

# Livre blanc

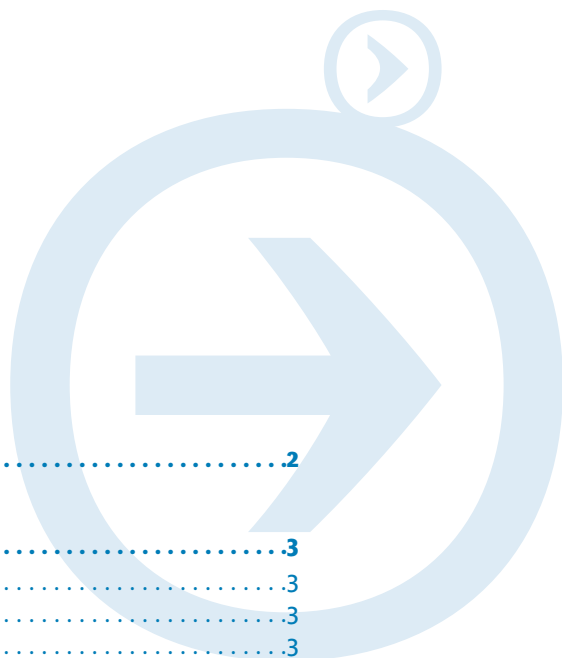
## Sécurité des réseaux

### Des enjeux aux solutions



Livre blanc - **Sécurité des réseaux - Des enjeux aux solutions**

# Sommaire



<b>Introduction</b> .....	<b>.2</b>
<b>La sécurité du système d'information : un enjeu d'entreprise</b> .....	<b>.3</b>
L'ouverture du système d'information, nécessaire mais pas sans danger .....	.3
Une ouverture incontournable .....	.3
Des risques accrus .....	.3
Les domaines de la sécurité et les solutions associées .....	.4
L'importance de la gestion de la sécurité .....	.7
Une démarche globale .....	.9
L'opérateur de réseaux au cœur de la sécurité de l'entreprise .....	.10
<b>Transpac : une organisation et des hommes au service de la sécurité</b> .....	<b>.12</b>
Des acteurs impliqués à tous les niveaux .....	.12
Des locaux et des équipements sous contrôle .....	.13
La sécurité des locaux .....	.13
Des matériels, logiciels et données protégés .....	.13
La protection contre les incidents .....	.14
Une démarche d'amélioration permanente .....	.14
La certification, une garantie pour nos clients .....	.15
<b>La sécurité des réseaux VPN IP</b> .....	<b>.16</b>
Principes de base du VPN IP et de la technologie MPLS .....	.16
Un cœur de réseau IP dédié aux entreprises .....	.17
Un réseau invisible et inaccessible depuis l'Internet public .....	.17
Des systèmes d'infrastructure hautement sécurisés .....	.18
Un réseau disponible et tolérant face aux perturbations externes .....	.18
Equant IP VPN, un service étanche et cloisonné .....	.19
Le cloisonnement des VPNs .....	.19
Le cloisonnement des flux VPN vis-à-vis d'Internet .....	.19
<b>Les services de sécurité managés et les prestations sur mesure</b> .....	<b>.20</b>
Des solutions managées pour renforcer la sécurité .....	.20
Contrôler l'accès au réseau de l'entreprise .....	.20
Sécuriser l'ouverture vers l'extérieur .....	.21
Les solutions de chiffrement .....	.22
Une offre de sécurité modulaire .....	.23
Des prestations de sécurité avancées, sur mesure .....	.23
<b>Conclusion</b> .....	<b>.24</b>
<b>Glossaire</b> .....	<b>.25</b>



## Introduction

L'ouverture du système d'information des entreprises est devenue incontournable : de nouvelles portes s'ouvrent aux frontières du réseau interne pour permettre les connexions mobiles, dont le nombre ne cesse de croître, notamment du fait de l'arrivée des technologies sans fil. L'informatisation quasi généralisée des échanges de l'entreprise avec les acteurs de sa chaîne d'activité passe aussi par des accès contrôlés depuis l'extérieur de l'entreprise. L'ouverture du SI se traduit également par le nombre de connexions à Internet qui se multiplient. **Dans ce contexte, assurer la sécurité du patrimoine que constituent les données de l'entreprise est vital.**

Deux phénomènes nouveaux rendent encore plus critique la sécurisation des données. **Sans parler de la croissance exponentielle des attaques (+ 100 % par an), leur nature même évolue et de nouvelles formes de virus peuvent désormais provoquer des dénis de service\* à l'échelle planétaire.** Par exemple, le nombre de machines infectées dans le monde par le ver\* SQL "slammer" doublait toutes les 8,5 secondes pendant sa période de propagation.

**Le second phénomène concerne le renforcement de la législation, qui entend répondre à l'augmentation des risques.** Par exemple, le projet de "loi pour la confiance dans l'économie numérique" (LEN) vise à légiférer sur divers volets tels que la communication publique en ligne, le e-commerce, la cryptologie ou encore les communications par satellite. Certains secteurs font l'objet de contrôles spécifiques. Par exemple, le récent accord de Basel II stipule que les banques doivent être soumises à un contrôle sur les fonds propres dont elles disposent pour faire face aux risques. Ainsi la qualité de leur gestion des risques, notamment informatiques, influe directement sur les exigences de fonds propres.

Toutes les entreprises sont donc confrontées à la **nécessité d'assurer un niveau de sécurité adapté aux risques encourus, et de maintenir ce niveau dans le temps.** Dans cette démarche globale, il est logique de commencer par la sécurisation du réseau, sur lequel circulent les données vitales pour l'entreprise et sont situées les "portes" d'accès vers l'extérieur.

**Transpac, intégrateur et opérateur de services de réseaux d'entreprise, met au service de ses clients son expertise technique pour offrir des solutions de réseaux privés hautement sécurisés.** Ainsi, le service Equant IP VPN, que Transpac distribue et opère en France, prend en compte, à tous les niveaux, les exigences de sécurité qu'une entreprise est en droit d'attendre. Pour renforcer la sécurité intrinsèque de ses solutions réseaux, **Transpac propose un ensemble de services de sécurité managés**, modulaires, qui permettent à l'entreprise de se décharger, 24h/24 et 7j/7, de l'exploitation des systèmes.

Ce document présente tout d'abord les enjeux de la sécurité informatique, puis montre comment Transpac met elle-même en œuvre une politique de sécurité globale pour assurer la protection des services qu'elle rend à ses clients. La troisième partie, plus technique, explique précisément comment la sécurité de l'offre Equant IP VPN est assurée à tous les niveaux. Enfin, vous y trouverez une présentation des services de sécurité managés et des prestations sur mesure.

Au travers de ce document, nous espérons que vous enrichirez votre "culture sécurité" pour une maîtrise toujours plus grande des enjeux de sécurité de votre entreprise.

\* voir glossaire page 25



# La sécurité du système d'information : un enjeu d'entreprise

## L'ouverture du système d'information, nécessaire mais pas sans danger

### ① Une ouverture incontournable

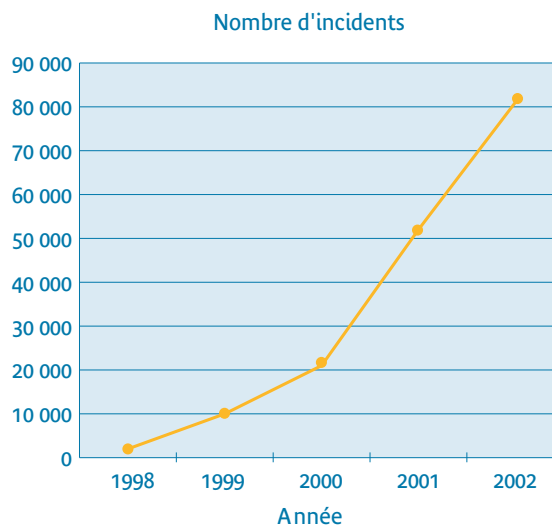
L'entreprise étendue dialogue avec ses clients et ses fournisseurs, mais aussi, de manière plus générale, avec tous les membres de sa chaîne de métier. Elle doit mettre à la disposition de ses salariés itinérants un environnement de travail qui se rapproche le plus possible de celui de leur bureau - c'est le concept de bureau virtuel. Elle utilise Internet à la fois en consultation, et pour mettre en œuvre un ou plusieurs sites web.

Par ailleurs, les restructurations, fusions ou acquisitions, conduisent l'entreprise à changer les organisations, avec un impact sur les échanges internes : il faut faire communiquer différents sites ou nouvelles filiales, définir les échanges inter-branches, les applications transverses auxquelles toute l'entreprise doit accéder, tout cela bien sûr en minimisant les risques en matière de sécurité. Avant de vérifier que tous les maillons sont à "l'état de l'art", il vaut mieux instaurer des barrières solides entre les différentes entités.

### ② Des risques accrus

Parallèlement à cette ouverture, la progression des incidents (intrusions, virus, attaques) est en croissance exponentielle de plus de 100 % par an. Il est donc de plus en plus difficile de conserver un niveau de sécurité satisfaisant sur un système d'information hétérogène et géographiquement dispersé.

Le tableau suivant (source CERT®/CC\*) montre le doublement du nombre d'incidents enregistrés dans le monde chaque année :



\* voir glossaire page 25



**Les attaques sur Internet s'automatisent et leurs conséquences sont de plus en plus graves** : les outils de scan\* plus rapides et efficaces incorporent des programmes exploitant directement la vulnérabilité ; les attaques distribuées démultiplient la puissance de l'attaque d'origine... Les attaques récentes, comme celle du ver\* SQL slammer en janvier 2003, nous ont montré que les perturbations induites affectent des domaines beaucoup plus larges (applications, systèmes et réseaux), se répandent plus rapidement et que les nuisances occasionnées sont plus fortes. Selon la société Network Associates, le virus a mis hors service entre 150 000 et 200 000 serveurs dans le monde. L'activité de certaines sociétés a été fortement perturbée. Par exemple, les 13 000 distributeurs de la Bank of America ont été indisponibles pendant plusieurs heures.

