

	Rapport de synthèse	Référence SEC/RP/PBI/041102/IG/01	Date 7 janvier 2003
		Version 1.0	Page 1/1

Cartel Sécurité (<http://www.cartel-securite.fr>) a mené un audit de sécurité sur les plate-formes accélératrices SSL i100, i140, i210, i215, i220 et i225 d'Ingrian Networks (IngrianOS 2.6.2).

Ces équipements proposent des fonctionnalités à la fois complètes et novatrices. Leur finition est excellente. Ils fournissent toutes les fonctionnalités qu'on peut attendre d'un reverse proxy SSL : accélération matérielle, prise en charge des échanges SSL, filtrage des données applicatives, etc. Ils se distinguent surtout par des fonctions inédites comme la possibilité de mettre en place des liens SSL avec les serveurs qu'ils protègent, les allégeant des tâches d'authentification et de négociation SSL qui sont les plus lourdes. On peut également leur demander le chiffrement de champs spécifiques au sein des requêtes traitées pour que ces informations soient stockées de manière sécurisée.

Ces produits, souvent vus comme des équipements réseau, méritent la qualification d'équipements de sécurité et trouvent leur place comme outils à part entière au sein d'une politique de sécurité. En effet, nous avons constaté au cours de notre audit et lors des échanges avec les équipes d'Ingrian Networks, que la sécurité n'a pas été qu'un simple élément rapporté dans l'obtention du produit final, mais a été pensée et appliquée pendant tout le processus de développement. En outre, les équipes d'Ingrian Networks, avec lesquelles nous avons collaboré durant cet audit, ont une très bonne réactivité. La plupart des failles ont été corrigées dans les deux jours. Une prochaine version de leur système d'exploitation devrait corriger la totalité.

Bien qu'interfaçables avec des architectures de PKI, les boîtiers Ingrian Networks ont été pensés comme des points privilégiés de stockage de clés de chiffrement et de certificats, voire d'autorité de certification (CA) : stockage chiffré, éventuellement sur support matériel agréé FIPS 140, environnement applicatif compartimenté, fichiers de configuration chiffrés, authentification par cartes à puce, gestion fine des droits des utilisateurs et administrateurs, sauvegardes chiffrées, mises à jour et extensions validées et signées. Dans le cas du matériel FIPS, nous n'avons pas été capables d'extraire les clés privées des CA, certificats et autres entités cryptographiques.

La sécurité physique de l'équipement est également prise très au sérieux, chose que nous n'avions jusqu'alors pas rencontrée sur ce segment de marché. Enfin, la maturité du produit est probante, en particulier en comparaison de produits concurrents dont certaines fonctionnalités sont en cours d'étude ou de développement.

En conclusion, à l'heure actuelle, les boîtiers Ingrian Networks sont le matériel que nous conseillons à nos clients ayant ce besoin.