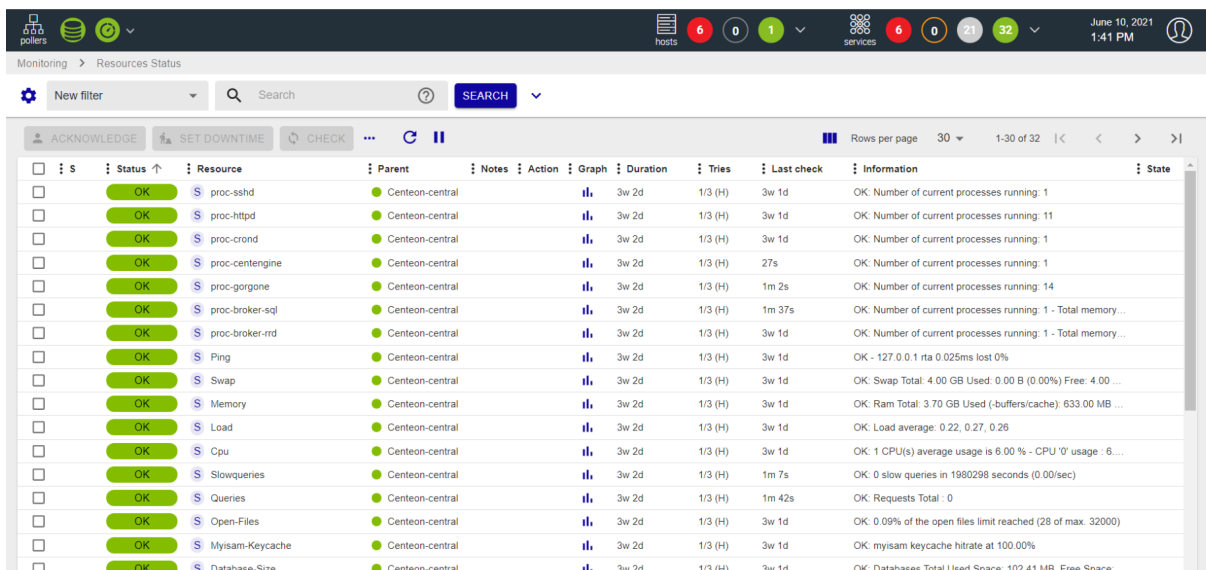
Toujours dans une optique de rajouter de la sécurité, dans l'application, l'ensemble des champs de saisie des formulaires sont contrôlés afin de vérifier leur validité et de ne pas permettre aux utilisateurs de rentrer autre chose que le type de données prévu.

Hachage et salage des mots de passe

L'aspect sécurisation de l'application passe par la protection du mot de passe de l'utilisateur. Du fait que le mot de passe ne nécessite qu'une simple action de comparaison entre ce qui est en base de données et ce qui a été entré par le client, il est possible de transformer les mots de passe de façon irréversible par hachage. Le hachage est implémenté en générant un sel aléatoire de 10 caractères qui est alors rattaché à un mot de passe avant d'être haché. L'algorithme utilisé est SHA512, pour générer une empreinte. La chaîne de caractères ayant servi à saler est différente pour chaque employé et est sauvegardée en base de données.

Monitoring des serveurs

L'utilisation d'un outil de monitoring et de supervision comme Centreon permet de superviser les applications, systèmes et réseaux de l'entreprise ACME en temps réel. Cette solution permet de visualiser les états des services, des machines du parc informatique de l'entreprise comme illustré ci-dessous :



The screenshot shows the Centreon monitoring interface. At the top, there's a navigation bar with 'Monitoring' and 'Resources Status' tabs. Below it, a search bar and a 'New filter' button are visible. The main table displays a list of services with columns for Status, Resource, Parent, Notes, Action, Graph, Duration, Tries, Last check, Information, and State. All services listed are in an 'OK' state.

