Installation de votre nouveau domaine Mini-HOWTO

Christopher Neufeld <neufeld@linuxcare.com>
Traduction française par Geneviève Gracian <ggracian@free.fr> le 7 février 2001 version 0.12 du 17 octobre 2000

Ce document survole les opérations que vous serez probablement amené à réaliser quand vous voudrez mettre en place un réseau d'ordinateurs sous votre propre domaine. Il couvre la configuration du réseau, des services réseau ainsi que les paramétrages relatifs à la sécurité.

Contents

1 Notes

1.1 Mise en garde

Ce texte est une introduction. J'ai passé sous silence beaucoup de choses qui pourraient être présentées bien plus en détail et j'ai, probablement, raté entièrement des paragraphes importants. Toute suggestion concernant des compléments, suppressions, ou aspects sur lesquels je devrais donner plus ou moins de précisions est la bienvenue.

1.2 Nouvelles versions de ce document

La version la plus récente de ce document peut être trouvée à : *http://caliban.physics.utoronto.ca/neufeld/Domain.HOWTO/* .

1.3 Copyright

2 Introduction

Le présent document est un guide pour mettre en place votre propre domaine de machines Linux ou d'un mélange de machines Linux et de machines Windows sur une connexion permanente avec une IP fixe et un domaine propre.

Il n'est pas vraiment approprié pour des installations qui utilisent des adresses IP dynamiques, ou qui sont régulièrement déconnectées de leur fournisseur d'accès pendant de longues périodes ; cependant, des conseils de base pour mettre en place de telles installations figurent dans la section 4.4 (Utiliser une IP dynamique).

Avec la démocratisation des connexions permanentes et des IPs statiques, il est devenu plus aisé pour les personnes et les organisations de mettre en place un véritable domaine avec la présence internet qui y est associée. Une planification rigoureuse peut réduire les problèmes pouvant se poser par la suite.

L'essentiel de ce document décrit les techniques pour mettre en place une sécurité discrète sur le réseau nouvellement exposé. Il traite de la protection contre les attaques extérieures et contre les attaques internes « fortuites ». Il ne prétend pas proposer une une installation extrêmement sécurisée mais en général suffisante pour dissuader les agresseurs les moins obstinés.

Ce document s'adresse en premier lieu à de petites organisations ayant un réseau préexistant, éventuellement une connexion « dial-up » partagée, qui cherchent à évoluer vers une connexion permanente relativement rapide, tant pour mettre en oeuvre des échanges de fichiers avec le monde extérieur que pour créer un site www ou ftp. Il concerne également de nouvelles organisations qui veulent sauter les étapes préliminaires et mettre en place tout de suite une connexion rapide et héberger des services sous leur propre domaine.

Tout au long de ce document, je traiterai de la configuration d'un nouveau réseau enregistré sous le nom de **example.com**. Notez que example.com est réservé par l'IANA pour une utilisation dans les documentations et, par conséquent, ne correspondra jamais à un domaine existant.

La plupart des informations du présent document est disponible ailleurs. J'ai essayé de synthétiser l'essentiel concernant la création d'un nouveau domaine. Si les détails sur un sujet spécifique semblent « simplets », vous pouvez consulter un des documents plus explicites.

Ce document couvrira également le cas d'un environnement mixte composé de plusieurs systèmes d'exploitation. Plus spécialement je suppose que les postes de travail fonctionnent sous Windows, alors que les serveurs et passerelles fonctionnent sous Linux.

3 Définir la topologie de votre réseau

Bien qu'il existe des arguments en faveur de différentes architectures, les exigences de bien des organisations peuvent être satisfaites en intégrant les postes de travail et les serveurs privés dans un réseau privé, et les machines publiques sur des adresses IP externes valides. Les machines possédant les adresses IP publiques seront appelées dans la suite de ce document « hôtes exposés ». Ceci conduit à la topologie suivante (exemple) :

```
+--------------+
|              |                +---------------+
| routeur du   |----------------| serveur FTP   |
| fournisseur  |         |      +---------------+
| d'acces      |         |
|              |         |
+--------------+         |      +----------------+
                         |------| serveur WWW #1 |
                         |      +----------------+
                         |
                         |      +----------------+
                         |------| serveur WWW #2 |
                         |      +----------------+
```

```
                          |
                          ~
                          ~
                          |
                          |      +---------------+
                          |------| passerelle    |
                                 | de reseau     |
                                 | prive         |
                                 +---------------+
                                         |
                                         |
                                         |
                                         |
+------------+                           |      +------------------+
| station #1 |---------------------------|------| serveur prive #1 |
+------------+                           |      +------------------+
                                         |
       .       --------------------|--------        .
       .                           |                .
       .       --------------------|--------        .
                                         |
+------------+                           |      +------------------+
| station #N |---------------------------|------| serveur prive #N |
+------------+                                  +------------------+
```

Dans cet exemple, le routeur du FAI (fournisseur d'accès Internet – provider–), le serveur FTP, les serveurs WWW et la machine désignée comme passerelle de réseau privé ont tous des adresses IP visibles depuis l'extérieur, alors que les stations et les serveurs privés ont des adresses IP réservées pour une utilisation privée. Voir la RFC1918 : *http://www.ietf.org/rfc/rfc1918.txt* ; *http://abcdrfc.free.fr/rfc-vf/rfc1918.html* en version française. Les adresses IP que vous choisissez pour votre réseau privé (tout ce qui est sous votre passerelle de réseau privé) doivent être uniques, mais pas seulement par rapport à l'ensemble des hôtes qui sont sous votre contrôle ; elles ne doivent pas non plus entrer en conflit avec des adresses attribuées dans les autres réseaux privés similaires, sur d'autres sites ou partenaires, avec lesquels vous pourriez vouloir un jour développer un réseau privé virtuel ; et ceci dans le but d'éviter déboires et reconfigurations lorsque les deux réseaux seront reliés de cette manière. Comme indiqué dans la RFC, vous pouvez opter pour un réseau de classe C entre les plages d'adresses 192.168.0.* et 192.168.255.*, un réseau de classe B compris entre les plages d'adresses 172.16.*.* et 172.31.*.*, ou bien, un réseau de classe A 10.*.*.*. Dans la suite de ce document, je supposerai que votre réseau privé (si vous avez choisi d'en créer un) est un réseau de classe C sur la plage 192.168.1.*, que l'interface extérieure de votre passerelle de réseau privé a l'adresse IP 10.1.1.9, une des adresses qui vous ont été allouées par le FAI (notez qu'il ne s'agit pas d'une adresse publique valide, je ne l'utilise que comme exemple). Je supposerai également qu'il y a une machine, betty.example.com à l'adresse 10.1.1.10, qui supporte simultanément le service FTP et le service www.

Faites le compte du nombre d'adresses IP externes dont vous avez besoin pour vos machines. Vous aurez besoin d'une adresse pour chacune des machines installées du coté externe de la passerelle de réseau privé, plus une pour la passerelle elle-même. Ce compte n'inclut pas toute IP qui pourrait être attribuée à d'autres routeurs, adresses de diffusion, etc. Vous devez demander à votre fournisseur d'accès un bloc d'adresses suffisamment grand pour mettre en place toutes vos machines. Par exemple, sur mon réseau professionnel, parmi les huit adresses IP allouées par le FAI, trois n'étaient pas utilisables par mes ordinateurs, laissant la place pour quatre machines à l'extérieur de la passerelle, plus la passerelle elle-même.

