Aspects Sécurités

L'aspect sécurité identifié dans cette rubrique se base sur les points suivants :

1- La sécurité physique et logique ;
2- La sécurité des données ;
3- La Gestion des incidents (plan de continuité et SLA) ;
4- Architecture d'interconnexion Voix et Data ;
5- Fonctionnalité Hermès et Gestion des flux ;

1. La sécurité Physique et logique

- L'accès aux locaux (espaces de production et salle technique) est contrôlé par des badgeuses (en entrée comme en sortie). Les badgeuses sont gérer depuis un serveur (grâce un logiciel) et qui permet de définir les droits et privilèges des employés. Afin d'éviter toute perte de carte d'accès d'un employé ou éviter qu'un employé ne vienne à la place d'un autre, nous avions opté pour l'enrôlement des empruntes (minimum deux doigts par employé). Tout accès est enregistré dans une base de données. Ce qui nous permet non seulement d'avoir une traçabilité des entrées et sortie mais aussi d'avoir un point sur la présence des employés (pour la paie à la fin du mois).
- Nos espaces sont surveilles par des caméras IP qui couvrent tous les angles. Ils sont relies à un serveur de vidéosurveillance, qui permet d'administrer les camera grâce un logiciel. Ce serveur est équipé d'un disque de grande capacité (1 To) qui permet de stocker les images enregistré pour une durée minimum de 15 jours. Les images peuvent être visualisées en temps réel et consultées à n'importe quel moment. Aussi, pour renforcer la sécurité du bâtiment et du personnel, nous avons :
    - Les détecteurs de fumée sur tous les plateaux de production et les bureaux administratifs ainsi que la salle technique ;
    - Les extincteurs au dioxyde de carbone ;
    - Les déclencheurs manuels boitiers à briser.

Caractéristiques des matérielles mises en place:

Matériels	Modèle	caractéristiques	Autres information
Caméra	xc-256	1/3 pouce SONY 960 EX view HAD CCD	976(H)X 582(V) pixel 976(H)X 578(V) pixel Plus de 650 TVL resolution
badgeuse	Fingertec R2	-processor 400 MHz -mémoire 8mb -emprunte 120000	TCP/IP, RS232, RS485, USB flash disk

2. Sécurité des données

DROITS D'ACCES

Pour mettre en place notre politique de sécurité, un domaine a été créé. Ce dernier est géré par un contrôleur de domaine. L'accès à des données vous obligent à avoir des identifiants (Login/mot de passe) pour accéder à une session et pouvoir y retrouver toutes les informations auxquelles ce profil à droit. Ceci nous permet donc de retracer toutes les activités des utilisateurs grâce aux journaux de logs et de pouvoir contrôler le flux et l'accès aux données. Une série de lecteur partagé est créé, chacun mappé avec les utilisateurs devant y avoir accès ainsi que les autorisations (lecture/écriture/non autorisé). Pour les bases de données, la définition des droits revient au DSI qui les attribue aux administrateurs ou développeur selon leur profil. Nous avons aussi un firewall qui nous protège contre les attaques ou accès depuis l'extérieur ;

MISE EN PLACE DES GPO

Les stratégies de groupes sont des ensembles de paramètres qui s'appliquent aux utilisateurs et ordinateurs. Elles permettent de gérer plus facilement la sécurité d'un poste ou de plusieurs postes dans un Domaine. Les GPO mis en place nous permettent de contrôler les différents profils et leurs droits. En effet grâce à ces GPO, nous arrivons à restreindre l'accès à certaines ressources des postes de travail en fonction des profils :

- Accès aux panneaux de configuration ;
- Accès au disque dur ;
- Accès à la carte réseau ;
- Port USB désactivée ;
- Accès aux différents programmes des postes de travail ;

- Raccourci clavier désactivé (pour lancer certain programmes système) ;
- Etc…

Plusieurs GPO ont été mis en place et sont classés en fonction des départements.

