france telecom

Livre blanc

Nomadisme

Travailler partout en toute sécurité

Introduction

Evolution profonde de la société, **"l'individualisme en réseau"** a fortement contribué à la diffusion des services mobiles et Internet.

Le temps s'ajoutant à l'espace, les individus souhaitent pouvoir communiquer en permanence, indépendamment du lieu où ils se trouvent, rendant ainsi nécessaire la virtualisation des contextes. Dans la vie professionnelle, cette évolution sociale vient s'ajouter à de nouvelles donnes économiques telles que la délocalisation de la production ou l'externalisation de certaines fonctions.

Ces évolutions conduisent à répartir les tâches dans des centres géographiquement dispersés. La circulation des biens, des personnes et des informations s'accélère et s'intensifie. Véritables outils de ces transformations, les technologies de communication, notamment les technologies sans fil, connaissent un véritable développement dans l'entreprise et constituent un enjeu majeur pour les DSI.

Le nomadisme **- travailler en n'importe quel lieu de façon aussi efficace qu'en étant au bureau -** doit être intégré dans les architectures réseau et système d'information de façon simple et sécurisée.

Sous le nom de code **Office+**, France Télécom a inscrit le **nomadisme** dans ses priorités sous les angles simplicité, qualité et sécurité.

Ce livre blanc a pour objectif de vous faire partager la vision de France Télécom sur les aspects sécurité du nomadisme.

LE NOMADISME EN ENTREPRISE

Utilisant son accès Internet personnel, un cadre dirigeant se connecte à sa messagerie depuis son domicile pour apporter ses commentaires à la version projet du plan stratégique de l'entreprise.

Lors d'une visite client, un commercial consulte l'état du stock et saisit en temps réel la commande qu'est en train de lui confirmer son acheteur. Bloqué à l'aéroport par un encombrement de l'espace aérien, un cadre consulte sur son mobile les horaires de la navette aéroport-centre ville et envoie un message à sa secrétaire pour l'avertir de son arrivée tardive. On peut multiplier ainsi les situations de nomadisme ; l'objectif est toujours le même : travailler et communiquer en n'importe quel lieu de façon aussi efficace qu'en étant au bureau.

Toutes les entreprises sont ainsi amenées à donner à leurs salariés, en situation de mobilité, les moyens de communiquer, travailler et optimiser les processus.

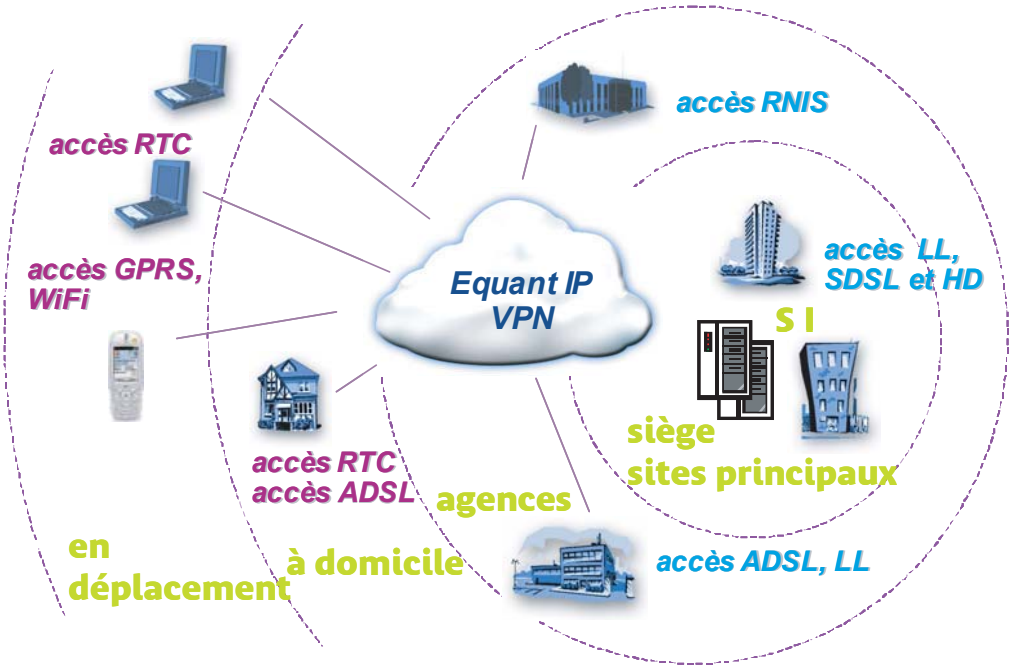
Le nomadisme en entreprise

Toutes les grandes entreprises sont concernées. 37 % des décideurs informatiques considèrent qu'il s'agit de projets prioritaires. D'ici 2005, 20 % des accès au SI se feront via des connexions sans fil, près de 700 000 cols bleus accéderont à des applications verticales en situation de mobilité tandis que plus d'un million de cols blancs travailleront à distance avec leur PC.

Perte ou vol de terminal contenant des données confidentielles, indiscrétions lors de communications dans un lieu public, utilisation de réseaux non fiables rendant possible l'acquisition d'informations sensibles, comportement négligent des utilisateurs ouvrant la voie aux usurpations d'identité, les menaces sont nombreuses et le nomadisme ne peut se développer sans sécurité associée.

SÉCURITE ET NOMADISME

Le système d'information faisant partie du patrimoine de l'entreprise, il est indispensable de disposer d'une connectivité réseau sécurisée pour les données et les applications.