Cette topologie de réseau ne vaut pas pour tout le monde, mais elle constitue un point de départ raisonnable pour beaucoup de configurations qui n'ont pas de besoin particulier. Les avantages de cette configuration sont les suivants :

- facilité de développement. Si vous souhaitez doubler le nombre de vos noeuds dans le réseau privé, vous n'avez pas besoin de faire appel à votre fournisseur pour obtenir une plage d'adresses supplémentaire ni reconfigurer l'ensemble des interfaces de vos machines.
- contrôle local du réseau. Ajouter une nouvelle station de travail sur votre réseau privé ne requiert aucune intervention de votre provider, contrairement à l'ajout d'hôtes exposés ; ceux-ci ont besoin d'être cartographiés (connus) dans les bases de données DNS (direct et inversé) s'ils veulent accomplir certaines tâches (ssh et ftpd risquent de se plaindre s'il ne peuvent faire du DNS direct ou du DNS inversé sur des connexions entrantes). Une requête DNS inversé se fait dans le but d'obtenir le nom d'hôte à partir de l'adresse IP.
- sécurité centralisée. La passerelle de réseau privé, en filtrant les paquets et notant les attaques, permet de mettre en vigueur les règles de sécurité sur l'ensemble du réseau privé plutôt que d'avoir à installer de telles mesures sur chacun des serveurs et stations du réseau privé. Ceci est applicable non seulement pour les paquets entrants mais aussi pour les paquets sortants de sorte qu'une station mal configurée ne peut pas, par erreur, diffuser au monde extérieur une information qui doit rester interne.
- déplacement facilité. Du fait que les adresses IP à l'intérieur du réseau privé sont les vôtres pour autant de temps que vous le souhaitez, vous pouvez transposer l'ensemble du réseau sur une nouvelle série d'adresses IP publiques sans avoir à effectuer une quelconque modification de la configuration du réseau privé. Bien sûr, les hôtes publics nécessitent quand même d'être reconfigurés.
- accès à Internet transparent. Les machines du réseau privé peuvent continuer à utiliser FTP, telnet, WWW, et autres services avec un minimum d'embarras moyennant un camouflage « Linux-Masquerading ». Les utilisateurs peuvent même n'avoir jamais conscience que leurs machines n'ont pas d'adresse IP visible depuis l'extérieur.

Les désavantages potentiels de ce type de configuration sont les suivants :

- certains services ne seront pas disponibles directement sur les machines du réseau interne. La synchronisation NTP avec un hôte extérieur, quelques obscurs services dont les règles de masquage ne sont pas supportées dans le noyau, et l'authentification .shosts sur des hôtes externes sont tous difficiles voire impossibles, mais il existe quasiment toujours des procédures de contournement.
- coûts de matériel réseau plus élevé. La passerelle de réseau privé nécessite deux cartes réseau, et vous avez besoin d'au moins deux concentrateurs (hubs) ou commutateurs (switchs), l'un sur le réseau visible, l'autre sur le réseau privé.
- Les machines localisées à l'extérieur du réseau privé ne peuvent pas facilement se connecter sur les machines à l'intérieur du réseau privé. Elles doivent d'abord ouvrir une session sur la passerelle de réseau privé, puis se connecter au travers de celle-ci sur l'hôte interne. Il est possible de router des paquets de manière transparente à travers le pare-feu (firewall), mais ceci n'est pas recommandé pour des raisons de sécurité qui seront abordées plus tard.

Vous devriez tenir compte de tous ces points lors de l'élaboration de la topologie de votre réseau, et décider si un réseau entièrement visible est mieux adapté à votre cas. Dans la suite du document, je supposerai que vous avez configuré votre réseau comme montré ci-dessus. Si vous avez opté pour un réseau entièrement visible, certains détails différeront, et j'essayerai de signaler de telles différences.

Au cas où vous n'auriez pas besoin de serveur externe, le routeur fourni par le provider peut être directement connecté à l'interface externe de la passerelle de réseau privé, plutôt que par l'intermédiaire d'un hub.

4 Vous procurer votre connexion

4.1 Choisir votre fournisseur d'accès

Comme pour tout, prospectez. Déterminez quelle est l'offre de services dans votre région, aussi bien que les coûts associés à chacun de ces services. Toutes les lieux ne sont pas câblés pour DSL, et certaines ne sont pas appropriés pour des connexions sans fils, à cause de contraintes géographiques, architecturales ou environnementales. Dans la mesure où la rapidité des liaisons DSL est intimement liée à la distance entre le point de liaison et le switch, soyez prêt à fournir l'adresse postale du lieu où la tête de votre liaison sera localisée, et posez également des questions précises sur la bande passante entre votre machine et le fournisseur d'accès, sur ce qui doit être fait pour installer la connexion et sur le matériel dont la location est comprise dans le forfait mensuel proposé. Vous devez également avoir une idée du nombre d'adresses IP dont vous avez besoin pour vos machines propres (rappelez-vous que les adresses de la série que vous obtiendrez ne seront pas toutes utilisables pour vos ordinateurs). Demandez au fournisseur d'accès quelle est sa bande passante totale vers l'extérieur car la vitesse déclarée dans sa proposition financière ne concerne que la liaison entre votre site et le sien. Si le provider a une bande passante insuffisante vers l'extérieur, ses clients auront à pâtir de goulots d'étranglements à l'intérieur de son réseau.

Une fois que vous avez présélectionné une liste de candidats, renseignez-vous, voyez si personne ne peut vous conseiller sur les prestataires que vous envisagez. Demandez leur quel type de bande passante ils obtiennent vers des sites non chargés. En outre, si vous avez l'intention d'avoir des connexions rapides entre le nouveau domaine et un accès internet personnel depuis chez vous, pour télétravailler ou bien pour faire de l'administration à distance, il est essentiel que vous fassiez un *traceroute* depuis votre connexion personnelle vers un hôte localisé chez le prestataire envisagé. Ceci vous renseignera sur le nombre de « pas », et la latence auxquels vous devez vous attendre entre chez vous et le nouveau domaine. Des latences supérieures à 100-200 millisecondes peuvent être problématiques pour des utilisations prolongées. Le *traceroute* doit être lancé aux moments de la journée pendant lesquels vous souhaitez utiler une connexion réseau entre votre domicile et le nouveau domaine.

4.2 Faire les préparatifs pour l'installation matérielle

Après avoir choisi le fournisseur et le type d'accès pour le nouveau domaine, renseignez-vous sur les détails de l'installation. Vous pouvez aussi bien avoir besoin d'une prestation de l'opérateur téléphonique en plus de celle du FAI afin de mettre en place l'accès, et les techniciens peuvent avoir besoin d'accéder à des zones contrôlées de vôtre bâtiment ; informez donc votre « responsable de la maintenance immobilière » des nécessités de l'installation. Avant que le technicien de l'ISP n'arrive, demandez les paramètres, tout spécialement les adresses IP, le masque de réseau, l'adresse de diffusion, l'adresse de la passerelle de routage, celle du serveur DNS, et également quel type de câblage est nécessaire pour le matériel apporté par le technicien (par exemple câble droit ou câble croisé RJ45, etc.).