☐	S	Status	Resource	Parent	Notes	Action	Graph	Duration	Tries	Last check	Information	State
☐		OK	proc-sshd	Centreon-central			3w 2d	1/3 (H)	3w 1d	OK: Number of current processes running: 1		
☐		OK	proc-httpd	Centreon-central			3w 2d	1/3 (H)	3w 1d	OK: Number of current processes running: 11		
☐		OK	proc-cron	Centreon-central			3w 2d	1/3 (H)	3w 1d	OK: Number of current processes running: 1		
☐		OK	proc-centengine	Centreon-central			3w 2d	1/3 (H)	27s	OK: Number of current processes running: 1		
☐		OK	proc-gorgone	Centreon-central			3w 2d	1/3 (H)	1m 2s	OK: Number of current processes running: 14		
☐		OK	proc-broker-sql	Centreon-central			3w 2d	1/3 (H)	1m 37s	OK: Number of current processes running: 1 - Total memory...		
☐		OK	proc-broker-rd	Centreon-central			3w 2d	1/3 (H)	3w 1d	OK: Number of current processes running: 1 - Total memory...		
☐		OK	Ping	Centreon-central			3w 2d	1/3 (H)	3w 1d	OK - 127.0.0.1 rta 0.025ms lost 0%		
☐		OK	Swap	Centreon-central			3w 2d	1/3 (H)	3w 1d	OK: Swap Total: 4.00 GB Used: 0.00 B (0.00%) Free: 4.00 ...		
☐		OK	Memory	Centreon-central			3w 2d	1/3 (H)	3w 1d	OK: Ram Total: 3.70 GB Used (-buffers/cache): 633.00 MB ...		
☐		OK	Load	Centreon-central			3w 2d	1/3 (H)	3w 1d	OK: Load average: 0.22, 0.27, 0.26		
☐		OK	Cpu	Centreon-central			3w 2d	1/3 (H)	3w 1d	OK: 1 CPU(s) average usage is 6.00% - CPU '0' usage: 6. ...		
☐		OK	Slowqueries	Centreon-central			3w 2d	1/3 (H)	1m 7s	OK: 0 slow queries in 1980298 seconds (0.00/sec)		
☐		OK	Queries	Centreon-central			3w 2d	1/3 (H)	1m 42s	OK: Requests Total: 0		
☐		OK	Open-Files	Centreon-central			3w 2d	1/3 (H)	3w 1d	OK: 0.09% of the open files limit reached (28 of max. 32000)		
☐		OK	Myisam-Keycache	Centreon-central			3w 2d	1/3 (H)	3w 1d	OK: myisam keycache hitrate at 100.00%		
☐		OK	Database-Size	Centreon-central			3w 2d	1/3 (H)	3w 1d	OK: Databases Total Used Space: 102.41 MB, Free Space: ...		

Image n°1 - Exemple d'interface graphique de la supervision avec Centreon

Accès à la base de données

Il est nécessaire d'avoir un profil dédié pour accéder à la base de données. La mise en place d'un profil de « manager » permet de gérer les différents employés et les ressources (clients, commandes, produits en BDD). Concernant les profils des employés, il est nécessaire qu'ils ne puissent accéder qu'à leurs clients sans avoir accès aux informations des autres employés.

Sécurisation du serveur

La sécurisation du serveur passe par la mise en place de Fail2Ban, d'un antirootkit et d'antivirus (qui sera chargé de scanner les e-mails et les partages de fichiers).

c) Mise en place d'une sauvegarde automatique des données sur un site tiers

Utilisation de la solution VEEAM Backup

Préconisation de la mise en place de la solution propriétaire VEEAM Backup afin de sauvegarder à une fréquence donnée les données de l'entreprise ACME sur un site tiers. Le type de sauvegarde retenu est celui de la sauvegarde incrémentale. La sauvegarde incrémentale permet uniquement de sauvegarder les fichiers modifiés depuis la sauvegarde précédente. Il est préconisé de partir sur une sauvegarde journalière la nuit vers le site tiers. Le site tiers où seront sauvegardées les données sera accessible via un VPN depuis le réseau ACME.