**Une autre tendance forte est l'augmentation de la perméabilité des pare-feux**. Ce phénomène n'est pas dû à un problème de permissivité des filtres au niveau des pare-feux mais plutôt à l'évolution des protocoles et objets utilisés sur Internet. On peut citer par exemple les protocoles IPP (Internet Printing Protocol) ou WebDAV (Web-based Distributed Authoring and Versioning) qui,

pour assurer une communication sans couture sur l'intranet, peuvent ouvrir une porte d'accès aux trafics malveillants.

Tous ces éléments peuvent expliquer que, selon de nombreux sondages, la **sécurité** soit aujourd'hui le **premier facteur de stress des DSI**.

Afin de comprendre les problématiques auxquelles sont confrontés les responsables sécurité, la section suivante présente les cinq domaines auxquels une politique de sécurité doit répondre et les solutions techniques associées.

## Les domaines de la sécurité et les solutions associées

La sécurité informatique recouvre la **confidentialité** des échanges, l'**authentification** des utilisateurs, l'**intégrité** des données et des échanges, la **disponibilité** des données et des systèmes, la **non-répudiation** des transactions. Dans la suite de cette section, on désigne par "réseau interne de l'entreprise" les réseaux locaux et le réseau d'interconnexion des sites (intranet), en général géré par un opérateur.

### 🔍 La confidentialité des échanges

La plupart des entreprises possèdent des données confidentielles et sensibles : fichiers de clientèle, données financières et comptables, informations sur le personnel, ensemble de documents liés au savoir-faire ou aux processus internes. Dès lors, le système d'information doit être protégé des intrusions et les échanges de données avec l'extérieur doivent être mis à l'abri des convoitises.

Le premier niveau de protection consiste à installer des pare-feux (firewalls) aux frontières entre le réseau interne et l'extérieur (internet, extranet, réseaux de partenaires...). Par des filtres contrôlant les données transitant par le pare-feu, on peut définir précisément la liste des personnes autorisées à entrer dans le réseau ou à en sortir, et les protocoles qui leur sont autorisés (ex : HTTP pour le web, SMTP pour la messagerie...).

En ce qui concerne le chiffrement des données, les réseaux WAN\* offrent un niveau de sécurité suffisant pour la plupart des entreprises. La protection physique et logique de l'infrastructure rendent pratiquement impossible toute capture du trafic si bien qu'il n'est pas nécessaire de chiffrer les données courantes.

De plus, le chiffrement des données est relativement complexe à mettre en place : il nécessite des boîtiers ou

\* voir glossaire page 25



des logiciels de chiffrement à toutes les extrémités du réseau, des échanges de clés... Aussi est-il adapté à certains cas particuliers :

- protection de données ultra-confidentielles (par exemple la Défense)
- protection des données transitant sur des réseaux non protégés : Internet, WIFI, GPRS...

### 🔍 L'authentification des utilisateurs

Pour protéger des informations sensibles, il convient de savoir qui a le droit d'accéder aux données et quels sont les privilèges associés à ces droits. En l'absence d'une gestion correcte des droits d'accès à l'information, l'entreprise prend le risque de voir des informations confidentielles divulguées, avec toutes les conséquences imaginables.

La détermination des droits et privilèges passe par un mécanisme d'identification et d'authentification qui va permettre de s'assurer que l'utilisateur est bien celui qu'il prétend être, et qu'il a bien le droit d'accéder au système. Ce mécanisme peut être simple (compte et mot de passe) ou fort (dit à 2 facteurs : compte, mot de passe et jeton\*).

Un nouvel enjeu lié à l'authentification est celui de son unicité. Les systèmes informatiques se multipliant, l'utilisateur possède autant d'identifiants que d'applications auxquelles il accède. Une solution d'authentification unique (SSO : Single Sign-On) permet de résoudre le problème. En ce domaine, il n'existe pas de solution réellement universelle, du fait de la grande diversité des applications et protocoles concernés. France Télécom R&D étudie, entre autres domaines, les solutions de SSO qui permettront de simplifier considérablement l'authentification des utilisateurs.

### 🔍 L'intégrité des données et des échanges

Il est primordial de s'assurer que des données ne sont lisibles que par leurs destinataires. Mais il est tout aussi important de s'assurer que la totalité des données à échanger a réellement été échangée, que les données reçues sont bien identiques aux données émises ou bien qu'elles n'ont pas été modifiées lors d'un stockage. On parle alors d'échange intègre ou d'intégrité des données.

Ce contrôle peut être réalisé pendant l'échange, par la mise en oeuvre de mécanismes prévus dans certains protocoles de transport, mais il convient de pouvoir aussi assurer cette intégrité sur des données déjà reçues, stockées et réutilisées.

Des mécanismes de signature des données ou de condensat\* (hash-coding) seront alors mis en oeuvre : ils permettent de mémoriser un état donné et de vérifier que l'état actuel est toujours identique à l'état signé. Ces signatures reposent sur des algorithmes cryptographiques plus ou moins complexes. Elles peuvent aussi servir à identifier de manière fiable le propriétaire des données signées. Certains protocoles, comme IPSEC ou PGP, assurent à la fois confidentialité, authentification et intégrité.

### 🔍 La disponibilité des données et des systèmes

Quand les télécommunications et les systèmes informatiques deviennent des outils de base d'une entreprise, leur utilisation permanente les transforme en ressources critiques. Leur disponibilité doit donc être maximale.

Cette facette de la sécurité informatique est souvent négligée car elle nécessite des investissements conséquents, dont le bénéfice n'est pas immédiatement perceptible. La plupart des entreprises ont de la peine à chiffrer le coût d'une indisponibilité de leur système d'information, même si elles estiment qu'il leur est indispensable.

La disponibilité repose la plupart du temps sur la création d'une redondance entre équipements, sur la mise en oeuvre de fonctions de reprise dans les logiciels et sur des procédures de sauvegarde / restitution des données fiables et régulièrement testées.

Les pannes ne sont pas les seules causes d'indisponibilité. Le déni de service\* est un type d'attaque Internet qui menace la disponibilité d'un système, en visant à dégrader ses performances. L'attaque consiste, par exemple, à envoyer un flot de requêtes massif que le système ne peut traiter, ou à exploiter une vulnérabilité mettant hors-service l'équipement. La protection contre le déni de service passe par différents moyens : anti-virus de messagerie pour protéger les PC de l'entreprise des virus ayant pour but de rendre indisponible le système attaqué, filtres réactifs installés par l'opérateur sur son cœur de réseau pour bloquer temporairement du trafic malveillant, pare-feu contrant certaines vulnérabilités.

\* voir glossaire page 25



## 🔍 La non-répudiation des transactions

Lorsque l'on met en place un service de commerce électronique ou une application transactionnelle "webisée" sensible, il est essentiel de fournir aux deux partenaires qui communiquent le moyen de prouver que l'autre a bien effectué une transaction, de manière à pouvoir réagir si l'interlocuteur prétend ne pas avoir effectué la dite transaction. C'est ce qu'on appelle la non-répudiation.

Elle repose sur des mécanismes d'authentification et de signature\*, ainsi que sur des mécanismes d'horodatage\*.

Elle introduit aussi la notion de tiers de confiance, qui va, comme un notaire dans la vie réelle, assurer l'enregistrement de la transaction, en l'horodatant et en gardant ensuite les traces qui serviront à prouver que la transaction a bien eu lieu, et que le contenu annoncé par l'une des parties est bien valide.

Le tableau suivant synthétise les cinq problématiques et les solutions pour y faire face.

	<b>Problématique</b>	<b>Mécanisme</b>	<b>Solution</b>
<b>Confidentialité</b>	Protéger des données sensibles	Chiffrement, mécanismes anti-intrusion	Boîtier ou logiciel de chiffrement, pare-feu
<b>Authentification</b>	Gérer correctement les accès aux données sensibles	Mécanismes d'authentification simple ou forte, Single Sign-On	Login/mot de passe statiques (authentification simple). Jeton ou signature électronique (authentification forte)
<b>Intégrité</b>	S'assurer de la non-modification des données	Signature, hash-coding	Boîtier ou logiciel de chiffrement (IPSEC, PGP). Solutions logicielles avec éventuellement cartes à puce
<b>Disponibilité</b>	Faire en sorte que les données soient accessibles	Routage dynamique, écrêtage de flux (rate limiting)	Redondance des équipements, plan de reprise, anti-virus, filtres
<b>Non-répudiation</b>	S'assurer de la réalité d'une transaction	Mécanismes d'authentification, de signature, de notariation	Solutions logicielles, avec éventuellement cartes à puce

\* voir glossaire page 25



## L'importance de la gestion de la sécurité

La section précédente a montré que pour couvrir les diverses problématiques, différentes solutions pouvaient être utilisées, certaines regroupant plusieurs fonctions imbriquées. La conception d'une architecture prenant en compte tous ces aspects et plaçant les solutions de protection au bon endroit, avec le bon paramétrage, est complexe. L'exploitation en continu des solutions mises en place, leur maintenance, le maintien d'une configuration *ad hoc* tenant compte des évolutions du réseau, ou de l'apparition de nouveaux virus par exemple, sont encore plus complexes.

De nombreuses grandes entreprises l'ont d'ailleurs mesuré en commençant par mettre en œuvre des solutions et en réalisant l'ampleur de la tâche d'administration et d'évolutivité de l'ensemble. Ces exigences sont de plus en plus pressantes aujourd'hui et beaucoup d'entreprises se trouvent démunies.

**La sécurité doit avant tout s'inscrire dans la durée et faire preuve de dynamisme et de proactivité.** Dès lors, il convient de s'intéresser de très près à la gestion des ressources et moyens utilisés.



- 64,2 % des entreprises citent les erreurs d'utilisation parmi les causes de leurs problèmes de sécurité,
- 38,7 % citent les erreurs de conception.

Ces chiffres sont à comparer avec les virus (78,8 %) et le cybercrime (8 %).

C'est donc bien la gestion des ressources et des moyens utilisés qui doit être mise au cœur de toute démarche sécurité.