Ayez une machine disponible pour les tests, et installez-la à proximité de l'endroit où le matériel de connexion au réseau sera localisé. Si possible, configurez-la avant que le technicien du prestataire n'arrive en paramétrant son adresse IP et le masque de réseau. Ayez également les câbles appropriés sous la main de façon à ce que les tests puissent être faits rapidement.

4.3 Tester la connexion

Une fois que votre machine de test est reliée au matériel du provider, assurez-vous que vous pouvez faire un *ping* sur une machine au delà du FAI. Si ce n'est pas possible, un *traceroute* vers l'extérieur peut vous aider à localiser la défaillance de la connexion. Si le traceroute ne montre aucun « pas » réussi, cela indique que la configuration réseau de votre machine (route par défaut, adresse de l'interface, pilote de la carte, DNS, etc.) n'est pas bonne. Si un seul « pas » est réussi, cela peut signifier que le routeur n'est pas correctement configuré pour communiquer avec le FAI. Si plusieurs « pas » sont réussis avant la défaillance, le problème est très certainement localisé chez le provider ou bien à l'extérieur, et hors de de votre contrôle immédiat.

4.4 Utiliser une IP dynamique

Les avantages d'une connexion d'entreprise avec une plage d'adresses IP statiques et l'hébergement de divers services entraînent un coût. Elle peut être 10 fois plus onéreuse qu'une connexion personnelle à haut débit avec DSL ou un modem-câble. Si votre budget ne peut supporter une telle connexion ou bien si ce type de connexion n'est pas disponible dans votre région, vous voudrez certainement essayer de mettre en place votre domaine sur une IP dynamique. En général, plutôt qu'une plage d'adresses vous n'obtiendrez qu'une seule adresse, ce qui veut dire que votre passerelle de réseau privé devra également héberger tous les services accessibles depuis l'extérieur.

D'abord vous devriez vérifier si c'est faisable. Beaucoup de contrats de prestataires interdisent explicitement la mise en place de services accessibles depuis l'extérieur sur des comptes personnels. Les prestataires peuvent faire appliquer cette règle par la mise en place d'un filtrage de paquets bloquant les connexions entrantes sur les ports http et FTP. Vous devez également être attentif au fait que la vitesse de transfert mentionnée dans l'offre pour des accès DSL ou modem-câble est la vitesse de la voie descendante, et que la voie montante peut être beaucoup plus lente. La bande passante montante est ce qui est important pour offrir des contenus web ou FTP.

Si vous avez une IP dynamique et que vous voulez avoir des connexions entrantes, vous devez vous inscrire à un service d'hébergement d'IP dynamique tels que ceux listés sur Dynamic DNS Providers (à l'adresse *http://www.technopagan.org/dynamic*). Ces services fonctionnent ordinairement en exécutant un logiciel sur votre machine qui communique votre adresse IP actuelle aux serveurs de l'hébergeur. Quand votre adresse IP est connue de ceux-ci, leurs tables DNS sont mises à jour pour tenir compte de la nouvelle valeur. Vous pouvez aussi obtenir un nom de domaine sous leur nom de domaine, tel que « example.dynip.com » ou bien « example.dynhost.com », ou bien vous pouvez enregistrer votre propre domaine et faire pointer le DNS primaire sur la société fournissant ce service (c'est habituellement plus cher).

Il existe également un service d'hébergement gratuit à Domain Host Services (à l'adresse *http://www.dhs.org*). Ce service semble assez récent et il y a peu de détails sur le site web pour l'instant, mais vous trouverez peut-être que cela vaut le coup d'être étudié.

Si vous avez mis en place une IP dynamique, et que vous êtes abonné à l'un de ces services, cela influera sur certaines décisions que vous ferez dans la section 6 (Décider des services que vous hébergerez). En particulier, cela ne sert à rien de vous abonner à un service d'hébergement d'IP dynamique si vous n'envisagez pas de mettre en place au moins un des services web ou FTP. Vous devrez configurer le DNS primaire de façon à ce qu'il pointe sur la société que vous avez choisie. Vous ne devez pas avoir un démon *named* qui répond à des requêtes émanant de l'extérieur de votre réseau privé. D'autres éléments tels que le transport du courrier électronique, dépendront des spécificités du service auquel vous vous êtes abonné, et peuvent mieux être expliqués par le service d'assistance de cette société.

Une remarque finale : si vous voulez avoir un accès distant à une machine avec une IP dynamique, machine qui n'hébergera pas d'autres services, une solution bon marché est de créer une « boite de dépôt » sur une machine publique avec une IP statique et de faire en sorte que l'hôte ayant une IP dynamique envoie son adresse IP à cet endroit, soit par mél ou tout simplement en l'inscrivant dans un fichier sous un compte shell. Quand vous voulez accéder à distance à votre machine, récupérez d'abord l'adresse IP actuelle dans la « boite de dépôt », puis utilisez *slogin* pour vous attacher directement à cette adresse IP. C'est, somme toute, tout ce que fait un service d'hébergement d'adresses IP dynamiques, il le fait juste de manière automatique au dessus des services standards, vous épargnant des manipulations.

5 Enregistrer un nom de domaine

Afin que les personnes du monde extérieur puissent localiser vos serveurs sous le nom de domaine de votre choix, que ce soit pour le web, pour le FTP ou pour la messagerie électronique, vous devrez enregistrer ce nom de domaine afin qu'il soit intégré dans la base de données du domaine de premier niveau adéquat.

Usez de prudence en choisissant votre nom de domaine. Certains mots ou locutions peuvent être interdits en raison de coutumes locales, ou pourraient être choquants pour des personnes dont le langage ou l'argot diffère de celui de votre région. Les noms de domaine peuvent contenir les 26 caractères de l'alphabet latin (sans accents), le tiret (quoique celui-ci ne peut être mis au début ou la fin du nom), et les dix chiffres. Les noms de domaines ne sont pas sensibles à la casse, et peuvent avoir une longueur maximale de 26 caractères (cette limite est susceptible de changer). Faites attention à ne pas enregistrer un nom de domaine à propos duquel vous ne pouvez pas raisonnablement faire valoir que vous ne saviez pas que celui-ci empétait sur des marques déposées par des sociétés existantes, les tribunaux ne sont pas indulgents pour les « cyber-squatters ». Des informations concernant les situations dans lesquelles votre nom de domaine humblement choisi peut être retiré de votre contrôle sont disponibles dans le document de l'ICANN « Politique pour une résolution des conflits sur les noms de domaines » à l'adresse *http://www.icann.org/udrp/udrp-policy24oct99.htm* (en français : *http://www.juriscom.net/pro/2/ndm20001011.htm*).