Architecture réseau d'une entreprise

La sécurité du Système d'Information est directement liée aux risques identifiés, en particulier dans :

- l'utilisation des technologies : systèmes d'exploitations, logiciels, technologies réseau, réseaux d'accès…

- l'environnement d'utilisation : bâtiment sécurisé, locaux partagés, lieu public, domicile…

- le comportement de l'utilisateur.

De l'analyse des menaces et de l'étude de leur impact potentiel découle la politique de sécurité de l'entreprise et la définition de l'architecture sécurisée à mettre en œuvre. L'introduction d'accès à distance révèle des menaces particulières pour le SI de l'entreprise au même titre qu'une ouverture à Internet ou la mise en oeuvre d'un extranet avec des fournisseurs ou des partenaires.

Au-delà des services de sécurisation du réseau de type pare-feu, antivirus ou navigation contrôlée sur Internet, l'acceptation du nomadisme dans l'entreprise passe par l'assurance de disposer d'un niveau de sécurité conforme à la politique de sécurité définie pour l'entreprise.

En tant qu'opérateur de référence, France Télécom a choisi d'offrir en toute sécurité à ses clients l'ensemble des technologies d'accès disponibles pour permettre aux entreprises de bénéficier de la solution la plus adaptée à leurs besoins. Au travers de son centre de recherche et développement (FTR&D), France Télécom en a acquis la maîtrise et définit les moyens nécessaires à une bonne sécurisation des accès, indépendamment de leur niveau de sécurité intrinsèque. Le skill center sécurité de FTR&D réunit les compétences de soixante-dix ingénieurs en recherche et experts spécialisés dans le conseil en sécurité, la sécurité applicative et la sécurité réseau. Les domaines d'application traités recouvrent :

- *les réseaux et services mobiles*
- *les infrastructures : plates-formes, cœur de réseau et système d'information*
- *les terminaux*
- *les applications et services avancés*
- *la définition d'une politique de sécurité, l'audit et la détection d'intrusion*
- *le paiement et les transactions*
- *les outils cryptographiques*

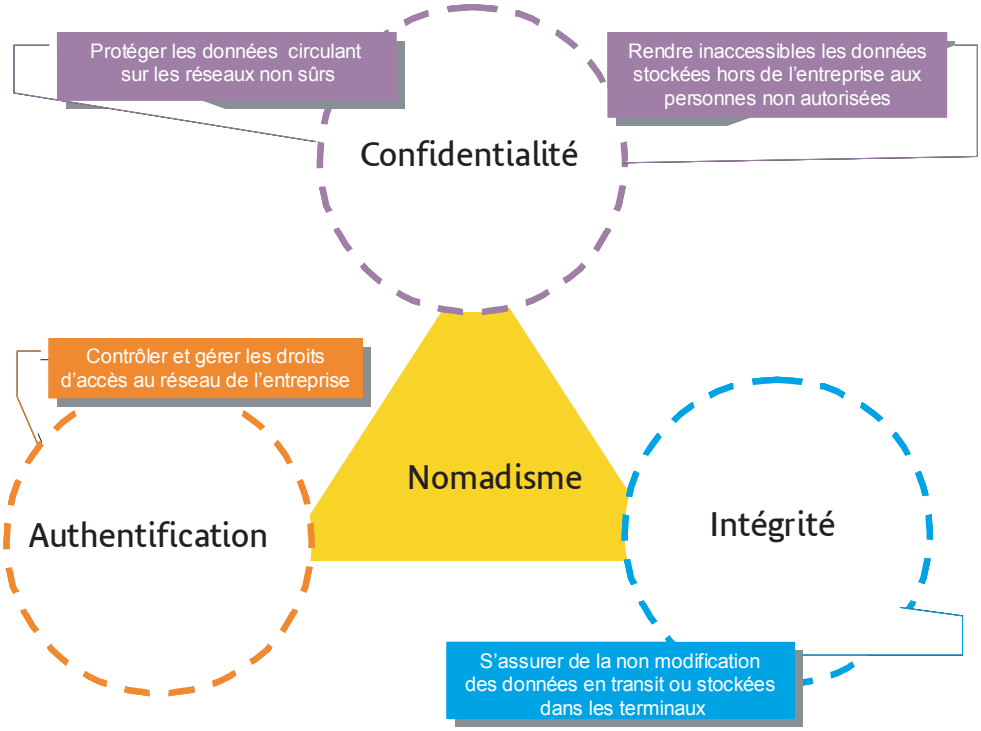
Préalablement à la mise en œuvre des hot spots WiFi d'Orange, le skill center sécurité de FTR&D a dû répondre à un cahier des charges très exigeant en matière de sécurité, de façon à apporter les réponses techniques permettant d'offrir aux utilisateurs un service final intégrant le niveau de sécurité adapté à leurs usages et leurs exigences. Ainsi le service d'accès WiFi à l'intranet des entreprises proposé par France Télécom intègre aujourd'hui la technologie IPsec pour garantir la sécurité des échanges **1** *. Par ailleurs, la mise en œuvre de mécanismes WPA, nouveau standard de sécurité pour WiFi, fait l'objet d'une évaluation technique complète via une expérimentation interne à FTR&D.*

Plus le terminal est intelligent, et plus l'usage est proche de celui effectué dans les murs de l'entreprise : plus les risques sont importants. L'utilisateur doit alors être sensibilisé aux problématiques de sécurité. Dans le cas d'un PC portable, on doit par exemple considérer :

- la protection de l'accès à distance aux ressources internes : contrôle de l'accès et des droits d'accès, en fonction du profil utilisateur
- la protection des données échangées : respect de la confidentialité
- la protection du terminal et des données stockées sur celui-ci

Le nomade est avant tout un utilisateur qu'il va falloir identifier de façon sûre avant de lui autoriser toute action et de lui permettre de travailler en toute confiance.