GESTION DE L'ANTIVIRUS

Un serveur d'antivirus a été mis en place dans le réseau. En effet sur ce serveur est installé ESET ANTIVIRUS qui effectue des mises à jours régulières en se connectant au serveur de mise à jour (l'entreprise) à partir d'internet. Il est également installé sur tous les postes de l'entreprise (Production, Administration). Vu la politique de sécurité mis en place, ces derniers effectuent directement leurs mises à jours depuis le serveur local et permet ainsi de nous protéger des risques d'infection virale ou de vers.

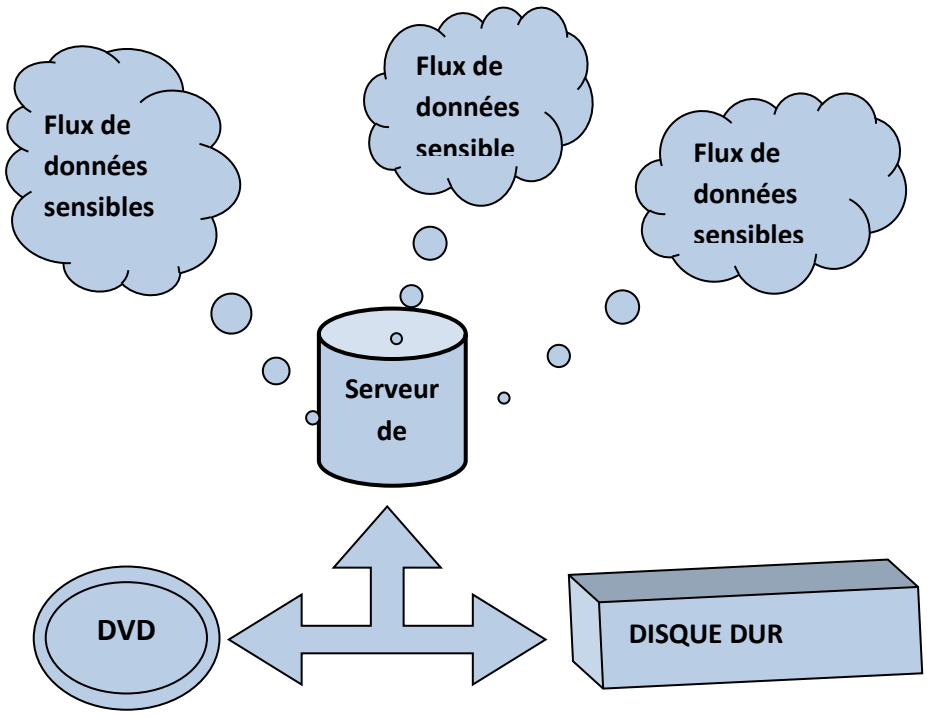
En cas d'infection, une analyse complète de tous les disques est immédiatement effectuée pour supprimer au plus tôt la menace.

SAUVEGARDE DES DONNEES

Afin de garantir une récupération complète des données sensible de l'entreprise et des clients, un backup est fait de façon régulière et automatique (tous les 3 jours). Nous avons opté pour deux types de sauvegarde :

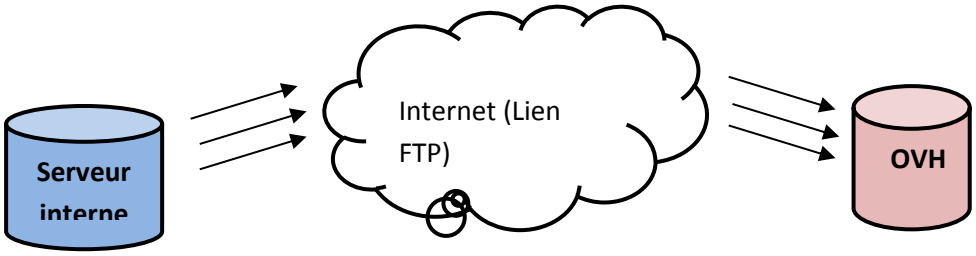
SAUVEGARDE INTERNE

Nous avons donc prévu de stocker sur des supports amovibles (Disque dur externe, DVD).



