
Table des matières

<i>Préface</i>	<i>i</i>
1. Introduction aux réseaux Linux	1
1.0. Introduction.....	1
2. Mettre en place une passerelle sous Linux	13
2.0. Introduction.....	13
2.1. Se familiariser avec la Soekris 4521.....	15
2.2. Configurer plusieurs profils Minicom.....	18
2.3. Installer Pyramid Linux sur une carte Compact Flash.....	19
2.4. Installer Pyramid en réseau à partir d'une Debian.....	20
2.5. Installer Pyramid en réseau à partir d'une Fedora.....	23
2.6. Amorcer Pyramid Linux.....	25
2.7. Trouver et modifier les fichiers de Pyramid.....	27
2.8. Sécuriser Pyramid.....	28
2.9. Obtenir et installer la dernière version de Pyramid.....	29
2.10. Ajouter des logiciels supplémentaires à Pyramid Linux.....	30
2.11. Ajouter de nouveaux pilotes matériels.....	33
2.12. Personnaliser le noyau de Pyramid.....	34
2.13. Mettre à jour le combIOS de Soekris.....	35
3. Construire un pare-feu avec Linux	37
3.0. Introduction.....	37
3.1. Équipement matériel pour construire un pare-feu sous Linux.....	45
3.2. Configurer les cartes d'interface réseau sous Debian.....	46
3.3. Configurer les interfaces réseau sous Fedora.....	49
3.4. Identifier chaque interface.....	51
3.5. Construire un pare-feu pour adresse IP externe dynamique.....	52
3.6. Construire un pare-feu pour une connexion avec une adresse IP WAN statique.....	57
3.7. Vérifier l'état de votre pare-feu.....	58

3.8.	Désactiver un pare-feu iptables.....	59
3.9.	Activer iptables au démarrage, puis gérer manuellement le pare-feu.....	61
3.10.	Tester son pare-feu	63
3.11.	Configurer le pare-feu pour une administration à distance avec SSH	66
3.12.	Permettre un accès distant par SSH à travers un pare-feu NAT.....	68
3.13.	Obtenir des clés d'hôtes SSH multiples pour une seule adresse IP traduite	70
3.14.	Exécuter des services publics sur des adresses IP privées.....	71
3.15.	Configurer un pare-feu local pour un poste de travail	73
3.16.	Configurer un pare-feu pour un serveur	78
3.17.	Configurer la journalisation d'iptables	81
3.18.	Écrire des règles d'interdiction (Egress).....	82
4.	<i>Créer un point d'accès sans-fil sous Linux</i>	85
4.0.	Introduction.....	85
4.1.	Construire un point d'accès sans-fil sous Linux	89
4.2.	Connecter ensemble un réseau sans-fil et un réseau filaire	90
4.3.	Mettre en place un serveur de noms.....	93
4.4.	Configurer des adresses IP statiques dans le serveur DHCP	96
4.5.	Configurer les clients DHCP statiques sous Linux et sous Windows ..	97
4.6.	Ajouter les serveurs de courrier électronique à dnsmasq	99
4.7.	Rendre WPA2-Personnel presque aussi performant que WPA-Entreprise	100
4.8.	Une authentification Enterprise avec un serveur RADIUS	104
4.9.	Configurer votre point d'accès sans-fil pour utiliser FreeRADIUS....	107
4.10.	Identifier les clients sur FreeRADIUS.....	109
4.11.	Se connecter à Internet et mettre en place un pare-feu	110
4.12.	Utiliser le routage à la place du pont	111
4.13.	Sonder votre carte interface sans-fil	116
4.14.	Changer le nom d'hôte du routeur Pyramid	117
4.15.	Désactiver la diversité d'antennes	118
4.16.	Gérer le cache DNS de dnsmasq.....	119
4.17.	Gérer les caches DNS de Windows.....	123
4.18.	Mettre l'heure à jour au démarrage	124
5.	<i>Mettre en place un serveur de VoIP avec Asterisk</i>	125
5.0.	Introduction.....	125
5.1.	Installer Asterisk à partir du code source	130
5.2.	Installer Asterisk sur Debian	134
5.3.	Démarrer et arrêter Asterisk.....	135
5.4.	Tester le serveur Asterisk.....	138
5.5.	Ajouter des extensions téléphoniques à Asterisk et passer des appels	138
5.6.	Mettre en place des téléphones logiciels.....	146
5.7.	Utiliser réellement la VoIP avec Free World Dialup	148