1 - Voir paragraphe confidentialité des échanges pour plus d'informations



Principales fonctions de sécurité et nomadisme

L'AUTHENFICATION

Michel Martin est technicien de maintenance d'extincteurs dans une PME. Après chaque intervention, il réalise un rapport d'intervention qui déclenche la facturation de sa prestation. Pour éviter toute fraude ou erreur d'imputation, l'accès au workflow est soumis à une autorisation qui nécessite une identification sûre de l'utilisateur de l'application. Michel Martin est donc équipé d'une carte **SecurID©**, solution d'authentification forte, qui lui permet de disposer d'un mot de passe différent pour à chaque session et d'éviter ainsi qu'on usurpe facilement son identité.

Un service d'authentification regroupe en effet deux fonctions complémentaires :

- **l'identification** : je dis qui je suis en tant que personne ou système ;

- **l'authentification** : le système vérifie et confirme que je suis celui que je prétends être. L'authentification est dite simple lorsque l'entité qui désire s'authentifier possède un seul facteur pour prouver son identité. Elle est dite forte quand au moins deux facteurs sont utilisés. Différentes solutions techniques peuvent être utilisées dans un service d'authentification.

Mot de passe statique

L'utilisation de mot de passe fixe (statique) est la technique la plus ancienne et la plus faible des techniques d'authentification. Cette authentification repose, pour la quasi-totalité des systèmes en service, sur le contrôle d'un mot de passe dont la fragilité n'est plus à démontrer :

- mot de passe écrit sur un papier
- mot de passe évident ne résistant pas à une attaque par dictionnaire (logiciel de "crack")
- divulgation ou vol
- capture du mot de passe par écoute de la ligne et possibilité de rejouer la procédure d'authentification.

Pour sécuriser une authentification basée sur un mot de passe statique, on peut encadrer la procédure d'authentification dans une solution assurant la confidentialité des échanges [1] . C'est par exemple la solution généralement retenue par les sites web qui proposent à l'utilisateur de saisir son login et son mot de passe dans une page protégée par https.

Mot de passe dynamique

Pour parer aux attaques courantes des solutions d'authentification basées sur un mot de passe fixe, l'approche la plus simple consiste à utiliser des mots de passe à usage unique, de façon à ce qu'ils ne puissent pas être réutilisés lors de la prochaine session d'authentification, limitant ainsi les risques liés à une attaque active. Les mots de passe sont générés par un logiciel, en mode synchrone dépendant du temps, ou un dispositif externe (jeton ou token) tels que la calculette RSA SecurID© ou la carte ActivCard©.

Pour disposer d'une procédure d'authentification forte, un deuxième facteur de preuve sera utilisé, par exemple un code PIN dans une solution **ActivCard©,** ou un mot de passe utilisateur comme dans le scénario d'authentification forte par **SecurID©** des services d'accès à distance par réseau téléphonique ou GPRS de France Télécom.

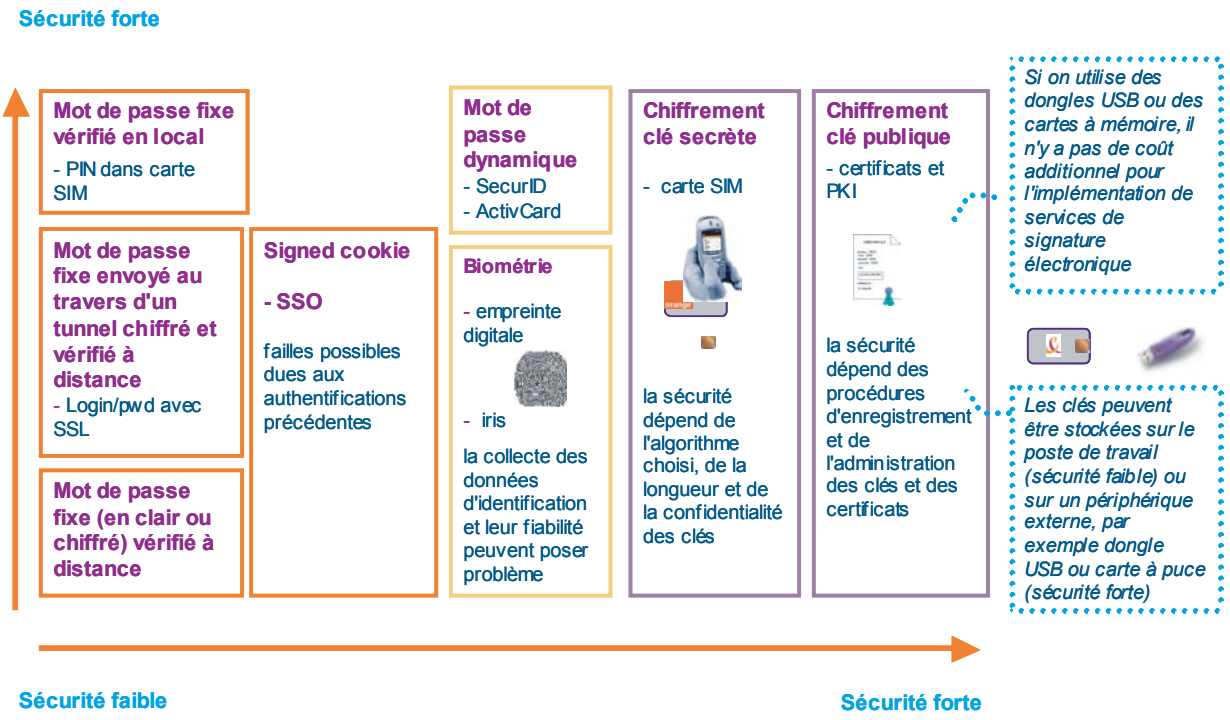
Certificats

L'authentification des entités, systèmes, terminaux ou utilisateurs, peut également être réalisée en s'appuyant sur des algorithmes asymétriques [1]. Le principe consiste à détenir un couple de clés électroniques, privée et publique, ainsi qu'un certificat contenant l'identité, et la clé publique de l'utilisateur et la signature de l'opérateur de certification, qui, associés à des procédures de signature avec la clé secrète, permet de garantir l'identité de l'émetteur du message en contrôlant sa signature avec la certification. La norme de certification la plus répandue est X509.