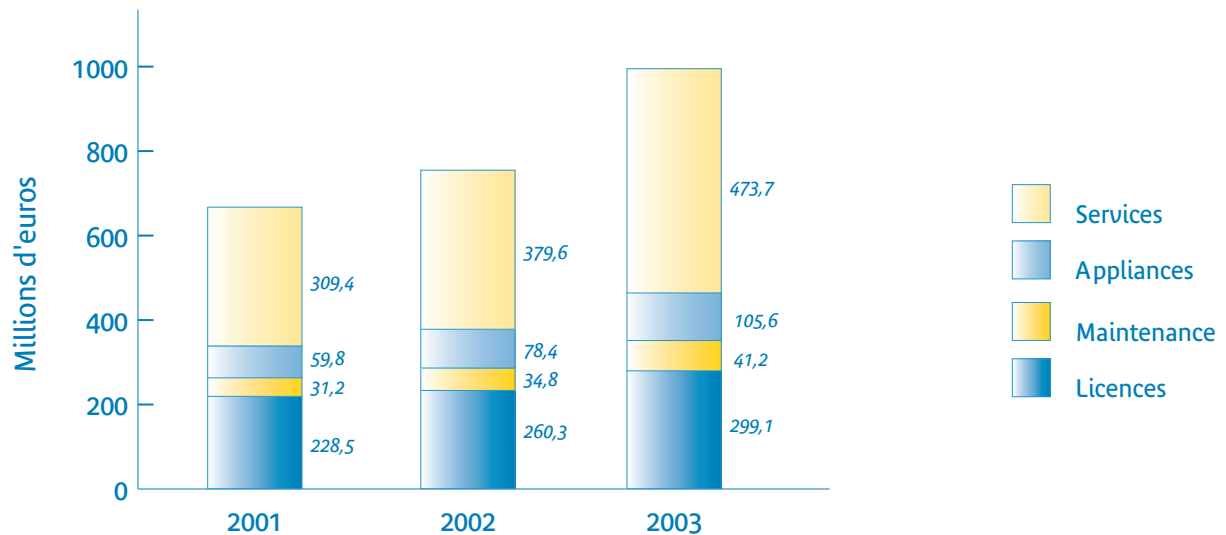
Source, IDC 2001 : le marché français de la sécurité des systèmes d'information – bilan et perspectives 2001-2005

Il n'est donc pas étonnant que les entreprises, après avoir récemment pris conscience de la nécessité de gérer la sécurité dans la durée, aient généré une forte croissance du marché des services de sécurité. Le phénomène le plus intéressant de cette évolution du marché est la croissance plus rapide des services et solutions par rapport à celle

des matériels et logiciels. L'étude IDC d'avril 2003, "Le marché français de la sécurité des systèmes d'information – bilan et perspectives 2001-2005", montre une croissance des services de sécurité de plus de 50 % entre 2001 et 2003, avec un chiffre d'affaires passant de 309,4 millions d'euros en 2001 à 473,7 millions d'euros en 2003.



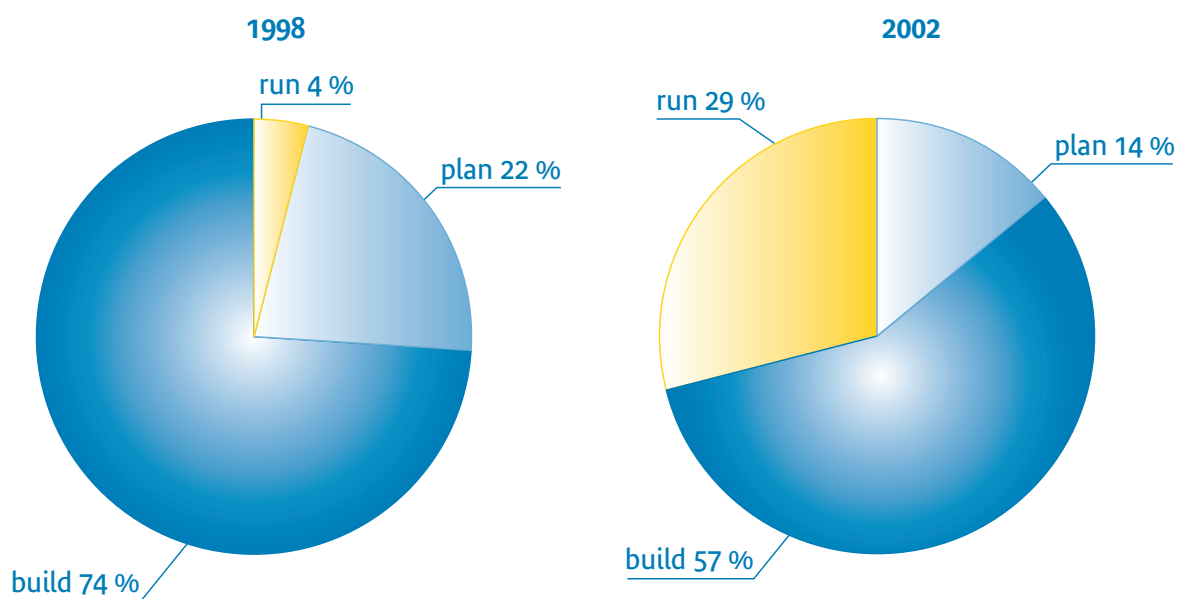
## Evolution du marché français de la sécurité entre 2001 et 2003



Source IDC, 2003 : le marché français de la sécurité des systèmes d'information – bilan et perspectives 2003-2007

La deuxième tendance qui ressort de ces études est l'augmentation sensible de la part des dépenses liées à **l'exploitation des équipements, qui est passée de 4 % en 1998 à 29 % en 2002** : le management continu de la sécurité est désormais perçu comme une nécessité.

## Evolution de la répartition des dépenses selon les phases du projet sécurité



D'après une étude IDC 2001



## Une démarche globale

La prise en compte de la sécurité dans une entreprise doit faire l'objet d'une démarche rigoureuse, progressive et surtout continue afin de vérifier en permanence l'état de l'art des protections mises en place, en regard des évolutions de l'environnement et de l'apparition de nouvelles vulnérabilités. Les étapes consistent à :

- **établir un état de l'environnement à sécuriser**, en identifiant tous les biens sensibles, matériels et immatériels, et **analyser les risques associés**,
- **concevoir la politique de sécurité** qui répondra à ces risques en englobant tous les aspects de la protection de l'information : protection des locaux, des réseaux et systèmes, sensibilisation du personnel...
- **définir une architecture complète** combinant les différents éléments techniques de protection de manière cohérente,
- **paramétrer et mettre en œuvre** ces éléments techniques.

Ensuite, en phase d'exploitation, les entreprises sont confrontées à deux enjeux majeurs :

- **l'évolution constante des attaques**. Chaque jour, de nouvelles failles sont exploitées par les hackers. Une veille technologique pointue et constante doit être assurée pour mesurer le risque associé à l'apparition d'une nouvelle vulnérabilité, étudier l'impact d'une mise à jour corrective des systèmes. Cette activité nécessite un haut niveau d'expertise du personnel et une surveillance constante.
- **l'exploitation et la supervision des équipements** : 24h/24 et 7j/7, il faut analyser les journaux d'alertes, prendre des mesures sur détection d'une attaque, suivre l'évolution des logiciels et des matériels.

**Ce sont ces deux volets, particulièrement coûteux en matière de ressources humaines, que Transpac prend en charge pour le compte de ses clients. Ainsi, l'entreprise peut déléguer les tâches répétitives, tout en gardant la maîtrise de sa politique de sécurité.**



### Les bonnes raisons de déléguer la gestion de sa sécurité réseau

Opter pour une solution d'externalisation de la gestion des composants de sa sécurité réseau présente des bénéfices importants, en permettant à l'entreprise de :

- **se recentrer sur son cœur de métier.**

Grâce aux services managés, les responsables réseaux et sécurité ont une plus grande latitude pour assurer leur mission centrale, à savoir l'accompagnement des utilisateurs du SI. En déléguant les activités quotidiennes, ils se réapproprient leur rôle de consultant et d'expert. Ils peuvent avoir le recul nécessaire pour appréhender l'environnement global du SI et apporter les meilleures réponses aux besoins des utilisateurs.

Ils peuvent aussi adopter une démarche plus prospective, en préparant l'arrivée des nouvelles technologies et des solutions de mobilité, de convergence voix-données qui apporteront un service plus performant aux utilisateurs.





**- externaliser les risques liés à l'investissement.**

Le risque majeur d'un investissement matériel ou logiciel réside dans le fait que les choix initiaux sont relativement figés dans le temps. Or la sécurité est un domaine encore jeune, dans lequel les nouveautés technologiques sont fréquentes. En achetant un service managé, basé sur des équipements loués, l'entreprise externalise les risques d'investissements chez l'opérateur. Celui-ci atteint une masse critique qui lui permet de modifier plus aisément ses choix, allant même jusqu'à changer de constructeur ou d'éditeur si nécessaire. Il fait évoluer les solutions choisies pour offrir les meilleures technologies à ses clients.

Ainsi, l'entreprise a accès à la dernière fonctionnalité, qui n'existait pas au moment de son investissement. Elle choisit la taille de sa configuration, comme par exemple le nombre d'utilisateurs protégés par un pare-feu, et peut la faire évoluer à tout moment, moyennant une évolution de l'abonnement. Elle n'achète donc que la puissance utile au moment voulu.

**- optimiser la gestion des compétences.**

Deux fonctions différentes sont requises pour la gestion de la sécurité.

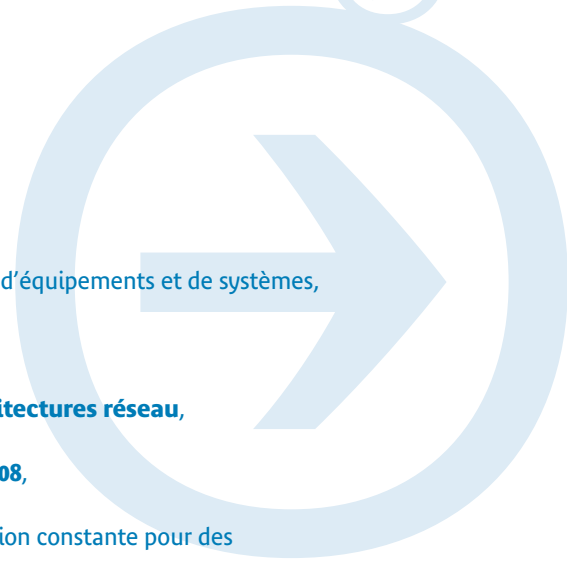
D'une part, les experts sont responsables de la définition de la politique, des choix techniques et de la veille technologique. D'autre part, des techniciens réalisent l'installation et l'exploitation au quotidien, 24h/24 et 7j/7.