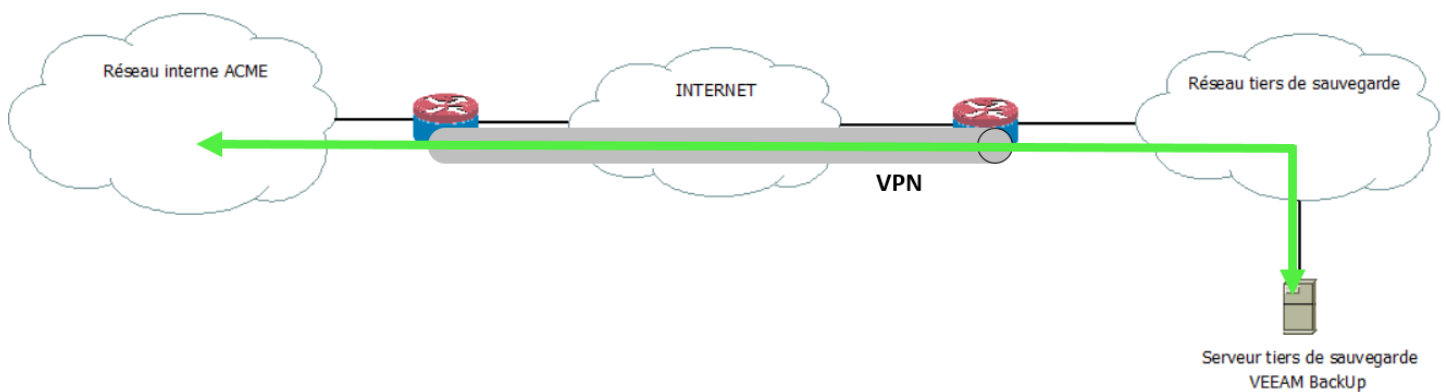


Schéma n°4 - Sauvegarde des données sur un site tiers distant - connexion via VPN

d) Amélioration de la gestion de parc de machines de la société en automatisant la configuration des machines

Il faut en premier lieu rénover l'ensemble des machines du parc informatique d'ACME en remplaçant les OS et distributions qui ne sont plus maintenus ou mis à jour par des machines avec des versions qui sont actuellement supportées (version LTS si possible : "long time support").

Monitoring et supervision avec Centreon

Comme décrit précédemment, l'utilisation de l'outil Centreon est retenue pour superviser les machines et serveurs du parc informatique de l'entreprise ACME ainsi que les services présents sur les dites machines.

Déploiement et automatisation des mises à jour avec Ansible.

La solution de déploiement via Ansible est retenue pour le déploiement et l'automatisation des mises à jour sur les différentes machines du parc : automatisation du déploiement des nouvelles mises à jour et des environnements de travail personnalisés pour les nouvelles machines qui arrivent sur le réseau.

Inventaire (GLPI)

Possibilité d'utiliser la solution GLPI afin de faciliter l'inventaire. GLPI est un logiciel libre de gestion des services informatiques et de gestion des services d'assistance.

e) Simplification de l'accès à l'application en relation avec la gestion du parc

Launcher sur les postes des employés

Création d'un raccourci sur les postes des employés de l'entreprise afin d'accéder plus facilement à l'application (pas besoin de saisir l'URL).

Connexion chiffrée (SSL/TLS)

Il est préconisé de mettre en place une connexion chiffrée de type SSL/TLS pour se connecter à l'application que ce soit au sein de l'entreprise ou à distance. Il est également proposé de mettre en place le protocole https pour l'accès à l'application CRM.

Accès au contenu de l'application en fonction des privilèges de l'utilisateur

Chaque employé a accès à ses clients et à un nombre limité d'actions sur ses propres clients. Le manager, quant à lui, peut effectuer toutes les actions sur les commandes, les clients, les produits etc.

f) Accès distant sécurisé à l'application

Pour sécuriser l'accès distant à l'application lors du déplacement d'un employé ou pour le télétravail, il est recommandé de mettre en place un VPN entre le réseau de l'entreprise et le poste de travail (pc portable) de l'employé.

g) Optimisation de l'infrastructure pour supporter la croissance de l'entreprise

Dans le but de prendre en compte la croissance de l'entreprise ACME pour les prochaines années, il est proposé de mettre le réseau global de l'entreprise sur deux bâtiments de plusieurs étages.

