Cahiers des charges

Le client a demandé un devis pour la création du réseau de sa nouvelle agence de maintenance/location/gestion de voiliers à la marina du Marin, les contraintes sont les suivantes :

- Les techniciens doivent pouvoir travailler sur des terminaux mobiles au nombre de 7 à bord des bateaux.
- 10 postes fixes dans l'agence.
- Les applications à déployer dans l'infrastructure sont les suivantes : messagerie ; comptabilité ; les ventes, la gestion de relation client (CRM), gestion de projets et des activités de services , logistique et gestion des stocks, gestion de production, comptabilité analytique et financière (conforme aux exigences françaises et suisses) et les ressources humaines.
- Sauvegarde et systèmes de secours.
- Faciliter le travail collaboratif
- Facilement extensible (rajout de nouveaux postes ou logiciels)

Pour satisfaire les différentes conditions j'ai étudié les solution suivantes :

1) Réseau décentralisé avec les applications métier installé en local sur les machines

   Les plus :
   Coûts de déploiement réduits ; pas de serveur central, un NAS suffit ; un réseau consistent en un simple accès internet wi-fi ;

   Les moins :
   Pas de gestion centralisée des données ; travail collaboratif et suivis difficiles ; gestion des sauvegardes complexifiée ; risque de vol de données si un des terminaux est volé.

2) Réseau centralisé avec applications métier en client/serveur :

   Les plus :
   Centralisation des données et sauvegarde facilitée, peu de risque de vol de données si un des terminaux est volé.

   Les moins :
   Coûts supérieurs, réseau complexe et choix matériel réduit (harmonisation de la configuration matérielle et logiciel des postes dans la mesure du possible)

J'ai retenu la solution du réseau centralisé.

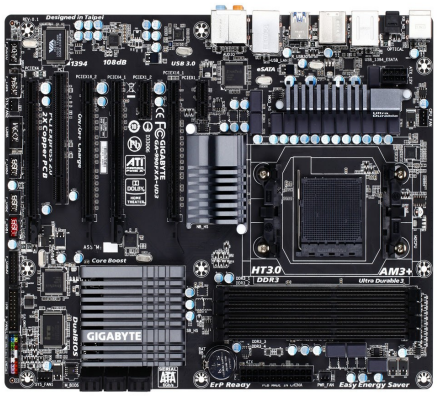
Réseau centralisé, considérations techniques et matérielles :

Pour la réalisation d'une telle infrastructure j'ai proposé le choix d'équipements suivant :
L'utilisation de logiciel libres permet ici l'économie de 4000$ de licences en comparaison avec une solution Microsoft (10*Windows 7
Pro 200$ +2*Windows server 2012 standard 1000$)

Serveur :

Processeur 8 cœurs AMD Athlon FX 4,00 GHz socket AM3+

Carte mère socket AM3+ Gigabyte GA-990XA-UD3
16 Go DDR3 1600Mhz
RAID 1 2*SSD 256 Go SATA 6 Gbps



NAS

Processeur 4 cœurs AMD Athlon FX 3,00 GHz socket AM3+
Carte mère socket AM3+ Gigabyte GA-990XA-UD3
4 Go DDR3 1600Mhz
8* 1To SATA 6 Gbps (7 disques en RAID5 un de rechange à chaud)
Système d'exploitation FreeNAS x64

Postes fixes (Ubuntu 12.04 LTS) :

Processeurs socket FM2 AMD A4-5300 2 cœurs 3,40 GHz
Cartes mères socket FM2 MSI FM2-A55M-E33
2 Go de RAM DDR3

Terminaux mobiles :