Les premiers sont des ressources rares. Sans déléguer la définition et le suivi de la politique, qui doit rester sous la responsabilité de l'entreprise, l'expertise technique pointue peut être externalisée. Il en résulte des économies financières et une moins grande dépendance à l'égard de compétences volatiles. De même, la fonction technique peut être déléguée dans la mesure où elle n'a pas d'impact stratégique sur le SI et où l'exploitation continue, jour et nuit, représente un coût important.

## L'opérateur de réseaux au cœur de la sécurité de l'entreprise

Dans un contexte économique mouvant et dans un domaine technique aussi jeune, s'appuyer sur un opérateur pérenne, sans s'engager sur des solutions susceptibles de disparaître du jour au lendemain, est pour les

entreprises un gage important de stabilité. Pour assurer au mieux ce rôle de Managed security service provider (MSSP = fournisseur de services de sécurité managés), France Télécom met au service de ses clients :

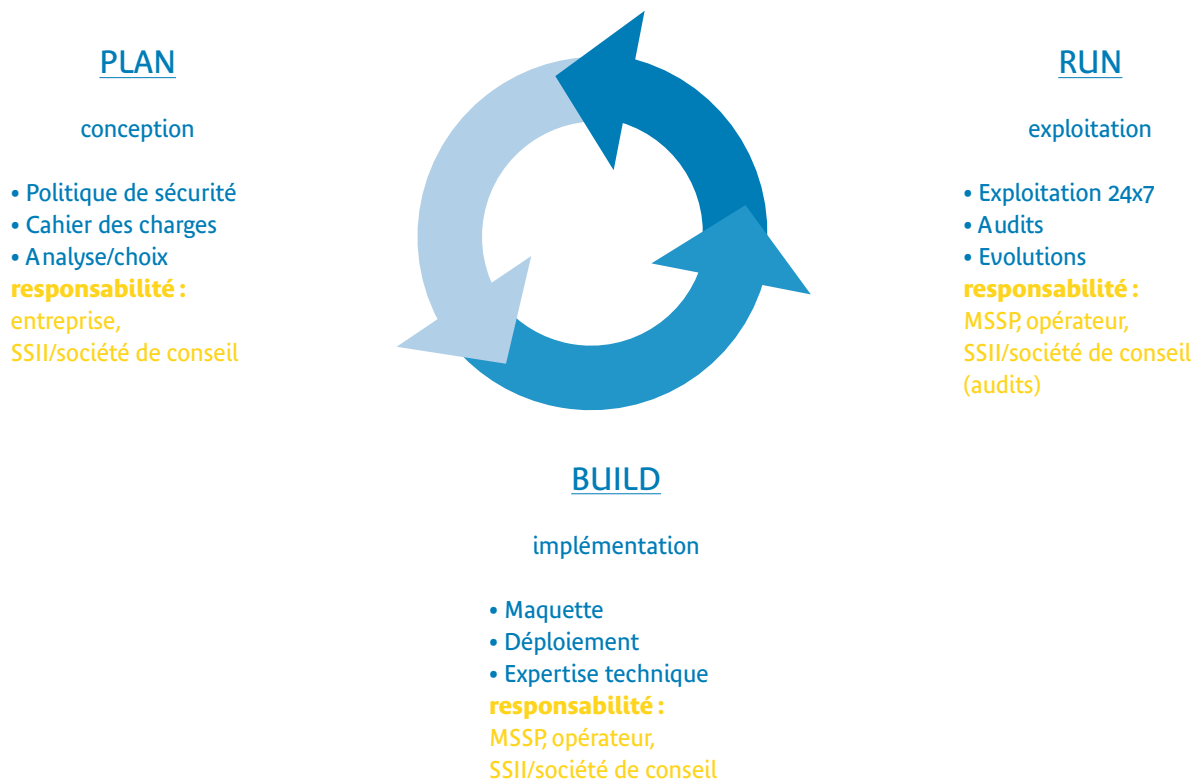


- **son organisation et ses process industriels**, centrés autour de l'exploitation d'équipements et de systèmes,
- **sa maîtrise de la chaîne des échanges de bout en bout**,
- **l'assurance d'une intégration cohérente de la sécurité au cœur des architectures réseau**,
- **sa méthodologie approuvée et certifiée ISO 9001 version 2000 et ISO 15408**,
- **son poids par rapport aux constructeurs**, qui lui permet d'exercer une pression constante pour des **équipements de sécurité en permanence à l'état de l'art**,
- **sa présence internationale** grâce à la couverture d'Equant, présent dans 220 pays,
- **son expérience en matière de management de services de réseau**.



Transpac est le premier opérateur européen en nombre de routeurs managés, avec 200 000 routeurs gérés pour le compte de ses clients. Elle gère également 1 000 pare-feux, 12 000 sites web dans le cadre de ses services d'hébergement et 1 000 000 de boîtes aux lettres de messagerie.

## Les différentes phases d'une démarche sécurité et les rôles





# Transpac : une organisation et des hommes au service de la sécurité

**Confier la gestion de son réseau, de l'hébergement de ses serveurs ou de ses services de sécurité n'est possible que dans une relation de confiance.** Cette confiance passe par la connaissance du niveau de sécurité de l'entreprise choisie pour l'externalisation, de son organisation, de ses process et des protections qu'elle met en oeuvre. Transpac applique une politique de sécurité pour, tout d'abord, assurer sa pérennité en protégeant son personnel, son patrimoine, ses activités. Fondée sur la volonté de respecter les lois et règlements, cette démarche est essentiellement motivée par le souci de la satisfaction des exigences de ses clients, qui attendent des services performants et sécurisés.

## Des acteurs impliqués à tous les niveaux

**Au sein de Transpac, la maîtrise des risques est assurée par la mise en œuvre d'un processus de gestion de la sécurité et l'organisation des actions correspondantes.**

Ce processus est porté par la **direction de la sécurité**, selon les principes suivants :

- **la direction générale** s'engage sur les grandes orientations en matière de sécurité,
- **la direction de la sécurité anime une démarche d'amélioration continue**, définit les recommandations, et fédère les démarches des différentes entités. Elle offre conseil et expertise aux directions, sensibilise le personnel, organise des audits. Enfin, elle assure les relations avec les organismes officiels et organise la veille technologique,
- **le comité sécurité, composé de représentants des différentes directions, analyse les risques, définit des recommandations** avec la direction de la sécurité, et traite les dysfonctionnements éventuels,

- **les responsables de chaque entité déclinent ces orientations en actions d'amélioration**, s'impliquent dans leur mise en œuvre, informent et responsabilisent les intervenants.

Les démarches Qualité et Sécurité, complémentaires, sont conduites en synergie, et leur action est mesurée par l'analyse d'indicateurs lors de revues régulières.

C'est ainsi que Transpac :

- informe son personnel des risques potentiels, des engagements pris vis-à-vis du client, et des responsabilités de chacun dans l'utilisation des équipements et des données,
- intègre dans sa politique de sécurité les différentes réglementations en vigueur et informe son personnel de ses obligations,
- forme son personnel à l'utilisation et à la maintenance des équipements, en respectant les pratiques de sécurité reconnues,



- diffuse une charte sur l'emploi des systèmes et équipements,
- veille à la stricte application par son personnel des règles de protection des informations et équipements, sur l'ensemble des systèmes d'information (sauvegardes, contrôles d'accès...).

Les intervenants de Transpac ne transmettent d'informations vers l'extérieur qu'avec l'accord de leur

hiérarchie. Des engagements de confidentialité sont également inclus dans les contrats avec les sociétés partenaires ou fournisseurs.

Les clients ayant choisi une prestation de sécurité renforcée disposent d'un interlocuteur dédié, **le Responsable Service Client Sécurité**, expert dans son domaine, chargé d'assurer le respect de la politique de sécurité et d'en accompagner les évolutions en étroite collaboration avec l'entreprise.

## Des locaux et des équipements sous contrôle

### Ⓢ La sécurité des locaux

Transpac a défini **les règles de sécurité d'infrastructure et d'installation à respecter dans ses sites**, et veille à leur application par des **contrôles et des audits périodiques** réalisés par des organismes extérieurs.

Ces règles couvrent notamment le contrôle des accès aux salles et aux bâtiments, la sécurité incendie, la fiabilité et la disponibilité de l'énergie, le bon fonctionnement de la climatisation, l'ingénierie pour l'installation et la maintenance des équipements, le contrôle de la mise en œuvre de ces règles.

Les sites opérationnels sont implantés dans des bâtiments soumis à des règles strictes de protection. Les bâtiments principaux sont contrôlés par un service de gardiennage, présent 24h/24, qui assure le contrôle d'accès, la supervision de la gestion technique centralisée et la réaction sur alarme. Une supervision centralisée des alarmes (intrusion, incendie, dégât des eaux, anomalie réseau...) est mise en place, permettant ainsi une intervention rapide et adaptée 24h/24.

### Ⓢ Des matériels, logiciels et données protégés

La **disponibilité des équipements**, des applications et des données est assurée par les redondances, les plans de secours et de reprise, les sauvegardes.

Tout d'abord, le cœur du réseau (backbone) de Transpac,

sur lequel sont construits les réseaux d'entreprise, dispose des redondances d'équipements opérationnels nécessaires à la continuité du service et à la disponibilité des données. La structure physique permet de disposer de chemin de secours en cas d'incident sur une liaison ou sur un noeud.

Pour les équipements d'exploitation, d'administration et de supervision du cœur de réseau, il existe un plan de secours, qui fait l'objet de tests réguliers. Les systèmes d'information internes non vitaux en temps réel pour assurer le service aux clients sont secourus "à froid" grâce à des plans de secours.

Des procédures d'alerte, d'escalade et de gestion de crise permettent de faire face à des incidents majeurs. En situation de crise, Transpac met immédiatement en place une cellule, chargée de suivre au plus près la situation sur le terrain, de prendre des décisions et de piloter la communication client.

