

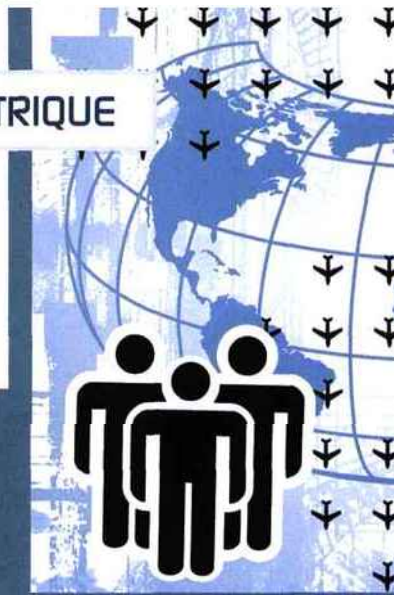
PROTECTION

LA DÉFENSE PÉRIMÉTRIQUE

SUR LE TERRAIN

Corsair défend ses lignes

Le terrain de jeu de Farid Boulakia est centré sur la sécurité du Système d'Information de son entreprise, la compagnie aérienne Corsair. Son rôle est non seulement d'en assurer la protection interne et périmétrique mais également de maintenir à disposition et ce, en permanence, les données de Corsair.



QUAND IL N'EST PAS AU FEU, Farid Boulakia consacre son temps à effectuer de la veille technologique afin de trouver de nouvelles solutions pour améliorer l'existant, ou tout simplement proposer des services inédits jusqu'alors. Comme le filtrage d'url ou la mise en place d'anti-spyware.

En premier lieu, le routage, les pare-feux et les commutateurs focalisent l'attention sécuritaire de Farid Boulakia. Au-delà, ce sont pas moins de sept cent postes qui sont également à protéger sur le territoire français sans oublier la dizaine de sites distants situés à l'étranger aux Dom-Tom, Antilles ou Réunion ou encore sur des territoires non français couverts par des partenaires.

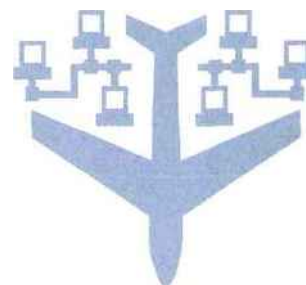
Renforcer la sécurité

Pour communiquer avec les zones distantes, **Corsair** passe, la plupart du temps, par

des interconnexions s'appuyant sur des lignes spécialisées pour relier les deux à quinze postes distants. Etant donné le coût de telles opérations, Farid Boulakia eut l'idée de centraliser la sécurité des différents applicatifs utilisés par l'entreprise, ainsi que l'accès à Internet et aux fichiers. En effet, les tarifs Internet et la banalisation de son utilisation dans le monde de l'entreprise a permis d'envisager de remplacer des liens Wan extrêmement coûteux par le passage via la toile. Cela a naturellement impliqué un renforcement non négligeable de la sécurité.

La solution choisie repose sur l'utilisation d'une unique marque (Sonicwall) sur tous les sites, distants ou non, afin, entre autres raisons, de simplifier tant le déploiement que l'administration de l'ensemble. Par conséquent, le déploiement d'une appliance sur chaque site distant fut opéré mais en tenant compte de la taille de chaque empla-

cement. Ainsi, les modèles installés dans les zones éloignées ne sont généralement pas identiques à ceux utilisés sur le site central. De moindre taille, ils supportent cependant quasiment les mêmes types de services et ils sont surtout administrés par une console unique que l'on retrouve sur le site central.



Ces modifications d'infrastructures tant télécoms que sécurité ont tout d'abord débuté par le site central. Là, Farid Boulakia assisté d'un consultant extérieur, Arnaud Flotté-Dubary travaillant chez Janus Consulting, a renforcé la sécurité de son périmètre physique. Il fit installer deux boîtiers entre le réseau de l'entreprise et Internet dotés des fonctions anti-spyware, filtrage urls et de gestion de trafic applicatif en plus de celles de pare-feu.