Il existe beaucoup de sociétés qui proposent l'enregistrement de noms dans les domaines de premier niveau « .com », « .net » et « .org ». Pour une liste à jour, vérifiez la liste de prestataires conventionnés à l'adresse *http://www.icann.org/registrars/accredited-list.html* . Pour enregistrer un nom dans un domaine de premier niveau géographique, tel que « .fr », « .ca », « .de », « .uk », etc., cherchez quelle est l'autorité appropriée, ce renseignement pouvant être trouvé dans la base de données des Country Code Top-Level Domains à l'adresse *http://www.iana.org/cctld.html* .

6 Décider des services que vous hébergerez

La plupart des fournisseurs d'accès « full-service » proposent à leur clients un éventail de services relatifs au domaine. Ceci est largement dû à la difficulté d'héberger ces services avec certains autres systèmes d'exploitation, plus populaires, pour machines de bureau et serveurs. Ces services sont beaucoup plus faciles à mettre en oeuvre sous Linux et peuvent être hébergés sur des matériels peu onéreux. Vous devriez donc décider des services que vous voulez garder sous votre contrôle. Certains de ces services sont :

- DNS primaire (le service DNS principal pour votre domaine). Voyez la section 6.1 (DNS primaire)
- Messagerie électronique. Reportez-vous à la section 6.2 (Messagerie électronique)
- Hébergement de site web. Reportez-vous à la section 6.3 (Hébergement de site web)
- Hébergement de site FTP. Reportez-vous à la section 6.4 (Hébergement de site FTP)
- Filtrage de paquets. Reportez-vous à la section 6.5 (Filtrage de paquets)

Pour chacun de ces services vous devez évaluer l'intérêt d'en garder le contrôle. Si votre FAI propose un ou plusieurs de ces services, vous pouvez généralement avoir l'assurance qu'il a du personnel expérimenté pour la gestion de ceux-ci ; aussi, vous aurez moins à apprendre et moins de soucis. Parallèlement à cela, vous perdez la maîtrise de ces services. La moindre modification impose que vous passiez par le FAI, chose qui peut ne pas être pratique ou demander des délais plus longs que vous ne le voudriez. Il y a aussi une question de sécurité, le FAI est une cible beaucoup plus tentante pour les agresseurs que votre propre site. Dans la mesure où les serveurs d'un FAI peuvent héberger la messagerie et/ou les sites web de douzaines de sociétés qui sont ses clients, un pirate qui endommage un de ces serveurs obtient une bien meilleure récompense à ces efforts que celui qui attaque votre serveur personnel où les seules données d'une entreprise sont stockées.

6.1 DNS primaire

Quand une personne, quelque part, dans le monde extérieur, demande à se connecter sur une machine du nouveau domaine example.com, les requêtes transitent par des serveurs divers sur internet ; et finalement l'adresse IP de la machine est renvoyée au logiciel de la personne qui demande la connexion. Le détail de cette séquence est au delà de l'objet de ce document. Sans entrer dans les détails, quand une demande est faite pour la machine fred.example.com, une base de données centralisée est questionnée pour déterminer quelle est l'adresse IP de la machine qui a l'autorité administrative sur la zone example.com. L'adresse IP obtenue est ensuite questionnée pour obtenir l'adresse IP de fred.example.com.

Il doit exister un DNS primaire et un DNS secondaire pour chaque nom de domaine. Les noms et adresses de ces deux serveurs sont enregistrés dans une base de données dont les entrées sont contrôlées par des autorités de nommage telles que « Network solutions » (à l'adresse *http://www.networksolutions.com*).

Si vous avez opté pour un DNS primaire hébergé par le FAI, ces deux machines seront probablement contrôlées par celui-ci. À chaque fois que vous voudrez ajouter à votre réseau une machine visible depuis l'extérieur, vous devrez contacter le FAI pour lui demander d'ajouter la nouvelle machine à sa base de données.

Si vous avez choisi de gérer le DNS primaire sur votre propre machine, vous devrez également utiliser une deuxième machine comme serveur secondaire. Techniquement, vous devriez la localiser sur une connexion internet redondante , mais l'hébergement du DNS secondaire sur l'une des machines du FAI est très répandu. Si vous voulez ajouter à votre réseau une machine visible depuis l'extérieur, vous devrez mettre à jour votre propre base de données et ensuite attendre que la modification se propage (chose qui, habituellement, prend un petit nombre d'heures). Ceci vous permet d'ajouter barney.example.com sans passer par votre FAI.

C'est une bonne idée de mettre en oeuvre le DNS secondaire sur un hôte distant du point vue géographique ; ainsi, une simple rupture de câble du coté de votre FAI ne met pas simultanément hors-ligne vos serveurs DNS primaire et secondaire. Le prestataire d'enregistrement de nom que vous avez utilsé pour enregistrer votre domaine peut fournir un service de DNS secondaire. Il existe également un service gratuit, Granite Canyon (à l'adresse *http://www.granitecanyon.com*), disponible pour qui le demande.

Indépendamment du fait que vous avez choisi ou non de constituer vous même l'autorité DNS principale pour votre domaine, voyez la section 7.1 (Mettre en place la résolution de noms) pour une aide concernant la configuration. Vous aurez besoin d'un système de résolution de noms au sein de votre réseau privé, même si vous déléguez le DNS primaire à votre FAI.

6.2 Messagerie électronique

En général, quand vous vous abonnez chez votre FAI, celui-ci vous fournit un certain nombre d'adresses de messagerie. Vous pouvez choisir de n'utiliser que cette possibilité, auquel cas tous les messages entrants sont stockés sur le serveur du FAI et vos utilisateurs lisent leur courrier avec des clients POP3 qui se connectent sur le serveur du FAI. D'une autre manière, vous pouvez décider d'installer la messagerie sur vos propres machines. Une fois de plus, vous devez peser le pour et le contre de chacune des deux possibilités et choisir celle qui vous convient le mieux.

Ce dont il faut se rappeler si vous utilisez les services de l'ISP pour la messagerie :

- Il sera plus facile d'accéder à la messagerie depuis votre domicile, ou depuis d'autres lieux quand vous êtes en déplacement professionnel, en fonction du type de sécurité que vous utilisez pour votre domaine.
- Les messages sont stockés sur les serveurs de l'ISP, ce qui peut poser problème si des données confidentielles sont envoyées sans avoir été chiffrées.
- Vous avez un nombre d'adresses limité, et vous pouvez être amené à payer un supplément si vous dépassez cette limite.

- Pour créer de nouvelles adresses, vous devez passer par le FAI.

Ce dont il faut se rappeler si vous gérez vous-même la messagerie :

- Les messages sont stockés sur vos serveurs, avec des enregistrements de sauvegarde chez l'ISP si votre serveur de messagerie tombe ou si le disque se sature.
- Vous avez un nombre illimité de comptes de messagerie, que vous pouvez créer et supprimer vous-même.
- Vous devez supporter les logiciels clients de messagerie utilisés sur votre réseau privé et, éventuellement, ceux utilisés par les personnes qui essayent de lire leur courrier depuis leur domicile.

