JSSI - Sécurité d'une offre de nomadisme

10 mai 2005

Olivier CHARLES – France Télécom R&D

France Télécom
Recherche & Développement

La vulnérabilité des nomades est un problème bien connu

- **Vol de PC portables**
  - Perte de données de l'entreprise
  - diffusion de mots de passe …
- **Confusion usages pro/perso**
  - Installation de logiciels douteux
  - Connexion à des sites non controlés
- **Réseaux de visite sans garantie : écoute intrusion**
  - Salles de réunion, hotspots…
- **Le périmètre du réseau de l'entreprise devient flou**
  - Les PC distants ont des adresses IP dans le plan de l'entreprise et dans le plan de l'opérateur local…

Les réponses à ces risques existent, ce n'est pas la peine de faire de la R&D

- Vol de PC => mot de passe + chiffrement du disque
- Confusion usage pro/perso => charte de bonne conduite, check-up, quarantaine et mise à jour à la connexion
- Réseaux de visite sans garantie => IPsec+ mode bloquant (avant de monter le tunnel!)
- Le réseau de l'entreprise devient flou => authentification forte + éventuellement DMZ

Le vrai challenge du nomadisme

- **Maximiser le ratio …**

$$= \frac{\text{SECURITE + SIMPLICITE}}{\text{COUT}}$$

… trois objectifs souvent contradictoires.

La (non)simplicité du nomadisme

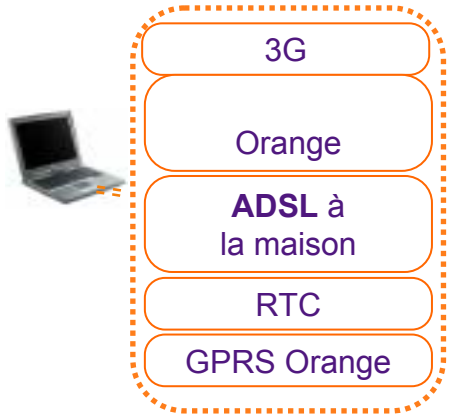
- **PC sur les genoux**
- **Loin du service informatique + décalage horaire**
- **Intégration de plusieurs technos de réseaux**
  - RTC, GPRS, ADSL, EDGE, Ethernet, WiFi, 3G
  - Drivers, connexion, gestion des profils et des mots de passe
  - Enchaînement de plusieurs étapes (connexion réseau, IPsec, appli)
- **Plusieurs mots de passe**
  - BIOS, Windows, réseau, IPsec.
- **Le mode bloquant d'IPsec**

Les coûts de la sécurité du nomadisme

- **Passerelle IPSec**
  - Nombre de connexions simultanées
- **Moyens d'authentification**
  - SecurID, carte à puce (pas abordable pour tout le monde)
- **Équipe de soutien en horaires élargis**
  - Très cher
- **Outil de chiffrement de disque**
- **Firewall nomade, Antivirus…**

Business Everywhere : l'accès au Système d'Information en toute simplicité et confort