Comme les connexions actuelles sont des connexions cuivrées, il est également recommandé de relier les LAN et le cœur du réseau avec de la fibre pour plus de performance.

Actuellement, tous les services de l'entreprise sont réunis au sein d'un seul et même réseau. Il est fortement recommandé de séparer les différents services d'ACME (administration, production, etc.) en différents LAN :

- LAN n°1 : Administration (bâtiment 1)
- LAN n°2 : Production (bâtiment 2)
- LAN n°3 : Salle de serveurs (bâtiment 2)

- LAN n°4 : Invités (bâtiment 1)

Un seul serveur est actuellement utilisé pour héberger tous les services courants (DHCP, DNS, MAIL etc.). Il est préconisé de séparer les différents services sur des serveurs différents, d'où l'intérêt de mettre en place une salle dédiée aux serveurs. La salle de serveurs accueillerait donc un serveur DNS, un serveur DHCP, un serveur de mail ainsi qu'un serveur pour l'application CRM. De plus, il est souvent recommandé de redonder le serveur DHCP pour des raisons de sécurité, aussi est-il proposé de mettre en place un serveur DHCP esclave du serveur maître (en salle des serveurs) afin d'avoir un serveur DHCP dans chaque LAN au cas où le cœur de réseau viendrait à être momentanément indisponible, ou au cas où le serveur maître serait hors service.