Une approche possible est d'héberger la messagerie vous-même et, en supplément, d'utiliser quelques unes des adresses fournies par le FAI. Les personnes qui ont besoin d'une messagerie accessible depuis l'extérieur du réseau privé peuvent avoir des adresses dans votre domaine qui sont redirigées sur l'une des adresses fournies par l'ISP. Les autres peuvent avoir une messagerie locale sur le réseau privé. Ceci requiert un petit peu plus de coordination et de configuration, mais donne plus de flexibilité que chacune des autres approches.

Si vous choisissez d'héberger la messagerie pour votre domaine, reportez-vous à la section 7.3 (Mettre en place la messagerie électronique)

Si vous décidez de ne pas héberger la messagerie pour votre domaine, reportez-vous à la section 7.2 (Configuration du DNS si vous n'hébergez pas le service de messagerie).

6.3 Hébergement du site web

Votre FAI peut vous allouer une certaine quantité d'espace sur ses serveurs web. Vous pouvez décider d'utiliser cette possibilité ou vous pouvez avoir un serveur web que vous mettez dans votre réseau externe, sur une des IPs externes.

Ce dont il faut se rappeler si vous choisissez d'utiliser l'hébergement web du FAI :

- Vous avez une certaine quantité d'espace-disque allouée que vous ne pouvez pas dépasser. Ceci n'inclut pas seulement le contenu du site web mais aussi les données collectées auprès des visiteurs du site.
- La bande passante entre votre serveur web et le monde extérieur sera certainement plus large que si vous hébergiez ce serveur sur votre propre matériel. Dans tous les cas, elle ne peut pas être plus lente.
- Il peut s'avérer difficile d'installer des CGI personnalisées ou des progiciels commerciaux sur votre serveur web.
- La bande passante entre votre réseau et votre serveur web sera certainement plus lente qu'elle ne le serait si vous hébergiez le service sur votre propre réseau.

Ce dont il faut se rappeler si choisissez d'héberger votre propre serveur web.

- Vous avez plus de maîtrise sur le serveur. Vous pouvez façonner votre sécurité de manière plus adaptée à votre utilisation.
- Les données potentiellement critiques, telles que des numéros de cartes de crédit ou des adresses mél, résident sur des machines que vous contrôlez.
- Votre stratégie de sauvegarde est probablement moins complète que celle de votre FAI.

Notez que je ne dis rien à propos du fait que l'ISP a du matériel plus performant, des taux de transfert de données plus élevés, et ainsi de suite. Au fil du temps, ces choses deviennent importantes, et l'on parle de connexions réseaux à très hauts débits, et, très franchement, vous auriez dû déléguer ces décisions à un consultant spécialisé, pas regarder dans un HOWTO Linux.

Si vous choisissez d'héberger l'espace web de votre domaine sur vos propres serveurs, reportez-vous à d'autres documents tels que le WWW-HOWTO (à l'adresse *ftp://metalab.unc.edu/pub/Linux/docs/HOWTO/WWW-HOWTO* ou *http://www.freenix.org/unix/linux/HOWTO/WWW-HOWTO.html* en version française), pour la configuration. Pour des raisons de sécurité, je vous recommande chaudement de faire fonctionner ce service sur une autre machine que la passerelle de réseau privé.

6.4 Hébergement du site FTP

Fondamentalement, les mêmes raisonnements qui s'appliquent à l'hébergement WWW s'appliquent à l'hébergement FTP, à l'exception du fait que le ftp n'est pas concerné par les contenus dynamiques et que les scripts CGI n'y apparaissent pas. La plupart des exploits récents sur des serveurs ftpd ont été réalisés par des débordements de tampon consécutifs à la création de répertoires ayant des noms longs dans des répertoires de téléchargement modifiables par n'importe qui ; ainsi, si votre FAI autorise le téléchargement et se montre négligent dans la maintenance des mises à jour de sécurité sur le serveur FTP, vous feriez aussi bien d'héberger le service vous-même.

Dans le cas où vous choisissez d'héberger FTP pour votre domaine sur vos propres serveurs, assurez-vous d'avoir la dernière version du démon FTP, et consultez les instructions de configuration. Une fois de plus, je recommande fortement, pour des raisons de sécurité, que ce service fonctionne sur une autre machine que la passerelle de réseau privé.

Pour *wu-ftpd*, je recommande les options de configuration suivantes :

- –disable-upload (à moins que n'ayez besoin du téléchargement anonyme)
- –enable-anononly (incite vos utilisateurs locaux à utiliser scp pour le transfert de fichier entre les machines)
- –enable-paranoid (désactive toute fonctionnalité de la version courante qui peut être sujette à caution)

6.5 Filtrage de paquets

Certains FAI mettent des filtres de paquets, pour protéger les utilisateurs du système les uns des autres ou vis à vis d'agresseurs externes. Les réseaux modem-câble et d'autres réseau à diffusion similaires posent problème quand, sans le faire exprès, des utilisateurs de Windows 95 ou 98 activent le partage de fichiers mettant ainsi le contenu entier de leurs disques durs à la vue de n'importe qui prend le soin d'explorer son « voisinnage réseau » à la recherche de serveurs actifs. Dans certains cas, la solution a été de dire aux utilisateurs de ne pas faire cela, mais certains fournisseurs d'accès ont mis en place un filtrage dans le matériel de connexion pour empêcher les gens d'exporter leurs données par inadvertance.

Le filtrage de paquet est vraiment une chose que vous devriez faire vous-même. Il s'intègre facilement dans le noyau fonctionnant sur votre passerelle de réseau privé et vous donne une meilleure idée de ce qui se passe autour de vous. En outre, il arrive souvent que l'on veuille, pendant l'installation, procéder à de menus ajustements sur le pare-feu pour l'optimiser, et c'est beaucoup plus facile à faire en temps réel plutôt que par l'intermédiaire d'un support technique.

Si vous choisissez de faire le filtrage de paquets pour votre domaine, reportez-vous à la section 7.6 (Mettre en place le filtrage de paquets).

7 Configurer les services hébergés

7.1 Mettre en place la résolution de noms

Vous devrez mettre en place un moyen pour que les ordinateurs sur votre réseau se reconnaissent par leur nom, et également que les personnes à l'extérieur connaissent par leur nom vos machines exposées. Il existe plusieurs moyens d'aboutir à ce résultat.

7.1.1 résolution DNS sur le réseau privé, le FAI gère le domaine

(remarque : si vous avez choisi de ne pas mettre en place un réseau privé, allez à la section 7.1.4 (Réseau entièrement exposé, hébergé par le FAI))

Dans cette configuration, vous avez délégué la responsabilité du DNS primaire de votre domaine au FAI. Vous continuez à utiliser DNS à l'intérieur de votre réseau privé quand les hôtes internes veulent communiquer ensemble. Vous avez communiqué au FAI une liste des adresses IP de l'ensemble des hôtes exposés. Si vous voulez qu'une des machines visibles depuis l'extérieur, par exemple betty.example.com, soit en même temps le serveur web et le serveur FTP, vous devez demander au FAI de mettre en place des entrées CNAME www.example.com et ftp.example.com qui pointent sur betty.example.com.