un seul contrat
une seule facture



une solution multi-supports

sécurité

Business Everywhere

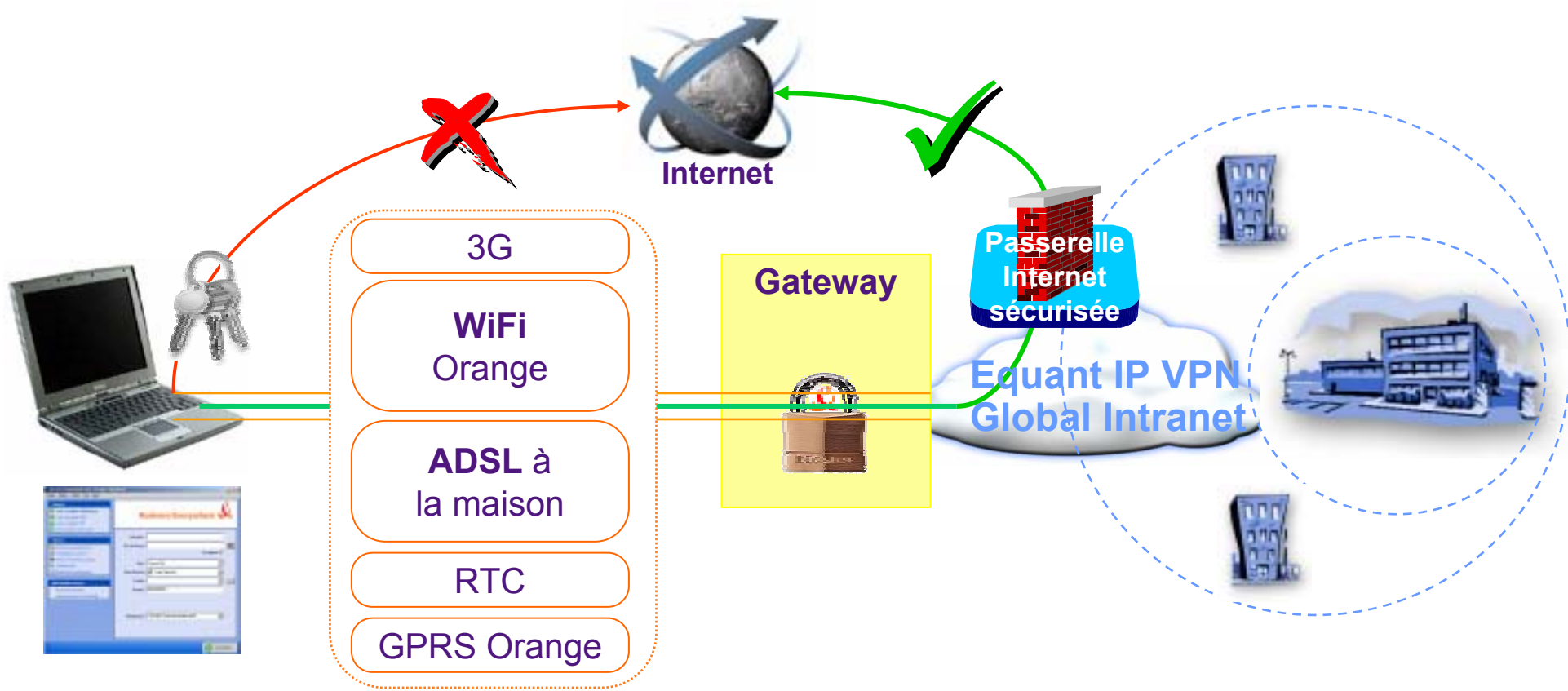
un seul
kit de connexion

service client
pour les gestionnaires
pour les utilisateurs

large couverture
géographique

Diffusion Libre

Business Everywhere : l'accès au Système d'Information en toute sécurité



Business Everywhere

La politique d'accès à Internet est centralisée et maîtrisée par l'entreprise

La sécurité de Business Everywhere

- **Authentification**
  - Mot de passe, SecurID®, certificats sur dongle USB
  - PKI made in France Télécom R&D. Coût de licence = 0. Customization facile.
- **Chiffrement des flux**
  - IPsec
- **Antivirus, Personal Firewall, Antispyware, patch management, mise en quarantaine**
  - Partenariats avec des éditeurs
- **Capitaliser sur la carte à puce**
  - SSO applicatif, WSO, Network Logon (fonction de présence)
  - Mail chiffré signé
  - Chiffrement du disque

Les Mobiles et les PDA

- **Push mail pour applications PIM**
  - Opérateur de confiance
- **IPsec sur un PDA pour applications métier**
  - Où mettre le certificat? Dans le réseau? Dans la SIM?
  - Où mettre les batteries? ;-)

La mobilité sans terminal

- **SSL**
  - SSLisation des applications
    - Si toutefois le navigateur est fiable
    - Problème des pièces téléchargées
  - VPN SSL
    - Il ne faut rien installer sur la machine
- **Un PC dans un dongle**
  - Les données
  - Les données + Les applications
  - Les données + Les applications + un OS

Vers la mobilité généralisée

- **Masquer totalement les réseaux, assurer un hand-over inter-techno efficace pour la applications multi-média**
  - Réauthentification rapide
  - SSO sur les réseaux de l'opérateur

Conlusion

- Le nomadisme est un nouveau comportement qui complique l'approche classique de l'informatique et induit des risques de sécurité importants.
- Le faire faire par un opérateur peut être une apporche valable sur un plan économique mais aussi pour la qualité de service
- Le couple carte à puce/PKI est une fondation solide pour sécuriser le poste de travail