5.8.	Connecter votre PBX Asterisk à des lignes téléphoniques analogiques.....	151
5.9.	Créer un standardiste numérique	154
5.10.	Enregistrer des instructions vocales personnalisées.....	156
5.11.	Gérer un « message du jour »	159
5.12.	Transférer des appels	161
5.13.	Acheminer des appels vers des groupes de téléphones.....	162
5.14.	Mettre des appels en attente	163
5.15.	Personnaliser la musique d'attente	164
5.16.	Jouer des fichiers MP3 avec Asterisk.....	165
5.17.	Diffuser un message vocal à tous les utilisateurs	165
5.18.	Conférences téléphoniques avec Asterisk	166
5.19.	Surveiller les conférences	168
5.20.	Faire passer le trafic SIP à travers un pare-feu NAT iptables.....	169
5.21.	Faire passer le trafic IAX à travers un pare-feu NAT iptables.....	171
5.22.	Utiliser AsteriskNOW, « Asterisk en 30 minutes »	172
5.23.	Installer et supprimer des paquets sur AsteriskNOW	173
5.24.	Connecter les routards et les utilisateurs distants	175
6.	<i>Routage avec Linux</i>	<i>177</i>
6.0.	Introduction.....	177
6.1.	Calculer des sous-réseaux avec ipcalc	180
6.2.	Mettre en place une passerelle par défaut	182
6.3.	Configurer un routeur local simple	184
6.4.	Configurer un partage de connexion Internet simple.....	186
6.5.	Configurer le routage statique à travers les sous-réseaux	188
6.6.	Pérenniser les routes statiques	190
6.7.	Routage dynamique RIP sous Debian	191
6.8.	Routage dynamique RIP sous Fedora	195
6.9.	Utiliser la ligne de commande de Quagga.....	196
6.10.	Se connecter à distance aux démons de Quagga	198
6.11.	Lancer les démons Quagga à partir de la ligne de commande	199
6.12.	Superviser RIPD	201
6.13.	Mettre des routes sur liste noire avec Zebra	202
6.14.	Routage dynamique simple avec OSPF	203
6.15.	Sécuriser RIP et OSPF	205
6.16.	Superviser OSPFD	206
7.	<i>Administration à distance sécurisée avec SSH</i>	<i>209</i>
7.0.	Introduction.....	209
7.1.	Démarrer et arrêter OpenSSH.....	212
7.2.	Créer des phrases de passe fortes	214
7.3.	S'authentifier simplement avec des clés d'hôte	215
7.4.	Générer et copier les clés SSH	216
7.5.	S'authentifier par clé publique pour protéger les mots de passe du système	218