Mettez en place le DNS sur votre passerelle de réseau privé. Ceci peut être réalisé de manière sécurisée, et rendre les mises à jour plus faciles, au cas où vous décidiez un jour d'héberger l'autorité primaire du DNS.

Je supposerai que vous avez décidé d'héberger le DNS sur la machine dns.example.com, qui est la passerelle de réseau privé, et un surnom (alias) pour fred.example.com à l'adresse 192.168.1.1. Si ce n'est pas le cas, de petites modifications doivent être faites à votre configuration. Je ne traiterai pas de cela dans ce HOWTO à moins que cela ne présente un véritable intérêt.

Vous devrez télécharger et compiler une version de BIND, Berkeley Internet Name Domain. Il est disponible sur le site de BIND (à l'adresse *http://www.isc.org/products/BIND/*). Ensuite vous devez configurer les démons. Créez le fichier `/etc/named.conf` suivant :

```
options {
        directory "/var/named";
        listen-on { 192.168.1.1 };
};

zone "." {
        type hint;
        file "root.hints";
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "pz/127.0.0";
};

zone "1.168.192.in-addr.arpa" {
        type master;
        file "pz/1.168.192";
};

zone "example.com" {
```

```
                type master;
                notify no;
                file "pz/example.com";
        };
```

Remarquez que nous nous sommes déclarés maîtres du domaine example.com. Cependant, notre FAI se déclare aussi comme l'autorité du même domaine. Ce n'est pas un problème tant que l'on fait attention à l'installation. Toutes les machines du réseau privé doivent utiliser dns.example.com pour mettre en oeuvre leur résolution de noms. Elles ne doivent *pas* utiliser le « resolver » de l'ISP dans la mesure où le le serveur de nom de l'ISP croit qu'il fait authorité sur l'intégralité du domaine mais ne connait pas les adresses IP ou les noms des machines sur votre réseau privé. De la même manière, les hôtes ayant les adresses publiques de votre domaine *doivent* utiliser le serveur de noms du FAI, pas le serveur de nom privé sur dns.example.com.

Les différents fichiers sous `/var/named` doivent maintenant être créés.

Le fichier `root.hint` est tel que décrit dans la documentation de BIND ou dans le DNS-HOWTO (à l'adresse *ftp://metalab.unc.edu/pub/Linux/docs/HOWTO/DNS-HOWTO* ; *http://www.freenix.org/unix/linux/HOWTO/DNS-HOWTO.html*). À l'heure où j'écris, Ce qui suit est un fichier root.hint valide.

```
     H.ROOT-SERVERS.NET.     6d15h26m24s IN A  128.63.2.53
     C.ROOT-SERVERS.NET.     6d15h26m24s IN A  192.33.4.12
     G.ROOT-SERVERS.NET.     6d15h26m24s IN A  192.112.36.4
     F.ROOT-SERVERS.NET.     6d15h26m24s IN A  192.5.5.241
     B.ROOT-SERVERS.NET.     6d15h26m24s IN A  128.9.0.107
     J.ROOT-SERVERS.NET.     6d15h26m24s IN A  198.41.0.10
     K.ROOT-SERVERS.NET.     6d15h26m24s IN A  193.0.14.129
     L.ROOT-SERVERS.NET.     6d15h26m24s IN A  198.32.64.12
     M.ROOT-SERVERS.NET.     6d15h26m24s IN A  202.12.27.33
     I.ROOT-SERVERS.NET.     6d15h26m24s IN A  192.36.148.17
     E.ROOT-SERVERS.NET.     6d15h26m24s IN A  192.203.230.10
     D.ROOT-SERVERS.NET.     6d15h26m24s IN A  128.8.10.90
     A.ROOT-SERVERS.NET.     6d15h26m24s IN A  198.41.0.4
```

Le fichier `pz/127.0.0.0` est comme suit :

```
@               IN      SOA     example.com. root.example.com. (
                                1       ; numero de serie
                                8H      ; mise a jour
                                2H      ; tentative apres echec
                                1W      ; delai d'expiration
                                1D)     ; duree de vie minimale
                        NS      dns.example.com.
1                       PTR     localhost.
```

Le fichier `pz/1.168.192` est comme suit :

```
$TTL 86400

@       IN      SOA             dns.example.com. root.dns.example.com. (
                                1       ; numero de serie
```

```
                                8H      ; mise a jour            8 heures
                                2H      ; tentative apres echec  2 heures
                                1W      ; delai d'expiration     1 semaine
                                1D      ; duree de vie minimale  1 jour
                        )
                NS      dns.example.com.

1               PTR     fred.example.com.
                PTR     dns.example.com.
                PTR     mail.example.com.
2               PTR     barney.example.com.
3               PTR     wilma.example.com.
```

et ainsi de suite, où vous créez un enregistrement PTR pour chacune des machines ayant une interface sur le réseau privé. Dans cet exemple, fred.example.com est à l'adresse 192.168.1.1 et il est « pointé » par les alias dns.example.com et mail.example.com. La machine barney.example.com est à l'adresse IP 192.168.1.2 et ainsi de suite.

Le fichier `pz/example.com` est comme suit :

```
$TTL 86400

@               IN      SOA     example.com. root.dns.example.com. (
                                1       ; numero de serie
                                8H      ; mise a jour             8 heures
                                2H      ; tentative apres echec   2 heures
                                1W      ; delai d'expiration      1 semaine
                                1D      ; TTL minimale            1 jour
                        )
                        NS              dns.example.com.
        IN              A               192.168.1.1
        IN              MX          10  mail.example.com.
        IN              MX          20  <IP de la machine de mail de l'ISP>.


localhost               A           127.0.0.1
fred                    A           192.168.1.1
                        A           10.1.1.9
dns                     CNAME       fred
mail                    CNAME       fred
barney                  A           192.168.1.2
wilma                   A           192.168.1.3
betty                   A           10.1.1.10
www                     CNAME       betty
ftp                     CNAME       betty
```

Dans la mesure où les machines à l'intérieur du réseau privé n'ont pas intérêt à questionner le serveur de noms du FAI pour une requête sur, disons, betty.example.com, remarquez que nous créons des entrées tant pour les machines localisées à l'intérieur du réseau privé que pour celles ayant des adresses IP externes. Nous déclarons également chacune des deux adresses IP de fred, l'adresse externe et l'adresse interne.

Une ligne dans la section « options » de `/etc/named.conf` appelle une explication :

```
listen-on { 192.168.1.1 };
```

Elle empêche votre démon named de répondre à des requêtes DNS sur son interface externe (toutes les requêtes émanant de l'extérieur doivent passer par le serveur de nom du FAI, pas par le vôtre).