1 - Voir paragraphe principes de chiffrement

Le certificat et les secrets peuvent être implantés directement dans le système à authentifier, stockés sur le disque dur, ou dans un dispositif externe tel qu'un dongle USB ou une carte à puce. Le niveau de sécurité de la solution est lié aux conditions de distribution et de stockage du certificat et des secrets.

Comparatif des différentes solutions d'authentification



Principales solutions d'authentification

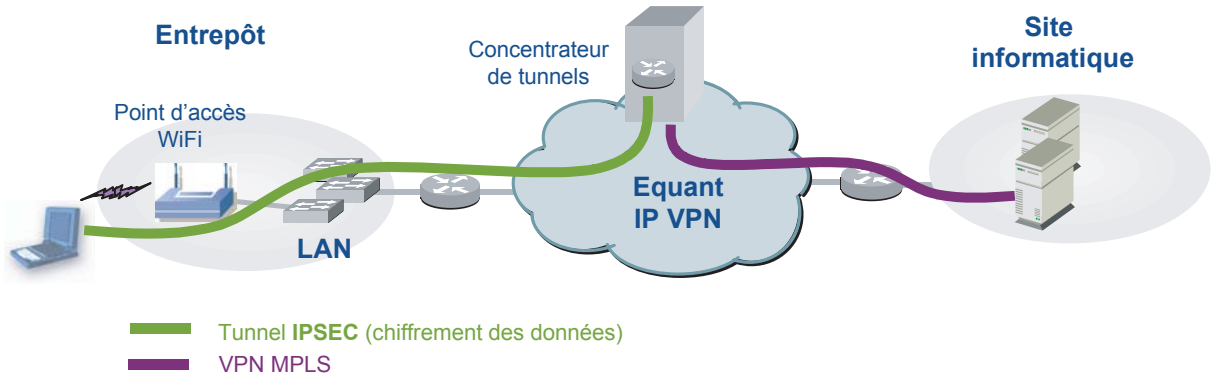
Le choix des solutions techniques s'effectue selon trois critères :

- le niveau de sécurité
- les coûts de déploiement et d'administration
- l'acceptabilité de la solution par les utilisateurs.

Dans ses différentes offres, France Télécom a la volonté de proposer un niveau d'authentification adapté aux exigences des entreprises et travaille en ce sens les items niveau de sécurité, tarifs et acceptabilité. Pour le nomadisme, l'heure est à la simplification des procédures d'authentification pour l'utilisateur, Single Sign On, et pour l'administrateur habilité à gérer les profils utilisateurs, droits et moyens d'accès. De nouveaux services client et l'utilisation de supports ergonomiques tels que le dongle USB au travers d'un client bureau mobile (ou kit de connexion) unique sont appelés à se développer.

Principes de tunnelling

Xavier Dupont est le responsable de production d'une entreprise spécialisée dans la plasturgie. En visite à l'entrepôt où se prépare activement la livraison du matin, il utilise le LAN WiFi dernièrement installé dans le bâtiment pour accéder à l'application de gestion des stocks. Il veut vérifier que les pièces moulées dont il a contrôlé la qualité ce matin ont bien été affectées à la catégorie "extra". Après la procédure d'authentification basée sur la clé secrète et le certificat personnel stockés dans son dongle USB, un tunnel chiffré est établi pour sécuriser l'accès à l'intranet de l'entreprise et à l'application hébergée sur le site principal de l'entreprise.



Principe d'intégration sécurisée d'un site Wireless LAN WiFi

Les mécanismes de tunnel sont donc utilisés pour assurer la sécurité d'une connexion entre deux systèmes. Il existe différents types de tunnels : IPSec, SSL et L2TP. Les VPN ainsi constitués se différencient des VPN de type cloisonnement de flux dans les réseaux IP tels que MPLS, les VPN MPLS apportant une souplesse de gestion et des garanties de débit et temps de transit.

Principes de chiffrement

Le chiffrement permet d'assurer l'authentification et la confidentialité des données. Le chiffrement est réalisé par des algorithmes cryptographiques.

Les algorithmes asymétriques, ou algorithmes à clé publique tels que **RSA©**, reposent sur un principe de bi-clés par entité : une clé privée, uniquement utilisable par son propriétaire, et une clé publique, connue de toutes les entités. La clé privée de l'entité est l'unique moyen de déchiffrer des données chiffrées à l'aide de sa clé publique. L'émetteur chiffre donc avec la clé publique du destinataire qui seul sera habilité à déchiffrer le message.