SAUVEGARDE A DISTANCE

Quant à la sauvegarde externe des données, elle consiste à déposer certaines données sur un espace distant. Dans notre cas, il s'agit d'un espace chez OVH (**O**n **V**ous **H**éberge) accessible via un lien FTP ou un client FTP. Cet espace est sécurisé. Il est aussi prévu des sauvegardes sur le cloud (Google drive) afin de permettre un accès au client suivant une politique d'accès.



3. Gestion des incendies

Interruption de services inferieure a 6heures

TYPE D'INCIDENT	CAUSES POSSIBLES	SOLUTION	TEMPS DE RESOLUTION
Patch Hermès	Messages récurrentes sur l'interface des agents	Mise à jour du CRM par le fournisseur	120 minutes
Accès difficile aux serveurs de production	Services lents, Mémoire surchargée, virus	Reboot immédiat des serveurs	30 minutes
Arrêt d'un service (SQL, Onnet32 Slave)	Service planté	Redémarrage des services concernés	15 minutes
Soucis d'énergie	Coupure de courant sur une longue durée	Prévoir des sources d'énergie alternative (groupe électrogène, onduleur)	5 minutes
Instabilité liaison	Mauvaise communication ou non réception des appels sur la Media Gateway	Revoir l'architecture réseau Interne et avec le client OCM	60 minutes
Impossible d'accéder au SI OCM	Impossibilité d'accéder aux applications métiers chez les OCM	Revoir l'architecture réseau avec le client OCM	60 minutes
Déconnexion du CRM	Suite à un souci réseau ou un service désactivé	Redémarrer les services concernés ou les serveurs	30min
Indisponibilité d'espace sur le serveur HMP	Espace disque insuffisant sur le disque principal à cause des fichiers audio	Vider régulièrement l'espace en disposant d'un serveur de stockage de fichier audio	20 min

Perte de données ou infection virale	Suppression ou données corrompues	Restaurer les sauvegardes effectuées au préalable	120 minutes

Si la résolution de la panne est supérieure à 60 minutes, un call conférence sera initié avec le service informatique OCM pour informer et situer les responsabilités. Une cellule de crise devra être mise en place et fournira des comptes rendus horaires. Au sein de cette cellule sera rédigé le plan d'action formalisé. La crise fera l'objet d'un retour d'expériences (REX).