**L'intégrité des informations** est principalement assurée par :

- le choix des équipements en fonction de leurs caractéristiques correspondant aux besoins de prévention des risques de type panne ou erreur,
- les contrôles d'accès (physiques et logiques) visant à parer les menaces de nature humaine,
- le respect des protocoles de transport et de raccordement normalisés par les organismes



internationaux, mis en œuvre pour la transmission.

Avant de mettre en œuvre ces équipements, Transpac les teste et les contrôle pour vérifier qu'ils satisfont aux normes internationales et aux règles d'ingénierie définies par ses équipes.

**La confidentialité des données** sur les liaisons à l'intérieur du réseau partagé repose sur :

- les mesures de sécurité physique mises en œuvre,
- la technique utilisée (routage adaptatif, multiplexage de différentes communications sur les liens internes du réseau partagé, rendant leur itinéraire imprévisible),
- des techniques de cloisonnement (réseau privé virtuel).

Des contrôles d'accès logiques sont mis en œuvre sur les équipements opérationnels des sites, les systèmes d'information, les systèmes d'administration et de supervision. Ils sont réalisés par une politique de mots de passe, la gestion des habilitations aux applications accédant aux données, la mise en œuvre de pare-feux.

## 🔍 La protection contre les incidents

Des mesures préventives et correctives contre les incidents permettent de réduire considérablement les probabilités de :

- panne matérielle, par la maintenance corrective et préventive,
- panne d'énergie, par des groupes électrogènes,
- attaques de virus, par la mise en place de pare-feux et la mise à jour très fréquente des bases d'anti-virus protégeant PC et serveurs internes,
- vols de matériels par contrôle des zones de livraisons, utilisation de câbles antivols sur les ordinateurs portables.

La traçabilité est assurée par l'enregistrement des journaux et des alertes, pour conserver l'historique de toute intervention ou événement sur un système. Les enregistrements, exploités *a posteriori*, permettent de

définir de nouvelles mesures préventives visant à réduire encore la probabilité et l'impact des incidents.

## 🔍 Une démarche d'amélioration permanente

Dans le cadre de sa politique de sécurité, **Transpac sollicite périodiquement** des organismes extérieurs indépendants ou des intervenants internes pour mener **des actions d'audit**.

Ces audits poursuivent quatre objectifs principaux :

- contrôler l'efficacité des moyens de protection,
- mettre en évidence les faiblesses et mesurer leur gravité,
- identifier les actions susceptibles d'améliorer, dans le domaine de la sécurité, les conditions de fonctionnement des systèmes actuels,
- sensibiliser les différents interlocuteurs.

Ils portent sur les sites opérationnels, sur des cas concrets de dysfonctionnements, sur des systèmes ou services particuliers. Ils concernent à la fois la sécurité physique et logique, les procédures associées et peuvent être ponctuels ou réguliers. Ils conduisent à des propositions d'amélioration qui sont validées par la direction de la sécurité, avant d'être mises en œuvre par les différentes entités concernées.



## La certification, une garantie pour nos clients

Répondre aux problématiques de confiance des entreprises passe par une démarche de certification.

Déjà certifiés ISO 9001 V2000 par l'AFNOR, Transpac et Equant ont reçu pour leur offre Equant IP VPN, en janvier 2002, le certificat "Critères Communs" délivré par la Direction centrale de la sécurité des systèmes d'information, dirigée par le secrétaire général de la Défense nationale. Ce certificat était le premier à être délivré pour un service dans son ensemble. Il garantit :

- l'étanchéité des flux entre deux réseaux et vis-à-vis d'Internet,
- la sécurité physique des équipements déployés,
- l'administration exclusive de ces équipements par des personnes autorisées.

Cette certification a depuis été adoptée par l'ISO sous le nom ISO 15408.



**Transpac a été le premier opérateur certifié par l'ENX** (European Network Exchange), le service de communication européen dédié à l'industrie automobile, en janvier 2002. La solution mise en place pour répondre aux besoins d'échanges de la communauté industrielle est basée sur le service Equant IP VPN, au-dessus duquel des tunnels chiffrés IPSEC\* renforcent confidentialité, intégrité et authentification des données.

Enfin, **Transpac adapte sa démarche sécurité pour la mettre en conformité avec la norme ISO 17799**, issue de la norme anglaise BS 7799 créée en 1995 et révisée en 1999. Elle constitue un code de bonnes pratiques pour la gestion de la sécurité de l'information et propose plus d'une centaine de mesures, réparties en dix chapitres, couvrant aussi bien la politique de sécurité que la sécurité du personnel, le contrôle d'accès ou le plan de continuité. Elle contient à la fois un ensemble de mesures techniques et organisationnelles à mettre en place pour gérer de manière sécurisée les informations, et un ensemble de propositions de solutions comme l'utilisation de pare-feu ou la composition des mots de passe. Malgré l'absence d'un organisme certificateur en France, elle devient une base de "benchmark" pour nos clients qui l'utilisent pour évaluer en avant-vente l'ensemble de notre sécurité. En juin 2002, la société Airbus a d'ailleurs attribué à Transpac/Equant un certificat de conformité correspondant aux critères ISO 17799, à la suite d'un audit sur site.



Dans une optique d'amélioration, sous le regard d'experts externes et reconnus, **cette démarche de certification constitue donc, pour nos clients, une garantie réelle sur la qualité et la sécurité des services.**

\* voir glossaire page 25



# ➤ La sécurité des réseaux VPN IP

Une grande partie de nos clients choisissent aujourd'hui la solution basée sur la technologie MPLS\*, Equant IP VPN, pour construire leur intranet, principalement pour les raisons suivantes :

- **la flexibilité**

Grâce à la connectivité any-to-any, chaque site peut communiquer avec tous les autres sites sans qu'il soit nécessaire de créer autant de circuits virtuels. Tous les sites, où qu'ils soient dans le monde, peuvent accéder à toutes les applications. Le réseau absorbe ainsi plus facilement les montées en charge et les déploiements, en affranchissant l'entreprise des contraintes géographiques. La souplesse des VPNs permet aussi de créer très simplement des VPNs modulaires, correspondant par exemple à une branche de l'entreprise, cloisonnant ainsi les communications au sein d'une communauté. Des VPNs transversaux, accessibles à tous, peuvent servir à atteindre des applications communes. En résumé, le réseau s'adapte vraiment à l'organisation, en toute sécurité.

- **les performances**

Les classes de services servent à prioriser les flux selon leur caractère critique, pour préserver la qualité de service des applications vitales, en contrôlant les flux consommateurs tels que la messagerie ou le transfert de fichiers, ou des flux moins importants tels que le trafic Internet. De plus, toutes les technologies d'accès sont disponibles, ce qui permet d'atteindre de très hauts débits.

- **l'accompagnement au quotidien et dans la durée**

Nos services client apportent les outils indispensables pour que nos clients maîtrisent la vie de leur réseau. Le Responsable Service Client est l'interlocuteur privilégié, disponible à tout moment pour apporter conseil et expertise.

- **la couverture géographique** inégalée grâce aux points de présence de Equant dans 220 pays.

A ces différents atouts s'ajoute **un très haut niveau de sécurité**, basé sur différents mécanismes décrits ci-après.

## Principes de base du VPN IP et de la technologie MPLS

Les réseaux privés virtuels sur IP (VPN IP) s'appuient sur un cœur de réseau (backbone) IP partagé. Pour donner au VPN IP une étanchéité comparable à celle que procurent les circuits X25, ATM ou Frame Relay, on utilise la technologie MPLS-VPN\*, qui permet de compartimenter ce réseau en autant de VPNs que de réseaux d'entreprises.

MPLS-VPN\* est issu de MPLS, protocole qui, grâce à la

commutation de trames, permet une maîtrise élevée des performances et de l'ingénierie du cœur de réseau. MPLS-VPN repose sur trois composants de base : le routeur client (CE, Customer Edge router), le routeur de périphérie (PE, Provider Edge router) auxquels les routeurs clients sont raccordés, et le routeur ou commutateur de cœur de réseau (P, Provider device).

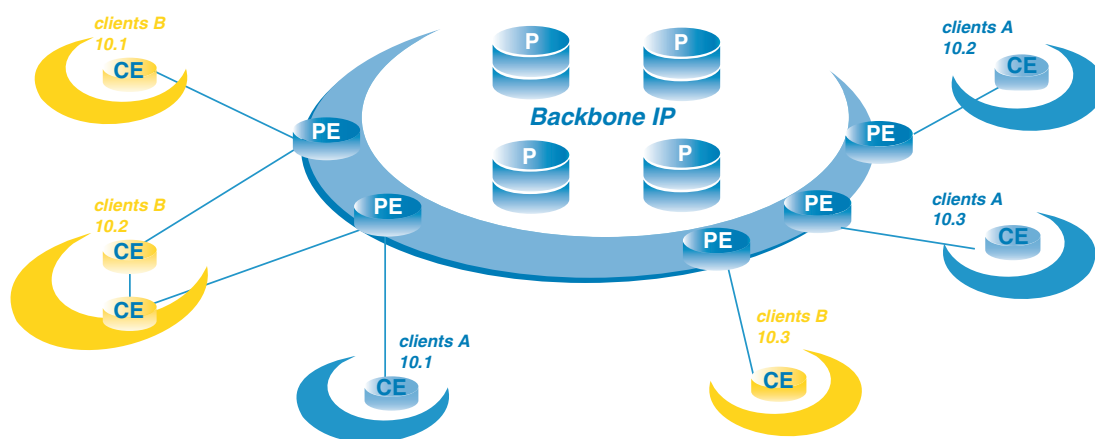
\* voir glossaire page 25



Au niveau des PE sont configurées autant de tables de routage (VRF : Virtual Routing and Forwarding table), étanches entre elles, que de VPNs. Des labels MPLS (courtes étiquettes placées devant le paquet IP) servent à commuter les trames entre les VRFs du même VPN. Il est techniquement impossible pour un paquet venant du VPN bleu par exemple, d'atteindre un site du VPN jaune. La meilleure preuve : le client peut utiliser n'importe quel

plan d'adressage, il ne risque aucun conflit avec l'environnement ouvert (monde Internet), ni avec les plans d'adressage des autres clients VPN.

