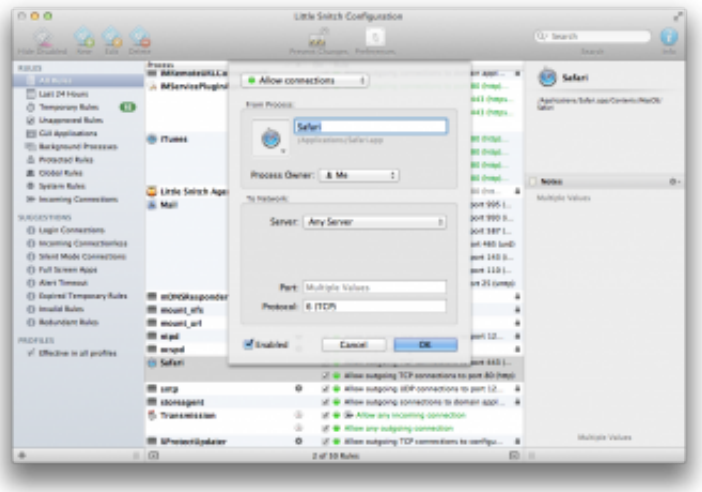
Tuto : Comment configurer le pare-feu Mac Little Snitch ?

Little Snitch gère les connexions sortantes, ce n'est pas le cas du Coupe-feu Mac

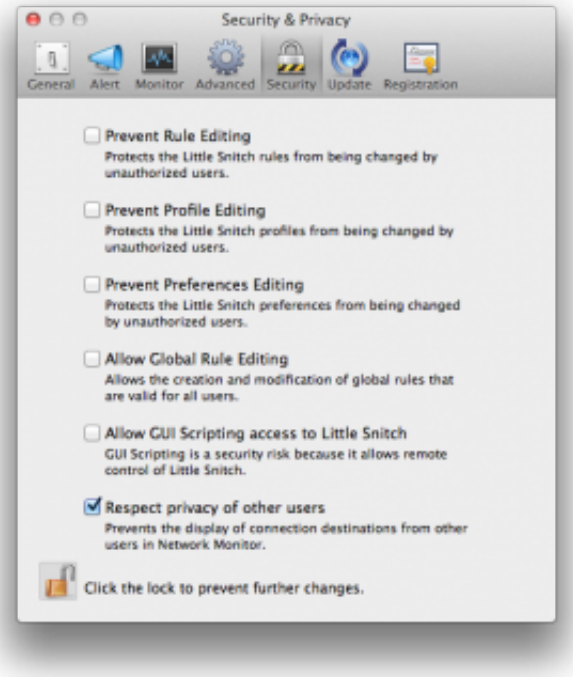
Nous avons récemment consacré un article sur le Coupe-feu du Mac. Ce dernier peut suffire pour l'utilisateur lambda. Une fois activé, le pare-feu Mac filtre les connexions entrantes, par conséquent il peut empêcher au cas par cas les programmes, apps et services que vous définirez d'accepter les connexions de l'extérieur vers votre Mac. La problématique qui se pose pour l'utilisateur avancé est double. Il s'agit de contrôler les connexions entrantes mais aussi les connexions sortantes. Pour cela, il existe plusieurs logiciels payants. Litte Snitch est celui qui nous intéresse aujourd'hui.



Little Snitch un pare-feu bi-directionnel (entrant et sortant)

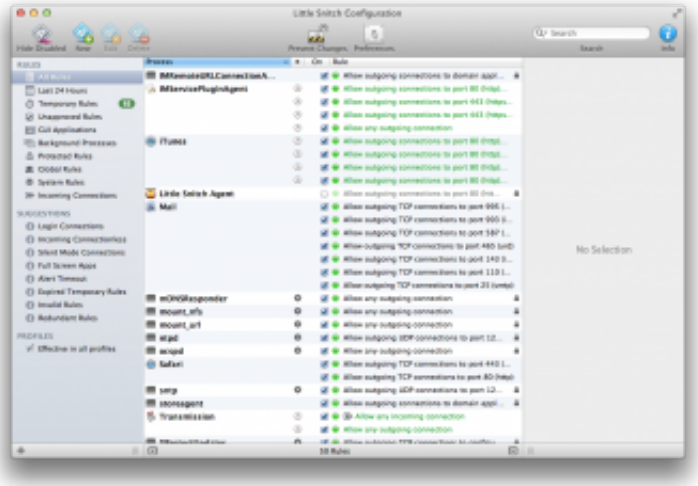
Little Snitch est primordial car il vous permet de gérer les communications de votre ordinateur vers l'extérieur. Un exemple ? Votre ordinateur a besoin d'effectuer la mise à jour d'une app.

Sans Little Snitch et sans votre accord, celle-ci peut s'exécuter. Autre exemple ? Votre Mac transmet des informations sans vous prévenir. Cela peut être grave, s'il s'agit de données personnelles. Il peut s'agit de données de statistiques ou marketing requis par un éditeur logiciel ou pire d'un programme suspect qui journalise vos activités et les envoient à votre insu… C'est à cela que sert le pare-feu Little Snitch à décider quels programmes (ports, protocoles, domaines, hôtes, IP, DNS, adresses Bonjour…) peuvent communiquer avec votre Mac . Little Snich est un pare-feu bi-directionnel, c'est à dire qu'il gère les connexions entrantes et sortantes.



Little Snitch : principe de fonctionnement

Little Snitch est très simple à configurer. Il crée des règles prédéfinies pour quelques programmes (App Store, Safari, Mail, identifiant Apple…) et pour le reste, une fenêtre vous demandera systématiquement ce que vous décidez de faire. Les règles de connexions sont souples et explicites, pour peu qu'on prenne le temps de réfléchir à une stratégie comportementale. Vous pouvez décider de refuser la connexion à un programme, de le laisser toujours communiquer. Les autres choix sont plus complexes et très intéressants. On peut autoriser une app à communiquer uniquement sur un port en particulier, sur un nom de domaine, une seule fois, jusqu'à la fermeture de session, jusqu'au redémarrage du Mac, durant un laps de temps (15 ou 30 min, d'1 à 2h)…



Litte Snitch Configuration : éditer, personnaliser, créer vos règles d'actions

Toutes les règles définies par vos soins avec Little Snitch apparaissent en zone « Temporary Rules » (Règles temporaires). Ces scripts d'actions, de même que les règles prédéfinies peuvent être éditées, peaufinées ou supprimées (bouton contextuel, Edit Rule…). Vous définirez des règles d'actions au fur et à mesure pour iTunes, Google Chrome, Firefox, Filezilla, Skype, Messages, Contacts, Facetime, Transmission… et tous vous autres programmes usuels. Vous créerez également (bouton New)

vos règles pour toutes les nouvelles apps installées. Une fois tout cela effectué, notez que Little Snitch permet même de surveiller le trafic entrant et sortant via Little Snitch Network Monitor qui se glisse dans la barre des menus. Ce peut également être un moyen de déterminer si des connexions suspectes ont lieux. Nous conseillons vivement Little Snitch à ceux qui souhaitent gérer leurs connexions sur le bout des doigts. Il vous en coûtera moins de 30 €, ce qui semble bien raisonnable vu les services qu'il vous rendra !