Interruption à long terme

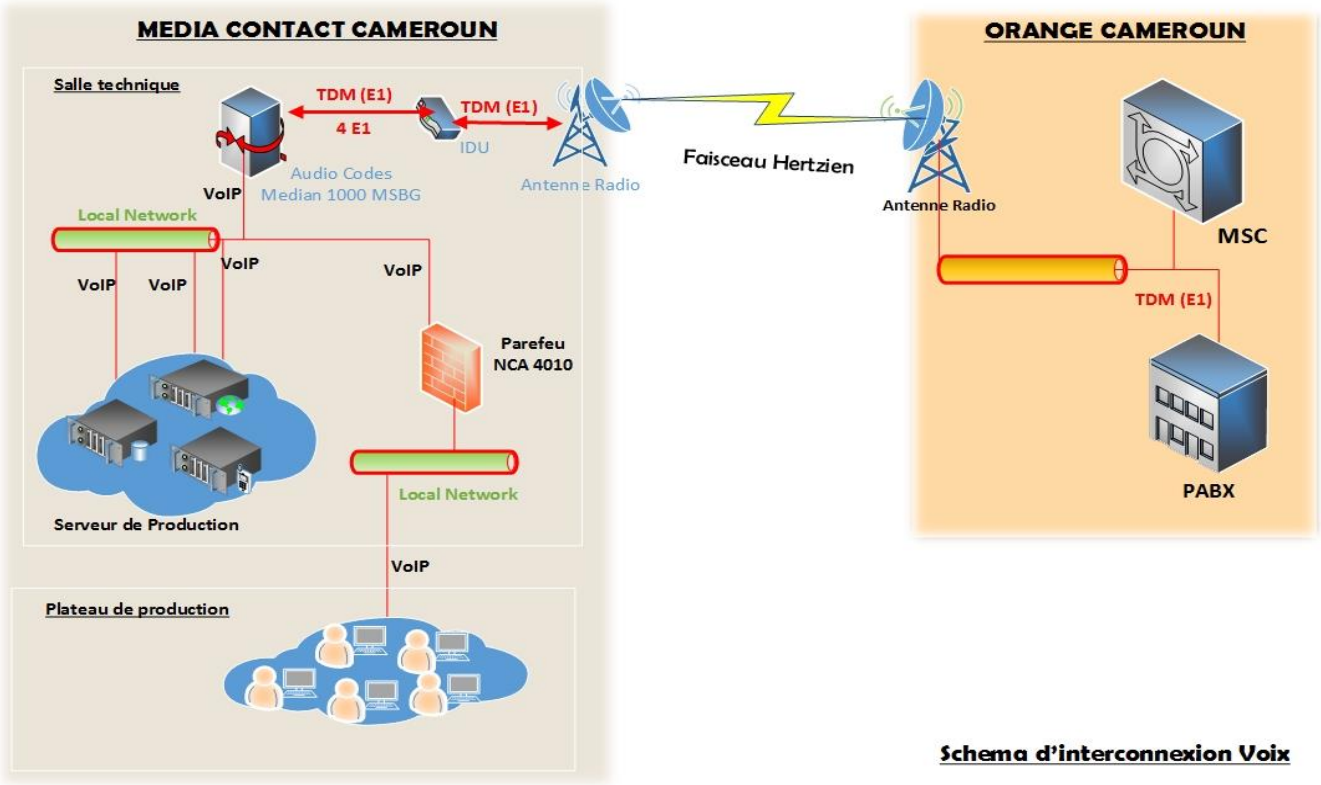
Cas d'incendie ou inondation

Dans ces deux cas, le temps de résolution dépassera les six heures.

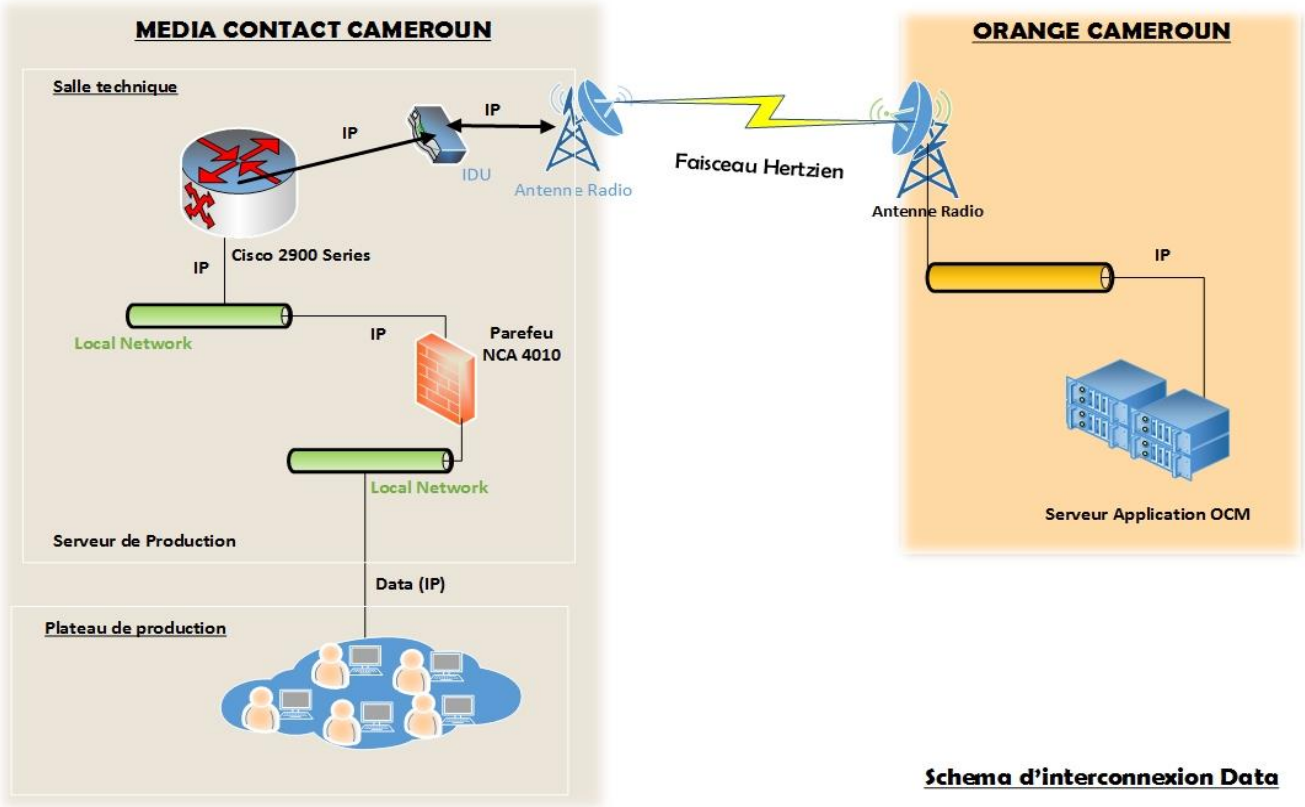
Une plateforme redondante sur le cloud (car notre solution supporte le deploiement sur cloud), sera mise en service avec une politique de synchronisation bien définie. L'administrateur devra notamment informer le service informatique OCM sur le plan de déploiement de la solution adoptée et un compte rendu détaillé sera transmis aux différents acteurs.