7.6.	Gérer plusieurs clés d'identité	220
7.7.	Sécuriser OpenSSH.....	220
7.8.	Changer une phrase de passe	222
7.9.	Retrouver l'empreinte d'une clé.....	222
7.10.	Vérifier la syntaxe du fichier de configuration	223
7.11.	Se connecter plus facilement grâce aux fichiers de configuration du client OpenSSH	224
7.12.	Encapsuler X Window dans un tunnel SSH	225
7.13.	Exécuter des commandes sans ouvrir de shell distant.....	227
7.14.	Utiliser des commentaires pour identifier les clés	227
7.15.	Limiter les attaques SSH avec DenyHosts.....	228
7.16.	Créer un fichier de démarrage pour DenyHosts.....	230
7.17.	Monter des systèmes de fichiers à distance avec sshfs	232
8.	Utiliser un bureau graphique universel.....	233
8.0.	Introduction.....	233
8.1.	Connecter Linux à Windows à travers rdesktop	235
8.2.	Créer et gérer les clés SSH pour FreeNX	238
8.3.	Se connecter à Linux depuis Windows avec FreeNX.....	238
8.4.	Se connecter à Linux depuis Solaris, Mac OS X ou Linux avec FreeNX	242
8.5.	Gérer les utilisateurs de FreeNX.....	244
8.6.	Surveiller les utilisateurs de Nxclient depuis le serveur FreeNX.....	244
8.7.	Démarrer et arrêter le serveur FreeNX.....	246
8.8.	Configurer un gestionnaire de bureau personnalisé	247
8.9.	Créer des sessions Nxclient supplémentaires	249
8.10.	Surveiller les sessions Nxclient à l'aide de l'administrateur de sessions NX2	49
8.11.	Activer le partage de fichiers, d'imprimantes et des composants multimédias dans Nxclient2.....	50
8.12.	Empêcher la mémorisation du mot de passe dans Nxclient.....	251
8.13.	Résoudre les problèmes de FreeNX.....	252
8.14.	Contrôler Windows depuis Linux avec VNC	252
8.15.	Contrôler Windows et Linux simultanément avec VNC	254
8.16.	Administrer Linux depuis un poste Linux avec VNC	256
8.17.	Partager le même bureau Windows avec plusieurs utilisateurs distants	258
8.18.	Modifier le mot de passe du serveur VNC sous Linux	260
8.19.	Personnaliser le bureau VNC distant	260
8.20.	Configurer la taille du bureau distant dans VNC	262
8.21.	Connecter VNC à une session X existante	263
8.22.	Encapsuler x11vnc dans un tunnel SSH	264
8.23.	Encapsuler TightVNC entre Linux et Windows	265

9. Des VPN inter-plateformes sécurisés avec OpenVPN	269
9.0. Introduction.....	269
9.1. Mettre en place un environnement de test OpenVPN sécurisé	271
9.2. Démarrer et tester OpenVPN.....	274
9.3. Tester le chiffrement avec des clés statiques	276
9.4. Se connecter à un client Linux distant avec des clés statiques	278
9.5. Créer votre propre infrastructure à clé publique pour OpenVPN....	280
9.6. Configurer le serveur OpenVPN pour des clients multiples	283
9.7. Configurer OpenVPN pour qu'il se lance au démarrage	285
9.8. Révoquer un certificat	286
9.9. Configurer le serveur OpenVPN en mode pont.....	288
9.10. Lancer OpenVPN en tant qu'utilisateur non privilégié	289
9.11. Connecter des clients sous Windows.....	290
10. Monter un serveur VPN PPTP	293
10.1. Introduction	293
10.2. Installer Poptop sous Debian Linux.....	296
10.3. Ajouter la prise en charge de MPPE au noyau Debian	297
10.4. Installer Poptop sous Fedora Linux	299
10.5. Ajouter la prise en charge de MPPE au noyau Fedora	300
10.6. Mettre en place un serveur VPN PPTP indépendant.....	301
10.7. Ajouter votre serveur Poptop à Active Directory	304
10.8. Connecter des clients sous Linux à un serveur PPTP.....	305
10.9. Faire passer PPTP à travers un pare-feu iptables.....	306
10.10. Surveiller votre serveur PPTP	307
10.11. Régler les problèmes de PPTP	308
11. Identification unique avec Samba sur un réseau mixte Linux et Windows.....	311
11.0. Introduction.....	311
11.1. Vérifier que toutes les pièces sont en place.....	313
11.2. Compiler Samba à partir du code source	315
11.3. Démarrer et arrêter Samba.....	318
11.4. Utiliser Samba en tant que contrôleur principal de domaine	319
11.5. Migrer un PDC NT4 vers un contrôleur principal de domaine Samba	323
11.6. Faire entrer Linux dans un domaine Active Directory	325
11.7. Connecter Windows 95/98/ME à un domaine Samba	329
11.8. Connecter Windows NT4 à un domaine Samba	330
11.9. Connecter Windows NT/2000 à un domaine Samba	330
11.10. Connecter Windows XP à un domaine Samba	331
11.11. Connecter un client Linux à un domaine Samba en ligne de commande.....	332
11.12. Connecter un client Linux à un domaine Samba avec une interface graphique.....	335