Cette étanchéité, auditée et certifiée par la DCSSI, assure l'isolation du VPN d'une entreprise par rapport aux VPNs d'autres entreprises, et par rapport à Internet.



## Un cœur de réseau IP dédié aux entreprises, invisible de l'Internet

Le service Equant IP VPN s'appuie sur un réseau IP MPLS-VPN\* mondial exclusivement dédié aux entreprises. Ce réseau, maîtrisé de bout en bout, est disjoint de l'Internet public. Cette spécialisation du backbone constitue la première fondation et un premier niveau d'assurance face aux problèmes de sécurité qui existent sur le Web.

Sur cette base, et afin d'assurer un niveau de sécurité maximal, Transpac a développé la sécurisation de son réseau IP autour de quatre axes majeurs :

- **l'invisibilité et l'inaccessibilité du réseau MPLS-VPN vis-à-vis de l'Internet,**
- **le haut niveau de protection,** vis-à-vis des attaques, des systèmes du réseau partagé,
- **la disponibilité** du réseau partagé,

- **l'étanchéité des flux VPN IP** entre différents réseaux client et vis-à-vis d'Internet.

### ► Un réseau invisible et inaccessible depuis l'Internet public

Afin d'améliorer la qualité et l'évolutivité des services IP entreprise, le réseau MPLS-VPN de Transpac, jusqu'à présent commun avec le réseau supportant les services IP grand public de France Télécom, a migré en 2003 vers une nouvelle architecture, appelée "réseau IP de nouvelle génération", exclusivement dédiée aux entreprises.

\* voir glossaire page 25



Pour minimiser l'exposition du réseau face à tous les types d'attaques externes (prise de contrôle ou déni de service), ce nouveau réseau a été conçu pour être invisible et inaccessible vis à vis de l'Internet public.

**Dans le réseau IP de nouvelle génération, tous les routeurs partagés (routeurs P et PE) possèdent des adresses IP non connues de l'Internet public.**

Ainsi, il est techniquement impossible d'établir des communications entre l'Internet public et ces routeurs : le trafic n'est pas routé. De la même manière, un client raccordé au réseau de Transpac ne peut pas envoyer de paquets à destination de ces routeurs, grâce aux filtres mis en place (ACL : access control lists).

## 🔍 Des systèmes d'infrastructure hautement sécurisés

En complément, les mesures suivantes sont mises en œuvre pour prévenir les intrusions sur les routeurs partagés :

- des filtres (ACL) sont configurés sur ces routeurs pour empêcher les flux d'administration (SNMP\*, TELNET\*...) provenant d'autres machines que celles des plate-formes d'administration Transpac,
- aucune écriture SNMP\* n'est autorisée,
- les requêtes TELNET\* sont systématiquement tracées et contrôlées par des serveurs TACACS\* capables de bloquer les comptes après un certain nombre d'essais infructueux,
- une politique de gestion des mots de passe est appliquée : règles de nommage strictes, durée de validité, tests de craquage réguliers,
- la production des VPNs sur les routeurs PE est assurée exclusivement par des outils spécialisés, qui ne donnent pas accès à l'ensemble des commandes de configuration aux techniciens, mais seulement à un ensemble minimal de commandes nécessaires. Ainsi, les erreurs de production sont évitées et un très haut niveau d'intégrité des configurations est assuré. Ces outils incorporent un système de traçabilité des commandes et de leur auteurs, permettant de piloter de très près les évolutions.

De plus, afin de s'assurer de la bonne application systématique de l'ensemble des mesures de sécurité, et d'identifier les tentatives d'action illicite sur les infrastructures, **une supervision (temps réel et statistique) de la sécurité est assurée par un ensemble d'outils spécifiques.** Cette supervision s'appuie, entre autres, sur les éléments suivants :

- contrôle de la conformité des configurations routeur par rapport aux règles de sécurité,
- contrôle de l'intégrité des configurations routeur,
- scans de port automatisés,
- tests automatisés de crackage des mots de passe,
- analyse des flux syslog\*,
- analyse des logs TACACS\*,
- supervision du routeur (disponibilité, charge unité centrale, mémoire) et de ses interfaces (disponibilité, taux de charge).

Des tests d'intégrité des VPNs sur le réseau partagé permettent de vérifier qu'aucune insertion illicite ne s'est produite dans la VRF du client, qu'aucun échange de route n'est paramétré, en dehors de la VRF d'administration. Des tests de mise en service permettent de valider chaque nouvelle interface produite au sein d'un VPN.

Les configurations des routeurs CE sont sécurisées, selon des modèles type adaptés au contexte client, modèles définis dans la politique de sécurité Transpac (présence de certaines commandes de sécurité paramétrées selon des règles strictes, suppression des éléments non indispensables, sources potentielles de vulnérabilités supplémentaires).

## 🔍 Un réseau disponible et tolérant face aux perturbations externes

Le réseau MPLS-VPN de Transpac est un réseau redondant qui s'appuie sur des technologies évoluées. **Tous les routeurs de transit et les liaisons internes sont systématiquement doublés.**

**Ce réseau est supervisé en temps réel 24h/24 et 7j/7, ce qui permet d'intervenir au plus tôt en cas de dysfonctionnement.**

\* voir glossaire page 25



## Equant IP VPN, un service étanche et cloisonné

Convaincu de l'importance de la sécurité dans l'environnement entreprise, Transpac a mené dès 2001 un vaste chantier destiné à démontrer l'étanchéité et le cloisonnement des flux VPN construits sur son réseau, chantier ayant abouti à la certification ISO 15408 (voir page 15).

### ⌚ Le cloisonnement des VPNs

La technologie MPLS-VPN\* garantit l'étanchéité d'un VPN par rapport à un autre, grâce à la présence d'une table de routage/commutation par VPN au niveau de chaque PE (voir "Principes de base du VPN IP et de la technologie MPLS" page 16). De plus, aucune manipulation de label MPLS n'est autorisée en dehors des routeurs partagés, qui sont sous la responsabilité exclusive de France Télécom et situés dans ses locaux. En particulier, aucun routeur CE ne peut manipuler de label MPLS de même niveau que ceux employés pour construire les VPNs sur le réseau MPLS-VPN.

### ⌚ Le cloisonnement des flux VPN vis-à-vis d'Internet

Au sein du réseau Transpac, les éléments assurant le cloisonnement entre les réseaux VPN et l'Internet, au niveau de chaque PE, sont :

- la table de routage globale, support du routage vers l'Internet, qui ne contient pas de routes VPN,
- les VRF, qui ne contiennent pas de routes Internet.

L'évasion vers Internet n'est possible que via la passerelle Internet Transpac (pare-feu réseau) ou via une passerelle localisée chez le client.

Les plate-formes de service mutualisées (centrex voix sur IP, caches, CDN...) sont embarquées dans des VPNs de service et sont donc protégées vis à vis de l'Internet public.

\* voir glossaire page 25



# ➤ Les services de sécurité managés et les prestations sur mesure

## Des solutions managées pour renforcer la sécurité

L'offre Equant IP VPN apporte la sécurité des flux transportés à l'intérieur d'un VPN. Ouvrir ce VPN vers l'extérieur (Internet, extranet, accès nomades RTC, GPRS, WiFi...) ou chiffrer des données ultra-confidentielles nécessite de disposer de solutions de sécurité complémentaires. Pour ce faire, Transpac propose des services :

- d'**authentification**, pour contrôler l'accès au réseau de l'entreprise,
- de **pare-feu, de proxy\* managés et de filtrage de contenu** pour contrôler les portes d'accès à Internet ou vers un extranet,
- d'**anti-virus** sur les contenus mails, web, FTP et d'**anti-spam** pour la messagerie,
- de **détection d'intrusion**,
- de **chiffrement**.

l'exploitation d'une négligence (mot de passe écrit sur le bureau, social engineering\*...).

La solution d'authentification forte pour le contrôle d'accès à Equant IP VPN propose la gestion des serveurs Radius\* d'authentification, des bases d'utilisateurs et la fourniture de calechettes pour générer des jetons, c'est-à-dire des mots de passe à usage unique.

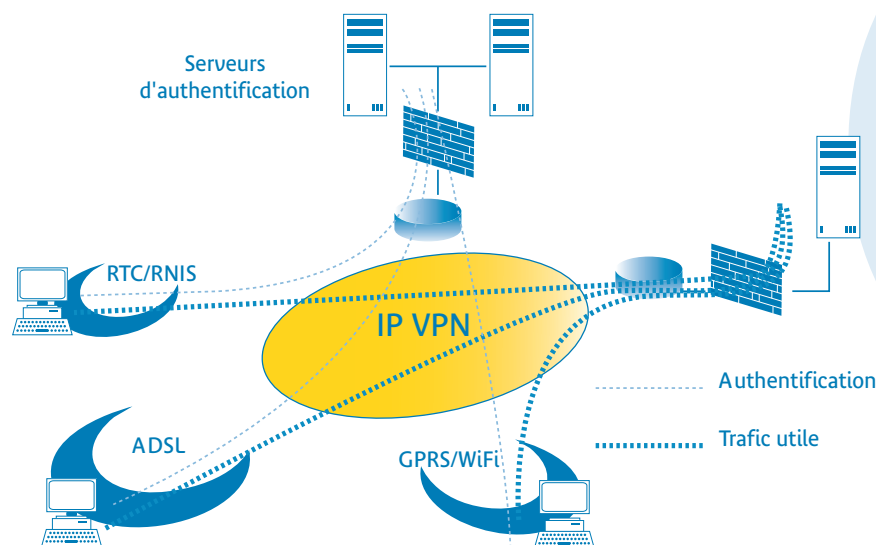
Un web d'administration est également mis à la disposition de l'administrateur réseau de l'entreprise afin de gérer le parc d'utilisateurs accédant à distance (création/suppression/modification de comptes) et de visualiser les statistiques de connexion.

### ➤ Contrôler l'accès au réseau de l'entreprise

La disponibilité de moyens d'accès hors des locaux de l'entreprise, justifiée par des besoins d'accès distants, de nomadisme ou de télétravail, impose la mise en place d'architectures de contrôle de l'accès au réseau de l'entreprise.