Après la résolution de l'incident et retour à la normal, une information sur l'incident est communiquée par mail à tous les acteurs suivi d'un rapport sur l'indicent à signer par toutes les parties.

4. Architecture d'interconnexion Voix et Data



Schema d'interconnexion Voix



Schema d'interconnexion Data

Caractéristiques des different equipment

- **Cisco 2900 série**

Routeur à utiliser dans le cadre de la mise en place de la liaison Data.

La série 2900 peut offrir 2 ou 3 ports GE avec 1 ports SFP, 4 EHWIC Machines à sous, 2 emplacements SM avec 1 slots SIM et 3 emplacements DSP. De plus, leur RAM et la mémoire flash sont évolutives, RAM maximum 2.5G et flash 8G. La série 2900 peut également offrir la fonction vocale.

- **Audio codes Mediant 1000MSBG** : passerelle voix (IPBX).

LA MISE EN RÉSEAU

Type : passerelle VoIP

Technologie de connectivité filaire

Protocole de liaison Ethernet, Fast Ethernet, Gigabit Ethernet

Protocole réseau / transport DHCP, L2TP, PPPoE, PPTP, TCP / IP, UDP / IP

Caractéristiques soutien BOOTP, DDos prévention des attaques, prise en charge DiffServ, protection contre les attaques DoS, prise en charge IPv6, la qualité de service (QoS), prise en charge Syslog, prise en charge VLAN, commutation de couche 2

INTERFACE VOIX FOURNIE

Type réseau

Interface T1 / E1 / J1

Quantité 1, 2, 3

Type de connecteur RJ-45

- **IDU**

Equipement modulateur /démodulateur. Il reçoit le signal de l'antenne et l'envoie sous forme d'E1 vers l'équipement Media Gateway.