12. Annuaire réseau centralisé avec OpenLDAP.....	339
12.1. Introduction.....	339
12.2. Installer OpenLDAP sous Debian	346
12.3. Installer OpenLDAP sous Fedora	348
12.4. Configurer et tester le serveur OpenLDAP	348
12.5. Créer une nouvelle base de données sous Fedora.....	351
12.6. Ajouter des utilisateurs à votre annuaire	355
12.7. Corriger des entrées dans l'annuaire	357
12.8. Se connecter à un serveur OpenLDAP distant.....	359
12.9. Effectuer des recherches précises dans votre annuaire LDAP.....	360
12.10. Indexer votre base de données.....	362
12.11. Gérer votre annuaire avec des interfaces graphiques.....	363
12.12. Configurer la base de données Berkeley DB	366
12.13. Configurer la journalisation d'OpenLDAP	370
12.14. Sauvegarder et restaurer votre annuaire.....	372
12.15. Affiner les contrôles d'accès	374
12.16. Modifier les mots de passe	377
13. Surveiller un réseau avec Nagios.....	379
13.0. Introduction.....	379
13.1. Installer Nagios à partir de son code source.....	380
13.2. Configurer Apache pour Nagios	384
13.3. Organiser intelligemment les fichiers de configuration de Nagios	387
13.4. Configurer Nagios pour surveiller l'hôte local	388
13.5. Configurer les permissions CGI pour un accès web complet à Nagios	398
13.6. Lancer Nagios au démarrage	399
13.7. Ajouter des utilisateurs Nagios.....	400
13.8. Accélérer Nagios avec check_icmp.....	401
13.9. Surveiller SSHD.....	402
13.10. Surveiller un serveur web	405
13.11. Surveiller un serveur de courrier électronique.....	408
13.12. Rassembler les services liés avec des groupes de services.....	411
13.13. Surveiller les services de noms	412
13.14. Configurer l'administration distante sécurisée de Nagios avec OpenSSH	413
13.15. Configurer l'administration distante sécurisée de Nagios avec OpenSSL	414
14. Superviser le réseau avec MRTG	417
14.0. Introduction.....	417
14.1. Installer MRTG	418
14.2. Configurer SNMP sous Debian	419
14.3. Configurer SNMP sous Fedora	422
14.4. Configurer le service HTTP pour MRTG.....	422

14.5.	Configurer et démarrer MRTG sous Debian.....	424
14.6.	Configurer et démarrer MRTG sous Fedora.....	427
14.7.	Surveiller la charge active du processeur.....	429
14.8.	Superviser les périodes User et Idle du processeur.....	432
14.9.	Superviser la mémoire physique.....	434
14.10.	Superviser l'espace d'échange et la mémoire.....	435
14.11.	Surveiller l'utilisation du disque.....	436
14.12.	Surveiller les connexions TCP.....	438
14.13.	Trouver et tester les MIB et les OID.....	439
14.14.	Tester les requêtes SNMP distantes.....	440
14.15.	Surveiller les hôtes distants.....	442
14.16.	Créer plusieurs pages d'index pour MRTG.....	443
14.17.	Lancer MRTG en tant que démon.....	444
15.	<i>Faire connaissance avec IPv6.....</i>	447
15.0.	Introduction.....	447
15.1.	Tester la prise en charge d'IPv6 sur votre système Linux.....	452
15.2.	Envoyer des requêtes ping à des hôtes IPv6 lien-local.....	453
15.3.	Établir une adresse unicast unique locale pour une interface.....	455
15.4.	Utiliser SSH avec IPv6.....	456
15.5.	Copier des fichiers avec scp sur un réseau IPv6.....	457
15.6.	Configuration automatique avec IPv6.....	458
15.7.	Calculer des adresses IPv6.....	459
15.8.	Utiliser IPv6 sur l'Internet.....	460
16.	<i>Installer automatiquement de nouveaux systèmes via le réseau.....</i>	463
16.1.	Introduction.....	463
16.2.	Créer des supports de démarrage pour installer Fedora par le réseau.....	464
16.3.	Installer Fedora à travers le réseau.....	466
16.4.	Configurer un serveur d'installation de Fedora par HTTP.....	468
16.5.	Configurer un serveur d'installation de Fedora par FTP.....	469
16.6.	Créer une installation personnalisée de Fedora Linux.....	471
16.7.	Installer Fedora « sans les mains » avec un fichier Kickstart.....	474
16.8.	Installer Fedora à travers le réseau avec PXE Netboot.....	475
16.9.	Installer un système Debian par le réseau.....	477
16.10.	Construire un miroir Debian complet avec apt-mirror.....	479
16.11.	Construire un miroir Debian partiel avec apt-proxy.....	481
16.12.	Utiliser le miroir local depuis vos postes clients.....	483
16.13.	Configurer un serveur d'amorçage Debian à travers le réseau avec PXE.....	483
16.14.	Installer de nouveaux systèmes avec votre miroir local.....	485
16.15.	Automatiser les installations Debian avec des fichiers Preseed.....	486