Les algorithmes asymétriques sont faciles à gérer au sein d'une communauté importante d'utilisateurs. La PKI (Public Key Infrastructure) est un système de gestion des clés publiques qui permet de gérer des listes importantes de clés publiques et des certificats associés qui ont été révoqués. Les quatre services principaux rendus par une PKI sont :

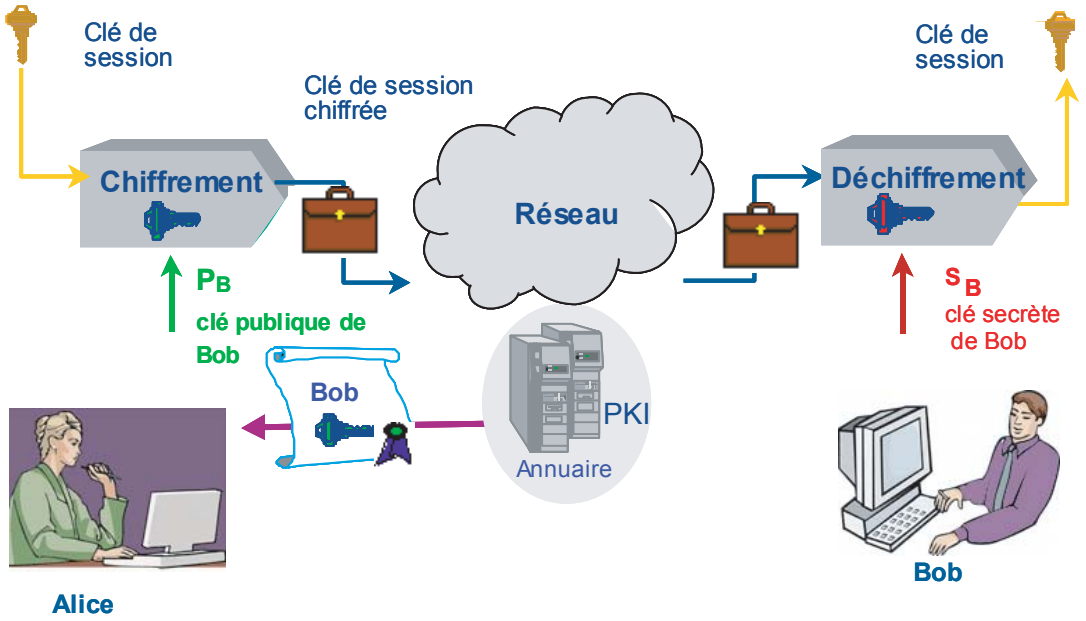
- la fabrication des bi-clés
- la certification de clé publique et la publication de certificats
- la révocation de certificats
- la gestion de la fonction de certification.

Les algorithmes symétriques, tels que **DES, 3DES** ou **AES**, constituent le deuxième type d'algorithmes de chiffrement. Ils reposent sur le partage d'une information confidentielle, clé secrète, entre les deux entités qui échangent. La même clé sert à chiffrer et déchiffrer les données.

Les algorithmes symétriques demandent moins de puissance de calcul que les algorithmes asymétriques et sont donc majoritairement utilisés pour chiffrer des documents entiers. Ils ne sont pas adaptés à une utilisation en réseau ouvert car ils supposent de mettre à disposition une clé par couple d'entités.

En conséquence, pour un compromis temps de traitement / niveau de sécurité acceptable, un scénario de chiffrement comprend le plus souvent deux étapes :

- une clé de session est générée aléatoirement par l'entité émettrice et transmise après chiffrement par un algorithme à clé publique à l'entité destinataire,
- la clé de session est alors déchiffrée avec la clé privée de l'entité destinataire puis utilisée comme clé de chiffrement d'un algorithme symétrique pour assurer la confidentialité des données à échanger.



Alice s'apprête à échanger des documents confidentiels avec Bob. Elle récupère la clé publique de Bob, certifiée, pour lui envoyer de façon sécurisée la clé de chiffrement/déchiffrement, clé de session, qui sera utilisée pour garantir la confidentialité des documents échangés dans un deuxième temps, pendant la session

Principes d'échange d'une clé de session par un chiffrement à clé publique

La robustesse des algorithmes de cryptologie dépend des moyens de calcul à mettre en œuvre pour "casser" l'algorithme. Ces moyens augmentent avec la longueur des clés. En pratique, on utilise donc des clés dont la longueur est juste suffisante pour que le décryptage ne puisse pas être réalisé dans un temps raisonnable avec les puissances de calcul existantes sur le marché. La progression très régulière de ces puissances de calcul engendre une augmentation régulière de la longueur des clés utilisées et alimente la recherche permanente de nouveaux algorithmes.

La technologie L2TP

L2TP est un mécanisme de tunnellisation de niveau 2 (liaison) par encapsulation des trames PPP. Ces tunnels peuvent eux-mêmes être sécurisés par cryptage IPSec.

La technologie IPsec

IPsec sécurise les échanges IP au niveau de la couche réseau du modèle OSI en faisant appel à deux protocoles :

- le protocole AH (Authentification Header) assure l'intégrité et l'authentification des paquets IP sans chiffrement des données. Il procède par l'ajout d'un champ dans le paquet IP, la vérification se fait à la réception du paquet.

- le protocole ESP (Encapsulating Security Payload) assure principalement la confidentialité des données en chiffrant les données et éventuellement l'en-tête du paquet IP à envoyer.

Ces mécanismes utilisés seuls ou de façon combinée, permettent entre autre la sécurisation d'une connexion sur un réseau jugé peu fiable, tel Internet, entre deux équipements terminaux, un équipement terminal et une passerelle de sécurité et entre deux passerelles de sécurité. Dans le cadre du nomadisme, IPsec est utilisé dans une configuration terminal-passerelle.

La technologie SSL

Développé à l'origine par Netscape pour des applications de commerce électronique, SSL est utilisé pour sécuriser les communications entre les navigateurs Web et les serveurs Web au niveau de la couche transport du modèle OSI (flux TCP). Il permet le chiffrement de données, l'authentification de serveurs, garantit l'intégrité des messages et de manière optionnelle réalise l'authentification entre les utilisateurs et leurs applications.

