



Patrick Gaudin
Responsable
Télécommunication
systèmes réseaux

« Nous n'avons pas connu d'incidents majeurs sur notre réseau, mais nous savons qu'en cas de problème, notre solution SecurActive nous alertera et nous permettra d'y remédier »

Présentation de Groupe E



Groupe E est un acteur majeur de l'électricité en Suisse occidentale. La société est née le 1^{er} janvier 2005 de la fusion des Entreprises Électriques Fribourgeoises (EEF) et d'Électricité Neuchâteloise SA (ENSA).

Groupe E est active dans le domaine de la production, de la distribution ainsi que de la vente d'énergie et fournit une palette de services associés (télécommunication, ingénierie, contracting chaleur, installations électriques, tableaux électriques, électroménager, etc.). Groupe E dessert un bassin de population d'environ 450'000 habitants pour plus de 268'000 clients et distribue 3 TWh électriques dont 60 % sont produits dans ses propres centrales. Groupe E emploie environ 750 collaborateurs. Son équipe télécom, composée de 12 personnes, opère un réseau de télécommunication et offre des services à des clients internes et externes. Elle gère trois types de réseaux IP : un réseau métier dédié à la conduite centralisée du réseau d'énergie, un réseau opérateur (SDH, Carrier Ethernet et IP) et un réseau d'entreprise LAN/WAN composé de deux data centers d'environ 1'500 adresses IP, 700 téléphones IP et 250 imprimantes sur 30 sites distants. Compte tenu de l'activité de Groupe E, son réseau doit impérativement être disponible 24h/24.

1 - Quelles sont les raisons qui ont motivé l'achat de la solution SecurActive ?

M. Patrick Gaudin, Responsable Télécommunication & systèmes réseaux indique : *« Courant 2007, nous avons entrepris un projet de refonte de notre réseau interne. Ce projet conduira à la modernisation de notre réseau LAN et WAN ainsi qu'à la mise en place d'un nouveau système de téléphonie VoIP. Le trafic de notre réseau interne est principalement de type serveurs de fichiers, messagerie, Web, SAP et VoIP. Jusqu'alors, notre équipe Télécommunications & systèmes réseaux n'avait pas une réelle visibilité de son réseau interne. Avant l'installation de la solution SecurActive, les seules informations dont nous disposions, fournies par le logiciel open source MRTG, étaient des données relatives à la volumétrie globale du trafic. Désormais au bénéfice d'une infrastructure rénovée, il devenait pour nous urgent de posséder une solution offrant une meilleure visibilité du réseau WAN, tant sur le plan de la volumétrie de bande passante que sur la typologie de trafic.*

Nous avons besoin d'une solution capable de nous fournir une vue globale sur notre réseau et d'obtenir des informations sur l'utilisation ainsi que la performance de notre réseau interne en temps réel afin de diagnostiquer et résoudre les éventuels problèmes de manière proactive. Notre équipe réseau n'étant pas extensible, cette solution devait être rapide à mettre en œuvre, intuitive et simple à exploiter.

Après l'évaluation de plusieurs solutions basées sur Netflow qui n'ont pas donné satisfaction, notre intégrateur eb-Qual, en liaison permanente avec notre équipe, nous propose la solution SecurActive.

Séduits par ses fonctionnalités lors de la présentation d'une maquette sur notre réseau interne, nous écartons définitivement les solutions Netflow trop compliquées à configurer et à administrer. »

2 - Comment utilisez-vous la solution SecurActive ?

M. Gaudin : *« Nous avons choisi d'utiliser la solution SecurActive pour détecter et diagnostiquer rapidement non seulement les comportements anormaux et les anomalies de configuration, mais également pour apporter un soutien en cas de problème informatique et trouver la réponse à l'affirmation habituelle « le réseau est lent » remontée par les utilisateurs de Groupe E. »*

Nous utilisons essentiellement les vues Réseau et Performance car nous souhaitons être capables d'identifier tout comportement anormal ou anomalie de trafic sur notre réseau afin de pouvoir intervenir rapidement pour résoudre les dysfonctionnements éventuels.

Nous avons d'ailleurs choisi de désactiver la vue Web, cette fonction assez sensible étant prise en charge par nos proxies. M. Gaudin souligne que le mode Expert est un véritable atout car il permet d'effectuer facilement une capture de trames de manière sélective et programmée dans le but d'examiner en détails l'ensemble des communications. Nous pouvons maintenant sniffer une partie du réseau sans avoir à nous déplacer. Notre objectif est de disposer d'un outil permettant de contrôler le réseau et surtout de réagir en cas de problème : analyser, diagnostiquer et « trouble shooter » ! »

3 - Qui utilise SecurActive au sein de votre équipe ?

M. Gaudin : « La solution SecurActive est utilisée par deux types de populations :

- L'équipe d'exploitation réseau
Grâce à l'implémentation de la solution SecurActive, nous pouvons contrôler le bon fonctionnement de notre réseau au quotidien, identifier un trafic anormal ou des flux non standard, surveiller la bande passante et également détecter la source d'un problème provenant du réseau ou d'une application.
- L'équipe en charge de l'infrastructure serveur et applicatif
L'utilisation de la solution SecurActive a permis à notre responsable infrastructure d'avoir une action préventive sur la gestion des serveurs applicatifs, de fichiers et de messagerie. Il est maintenant en mesure de détecter des anomalies de type « mauvaise configuration serveur », « back-up qui ne se font pas au bon moment » ou encore d'obtenir des informations sur la répartition de charge sur des serveurs en cluster. »

La fonction "Reporting" est principalement utilisée pour contrôler le bon fonctionnement de l'infrastructure serveur et applicatif. **Une fois les rapports configurés, ils sont utilisables très rapidement et facilitent énormément le quotidien de notre responsable infrastructure ».**

4 - Après 6 mois d'utilisation, quel bilan tirez-vous de la solution SecurActive ?

M. Gaudin : « Le projet d'implémentation, réalisé conjointement par nos équipes et eb-Qual, nécessitant peu de ressources et de temps, ne nous a mobilisés que quelques jours. Nous avons constaté que la solution était facile à implémenter et à administrer. Nous avons réalisé ce projet en optant pour le mode transfert de compétences. Il est, en effet, primordial de maîtriser, en interne, un premier niveau de connaissances de la solution. **Nous tirons un premier bilan très positif. Nous avons pu constater la relative bonne santé de notre réseau et de notre infrastructure. SecurActive nous permet de voir en détails ce qui se passe sur le réseau en temps réel (notamment le Top 5 des protocoles qui ne montre que le trafic utile...).** **Auparavant, nous naviguions à vue ! ».**

5 - Quels sont vos prochains projets autour de la sonde SecurActive ?

M. Gaudin : « Aidés par notre partenaire eb-Qual, nous allons ajouter et mettre en place, dans les prochaines semaines, des points de mesures nous permettant d'augmenter la qualité des informations collectées. Nous avons également le projet de rajouter une nouvelle sonde sur notre second data center dans le but d'augmenter le périmètre d'écoute. Nous réfléchissons également à la possibilité de mettre la solution à disposition de notre helpdesk afin de faciliter le premier niveau de diagnostic utilisateur. »



eb-Qual fournit une large palette de produits de gestion du réseau et des services dans le domaine ITC-Security et performance des réseaux. eb-Qual est le partenaire de SecurActive depuis plus d'un an sur la Suisse romande et alémanique. Son expertise autour de la solution SecurActive permet de satisfaire de nombreux clients dans les grandes et moyennes entreprises. www.eb-qual.ch - info@eb-qual.ch