



DE LA SÉCURITÉ POUR DES ÉQUIPEMENTS VITAUX ET DES SYSTÈMES DE TRANSPORT

Fondée le 1er janvier 1949, la RATP est une agence de Transport Public dont la mission est la fourniture de transport. La RATP emploie 44 860 personnes pour l'exploitation, l'ingénierie et la maintenance des équipements. Ce réseau englobe les modes de transport variés comme les bus, métro, RER et Tramway. 10 millions de passagers utilisent le réseau de transport RATP chaque jour.



Avec Christian Borne

Responsable de la sécurité des systèmes d'information du département des équipements et systèmes du transport de la RATP

L'OBJECTIF ÉTAIT D'OUVRIER ET DE PROTÉGER DES SYSTÈMES D'INFORMATIONS INTERNES SENSIBLES

« Nous gérons et contrôlons la sécurité des systèmes d'information qui hébergent notre cœur du métier que sont la gestion et la régulation des lignes de métro et RER ainsi que l'alimentation en énergie de l'ensemble des installations appartenant à la RATP », dit Christian Borne. « Dans le passé, ces systèmes d'informations n'avaient pas besoin de communiquer avec l'extérieur, mais, aujourd'hui, ces systèmes doivent pouvoir fournir de l'information à nos clients internes et externes.

Les systèmes doivent donc s'ouvrir tout en garantissant un niveau de sécurité le plus élevé possible.

En dehors de la volumétrie des flux à traiter, des contraintes fortes de disponibilité ont été fixées. Un besoin de maîtrise des systèmes de cloisonnement a été aussi un critère fort de choix de la solution finale. En cas d'incident majeur, il devait être possible d'intervenir sur les systèmes de

protection en dehors de toutes interfaces évoluées de gestion et d'accéder au plus près du cœur de ces systèmes afin de les remettre en configuration de production.

« L'avantage principal pour nous, mise à part la stabilité du système, c'est la maîtrise du système lié à notre grande culture UNIX », dit Christian Borne. « Travailler sur ce type de machine nous va tout à fait. L'équipement que nous avions préalablement tournait également sur une plate-forme UNIX, mais celle-ci n'offrait pas de gestion centralisée ni des fonctionnalités de rapports de logs comme la solution NETASQ. »

Les systèmes devaient en outre s'insérer dans une chaîne de la gestion de la sécurité sans devoir modifier celle-ci pour leur intégration (corrélation de logs, remontées d'alertes, ...).

« Aujourd'hui, nous avons environ 20 appliances NETASQ allant du F50 jusqu'au F1000 », dit Mr. Borne. « Le F1000 est une solution très performante offrant une bonne évolutivité et une haute disponibilité; ils sont installés sur les sites informatiques centraux supportant un trafic élevé et nécessitant une haute disponibilité, même quand l'ensemble du trafic (métro, RER et Tramway) est arrêté et que nos clients ne sont plus sur nos réseaux de transport. »

¹ Régie Autonome des Transports Parisiens.

² Réseau Express Régional.



L'ouverture d'un réseau, d'un système d'information, exige de prendre des précautions, notamment en terme de cloisonnement ; les solutions retenues doivent donc répondre à un cahier des charges et satisfaire à des tests afin de vérifier que celles-ci correspondent bien à notre attente.

Christian Borne



LA SOLUTION ÉTAIT DE MIGRER VERS DES SYSTÈMES NETASQ

« Nous avons préparé le terrain et avons établi un plan de migration. Quand est venu le moment de remplacer les équipements obsolètes, l'opération, qui s'est montrée assez simple, consistait dans un premier temps à récupérer l'ensemble des configurations existantes, puis de les porter sur les nouveaux équipements de protection », dit Christian Borne. Ces opérations, se sont effectuées en nuit et en dehors de toute période d'exploitation des réseaux de transport. Effectivement, même lorsque tous les trains sont garés et que tous les clients sont rentrés chez eux, il reste des agents de la RATP qui assurent des activités de maintenance nécessaires au bon fonctionnement des lignes de RER et des 16 lignes de métro. La migration s'est déroulée sans incident technique notable.

L'ensemble des sites a été migré progressivement et les sites informatiques non équipés l'ont été avec les mêmes préconisations que celles appliquées sur les sites déjà équipés. L'ensemble des systèmes de protection sont administrés avec les outils fournis par la société NETASQ. Christian Borne a souligné que la RATP

utilisait les solutions NETASQ depuis maintenant 4 ans.

UNE ÉTUDE DE MARCHÉ ÉTENDUE ET DES TESTS ONT ÉTÉ NÉCESSAIRES POUR FAIRE CE CHOIX TECHNOLOGIQUE SI IMPORTANT

« En ce qui concerne les pare-feu », a ajouté Christian Borne, « chacun a sa propre façon de choisir son produit. Nous voulions faire un choix technique



Il y a environ 3000 clients (utilisateurs ou système) qui utilisent aujourd'hui les flux qui transitent au travers de nos pare-feux. Les systèmes d'information fonctionnent 24h/24 et 7j/7.

Christian Borne

et non pas un choix guidé par le marché. Cet axe de choix était guidé par la particularité de nos systèmes et des flux transitant au travers de nos systèmes de cloisonnement ».

En s'appuyant sur une étude de marché et sur leurs besoins propres, ils ont identifié un lot de solutions pouvant les satisfaire. « La seconde étape nous a conduit chez les éditeurs de solutions avec un cahier de tests à satisfaire.

Parfois tout se passait bien ; parfois nous trouvions des dysfonctionnements ou des solutions qui ne pouvaient nous satisfaire. Les produits NETASQ ont été retenus à la suite de ces étapes » dit Christian Borne.



LES AVANTAGES CLIENTS

- Système stable fonctionnant sur UNIX
- Une administration centralisée du Firewall
- Migration simple à partir d'anciens systèmes de cloisonnement
- 1 seul disque dur en panne en 4 ans sans arrêt d'exploitation
- Aucun autre incident majeur sur nos systèmes de cloisonnement



A PROPOS DE NETASQ

Fondée en 1998, NETASQ est le premier constructeur européen de solutions de sécurité unifiée destinées aux entreprises de toutes tailles : PME-PMI, Grands Comptes et Administrations. La société conçoit et commercialise des appliances qui associent une technologie unique de Prévention d'Intrusion en Temps Réel, l'ASQ (« Active Security Qualification ») aux fonctions de pare-feu réseau et applicatif, VPN IPSec et SSL, filtrage de continue et sécurisation de la VoIP. Véritable innovateur technologique, NETASQ offre ainsi toutes les fonctions de sécurités indispensables, intégrées dans un seul et même boîtier.