7.1.2 pas de résolution DNS sur le réseau privé, le FAI gère le domaine

(note : si vous avez décidé de ne pas mettre en oeuvre de réseau privé, reportez-vous à la section 7.1.4 (Réseau pleinement exposé, hébergé par le FAI))

Dans cette configuration, vous avez tranché sur le fait que, somme toute, votre réseau est peu étendu et qu'il est improbable qu'il s'étende. Vous avez décidé de ne pas utiliser la base de données centralisée d'un serveur de noms, et, en conséquence, de maintenir la résolution de noms séparément sur chacune des machines. Toutes les machines doivent donc utiliser le serveur de noms de l'ISP pour résoudre les noms d'hôtes situés au delà de la passerelle de réseau privé. Pour la résolution de nom au sein du réseau privé, un fichier des hôtes doit être créé. Sous Linux, cela signifie entrer les noms et les adresses IP de toutes les machines dans le fichier `/etc/hosts` sur chacune des machines. À chaque fois qu'un nouvel hôte est ajouté, ou qu'une adresse IP est changée, ce fichier doit être modifié sur chaque Linuxette.

Comme dans la section 7.1.1 (le DNS est sur le réseau privé, le FAI gère le domaine), la liste des hôtes ayant des adresses IP publiques doit être communiquée au FAI et chaque alias (tels que les noms www et ftp) doit être spécifié dans une entrée CNAME créée par le FAI.

7.1.3 vous êtes l'autorité DNS primaire pour le domaine

Bien que vous puissiez mettre en oeuvre la résolution *named* sur les hôtes exposés, et une base de données privée de résolution pour le réseau privé, je ne m'étendrai pas sur ce cas. Si vous envisagez d'utiliser named pour un service, vous devriez vraiment le faire pour tous, juste pour simplifier la configuration. Dans cette section je supposerai que la passerelle de réseau privé gère la résolution de noms tant pour le réseau privé que pour les requêtes extérieures.

À l'heure où j'écris, sous la version 8.2.2 du paquet BIND, il n'est pas possible pour un démon *named* unique de produire des réponses différenciées en fonction de l'interface sur laquelle arrive la requête. On veut que la résolution de noms se comporte de manière différente si la requête vient du monde extérieur parce que les adresses IP du réseau privé ne doivent pas être envoyées à l'extérieur ; par contre, on doit être capable de répondre à des requêtes émanant du réseau privé. Une réflexion existe sur de nouveaux mot-clé « view » qui pourraient, à l'avenir, être intégrés à BIND pour combler cette lacune, mais, avant que cela ne soit effectif, la solution est de faire fonctionner deux démons *named* avec des configurations différentes.

D'abord, configurez le serveur de noms du domaine privé comme décrit dans la section 7.1.1 (résolution DNS sur le réseau privé, le FAI gère le domaine), il constituera le « resolver » visible depuis le réseau privé.

Ensuite, vous devez mettre en place le DNS de votre domaine de façon à ce qu'il soit visible des hôtes du monde extérieur. D'abord, vérifiez auprès de votre FAI s'il se déléguera lui-même les recherches DNS inversé sur vos adresses IP. Bien que la norme DNS d'origine ne donne pas la possibilité de contrôler le DNS inversé sur des sous-réseaux plus petits qu'un réseau de classe C, une méthode de contournement a été développée qui fonctionne avec tous les clients compatibles DNS et a été ébauchée dans la RFC 2317 (à l'adresse *http://www.ietf.orf/rfc/rfc2317.txt*). Si votre provider accepte de vous déléguer le DNS inversé sur votre série d'adresses IP, vous devez obtenir de lui le nom du pseudo-domaine in-addr qu'il a choisi pour la délégation (la RFC ne propose pas de normalisation pour une utilisation ordinaire) et vous devrez déclarer votre autorité sur ce pseudo-domaine. Je supposerai que le FAI vous a délégué l'autorité et que le nom du pseudo-domaine est 8.1.1.10.in-addr.arpa. L'ISP devra créer des entrées sous la forme :

```
8.1.1.10.in-addr.arpa.     2H IN CNAME 8.8.1.1.10.in-addr.arpa.
9.1.1.10.in-addr.arpa.     2H IN CNAME 9.8.1.1.10.in-addr.arpa.
10.1.1.10.in-addr.arpa.    2H IN CNAME 10.8.1.1.10.in-addr.arpa.
etc.
```

dans son fichier de zone pour le domaine 1.1.10.in-addr.arpa. La configuration de votre fichier de zone 8.1.1.10.in-addr.arpa est donnée plus loin dans cette section.

Si votre provider accepte de vous déléguer le contrôle du DNS inversé, il créera, pour les adresses IP sous votre contrôle, des entrées CNAME dans la table des zones de son DNS inversé qui pointent vers les enregistrements correspondants dans votre pseudo-domaine comme montré ci-dessus. S'il n'envisage pas de vous déléguer l'autorité, vous devrez lui demander de mettre à jour son DNS à chaque fois que vous ajouterez, supprimerez ou changerez le nom d'un hôte visible depuis l'extérieur dans votre domaine. Si la table DNS inversé n'est pas synchronisée avec les entrées DNS direct, certains services peuvent émettre des avertissements ou bien refuser de traiter des requêtes produites par des machines affectées par ce dysfonctionnement.

Vous devez maintenant mettre en place un second *named*, celui là pour traiter les requêtes provenant de machines à l'extérieur de la passerelle de réseau privé.

D'abord, créez un second fichier de configuration, par exemple `/etc/named.ext.conf` pour les requêtes sur l'interface externe. Dans notre exemple, il pourrait être comme suit :

```
options {
        directory "/var/named";
        listen-on { 10.1.1.9; };
};

zone "." {
        type hint;
        file "root.hints";
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "pz/127.0.0";
};


zone "8.1.1.10.in-addr.arpa" {
        type master;
        file "ext/8.1.1.10";
};

zone "example.com" {
        type master;
        notify no;
        file "ext/example.com";
};
```

Les fichiers `root.hint` et `pz/127.0.0`, tous les deux sous/`var/named`, sont partagés par les démons actifs. Le fichier `/ext/8.1.1.10` est comme suit :

```
$TTL 86400

@       IN      SOA             fred.example.com. root.fred.example.com. (
                                1               ; numero de serie
                                10800           ; mise a jour           3 heures
                                3600            ; tentative apres echec  1 heure
                                3600000         ; delai d'expiration     1000 heures
                                86400 )         ; TTL minimale           24 heures
                NS      dns.example.com.
9       IN      PTR     fred.example.com.
                PTR     dns.example.com.
                PTR     mail.example.com.
10      IN      PTR     betty.example.com.
                PTR     www.example.com.
                PTR     ftp.example.com.
```

Le fichier `ext/example.com` contient ce qui suit :

```
$TTL 86400

@               IN      SOA     example.com. root.fred.example.com. (
                                10021   ; numero de serie
                                8H      ; mise a jour           8 heures
                                2H      ; tentative apres echec  2 heures
                                1W      ; delai d'expiration     1 semaine
                                1D      ; duree de vie minimale  1 jour
                        )
                        NS              fred.example.com.
        IN              A               10.1.1.9
        IN              MX          10  mail.example.com.
        IN              MX          20  <machine mail du FAI>.


localhost               A           127.0.0.1
fred                    A           10.1.1.9
betty                   A           10.1.1.10
dns                     CNAME       fred
mail                    CNAME       fred
www                     CNAME       betty
ftp                     CNAME       betty
```

Démarrez les deux démons sur votre passerelle de réseau privé. Mettez ce qui suit dans vos scripts d'initialisation :

```
/usr/sbin/named -u dnsuser -g dnsgroup /etc/named.conf
/usr/sbin/named -u dnsuser -g dnsgroup /etc/named.ext.conf
```

J'ai supposé ici que vous avez créé l'utilisateur sans privilège « dnsuser » et le groupe sans privilège correspondant « dnsgroup ». Si un bogue se fait jour, permettant à un attaquant d'exécuter du code à l'intérieur de *named*, l'agresseur sera limité aux actions permises à un utilisateur sans privilège. Le répertoire `/var/named` et les fichiers qui y sont inclus ne doivent pas être modifiables par « dnsuser ».

