« Avec Telenet, la collaboration a toujours été très enrichissante, basée sur la confiance et la proactivité. »

Bruno Delcourt, responsable du Service Réseaux & Voix de l'Université

Les défis

- Un maximum de sécurité réseau
- Un minimum de contraintes pour les usagers
- Une intégration sans faille à l'architecture existante

Les solutions

- Un pare-feu next-gen Palo Alto Networks
- Accompagnement proactif et installation par Telenet
- Une formation sur l'utilisation du firewall

Les avantages

- Sécurisation globale du réseau
- Gain en confort d'utilisation pour les usagers
- Monitoring et reporting beaucoup plus détaillés

Un pare-feu sur mesure pour l'Université de Namur

Sécuriser un réseau en toute transparence

L'Université de Namur compte aujourd'hui six facultés, soixante-deux laboratoires, environ six mille quatre-cents étudiants et un millier de chercheurs. De nos jours, l'usager de l'Université ne peut plus se passer des outils informatiques, fixes et mobiles. « L'institution doit continuellement adapter ses infrastructures et technologies », nous explique Bruno Delcourt, responsable du Service Réseaux & Voix de l'Université.

Le momentum

« Par rapport à une dizaine d'années en arrière, les gros changements sont d'abord l'évolution des comportements et pratiques des utilisateurs, qui ne se contentent plus de consulter leur boîte e-mail. Ensuite, le nombre d'utilisateurs a explosé ! De même que le nombre d'appareils mobiles pouvant se connecter au réseau. Si l'on compte 2 ou 3 appareils par usager, on arrive à 13 à 18.000 appareils, qui vont *potentiellement* pouvoir se connecter au réseau de l'Université… En plus, les étudiants veulent également accéder à leurs données, partout et tout le temps. », explique Bruno Delcourt. « Nous avons changé de solution parce que nous sentions que des attentes n'étaient plus rencontrées. C'était le *momentum* ! Il était important d'aller au-delà des simples mesures de contrôle des ports. », précise-t-il.

Une question de confiance

« Pour que tout fonctionne, il faut bien entendu un bon produit au départ, mais ce n'est pas suffisant ! Il faut que le partenaire ait du répondant. Cela fait partie des éléments garantissant le succès. » En effet, Bruno Delcourt a pu apprécier la qualité et la richesse des échanges avec les spécia-

listes de Telenet Security, sur les plans technique et commercial, tout au long de l'utilisation de la solution précédente. D'autres éléments ont fini de le convaincre : l'installation sur mesure du nouveau pare-feu, de nouvelle génération (next-gen) Palo Alto Networks, et la formation à son utilisation, sur site.

Un processus continu

Sécuriser un réseau informatique est un processus continu, qui dépasse de loin les caractéristiques techniques d'un outil très performant. « Un des gros challenges était de mettre en place une infrastructure et des mesures, qui tiennent compte de l'hétérogénéité des profils et des besoins, et qui protègent au mieux toutes les personnes, en leur imposant le moins de contraintes possibles. », commente Bruno Delcourt. Faciliter la disponibilité des ressources, en trouvant le juste équilibre, entre respect de la liberté individuelle et contrainte-contrôle, pour le bien de la communauté.

Monitoring et reporting

Un monitoring et un reporting détaillés, par la solution Palo Alto Networks, permettent d'offrir plus de transparence, grâce à des « analyses assez riches, qui vérifient que les mesures mises en place fonctionnent correctement. » Pour Bruno Delcourt, le reporting est également très bien fait : « bien souvent, des captures d'écran suffisent ; je n'ai pas de travail de présentation à fournir en plus. Les non-spécialistes les comprennent facilement ! Nous gagnons donc beaucoup de temps ! »

Des actions et analyses plus fines

Le pare-feu next-gen Palo Alto Networks autorise maintenant des actions plus précises en matière de sécurisation. Il fournit des analyses beaucoup plus fines : elles indiquent les nouvelles tendances sur le réseau et permettent de prévenir les menaces potentielles. « On comprend mieux encore les changements apportés par le nouveau firewall, en prenant l'exemple d'une ville fortifiée du Moyen-Âge, qui aurait évolué vers une ville plus moderne, plus ouverte, mais néanmoins avec un contrôle efficace », explique Bruno Delcourt. En outre, le pare-feu synchronise également au mieux les informations avec les autres systèmes et bases de données, développés en interne à l'Université. « Grâce à lui, c'est tout le réseau de l'Université de Namur qui a gagné en puissance globale et en souplesse ! », reconnaît Bruno Delcourt.

Un feed-back positif

« Le feed-back des utilisateurs est positif parce que le système est resté assez transparent. On continue d'offrir une protection, sans trop perturber l'expérience des utilisateurs vis-à-vis d'Internet. Moins ils perçoivent les solutions de sécurité et plus nous sommes contents ! », se réjouit Bruno Delcourt. « Avec les interfaces intuitives de Palo Alto Networks, il est assez simple et facile de définir des zones réseau différentes, chacune avec des mesures de sécurité particulières. On peut même confier certaines interventions aux autres membres de l'équipe, qui n'y travaillent pas régulièrement. »

Résultats et évolutions

Les résultats obtenus ont été conformes aux attentes de l'Université. L'installation du nouveau firewall Palo Alto Networks et son intégration avec les outils existants se sont déroulées sans incident. Les différents profils utilisateurs ont gagné en confort et souplesse d'utilisation.
De son côté, l'équipe de Bruno Delcourt a pu, elle aussi, se perfectionner. La nouvelle structure est ouverte et évolutive : « les lignes de conduite pourront rester viables pour les 3 à 5 ans à venir. Nous mettons donc en place les fondations d'un système, pour construire des choses solides», conclut Bruno Delcourt.