- **Par feu NCA 4010**

Pare-feu respectant les caractéristiques ci-dessous :

- Filtrage par IP source et destination, le protocole IP, la source et port de destination pour le trafic TCP et UDP

- Permet de limiter les connexions simultanées basées sur une règle
- Politique de routage très flexible ;
- Gestion par interface graphique ;
- Monitoring en temps réel des différents Traffic ;
- Conserve l'historique des trafics pour des rapports ;
- Options pour la connectivité VPN, IPsec, OpenVPN et PPTP ;
- Fonction de portail captif pour protéger l'accès aux réseaux local ;
- Fonction de NAT / PAT ;
- Fonction de routage inter-réseau (VLAN) ;
- Fonction Multi-WAN pour l'usage de connexions internet multiple ;

5. Fonctionnalité Hermès et Gestion des flux :

Fonctionnalités d'hermès

Hermes.Net est une solution complète de centre d'appels utilisant un simple navigateur internet, donnant accès à toutes les fonctions d'un centre de contacts :

- Appels entrants ;
- Appels sortants ;
- Campagnes tchat ;
- Des Robots calls ;
- Campagne de prise de rendez-vous pour les commerciaux ;
- Campagnes des réseaux sociaux (Facebook, Emailing, Twitter et WhatsApp) ;
- Mise en place des SVI dynamique et complexe (interaction avec des bases de donnes SQL et Oracle).

Le traitement est effectué sur un serveur central, possédant un automate interne qui permet la distribution automatique des appels aux agents avec la gestion d'une file d'attente.

Il présente cinq modules de gestion à savoir :

- le module administration (pour le personnel Informatique)
- le module supervision (pour les chefs d'équipe ou team leader)
- le module agent (pour le traitement des appels par les agents)
- le module reporting (pour les chefs d'équipe ou team leader afin de suivre les PKI de la production)
- le module scripter (pour la création des interfaces agents et SVI)

Le module agent permet de lancer l'interface donnant accès aux fonctions téléphoniques. Le bandeau CTI peut être intégré dans un script écran (crée à partir du module scripter) qui donne accès au guide d'entretien, aux informations issues des bases de données et permet à l'agent de déclencher toutes les actions post- appels avec un simple clic sur l'écran.

Hermes.Net est d'une administration simple et intuitive ; la solution permet l'utilisation dans un environnement multi-sites ou mono-site. L'administrateur hermes.Net grâce à l'interface graphique conviviale gérer en toute confiance les campagnes et les ressources humaines.

En quelques clics de souris, l'administrateur configure les campagnes d'appels entrants et sortants ou les campagnes d'e-mail et établi le lien CTI en la téléphonie, le traitement de données et les ressources humaines. L'administrateur gère les groupes d'agents, les compétences, les profils et les règles de call blending. Les stratégies d'appels peuvent être adaptées en quelques secondes, favorisant une réponse rapide et efficace en cas d'événement inattendus ou de fausse estimation pendant la préparation d'une campagne ou en cas de manque de personnel. Sa caractéristique la plus intéressante est la facilité avec laquelle un personnel non technique peut réaliser une campagne. Le scripteur de Hermes.Net permet de développer rapidement des scripts légers utilisables dans tout navigateur internet. Connecté à une base de données, vous conservez la trace de vos interactions client.

DISTRIBUTION DES APPELS

- Cas des campagnes de réception d'appel

Les points d'entrée pour les appels entrants sont des entités appelées campagnes. Les campagnes (ou scénarios SVI liés à elles) sélectionnent la file dans laquelle l'appel sera placé. Le choix de la file est trivial quand on n'utilise pas un scénario SVI : le champ de file est pris depuis la définition de la campagne. Quand on utilise un SVI, cette valeur par défaut peut être changée et toute file peut être choisie dynamiquement selon les conditions dépendantes du SVI.

Les agents peuvent prendre des appels des files si on leur a assigné les compétences sur cette file. Quand plusieurs agents sont disponibles, l'agent avec le niveau le plus approprié est choisi.

- Cas des campagnes d'émission d'appels

Pour ce qui est de l'émission d'appel, un fichier client est injecté dans la base de données hermès lié à la campagne. L'ACD se charge alors de la numérotation vers les prospects ainsi que de la distribution automatique des appels vers les télévendeurs.

SCHEMA SYNOPTIQUE DU FLUX D'APPELS