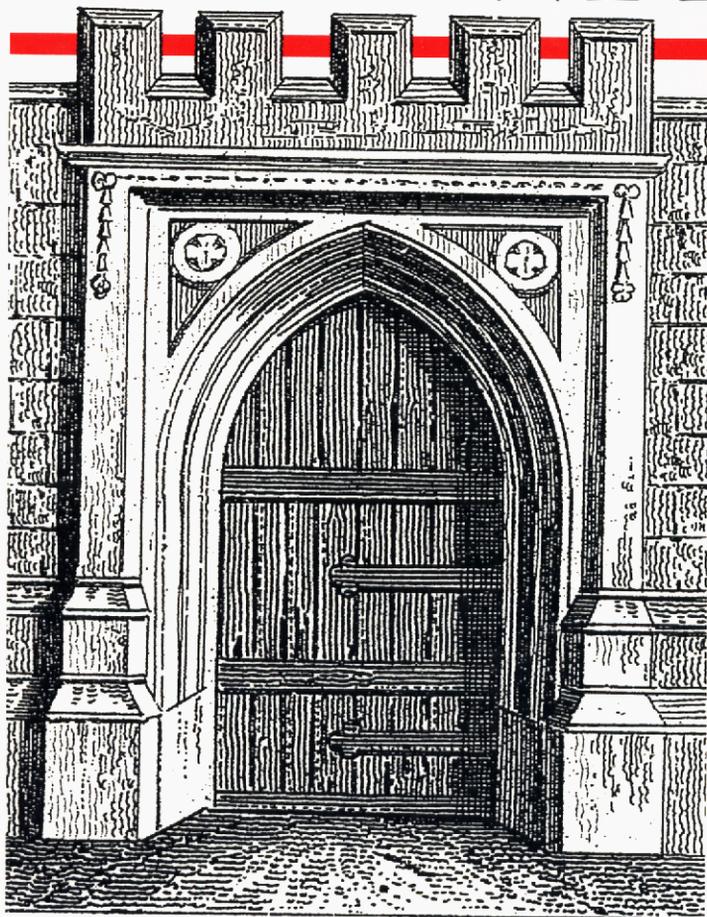


Edition
française

La sécurité sur l'Internet

FIREWALLS



BIBLIOTHEQUE DU CERIST

O'REILLY®

D. Brent Chapman & Elizabeth D. Zwicky
Traduction de Jean Zundel

Firewalls

La sécurité sur l'Internet

BIBLIOTHEQUE DU CERIST

INV: 7384

D. Brent CHAPMAN & Elizabeth D. ZWICKY

157 2605

Firewalls

La sécurité sur l'Internet

Traduction de Jean Zundel

Éditions O'REILLY
18 rue Séguier
75006 Paris
FRANCE

france@oreilly.com
<http://www.editions-oreilly.fr/>

O'REILLY®

Cambridge • Cologne • Paris • Pékin • Sebastopol • Taipei • Tokyo

BIBLIOTHEQUE DU CERIST

157 2605

L'édition originale de ce livre (ISBN 1-56592-124-0) a été publiée aux États-Unis par O'Reilly & Associates sous le titre *Building Internet Firewalls*.

Historique :

– Révision mineure de la traduction française : mai 1999

© O'REILLY & ASSOCIATES, 1995

Couverture conçue par Edie Freedman.

Édition : Xavier CAZIN.

Les programmes figurant dans ce livre ont pour but d'illustrer les sujets traités. Il n'est donné aucune garantie quant à leur fonctionnement une fois compilés, assemblés ou interprétés dans le cadre d'une utilisation professionnelle ou commerciale.

7394

© ÉDITIONS O'REILLY, Paris, 1996
ISBN 2-84177-018-4

Toute représentation ou reproduction, intégrale ou partielle, faite sans le consentement de l'auteur, de ses ayants droit, ou ayants cause, est illicite (loi du 11 mars 1957, alinéa 1^{er} de l'article 40). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée par les articles 425 et suivants du Code pénal. La loi du 11 mars 1957 autorise uniquement, aux termes des alinéas 2 et 3 de l'article 41, les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective d'une part et, d'autre part, les analyses et les courtes citations dans un but d'exemple et d'illustration.

Table des matières

<i>Avant-propos</i>	xvii
<i>Préface</i>	xxi
<i>I Sécurité réseau</i>	1
<i>1 Pourquoi des firewalls Internet ?</i>	3
Qu'essayez-vous de protéger ?	4
Contre quoi essayez-vous de vous protéger ?	7
Comment pouvez-vous protéger votre site ?	14
Qu'est-ce qu'un firewall Internet ?	18
<i>2 Les services de l'Internet</i>	27
Courrier électronique	28
Transfert de fichiers	30
Accès par terminal et exécution de commandes à distance	32
News Usenet	34
World Wide Web	35
Autres services d'informations	37

8 Configuration des services Internet	213
.	216

Particularités du filtrage de paquets NIS/YP	329
Particularités du mandatement de NIS/YP	330
Résumé des recommandations concernant NIS/YP	330
X Window System	330
Particularités du filtrage de paquets X11	331
Résumé des recommandations concernant X11	334
Protocoles d'impression (lpr et lp)	334
Particularités du filtrage de paquets lpr	335
Particularités du mandatement de lpr	335
Particularités du filtrage de paquets et du mandatement de lp	336
Résumé des recommandations concernant les protocoles d'impression	336
Analyse d'autres protocoles	336
9 Deux exemples de firewalls	339
Architecture de sous-réseau à écran	339
Architecture d'hôte à écran	360
10 Authentification et services entrants	369
Les risques dus aux services entrants	370
Qu'est-ce que l'authentification ?	373
Mécanismes d'authentification	377
Systèmes d'authentification complets	383
Chiffrement au niveau réseau	388
Serveurs de terminaux et pools de modems	392
 III Gardez votre site en sécurité	 395
11 Politiques de sécurité	397
Votre politique de sécurité	398
Mise en place d'une politique de sécurité	404
Faire prendre des décisions stratégiques et politiques	407

12 Maintenance des firewalls	415
Les tâches ménagères	415
La surveillance du système	419
Les mises à jour	428
Combien de temps cela prend-il ?	431
Quand devez-vous recommencer ?	432
13 Réagir aux incidents de sécurité	433
Réagir à un incident	433
Que faire après un incident	441
Poursuite et capture de l'intrus	442
Planifiez votre réaction	445
Préparez-vous	454
IV Annexes	461
A Ressources	463
Pages WWW	463
Sites FTP	464
Listes de diffusion	465
Groupes de news	467
Équipes de réaction et autres organisations	468
Conférences	471
Articles	474
Livres	476
B Outils	479
Outils d'authentification	480
Outils d'analyse	481
Outils de filtrage de paquets	483
Outils de mandatement	484
DémonS	485
Utilitaires	486

<i>C Les bases de TCP/IP</i>	489
Introduction à TCP/IP	489
Un modèle de communications de données	491
Architecture des protocoles TCP/IP	494
Couche d'Accès Réseau	496
Couche Internet	497
Couche Transport	502
Couche Application	507
Adressage, routage et multiplexage	509
L'adresse IP	510
Architecture du routage Internet	516
La table de routage	518
Protocoles, ports et sockets	522
Sockets	525