17. Administrer un serveur Linux avec la console série.....	489
17.0. Introduction.....	489
17.1. Préparer un serveur pour l'administration par console série	491
17.2. Configurer un serveur sans écran avec LILO.....	494
17.3. Configurer un serveur sans écran avec GRUB	497
17.4. Démarrer en mode texte sur Debian	499
17.5. Configurer la console série.....	501
17.6. Configurer votre serveur pour l'administrer par ligne commutée	504
17.7. Se connecter au serveur par ligne commutée	507
17.8. Sécuriser	509
17.9. Configurer la journalisation	510
17.10. Déposer des fichiers sur le serveur	511
18. Un serveur d'accès par ligne téléphonique sous Linux.....	513
18.0. Introduction.....	513
18.1. Configurer un accès unique par ligne téléphonique avec WvDial ...	513
18.2. Configurer plusieurs comptes avec WvDial.....	516
18.3. Rendre la connexion par ligne téléphonique accessible aux utilisateurs autres que root.....	517
18.4. Créer des comptes WvDial pour les utilisateurs non privilégiés	519
18.5. Partager un compte Internet pour l'accès par ligne téléphonique... ..	520
18.6. Mettre en place une connexion à la demande	521
18.7. Planifier la disponibilité de la connexion téléphonique avec cron.....	523
18.8. Composer malgré les tonalités courtes de la messagerie vocale	524
18.9. Neutraliser le service d'appel en attente.....	525
18.10. Conserver le mot de passe ailleurs que dans le fichier de configuration.....	526
18.11. Créer un fichier journal distinct pour pppd.....	527
19. Dépanner un réseau.....	529
19.0. Introduction.....	529
19.1. Configurer un ordinateur portable de diagnostic et de réparation réseau	530
19.2. Tester une connexion avec ping.....	534
19.3. Dresser un profil de votre réseau avec FPing et Nmap	536
19.4. Trouver des adresses IP en double avec arping	538
19.5. Tester le débit et la latence HTTP avec httping.....	540
19.6. Utiliser traceroute, tcptraceroute et mtr pour identifier des problèmes de réseau.....	542
19.7. Utiliser tcpdump pour intercepter et analyser le trafic.....	544
19.8. Intercepter les drapeaux TCP à l'aide de tcpdump	548
19.9. Mesurer le débit, la gigue et les paquets perdus avec iperf	550
19.10. Utiliser ngrep pour la capture avancée de paquets.....	553
19.11. Utiliser ntop pour une surveillance réseau rapide et colorée	555

19.12. Dépanner des serveurs DNS	558
19.13. Dépanner les clients DNS	561
19.14. Dépanner des serveurs SMTP	562
19.15. Dépanner un serveur POP3, POP3s ou IMAP	565
19.16. Créer des clés SSL pour votre serveur Syslog-ng sur Debian	567
19.17. Créer des clés SSL pour votre serveur Syslog-ng sur Fedora	573
19.18. Configurer stunnel pour Syslog-ng	575
19.19. Mettre en place un serveur Syslog.....	576
A. Références essentielles	579
B. Glossaire des termes réseau	583
C. Référence de compilation du noyau Linux.....	609
Compiler un noyau personnalisé.....	609
Index.....	617

*À Terry Hanson-merci !
Grâce à toi, tout cela en vaut la peine.*