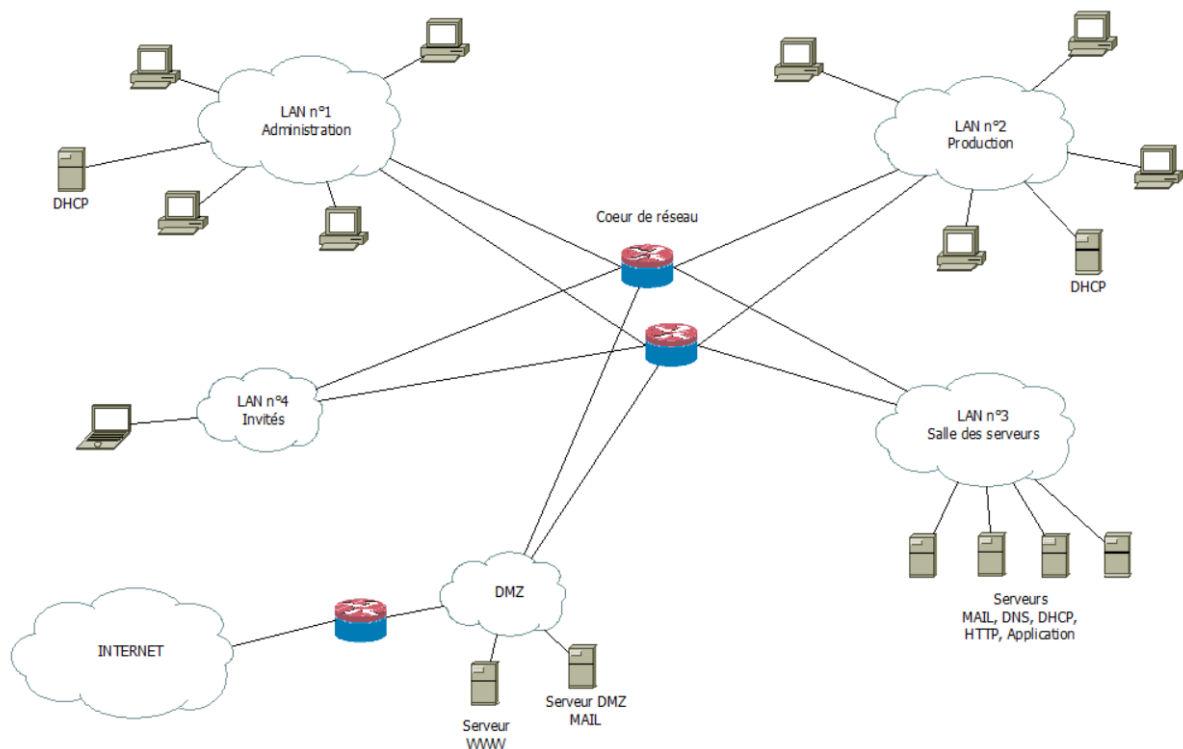


Schéma n°5 - Réseau logique de la nouvelle version de l'entreprise ACME

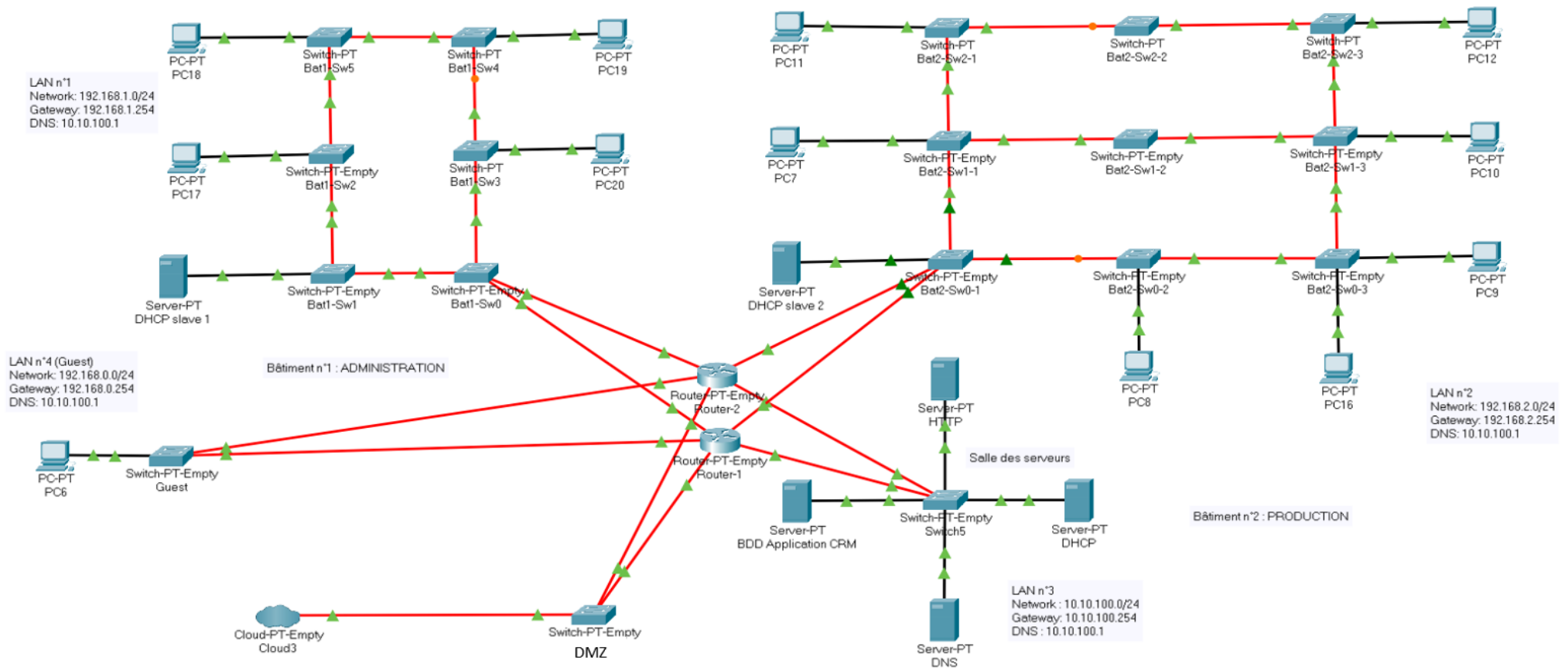


Schéma n°6 - Réseau physique de la nouvelle version de l'entreprise ACME