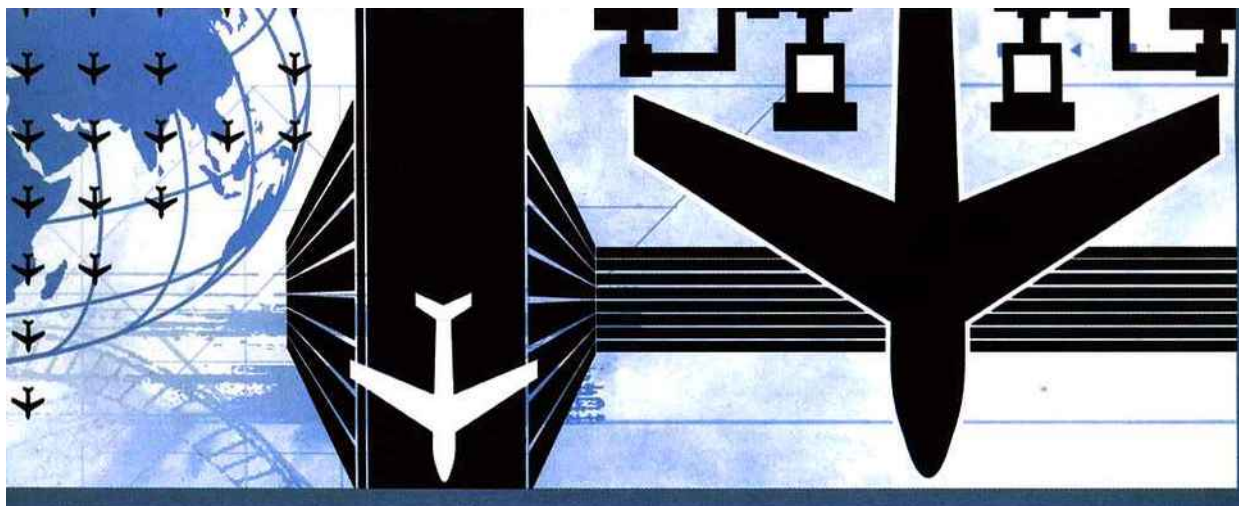
Basculer vers l'ADSL

Ce qui a motivé la décision de Corsair de faire enfin le pas fut non seulement la rapidité de déploiement de la solution choisie mais également son coût compétitif. Prochaine étape pour le tandem : couvrir les sites distants avec une solution adaptée en termes de taille de boîtier en même

POUR LES UTILISATEURS NOMADES : UN BOÎTIER VPN

En ce qui concerne les échanges avec les utilisateurs nomades, un boîtier VPN reposant sur SSL assume le cryptage des flux et l'authentification de l'employé. Le mode de fonctionnement choisi est non seulement simple à déployer mais également rapide à utiliser pour le salarié mobile. Il est orienté, suite à sa requête de connexion au site central, sur une URL qui lui permet de télécharger un ActiveX qui lui servira pour s'authentifier via un login-mot de passe.

Derrière, la base de données qui recense les autorisations et profils repose sur un annuaire Active Directory. Le client VPN d'antan fut donc abandonné sans remord aucun regard à la lourdeur d'utilisation qu'il demandait car on ne pouvait pas se connecter de n'importe où. Quant à installer quelqu'un à distance à la volée et lui permettre de se connecter, ce schéma n'était même pas, dans le cadre d'un VPN, envisageable. Pour les PC mobiles internes, chaque poste possède son propre pare-feu et anti-virus. La fonction IPS personnelle est à l'étude et ne saurait tarder à débarquer sur les postes mobiles.



temps que de basculer sur une communication de type ADSL

Côte administration, le site central supervise non seulement l'ensemble des sites en plus du sien mais son rôle est également d'effectuer des relevés d'activité Web, HTTP et VPN Elle permet d'avoir une vision un peu plus « proactive » de ce qui se passe sur les différents réseaux de Corsair Il est également à noter que la granularité permise en termes de configuration est un autre des aspects qui a séduit le spécialiste sécurité de Corsair, « *Le niveau d'analyses permis avec les logs vont grandement me simplifier la vie à l'avenir* » précise-t-il

De multiples protections internes

Mais la protection mise en œuvre par Farid Boulakia ne s'arrête pas aux dangers en provenance de l'extérieur Il multiplie les boîtiers en interne afin de sécuriser également les

flux internes La politique de défense interne n'étant pas envisageable avant l'avènement des boîtiers multifonctions au sein même du périmètre de l'entreprise Car le mode de fonctionnement de ce type de matériel se prête à la mise en œuvre de façon simple de protections sur le réseau interne L'objectif est d'installer des brins de réseaux que l'on puisse mettre en quarantaine en cas de souci d'intrusion Pour détecter l'intrusion potentielle, un filtrage IPS devrait être instauré à terme entre les Vlans (Virtual Lan, réseau que l'on segmente en brins logiques, de manière virtuelle) de façon à pouvoir isoler un VLAN en cas d'infection d'une machine, que ce soit un serveur ou un poste de travail, située sur la portion de réseau considérée

D'une façon générale, tous les boîtiers installés sur le réseau sont mis en place en mode « fail over » pour assurer une tolérance aux pannes et une permanence de service maximale Les sites concernés ont été le site technique basé sur Orly, Corsair Fly situé à Rungis et les trois

sites distants en Guadeloupe, Martinique et Réunion En sus de ces installations, un système de backup est venu compléter l'infrastructure de sécurité pour sauvegarder les données critiques issues de la Direction Quant au futur projet, le NAC, Network Access Control ou contrôle d'accès sécurisé, il constituera la prochaine étape pour Corsair Il reposera sur les profils de personnes et de groupes stockés dans un Active Directory qui servira de meta-annuaire, résultat de la future consolidation du pool d'annuaires dont se sert déjà l'entreprise, des annuaires issus des différents départements ou activités (paye, utilisateurs, technique) ■

5 BONNES RAISONS POUR NE PAS EXTERNALISER LA SÉCURITÉ

À la question « *Pourquoi ne pas avoir externalisé la sécurité ?* », Farid Boulakia répond « *Les délais de mise en œuvre et d'exécution sont relativement longs quand on outsource sa sécurité alors que bien souvent il faut être réactif. Par ailleurs, garder la main sur ce domaine me semble vital. Par ailleurs, notre structure nécessite une souplesse de configuration au niveau des équipements car nos besoins ne sont pas standards et ce genre de services n'est pas facile en passant par des opérateurs. Cela engendre des modifications de contrat alors que la plupart du temps les offres sont pré-packagées. Sans oublier le délai de mise en œuvre de chaque modification demandée ... Au bout du compte le rapport coût-service rendu par la mutualisation n'est plus très bon. Et même le prix est très élevé avec une souplesse d'administration très faible.* »