C'est pourquoi **les solutions d'accès distants d'Equant IP VPN (RTC/RNIS/xDSL/GPRS/WiFi...) sont couplées à des mécanismes d'authentification utilisant les techniques Chap/Radius\***. Il est possible de mettre en place une **authentification renforcée** au moyen de solutions de mots de passe à usage unique, évitant l'utilisation par un tiers d'un mot de passe obtenu par

\* voir glossaire page 25



## 🔍 Sécuriser l'ouverture vers l'extérieur

Lorsqu'une passerelle est mise en place entre un VPN et Internet, ou entre un VPN et un extranet, il est nécessaire de la sécuriser pour contrôler les flux.

**Transpac propose un service de pare-feu dédié et managé, installé soit dans les locaux de l'entreprise cliente, soit dans ses propres centres.** Les règles de filtrage sont définies par le client et modifiables rapidement pour correspondre aux changements de droits, très fréquents dans une grande entreprise.

Le pare-feu est la brique indispensable pour contrôler les connexions autorisées, mais il n'a pas vocation à assumer l'ensemble des contrôles de sécurité. Il est nécessaire de

le compléter au moyen de solutions d'antivirus, de filtrage d'URL, de proxy\* et de systèmes de détection d'intrusion afin de disposer d'une passerelle complètement sécurisée. L'ensemble de ces fonctions est disponible au sein de **l'offre Equant Secure Gateway**. Au sein de ce service modulaire, chaque brique peut être secourue par doublement et dimensionnée en fonction du volume des flux à traiter.

**Ces services sont supervisés 24h/24 et 7j/7** par des équipes sécurité de France Télécom et font l'objet de fourniture de tableaux de bord. **Une veille technologique** sécurité avancée est réalisée sur l'ensemble de ces solutions, afin de détecter au plus vite les menaces potentielles et de proposer des solutions sans attendre la diffusion des failles.



**Equant Secure Gateway** est composé de trois services, managés 24h/24 et 7j/7 :

- **Managed firewall** : service de pare-feu managé,
- **Managed anti-virus** : protection SMTP (messagerie), protection HTTP (web) et protection FTP (transfert de fichiers),
- **Managed employee access** : authentification des utilisateurs de l'entreprise.

L'offre Equant Secure Gateway apporte à l'entreprise :

- un **accompagnement** dans la définition de sa politique de sécurité,
- le **choix entre différentes configurations**, simples ou secourues,
- un **management complet**, comprenant la fourniture, l'installation, la configuration et l'exploitation des équipements, des statistiques en temps réel et des rapports périodiques, des alertes de sécurité,
- une **solution internationale** avec des supports clients locaux dans plus de 165 pays.

\* voir glossaire page 25



### > Le pare-feu

Ce service définit les flux autorisés à traverser la passerelle, au moyen de règles de filtrage, à la fois en entrée et en sortie du réseau d'entreprise, en fonction d'une politique de sécurité définie par l'entreprise. Il permet de détecter les tentatives d'accès sur le réseau d'entreprise. Différents niveaux de service permettent de répondre à tous les besoins, quels que soient le nombre d'utilisateurs et la taille du réseau à protéger.

### > L'anti-virus de contenus mails, web, FTP et l'anti-spam de messagerie

L'anti-virus permet d'analyser les contenus reçus et envoyés et de détecter les virus en comparant les contenus à une liste de signatures, mise à jour régulièrement. Ce service permet d'éviter l'infection du réseau de l'entreprise par des contenus externes ainsi que l'émission de virus vers des partenaires ou des clients, nuisible à l'image de marque de l'entreprise.

Il fournit une triple protection :

- protection SMTP (messagerie) : analyse le trafic de messagerie entrant et sortant, et détecte d'éventuels virus avec choix par l'entreprise de l'action sur apparition d'un virus : destruction, notification à l'émetteur, au destinataire...
- protection HTTP (web) : empêche le téléchargement de fichiers infectés, protège contre les programmes malveillants Java et ActiveX,
- protection FTP (transfert de fichiers) : empêche le téléchargement de fichiers infectés à partir de sites distants non sécurisés.

Des solutions d'anti-spam permettent de bloquer le courrier indésirable. Peuvent y être définis des listes noires et/ou des listes blanches d'émetteurs, des filtres sur mots-clés dans les contenus, et des règles heuristiques évoluées, permettant de composer des filtres complexes dans le cas où le spam n'est pas détectable par mot clé ou par émetteur. Le client choisit les actions prises sur détection de spam : destruction, mise en quarantaine...

### > Le filtrage de contenu

Les solutions de filtrage de contenu viennent en complément du pare-feu. Elles offrent à l'entreprise la possibilité de restreindre et de contrôler l'accès des utilisateurs de l'entreprise aux contenus non

professionnels : sites adultes, jeux, eTrading, chat... Elles peuvent être complétées par des solutions de proxy-cache. Elles permettent à l'administrateur de gérer sous forme de listes blanches et/ou de listes noires les sites autorisés.

Leur utilisation est soumise à une information auprès de la CNIL et des instances représentatives de l'entreprise (Comité d'entreprise).

### > Le proxy-cache

Le proxy-cache améliore les performances de consultation sur Internet en mémorisant les contenus fréquemment visités par les utilisateurs. Il est possible de le coupler à une base d'authentification LDAP\* afin de définir la liste des personnes ayant le droit de consulter Internet.

### > Les systèmes de détection d'intrusion

Les systèmes de détection d'intrusion sont des équipements de type sonde, capables de mettre en corrélation plusieurs signatures d'attaques référencées avec le trafic capturé, afin de détecter une activité suspecte. La remontée d'alerte permet alors d'agir au niveau de la politique de sécurité et de réduire les risques d'intrusion dans les systèmes.

## 🔗 Les solutions de chiffrement

Certains flux nécessitent une prise en compte renforcée de la sécurité, notamment pour ce qui concerne l'authentification, la confidentialité et l'intégrité des échanges.

Pour répondre à ces besoins, des solutions de chiffrement peuvent être mises en place afin d'éviter l'écoute de données sensibles et d'assurer l'intégrité des données transportées.

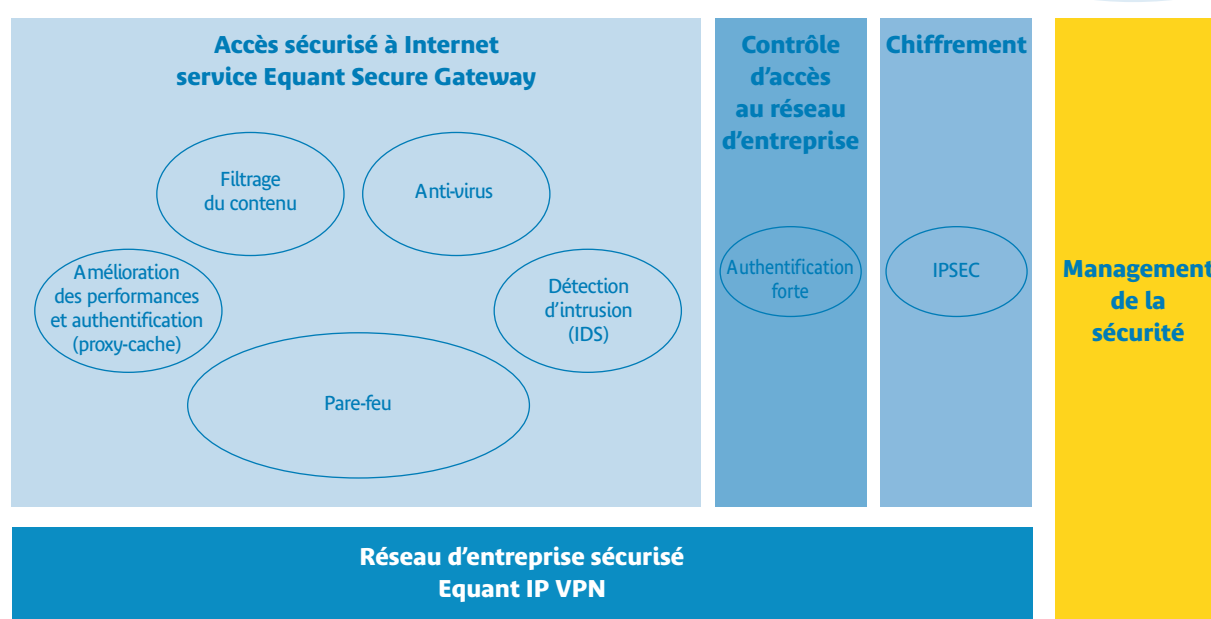
Ces solutions sont envisagées pour sécuriser des secrets industriels, bancaires, ou liés à la Défense. Afin d'y répondre, Transpac apporte un service de chiffrement au-dessus des solutions Equant IP VPN. Il comprend la gestion de boîtiers de chiffrement IPSec et la gestion des clés de chiffrement, que ce soit pour des sites permanents ou pour des solutions nomades reposant sur le RTC, le xDSL, le GPRS ou le WIFI.

\* voir glossaire page 25



## ① Une offre de sécurité modulaire

L'offre de sécurité que nous venons de décrire est modulaire : l'entreprise choisit les briques dont elle veut déléguer la gestion. Le diagramme suivant illustre la complémentarité de nos services, basée sur le socle fédérateur réseau, Equant IP VPN :



## Des prestations de sécurité avancées, sur mesure

A la demande de certaines grandes entreprises, notamment des banques, **Transpac propose des prestations de sécurité avancées, sur mesure, afin de répondre aux hautes exigences de protection du système d'information.**

En amont de la mise en place d'une solution réseau, Transpac et l'entreprise étudient ensemble les exigences et les contraintes de sécurité. Ce travail conjoint permet également à l'entreprise d'acquérir une connaissance avancée du niveau de sécurité de Transpac, aussi bien dans les domaines techniques qu'organisationnels.

Ces travaux aboutissent à la définition d'une politique de sécurité commune, applicable au périmètre du réseau. Elle contient une analyse de l'existant et des risques associés, un ensemble de procédures de suivi de la sécurité et une organisation sur-mesure.

