Préface

Le filtre de paquets d'OpenBSD, Packet Filter (ou PF), jouit d'un grand succès et d'une grande attention depuis sa toute première publication dans OpenBSD 3.0, fin 2001. Packet Filter – dont l'histoire est détaillée plus loin dans ce livre – est né du besoin des développeurs et utilisateurs d'OpenBSD. Depuis sa première version, il a grandement évolué : il est devenu l'outil libre le plus puissant pour jouer le rôle de pare-feu, mais aussi pour équilibrer la charge et gérer le trafic réseau. Combiné à CARP et à `pfsync`, il permet aux administrateurs système de protéger leurs services des attaques, de les fiabiliser grâce à de la redondance, et permet la montée en charge en recourant à des grappes de serveurs gérées via `hoststated`.

Certes, je me suis impliqué dans le développement de Packet Filter ; mais j'en suis d'abord et avant tout un très grand utilisateur. J'emploie cet outil d'une part pour la sécurité – afin de gérer les menaces tant internes qu'externes – et d'autre part pour la fiabilité – pour faire tourner de larges pans d'infrastructures critiques de manière redondante et avec prise en compte de la montée en charge. Cela représente des économies pour mon employeur (l'Université d'Alberta, dont je dirige l'équipe d'administration système), tant en termes de temps d'indisponibilité qu'en termes de matériel et de logiciel. PF vous apportera les mêmes choses.

La complexité est un mal nécessaire quand on travaille avec de telles fonctionnalités. Pour quelqu'un qui connaît bien TCP/IP et OpenBSD, la documentation système de PF est plutôt importante et elle se suffit à elle-même. Mais, malgré les nombreux exemples qu'on y trouve, elle ne peut couvrir en détail tout ce qu'on peut faire avec PF (et les outils qui lui sont associés) sans risquer de devenir verbeuse au point d'être inutile pour les personnes expérimentées, qui en ont besoin en tant que référence.

Ce livre comble ce manque. Si vous êtes nouveau venu, il peut bien sûr vous aider à vous mettre à OpenBSD et à PF. Si vous êtes un utilisateur plus expérimenté, cet ouvrage vous montrera des exemples plus complexes, qui servent dans des cas dépas-

sant ceux de la moyenne. Depuis plusieurs années, Peter N. M. Hansteen est une excellente référence pour les personnes qui apprennent à utiliser PF au-delà de son simple rôle de pare-feu. Ce livre prolonge sa vocation à partager ses connaissances avec autrui.

Les pare-feux sont désormais omniprésents : beaucoup en utilisent un, voire plusieurs. Mais ce livre ne se contente pas de décrire la construction d'un pare-feu ; il enseigne aussi les techniques permettant de manipuler le trafic réseau – dont la compréhension est absolument indispensable à tout administrateur système et réseau. Il est aisé de construire ou d'acheter un pare-feu simple ; en revanche un pare-feu que vous pouvez modifier et gérer par vous-même est plus complexe.

Ce livre vous guidera dans cet apprentissage. Vous comprendrez non seulement comment construire un pare-feu, mais aussi comment PF fonctionne et comment exploiter sa puissance. L'ouvrage que vous tenez entre les mains est un investissement pour bien démarrer, sans faux départs ni temps perdu à bidouiller.

Bob Beck,
Directeur de la Fondation OpenBSD
http://www.openbsdfoundation.org
Edmonton, Alberta, Canada