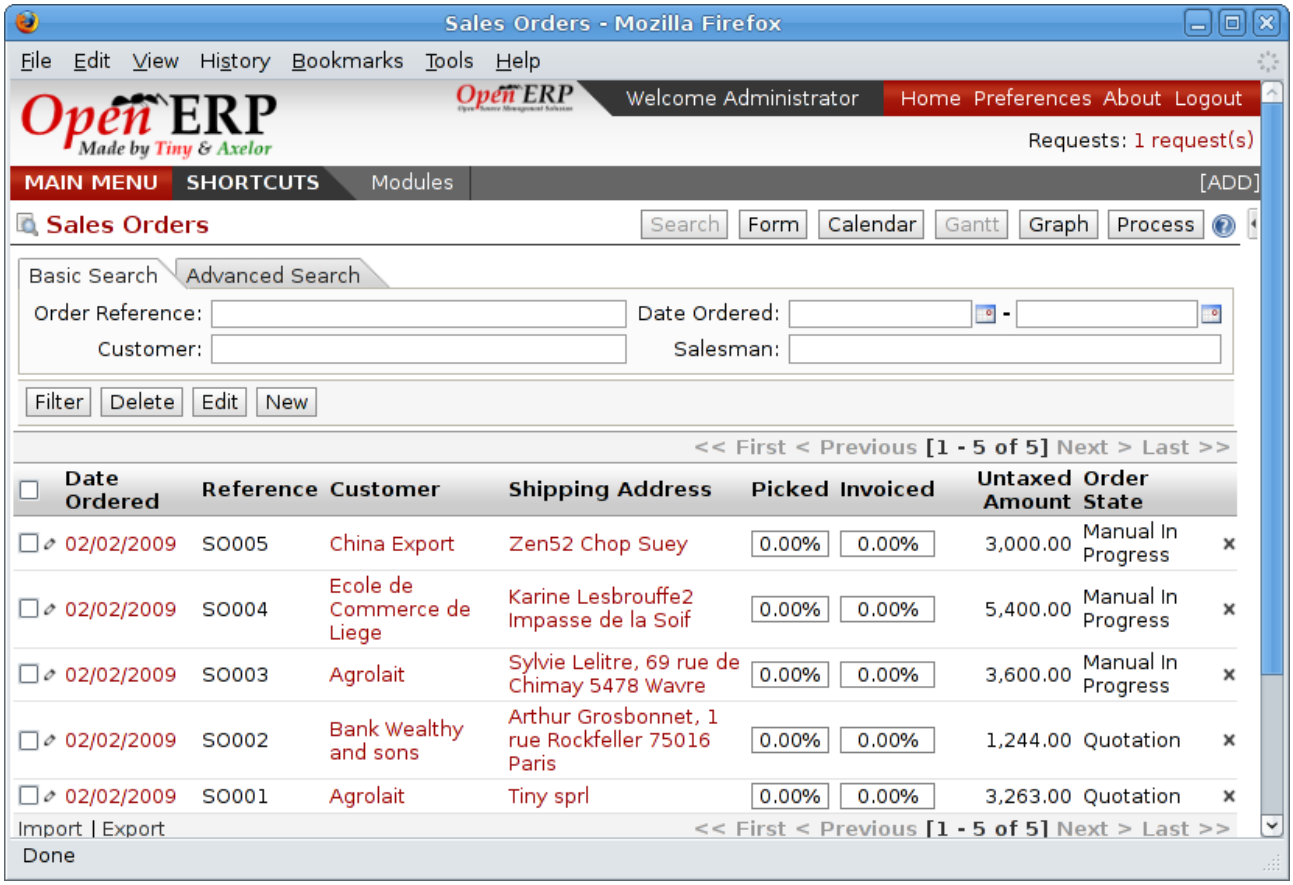
Asus Transformer TF700
Processeur NVIDIA Tegra 3, 4 cœurs, 1 Go de RAM, 32 Go de flash

A l'origine ces terminaux fonctionnent sous Android 4.0 mais pour les besoins de l'entreprise ce système d'exploitation n'offre pas les fonctionnalité nécessaire, j'ai donc installé Ubuntu 12.04 LTS sur les tablettes ce système d'exploitation libre offrant de plus grandes possibilités et performance tout en permettant une meilleure sécurité des données (système de fichier crypté).