Comparatif IPsec / SSL

Régulièrement opposés, IPsec et SSL présentent des particularités propres dont la connaissance facilite la prise de décision sur le choix technique à réaliser.

Avec IPsec, tous les flux IP peuvent être protégés alors que SSL est principalement adapté à la protection des flux http.

Bien que normalisé, IPsec connaît des implémentations différentes dans les différents équipements concernés, terminaux et passerelles, ce qui se traduit par des problèmes d'interopérabilité. Par ailleurs, IPSec doit être rendu transparent -- par encapsulation niveau 2 ou 3 -- au protocole NAT, implémenté dans les routeurs ou proxy, car la translation d'adresse pertuberait le controle d'intégrité du paquet initial. Les solutions de contournement, NAT-transversal (encapsulation dans un flux UDP) ou pass-through (utilisation du champ SPI du paquet IPsec) ont un impact sur les performances des équipements et leur interopérabilité.

L'intégration d'applications n'utilisant pas http au chiffrement par SSL impose soit l'utilisation d'un frontal http/SSL devant le serveur d'application, soit le redéveloppement des applications pour insérer une couche SSL entre les couches applications et réseau.

IPsec est largement diffusé sur les postes de travail car les systèmes d'exploitation de Microsoft incluent systématiquement un client IPsec. SSL est largement distribué puisque tous les navigateurs Web embarquent un client SSL.

L'utilisation des deux technologies répond donc dans l'immédiat à des besoins différents : sécurisation de flux http dans le cas de SSL et sécurisation de l'ensemble des flux IP dans le cas d'IPsec.

Pour sécuriser les communications de bout en bout quelles que soient la fiabilité du réseau traversé et l'application utilisée, France Télécom a choisi d'intégrer des mécanismes de tunnelling et de chiffrement dans ses offres de nomadisme. Pour le service WiFi Extend, offre intranet Mobile WiFi, par exemple, France Télécom a fait dans l'immédiat le choix d'IPsec pour les offres de connexion nomade au VPN fournis par Equant, Transpac ou Oléane, et SSL pour les offres Wanadoo. France Télécom prend ainsi à sa charge les problématiques de mise en œuvre et d'interopérabilité en incluant la fourniture du logiciel client IPsec dans le kit de connexion utilisateur, la gestion opérationnelle de passerelles de sécurité dans le réseau et la distribution et la gestion des secrets nécessaires au fonctionnement de l'ensemble. De plus, l'intégration de WPA, nouveau standard de sécurité pour WiFi, est à l'étude. L'expertise développée dans l'ensemble du groupe est mise à contribution pour la délivrance de services nomades sécurisés de haute qualité.

LA PROTECTION DU TERMINAL ET DE SES DONNÉES

Le terminal utilisé par un nomade est particulièrement exposé :

- perte ou vol du terminal pouvant occasionner la prise de connaissance des données stockées sur celui-ci par une personne non autorisée

- connexion à un réseau non sécurisé permettant la modification des données stockées sur le terminal. Le téléchargement d'une page contenant un virus lors d'une consultation à distance pourra par exemple contaminer le réseau de l'entreprise lors du retour au bureau.

Au-delà de la sensibilisation forte des utilisateurs sur l'utilisation du terminal en situation de mobilité, il est nécessaire de protéger le terminal et les données stockées. La protection de l'accès au terminal et à ses données passe d'abord par la mise en place d'une procédure de déverrouillage : code PIN, mots de passe logiciels, hardware …La mise en place de solutions de type antivirus résidant et pare-feu personnel complète le dispositif en protégeant le poste de travail des attaques extérieures pendant la connexion. Enfin, le chiffrement des données stockées sur le terminal permet d'assurer leur confidentialité ; le chiffrement d'une partition disque peut ainsi être opéré à l'aide d'une clé stockée dans un dongle USB et d'une fonction intégrée au "logiciel client bureau mobile". Le directeur financier d'une banque pourra ainsi rendre inaccessibles les données confidentielles stockées sur son PC avant de prendre l'avion pour rencontrer le directeur de la filiale américaine.

L'ADMINISTRATION DE LA SÉCURITÉ

Toutefois l'entreprise vit, le nomade bouge. La politique de sécurité et les outils mis en œuvre doivent apporter la flexibilité nécessaire à cette dynamique. Les réponses à apporter concernent plus particulièrement :

- la gestion des profils d'utilisateurs : droits d'accès aux applications et moyens de connexion autorisés/possibles
- la gestion des outils du nomade
- la gestion de la sécurité du réseau de l'entreprise

L'effort d'administration à consentir est directement lié aux mécanismes de sécurité choisis et au nombre d'entités auxquels ils s'appliquent. Les méthodes et procédures d'attribution et de distribution des secrets doivent par exemple être sécurisés en s'appuyant notamment sur des mécanismes d'annuaires et de certification, qui peuvent rapidement devenir difficiles à exploiter quotidiennement et demander des ressources importantes. La dimension support de l'utilisateur ne doit également pas être négligée.

