STORMSHIELD

TÉMOIGNAGE CLIENT

Comment une agence gouvernementale renforce la sécurité de son réseau

INSTITUTION PUBLIQUE

La cybersécurité des institutions publiques est critique, en raison de la nature de leurs activités. Elle l'est d'autant plus lorsqu'il est question d'une agence gouvernementale qui exploite des données sensibles liées à la création d'entreprises sur le territoire malaisien.

C'est pourquoi renforcer la sécurité de son infrastructure réseau pour éviter tout accès extérieur aux données était devenu indispensable pour cette agence malaisienne.

Une infrastructure réseau indépendante pour un meilleur contrôle

L'infrastructure réseau du gouvernement malaisien repose sur deux datacenters dédiés et une mutualisation des équipements réseaux (pare-feux, switchs…) pour la plupart de ses agences, sans aucune possibilité de surveillance et de contrôle pour ces dernières.

Or, l'avènement du télétravail depuis la crise du Covid-19 a révolutionné les besoins de mobilité des collaborateurs de cette agence gouvernementale. Et face à la criticité des données transitant entre les employés, il était devenu essentiel à cette agence de pouvoir s'appuyer sur sa propre infrastructure, en toute indépendance du réseau gouvernemental.

« Notre client est très satisfait des performances du pare-feu SN710 et de la rapidité de déploiement de cette nouvelle infrastructure. D'autres projets sont en cours pour sécuriser son centre de données, notamment le projet Disaster Recovery Center (DCR) qui a été récemment réalisé par Network Transit Asia. »

Un renforcement du niveau de sécurité

Dans le cadre de ce projet, plusieurs intégrateurs et constructeurs de pare-feux ont été sollicités, afin de pouvoir comparer les différentes offres proposées sur le marché. Le client a fait appel à l'intégrateur Network Transit Asia afin de réaliser dans un premier temps un POC (Proof Of Concept) multiproduits.

À l'issue des tests techniques réalisés pendant cette période, c'est la solution Stormshield Network Security qui a été retenue, notamment pour sa fonctionnalité VPN intégrant une authentification renforcée, qui répondait parfaitement aux besoins de mobilité et de communications sécurisées de ce client hautement sensible.

Network Transit Asia a donc ensuite déployé deux pare-feux UTM SN710, positionnés à l'intérieur et à l'extérieur du réseau du client, afin de bloquer tout trafic inconnu et garantir un niveau de sécurité renforcé.

LA SOLUTION MOBILISÉE

→ SN710

Certifié au plus haut niveau européen et conçu pour des organisations de taille moyenne et de grosses agences à architecture complexe, le pare-feu SN710 est un produit modulaire de la gamme d'applications matérielles Stormshield Network Security, avec une sécurité tout-en-un et de multiples fonctionnalités : antivirus, antispam, VPN IPSec, IPS, filtrage web/URL, ...

Le déploiement s'est fait sans aucune difficulté en une semaine, le temps d'implémenter toutes les règles définies sur l'ancienne configuration. Il a fallu ensuite trois semaines supplémentaires pour finaliser plus finement l'ensemble des paramétrages.

« *Notre client est très satisfait des performances du pare-feu SN710 et de la rapidité de déploiement de cette nouvelle infrastructure. D'autres projets sont en cours pour sécuriser son centre de données, notamment le projet Disaster Recovery Center (DCR) qui a été récemment réalisé par Network Transit Asia.* »

« *Leurs compétences et leur savoir-faire technique concernant le produit ont contribué à faciliter le processus d'installation*", a déclaré Izheir Azam Bin Ibrahim Rais, du Business Licensing Electronic Support System (BLESS).