Lorsque le réseau est en place, les outils de supervision en temps réel et les tableaux de bord fournis par Transpac donnent au client une vue précise, à tout moment, du niveau de sécurité de son réseau. En complément, des tests et audits périodiques sont menés sur son infrastructure. Il reçoit les alertes en temps réel et décide, avec son Responsable Service Client sécurité Transpac,



l'action à réaliser en fonction de la gravité de l'alerte.

Le client bénéficie de l'expertise de l'opérateur en matière de sécurité réseau et de la qualité de ses procédures, permettant une réactivité forte en cas d'attaques. Périodiquement, il rencontre le RSC sécurité pour faire le point sur les alertes et le plan d'action associé, contrôler que les évolutions du réseau prévues sont conformes à la politique sécurité. Il est assuré de la bonne application de

cette politique grâce au RSC sécurité qui en est responsable. Enfin, il gère avec le RSC les évolutions de cette politique pour l'adapter en permanence aux changements d'environnement.

## Conclusion

La place prépondérante du système d'information dans le fonctionnement d'une grande entreprise fait de la sécurité un facteur clé dont peut dépendre la survie de l'entreprise, en particulier dans certains secteurs comme la banque, les assurances ou la finance.

La sécurité ne peut donc plus être considérée comme un élément à part mais doit vraiment être "embarquée" dans une organisation. Elle doit être prise en compte en amont des choix de solutions informatiques et réseaux comme un critère de sélection à part entière. Beaucoup de grandes entreprises l'ont compris et France Télécom l'observe dans l'augmentation des volets sécurité présents dans les consultations. Les questionnaires portent, bien sûr, sur les aspects techniques mais les demandes concernent de plus en plus souvent l'organisation de l'opérateur en matière de sécurité, ses processus, ses méthodes de veille technologique et de traitement des attaques.

On comprend alors l'importance de s'appuyer sur un partenaire fiable, pérenne, dont les processus sont éprouvés et certifiés. 75 % des grandes entreprises françaises font ainsi confiance à France Télécom pour la gestion de leur réseau de données et peuvent bénéficier des solutions internationales d'Equant pour accompagner leur internationalisation.

Elles sont assurées de bénéficier des innovations technologiques grâce aux recherches menées par les 3 000 chercheurs de France Télécom Recherche et Développement. Les innovations en préparation dans leurs laboratoires augurent un avenir riche en nouveautés, en particulier dans les techniques de signatures, de chiffrement et d'horodatage. Elles ouvrent la voie à la

dématisation complète des procédures administratives (télé-procédures), qui vont grandement simplifier la vie des citoyens et des entreprises. Vote électronique, demandes de passeport en ligne, formalités entreprises-administration allégées, les applications sont innombrables. La biométrie, c'est-à-dire l'identification par une caractéristique physique, comme l'empreinte digitale ou la forme de l'iris, promet également de révolutionner l'authentification. Où la réalité rejoint la fiction...



Pour en savoir plus sur nos services, nous vous invitons à consulter [www.francetelecom.com/entreprises](http://www.francetelecom.com/entreprises) et [www.transpac.fr](http://www.transpac.fr)



## Glossaire

**CERT@/CC** : le CERT Coordination center est un centre majeur de reporting des problèmes de sécurité Internet. Il a été créé en 1988 à l'initiative de la DARPA (Defense Advanced Research Project Agency), émanation directe du Ministère de la Défense américain, hébergée par la Carnegie Mellon University.

**Certificat** : document numérique dont l'objectif est de garantir à une personne qui utilise une clé publique pour vérifier une signature, que cette clé publique appartient bien à qui elle est censée appartenir (non usurpation d'identité). Parce qu'il est signé par une tierce partie de confiance, il lie de manière sûre l'identité du possesseur à sa clé publique, le tiers de confiance ayant vérifié l'identité du possesseur lors de la délivrance du certificat.

**CHAP** (Challenge-Handshake Authentication Protocol) : protocole d'authentification utilisant un système de défi-réponse, dans lequel le serveur envoie au client, lors de la demande d'accès, une clé destinée à chiffrer le nom d'utilisateur et le mot de passe.

**Condensat** (ou hash) : résultat d'une fonction de hachage (H) transforme un message M de longueur quelconque en un version "digérée" H(M) de longueur fixe. C'est une fonction à sens unique, c'est-à-dire qu'étant donné un Y, il est impossible de trouver un message M, tel que le hachage de M, H(M), donne Y. Elle est utilisée dans les mécanismes de signature électronique.

**Déni de service** : attaque consistant à saturer une ressource en effectuant de manière malveillante des demandes de réservation excessives ou en occupant le service illicitement. Parmi les attaques de déni de service les plus connues : SYN flooding, UDP flooding, ping of death, LAND attack, SMURF attack, mail bombing...

**GPRS** (General Packet Radio Services) : technologie de

transport de données utilisant les infrastructures des réseaux GSM.

**Hash** : voir condensat

**Horodatage** : service qui associe de manière sûre un événement et une heure afin d'établir de manière fiable l'heure à laquelle cet événement s'est réalisé.

**ICP ou PKI** (Infrastructure à Clés Publiques ou Public Key Infrastructure) : infrastructure technique et procédures d'administration et d'exploitation associées permettant de délivrer et de 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.

**IDS** (Intrusion Detection System) : système de détection d'intrusion basé sur un équipement de type "sonde réseau" permettant de détecter en temps réel les tentatives d'intrusion sur un réseau.

**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 (confidentialité et protection contre l'analyse du trafic, authentification des données et de leur origine, intégrité des données, protection contre le jeu, et gestion des clés).

**Jeton** (ou token) : mot de passe non re-jouable émis par un dispositif électronique. Il s'agit en général d'une





calculatrice capable de dérouler un algorithme identique à celui déroulé par le serveur d'authentification. La calculatrice génère ainsi des mots de passe en même temps que le serveur. L'utilisateur se contente de recopier le mot de passe présenté sur l'écran de la calculatrice à un instant donné. Le mot de passe généré changeant à chaque connexion, il ne peut être réutilisé par une tierce personne pour une future tentative de connexion. Ce code non rejouable est complété d'un code PIN pour parer à la perte de la calculatrice. Ce type de dispositif nécessite une synchronisation temporelle du serveur et de la calculatrice.

**LDAP** (Lightweight Directory Access Protocol) : protocole permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases 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 une destination. Elle est basée sur l'étiquetage par "label" de chaque paquet qui entre dans un réseau et qui va progresser le long du chemin, appelé "LSP" (Label Switched Path : chemin commuté par étiquette), par commutation des labels.

**MPLS-VPN** : adaptation de la technologie MPLS pour construire des réseaux privés virtuels au-dessus d'un réseau IP partagé. Par rapport à MPLS, MPLS-VPN utilise deux niveaux d'étiquettes, l'étiquette extérieure à la trame servant à la commutation dans le cœur de réseau, l'étiquette intérieure servant à déterminer l'interface de sortie sur le dernier routeur du cœur de réseau.

**PKI** : voir ICP

**Proxy** : fonction, assurée par un serveur, ayant le rôle d'intermédiaire entre les ordinateurs du réseau interne d'une organisation et Internet. Un proxy a plusieurs usages : il a une fonction de cache, c'est-à-dire qu'il garde en mémoire (en "cache") les pages les plus souvent

visitées par les utilisateurs du réseau interne afin de pouvoir les leur fournir le plus rapidement possible et pour économiser de la bande passante. Il sert à filtrer le trafic pour empêcher l'accès à certaines URLs ou à des sites comportant des mots clés donnés. Il peut authentifier les utilisateurs en leur demandant un nom et un mot de passe lorsqu'il veulent consulter Internet.

**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).

**Scan** : action réalisée par un programme pour parcourir la configuration d'un système dans le but de détecter des vulnérabilités. Par exemple, le scan peut servir à détecter les ports protocolaires ouverts sur un système.

**Signature électronique** : données chiffrées ajoutées à une information numérique pour en authentifier son auteur et en garantir son intégrité.

**SNMP** (Simple Network Management Protocol) : protocole d'administration à distance permettant de superviser la fonction réseau de tout équipement connecté à un réseau : serveur, station de travail, hub, commutateur...

**Social engineering** : pratique consistant à abuser de la confiance d'une ou de plusieurs personnes, dans le but de récupérer des informations confidentielles.

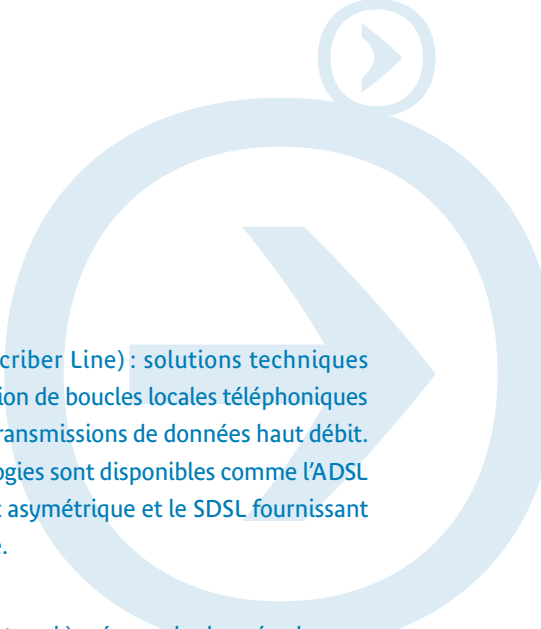
**Syslog** : fichier servant à enregistrer les événements d'un système.



**TACACS** (Terminal Access Controller Access Control System) : protocole d'authentification permettant de contrôler l'accès à la configuration d'un équipement de réseau.

**TELNET** : protocole servant à l'émulation de terminal, c'est-à-dire qu'il permet à un ordinateur de se connecter sur un équipement IP (serveur, routeur) comme s'il était un simple terminal raccordé localement à cet équipement.

**Ver** : forme de virus ayant la propriété de se dupliquer au sein d'une machine, voire de se copier d'une machine à l'autre à travers le réseau. Un ver peut facilement échapper à tout contrôle et consommer toutes les ressources des machines infectées qui n'arrivent plus à faire tourner toutes les copies du programme.



**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.

**Wan** (Wide Area Network) : réseau de données longue distance permettant d'interconnecter les différents sites d'une organisation.

**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.