La conception des services de France Télécom s'appuie sur une approche globale qui permet de considérer la sécurité de bout en bout et de s'en préoccuper dans l'ensemble des composants qui constituent ses offres de services. C'est notamment le cas pour le déploiement et la gestion opérationnelle des services réseaux **1** *, organisés sous le signe de la rigueur méthodologique et certifiés ISO 9001 V2000. Equant IP VPN bénéficie ainsi de la certification critères communs décernée par la Direction centrale de la Sécurité des Systèmes d'Information et garantit à ce titre :*

- *l'étanchéité entre deux réseaux privés,*
- *l'étanchéité entre un réseau privé et l'Internet*
- *des procédures rigoureuses d'administration telles que l'accès identifié pour la configuration des équipements.*

Les services de nomadisme bénéficient de la même approche globale et intègrent la sécurité à tous les niveaux où elle est nécessaire. Privilégiant la simplicité, les offres visent à banaliser les technologies d'accès par un kit de connexion unique et des services web sur lesquels l'administrateur du client peut s'appuyer pour gérer de façon efficace l'ensemble des profils de ses utilisateurs, France Télécom assumant la responsabilité de l'ensemble des autres tâches de gestion opérationnelle (création des comptes, hébergement des plates-formes de sécurité, service client, ...). L'entreprise peut alors envisager sereinement le nomadisme et en tirer les meilleurs bénéfices.

1 - Se reporter au livre blanc sécurité des réseaux pour plus d'informations

LE QUOTIDIEN D'UN NOMADE

Jacques Durand est responsable de secteur pour une entreprise agro-alimentaire et couvre l'ensemble de la région PACA. Ayant principalement affaire à la grande distribution sur une gamme de produits très concurrencée, il se doit de réagir rapidement et efficacement à toute demande client ou initiative de l'un de ses concurrents. Son entreprise a donc fait appel aux services d'intégration de son opérateur privilégié pour le doter des moyens de communication les plus performants, même en situation de mobilité.

Chez cet industriel, on est bien sûr sensible aux problématiques de sécurité et l'entreprise met en œuvre les moyens et procédures qui minimisent les risques.

Lundi matin 9h, au bureau

Tous les lundis matin, Jacques Durand passe à son bureau de Lyon avant de commencer sa semaine sur le terrain.

« Le lundi matin, j'emporte mon PC portable au bureau. Mon réflexe est toujours de verrouiller mon câble antivol, précaution élémentaire. Pas de branchement particulier en dehors du chargeur énergie : je me connecte sans fil grâce au réseau interne WiFi de l'entreprise.»

Sans le savoir, Jacques Durand utilise le protocole WPA (WiFi Protected Access) qui garantit la confidentialité et l'intégrité des données échangées sur le LAN radio au sein de l'entreprise. Pour les postes sensibles, DG, DF, DSI …, il existe un réseau filaire de secours. Ainsi, même en cas de brouillage hertzien, l'information de crise passera toujours.

« Pour m'identifier, je dois enficher mon dongle, et je saisis mon code PIN à 4 chiffres dans la fenêtre d'identification. Une fois connecté, j'ai un accès sécurisé à l'ensemble de mes applications :

- *mon agenda, partagé avec l'assistante qui suit mon secteur*
- *mes workflows : suivi des commandes, gestion de l'activité commerciale, notes de frais et ressources humaines (congés, maladie…)*
- *l'intranet ouvert : informations générales, comité d'entreprise…*
- *mon intranet métier : le catalogue des produits et leurs photos, les actions de promotion programmées, avec les vidéos des têtes de gondoles, des spots de publicité, les bandes son des spots radio et autres outils marketing*

Ce que j'apprécie particulièrement, c'est de pouvoir m'identifier d'une seule façon, quel que soit l'application utilisée et mon mode de connexion, fixe, sans fil, ou mobile. On appelle ça le "SSO".»

10h15, réunion de revue des ventes

Le lundi, c'est aussi le jour où sont fixés les objectifs de la semaine. Tous les commerciaux du secteur sont réunis pour passer en revue les dossiers en cours et décider des actions de promotion qui seront relayées sur le terrain. En attendant les retardataires, Jacques Durand profite de l'intranet WiFi pour répondre au mail urgent d'un client, soumettre sa demande de remboursement de frais et préparer le partage du document promotions du mois qui servira de support pendant la réunion. Tout le monde étant présent, la réunion peut débuter.

« Au bout de 5 minutes d'inactivité, mon PC se met en mode veille. Pour le sortir de ce mode, je dois alors utiliser le mot de passe windows. Lorsque je sais que je ne vais pas utiliser mon PC, à la pause du déjeuner par exemple, je retire le dongle pour verrouiller l'accès à mes données. A mon retour, je réenfiche le dongle et je saisis tout simplement le code PIN à 4 chiffres. Lorsqu'on m'a remis en main propre mon dongle personnel, j'ai dû signer une convention. Je sais que toutes mes connexions sont désormais mémorisées et que je suis responsable de l'usage de ma clé d'accès. »

13h30, premier rendez-vous client

« Lorsque je pars en clientèle, j'emmène toujours mon PC. Pour ouvrir mon fichier clients, je suis obligé d'utiliser mon dongle et mon code PIN car ces données sont particulièrement sensibles. Ainsi, même en cas de vol de mon PC, ces informations restent inaccessibles. En revanche, je n'ai pas intérêt à perdre mon dongle ! »

Les fichiers sensibles sont en effet chiffrés sur le disque du PC. Bien sûr, un processus de recouvrement de clef est défini en cas de perte du dongle.

« Cette fois encore, mon client a décidé d'être ferme sur les prix, je dois revenir avec une nouvelle proposition demain à 9H précises. »

20h00, gare de la Part-Dieu

En rentrant de son rendez-vous client, Jacques Durand a du laisser son véhicule au garage pour une légère révision. En attendant le TER qui doit le ramener à son domicile, il prépare une nouvelle proposition commerciale. Pour cela, il a besoin d'accéder à l'application qui gère l'ensemble des plans de remises. Il utilise donc le hot spot WiFi public, pour accéder à son intranet métier en toute sécurité grâce à l'identification via dongle, l'activation d'IPSec, du Pare-feu personnel et de l'antivirus résidant.