Le second avantage offert par cette solution est le dock qui une fois connecté à la tablette permet de porter l'autonomie à 10h contre 5h sans et permet d’économiser l'achat de 7 postes fixes car le dock possède un port USB et carte SD.

Serveur

Pour le serveur la solution que j'ai retenu est l'utilisation du logiciel OpenERP qui satisfait toutes les exigence du cahier des charges en intégrant toutes les fonctionnalités requises dans une interface Web, tout les services et données gérées par le serveur, de plus ce logiciel est libre et gratuit (licence AGPL v2.0).



OpenERP avec le navigateur Mozilla Firefox 16

Les postes clients ne nécessites qu'un navigateur web gérant Javascript, CSS3, HTML5 et le SSL, aucune données n'est stockée sur le poste client d'un point de vue sécurité c'est idéal.

Sur le serveur le système d'exploitation est Debian 6 dans lequel sont virtualisés à l'aide de KVM et Proxmox un système Ubuntu 12.04 Server 64 bits sur lequel est installé OpenERP et un système OpenBSD sur lequel est installé le serveur Kerberos (sécurité sans fil)

Le réseau

Internet : Orange Caraïbes 13,7 mbps descendant 0,8 mbps montant
Téléphonie : Orange Caraïbes VOIP

Le routeur : Routeur Gigabit sans fil N double bande TPLINK N900 (TL-WDR4900)
4 ports Ethernet gigabit
Fonctionnant sous OpenWRT ce qui permet la gestion des VLAN, VPN, administration SSH et gestion de la sécurité sans fil par serveur de certificat avec authentification forte (RADIUS).

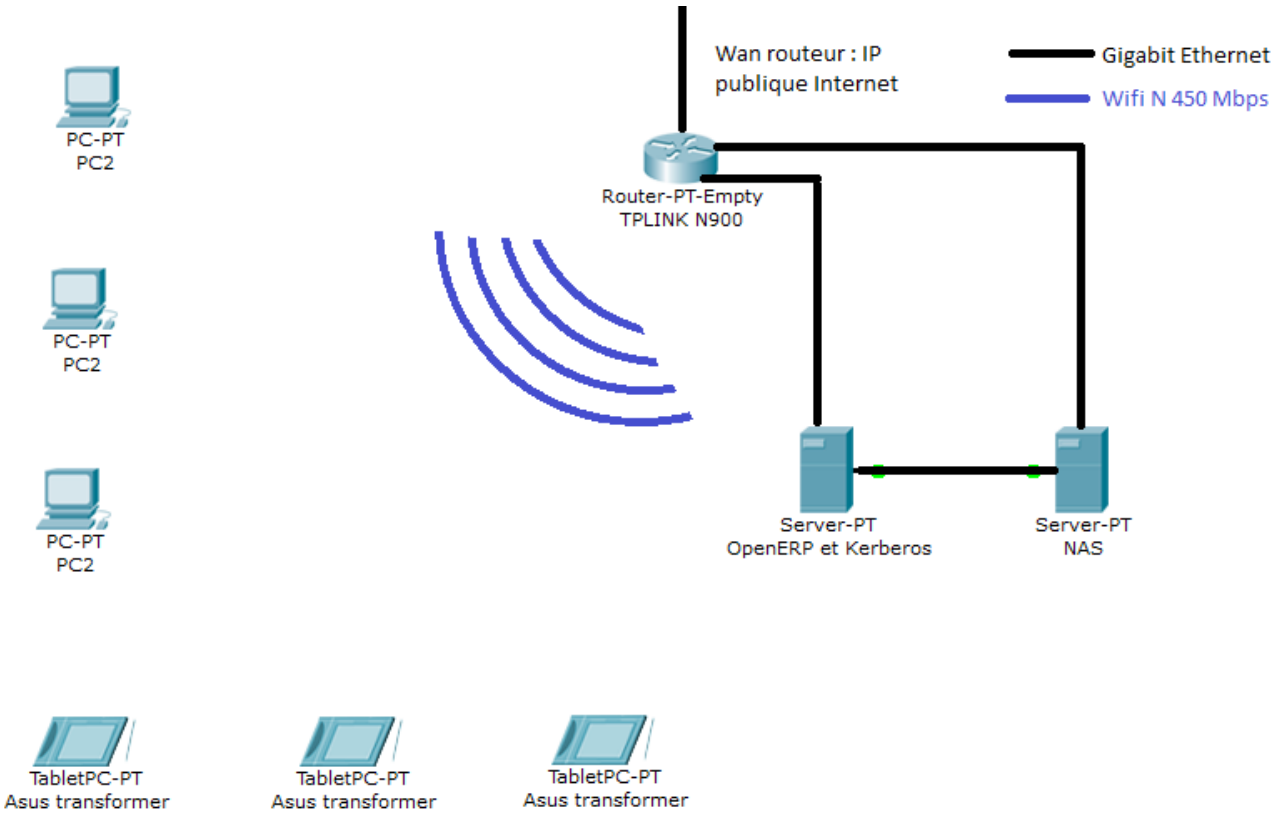
Les liens avec le serveur, le NAS et le routeur se font en filaires tandis que tout les postes de travail sont en Wi-fi.

