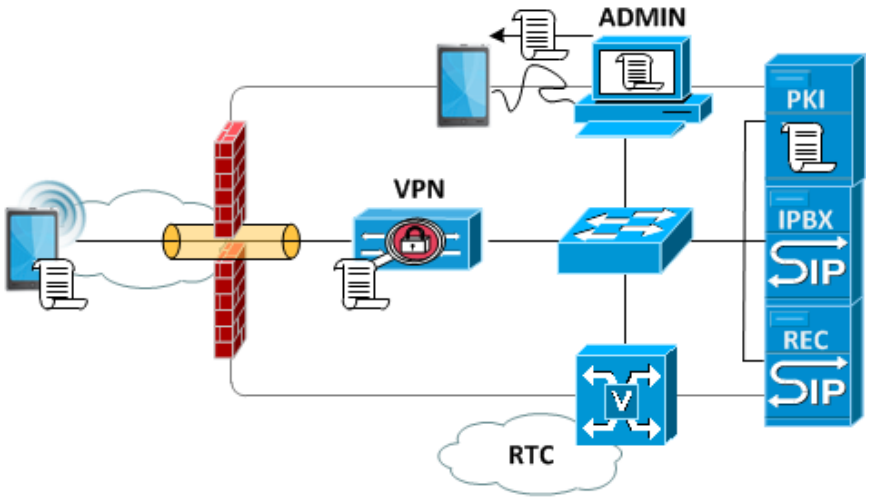
VoIP Mobile Sécurisée (SMV)

Dans certains domaines de l'industrie, notamment liés à la Défense, un besoin fort en communications sécurisées existe. La plateforme de VoIP Mobile Sécurisée (ou SMV, *Secured Mobile VoIP*) apporte une solution pour les terminaux mobiles (de type *smartphones*) qui équipent de plus en plus de personnes.

Description

L'objectif de ce projet est de proposer une plateforme fortement sécurisée, isolée au maximum du monde extérieur, et fonctionnant sur les réseaux mobiles actuels (3G/3G+). Dans un souci d'évolutivité (ajout de services supplémentaires de type email, …), l'accès à la plateforme est assuré par un unique point d'entrée, assuré par un service d'accès distant (VPN SSL) fortement restreint.



L'accès au service est en effet uniquement autorisé si le client fourni un certificat signé par l'autorité de certificat (CA, *Certificate Authority*) incluse à la plateforme. Couplés à un mot de passe unique pour chaque utilisateur, le service est effectivement protégé par une sécurisation à double authentification (*dual-factor authentication*) via deux informations distinctes (mot de passe et certificat). Cette méthode d'authentification représente aujourd'hui un des meilleurs compromis entre efficacité de la sécurisation et facilité d'utilisation.

Le choix d'une solution de type VPN (opposée au chiffrement de bout en bout qu'offrirait de la voix sur IP sécurisée traditionnelle) permet de chiffrer le trafic uniquement lorsque nécessaire, à savoir sur un réseau public (Internet). Cette méthode laisse la possibilité d'étendre facilement les fonctions de la plateforme (email, …) sans nécessiter la mise en place de mécanismes de sécurisation dédiés : tout le trafic à destination de la plateforme transite systématiquement via le tunnel VPN sécurisé ! Ce choix permet également de pouvoir contrôler la sécurisation de la plateforme et ainsi l'adapter facilement aux diverses législations et règlementations nationales (restrictions sur les algorithmes de chiffrement, par exemple).

Au sein même de la plateforme, la partie voix (sur IP ou VoIP) est gérée un serveur central, chargé de

distribué efficacement les appels. Ceux-ci peuvent notamment être routés directement vers un autre utilisateur, ou peuvent être enregistrés, auquel cas le trafic transite au préalable par le serveur d'application SIP dédié. Une passerelle AudioCodes permet également de recevoir des appels entrants depuis le RTC (Réseau Téléphonique Commuté). La gestion de l'ensemble de la plateforme est assurée par une interface Web d'administration centralisée facilitant l'usage au quotidien de la solution.

Rôle de NEXCOM Systems

Projet réalisé dans le cadre d'une demande d'un acteur français de la Défense, NEXCOM Systems avait à charge de développer, déployer et configurer l'intégralité de la solution. A la suite d'une étude préliminaire ayant pour objectif la définition claire des possibilités et des solutions envisageables, grâce notamment à la réalisation d'un prototype simplifié (PoC ou *Proof of Concept*), des choix définitifs ont été faits en collaboration étroite avec le client.

À la suite de ces décisions, le prototype a pu être industrialisé et finalisé en y incluant l'ensemble des composants requis initialement. L'objectif étant d'offrir une solution complète, permettant à la fois de passer des appels en voix sur IP sécurisée, mais également de gérer et configurer facilement la flotte de terminaux mobiles utilisés pour ces appels. Une des contraintes majeures était de fournir une solution clé en main, d'usage aisé pour les utilisateurs finaux de la plateforme : application client intégrée, interfaces d'administration… Ces aspects ont été une priorité pour l'ensemble de l'équipe de développement tout au long de la réalisation de ce projet.

Technologies utilisées

Pour des questions liées à la sécurité (pouvoir vérifier qu'aucune *backdoor* n'existe, notamment), l'ensemble des services déployés par NEXCOM Systems repose sur les solutions Open Source (OSS, *Open Source Software*) suivantes :

- Intégration et configuration de l'accès distant sécurisé (VPN SSL) : *OpenVPN*.
- Intégration et configuration de la gestion centralisée des certificats (PKI) : *EJBCA*.
- Intégration et configuration du serveur de routage d'appels (VoIP SIP) : *OpenSIPS*.
- Intégration et configuration du serveur d'enregistrement d'appels (VoIP SIP) : *FreeSWITCH*.
- Développement d'une interface d'administration Web développée directement par NEXCOM Systems et permettant une gestion simplifiée de la flotte des terminaux mobiles et simplifiant leur configuration : serveur *Jetty*, développement JAVA (JSP).
- Développement d'une application cliente unifiée pour terminaux Android intégrant deux applications Open Sources : *OpenVPN for Android* (VPN) et *CSipSimple* (VoIP), développement Android (JAVA, JNI et C++).

Ressources engagées

Les ressources engagées dans ce projet ont été les suivantes :

- Un chef de projet et responsable technique, en charge de l'infrastructure système.
- Un ingénieur en soutien sur l'infrastructure système.
- Un validateur et testeur de la solution.
- Un développeur pour l'application de gestion Web.
- Un développeur pour l'application unifiée Android.

La charge de travail a été évaluée en fonction de la contrainte forte du projet : les délais de réalisation. Celle-ci s'est élevée à environ 1 homme/an. La répartition de la charge s'est effectuée selon la méthode Agile, en itérations successives, afin de réduire autant que possible la prise de risque tant pour le client que pour NEXCOM Systems, toute en optimisant au mieux les coûts et délais de réalisation. En l'occurrence, une séparation en trois itérations a été choisie :

- Une première étape étudiant la faisabilité d'une telle solution via la réalisation d'un prototype technique (PoC) et permettant de définir précisément les possibilités à disposition.
- Les deuxième et troisième étapes, liées, industrialisant le prototype et ajoutant/développant toutes les fonctions requises (routage et enregistrement d'appels, interfaces d'administration, …).