22h00, à domicile

Pour aborder sereinement son rendez-vous matinal du lendemain, Jacques Durand souhaite vérifier que sa demande de dérogation tarifaire est acceptée. WPA est activé dans le LAN privé de Jacques Durand. Par mesure de sécurité, la direction informatique de son entreprise a imposé l'utilisation de tunnels chiffrés IPSec jusqu'au pare-feu managé qui protège l'intranet de l'entreprise. Le pare-feu personnel télécharge la politique de sécurité et paramètre le client IPSec pour interdire toute connexion simultanée avec l'Internet. Tout accès Internet se fera donc au travers du point d'accès de l'entreprise via les filtres HTTP et les antivirus managés par l'opérateur de services global privilégié de l'entreprise.

« Chez moi, j'utilise l'accès Internet haut débit sans fil pour me connecter à l'informatique de l'entreprise. J'utilise une fois de plus mon dongle et mon code PIN. Il m'arrive de recevoir des messages d'alerte sur les virus de la part de la direction informatique.»

L'administrateur, tout comme les autres salariés de l'entreprise, dispose également d'un accès sécurisé, étendu aux fonctions d'administration. Il peut donc, à distance, gérer les urgences liées à la sécurité.

Glossaire

Certificat		Document numérique dont l'objectif est de lier de manière sûre l'identité du possesseur à sa clé publique et d'éviter les usurpations d'identité, grâce à la signature par l'autorité de certification et à la gestion de listes noires
Cracking		Activité visant à percer les secrets utilisés en sécurité, mots de passe, clés, …
DES	Digital Encryption Standard	3DES, AES (Advanced Encryption Standard) : algorithmes cryptographiques symétriques reposant sur le partage d'une clé unique
Dongle		Périphérique disposant de fonctions cryptologiques se connectant sur un port USB
GPRS	General Packet Radio Services	Technologie de transport de données utilisant les infrastructures des réseaux GSM
ICP ou PKI	Infrastructure à Clés Publiques ou Public Key Infrastructure	Infrastructure technique et procédures d'administration / exploitation associées permettant de délivrer et stocker des certificats numériques de manière sécurisée. Ces certificats permettent d'accéder aux clés de chiffrement publiques utilisées dans la plupart des équipements ou applications utilisant de la cryptographie pour protéger des données sensibles
IP	Internet Protocol	Protocole de transmission en vigueur sur l'Internet, assurant le transport de données au sein d'éléments baptisés datagrammes
IPsec	Internet Protocol security	Suite de protocoles délivrant tous les éléments nécessaires pour la sécurisation d'échanges de données sur le protocole IP au travers d'un réseau partagé
Jeton	ou token	Mot de passe non-rejouable émis par un dispositif électronique
L2TP		Mécanisme de tunnel sécurisé pour assurer la terminaison d'une liaison PPP en un point désigné du réseau téléphonique
LDAP	Lightweight Diredtory Access Protocol	Protocole permettant l'accès à des bases d'annuaires ou d'informations sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP
MPLS	Multi Protocol Label Switching	Technologie standardisée par l'IETF permettant de construire sur un réseau un chemin balisé entre un point de départ et un point de destination. La progression du paquet dans le chemin établi s'effectue par la commutation de labels (étiquettes)
NAT	Network Translation Address	Technique utilisée pour masquer les adresses IP privées d'un réseau en les traduisant par une adresse publique temporaire
PKI		PKI : voir ICP

Radius	Remote Authentication Dial-In User Service	Protocole permettant de réaliser l'authentification d'un utilisateur en comparant l'authentification saisie à une base d'utilisateurs/mots de passe. Le protocole Radius permet également de comptabiliser les sessions et peut être associé avec une base LDAP ou un système d'authentification forte (mots de passe à usage unique)
RSA	Rivest, Shamir, Adleman	Algorithme de cryptographie asymétrique reposant sur le principe d'une double clé, le cryptage étant porté par l'une et le décryptage par l'autre et réciproquement
Signature électronique		Signature électronique : données chiffrées ajoutées à une information pour en authentifier son auteur et garantir son intégrité
SSL	Secure Socket Layer	Protocole permettant d'assurer des services d'authentification et de tunnel chiffré au niveau du transport HTTP
SSO	Single Sign On	Fonction permettant de disposer d'une identification unique, quel que soit le service applicatif
USB	Universal Serial Bus	Interface de connexion de périphériques externes en mode série
XDSL	Digital Subscriber Line	Solutions techniques permettant l'utilisation de boucles locales téléphoniques en cuivre pour des transmissions de données haut débit. Différentes technologies sont disponibles comme l'ADSL fournissant un débit asymétrique et le SDSL fournissant un débit symétrique
VPN	Virtual Private Network	Fonction de réseau privé construite sur un réseau partagé
WiFi	Wireless Fidelity	Technologie radio basée sur le standard 802.11b permettant l'échange de données à haut débit dans un rayon de quelques centaines de mètres autour de l'antenne
WPA	WiFi Protected Access	Standard développé par "WiFi Alliance" et visant à l'amélioration de la sécurité des réseaux sans fil par l'introduction de mécanismes d'authentification, de confidentialité, d'intégrité et de gestion de clés robustes

Livre Blanc - Nomadisme

Solutions Grandes Entreprises

www.francetelecom.com/grandesentreprises

SA au capital de 4 098 463 604 □ - 380 129 866 RCS PARIS - FT/SGE - Janvier 2004