Le Wi-Fi

Pour le réseau Wi-fi le principal problème vient de la sécurité, la société exploitante jouissant d'une autorisation de l'ARCEP (normalement la limite légale exprimée en PIRE : puissance isotrope rayonnée équivalente est de 100mW) , la puissance d'émission du routeur est débridée à son maximum (503mW) et les locaux de la société se trouvent en front de mer, de mon lieu de résidence à 6 km de là, je captais le réseau wifi avec l'ellipsoïde de Fresnel complètement dégagée grâce à la carte wifi de mon ordinateur portable.

J'ai donc sécurisé le réseau de la façon suivante :

WPA 2 AES enterprise RADIUS/Kerberos
Le réseau WIFI seul ne donne accès qu'au port UDP 1194 qui ne laisse passer que le protocole OpenVPN sur lequel repose la deuxième couche de sécurité.
Chaque poste client se connecte sur le routeur en wi-fi, puis à travers ce dernier via un tunnel OpenVPN chiffré en AES 512 bits qui lui ouvre un accès au réseau local et à Internet.
De plus l'intégralité des données de travail échangées à travers le Wi-fi le sont par le protocole HTTPS permettant une authentification forte et une troisième couche de chiffrage
Les empreintes de 512 bits sont très robustes (64 octets) du point de vue cryptographique. Une attaque par le paradoxe des anniversaires nécessiterait au moins 2^{256} opérations, un nombre très grand.



Problèmes rencontrés

Lors de ma première tentative d'installation d'Ubuntu 12.04 LTS sur les terminaux mobiles j'ai été confronté à un blocage du chargeur de démarrage :

Les différentes causes possibles sont les suivantes :

1) L'image système est endommagée et provoque une panne.

Pour invalider cette hypothèse j'ai ré-téléchargé une image du système que j'ai vérifié avec son empreinte SHA-512.

2) Le matériel est endommagé.

Pour écarter cette hypothèse j'ai utilisé un outil de diagnostic avec le système d'origine (Android 4.0.1) .

3) Le matériel n'est pas compatible (les tests préalables n'ont pas été effectué sur la même version du matériel faute d'approvisionnement).

Après analyse des différents numéros de version des composants logiciels de l'appareil il s'est avéré que le bootloader du terminal n'était pas capable de lancer un autre système que Android, pour palier à ce problème j'ai mis à jour avec une version antérieure du système (Android 4.0.0) livré avec un bootloader plus ancien n'empêchant pas le chargement d'un système d'exploitation alternatif.

J'ai ainsi pu procéder à l'installation d'Ubuntu 12.04 LTS.