Les machines du réseau privé doivent avoir leur résolution de noms réglée pour s'en référer à dns.example.com (à l'IP 192.168.1.1 dans notre exemple) alors que les machines visibles depuis l'extérieur peuvent envoyer leurs requêtes à l'interface externe de la passerelle réseau (à l'IP 10.0.1.9) ou au serveur de noms du FAI.

7.1.4 réseau pleinement exposé, hébergé par le FAI

Dans cette configuration, vous avez choisi d'exposer tous vos hôtes. Vous avez une « véritable » adresse IP pour chacune des machines de votre domaine et vous avez communiqué à votre FAI la liste des noms de machines et de leurs adresses IP. Le FAI vous a donné l'adresse d'un au moins de ses serveurs de noms. Vos machines Linux sont alors configurées pour la résolution de noms dans /etc/resolv.conf :

```
search example.com
nameserver <premier hote DNS>
nameserver <deuxieme hote DNS>
```

Les machines Windows sont configurées de la même manière dans les boites de dialogue de configuration du réseau.

7.1.5 préparer le DNS avant de déplacer votre domaine

Si vous décidez de déplacer votre domaine sur de nouvelles adresses IP, soit parce que vous devez changer de FAI soit parce que vous avez apporté des modifications à vos services et que ceci vous impose de migrer vers de nouvelles adresses IP chez le même FAI, vous devrez faire quelques préparatifs avant la migration.

Vous devez mettre les choses en place de façon à ce que, avant la migration, l'adresse IP demandée par une recherche DNS quelque part dans le monde pointe correctement sur l'adresse IP d'origine et, qu'ensuite, après la migration, elle pointe rapidement sur la nouvelle adresse IP. Des sites distants peuvent avoir mis en cache votre adresse IP, et des requêtes postérieures peuvent obtenir une réponse localement, depuis le cache, plutôt qu'en questionnant les serveurs appropriés. L'effet de ceci peut être que des personnes ayant visité votre site récemment sont dans l'impossibilité de se connecter alors que de nouveaux visiteurs récupèrent des informations valides non mises en cache. Le fait que les serveurs racine ne soient mis à jour que deux fois par jour complique encore plus les choses ; ainsi il est difficile d'accélérer un changement fait à l'identité de vos serveurs DNS primaire et secondaire dans les serveurs racine.

La manière la plus simple de faire la transition est sûrement de dupliquer son site en entier, ou au moins ses composantes visibles publiquement, sur la nouvelle IP, déclarer la modification et attendre que le trafic bascule complètement sur la nouvelle adresse IP. Cependant, ce n'est probablement pas très faisable.

Ce que vous pouvez faire est de vous arranger avec votre nouveau FAI (ou avec votre FAI actuel si vous changez juste d'adresses chez le même FAI) afin qu'il héberge le DNS primaire et le DNS secondaire pendant le transfert. Ceci devrait être fait au moins un jour avant le déplacement. Demandez-lui de positionner la TTL (durée de vie) de cet enregistrement sur quelque chose de suffisamment petit (par exemple 5 minutes). Les exemples de fichier DNS montrés plus haut dans cette section ont tous des valeurs TTL positionnées sur 86400 secondes (1 jour). Si votre TTL est plus longue que cela, vous devrez faire le changement plus longtemps à l'avance. En définitive, voici ce que vous devez faire. Si la configuration actuelle de la TTL de votre domaine est, disons, N heures, alors ce qui suit doit être réalisé plus que N heures avant le déplacement :

- L'enregistrement de votre domaine doit désigner les DNS primaire et secondaire de votre nouvel ISP dans sa base de données racine. Comptez au moins un jour entre le moment où vous soumettez la modification et le moment où cette modification sera prise en compte dans la base de données.

- Les nouveaux DNS primaire et secondaire doivent pointer sur les IP d'origine de votre site avec une TTL très petite.

Remarquez que vous ne pouvez pas accélérer le processus en réduisant la valeur actuelle de la TTL de votre domaine, à moins que vous ne l'ayez déjà fait au moins N heures avant le déplacement.

Maintenant, vous êtes prêt pour le transfert. Migrez vos machines sur les nouvelles adresses IP. Synchronisez ceci avec une mise à jour des enregistrements DNS de votre FAI de façon à ce qu'ils pointent sur les nouvelles adresses. Dans un délai de 5 minutes (la petite TTL que vous avez enregistrée pour le transfert), le trafic devrait avoir basculé sur le nouveau site. Vous pouvez maintenant arranger la section autorisée du DNS à votre goût, vous rendant primaire si c'est ce que vous voulez et repositionant la TTL sur une valeur raisonnablement grande.

7.2 Configuration du DNS si vous n'hébergez pas de service de messagerie

Les configurations décrites dans la section 7.1 (Mettre en place la résolution de noms) ont des enregistrements MX qui pointent sur une machine « mail.example.com ». L'enregistrement MX avec la valeur de priorité la moins grande signale aux sites distants où envoyer le courrier électronique. Les autres enregistrements de MX avec des valeurs de priorité plus élevées sont utilisés comme des échangeurs de mél de secours. Ces « secours » retiendront les messages pendant une certaine durée si l'échangeur primaire n'est pas en mesure, pour une raison quelconque, d'accepter les messages. Dans les exemples de cette section, j'ai supposé que fred.example.com sous son alias de mail.example.com, gère la messagerie pour le domaine. Si vous avez choisi de laisser le FAI héberger de votre messagerie, vous devrez modifier ces enregistrements MX de façon à ce qu'ils pointent sur les machines appropriées du FAI. Demandez à l'assistance technique de votre fournisseur quels sont les noms des hôtes que vous devez utiliser pour les enregistrements MX dans les divers fichiers.

7.3 Mettre en place la messagerie électronique

Si vous avez choisi d'héberger intégralement la messagerie pour votre domaine, vous devrez prendre des mesures spéciales pour les messages entrants sur les hôtes du réseau privé. À moins que vous ne soyez vigilant, les messages ont de fortes chances de rester en rade s'ils attendent sur une machine et que le destinataire correspondant est connecté sur une autre machine. Pour des questions de sécurité, je recommande que les messages entrants ne soient pas accessibles depuis les hôtes publiquement visibles (ceci pouvant aider à dissuader un PHB qui veut que sa station de travail soit sur une adresse IP réelle et qui s'étonne de se faire planter sa machine par un ping de la mort deux fois par jour). Sendmail s'accomode très bien d'un système de distribution de courrier transparent sur le réseau privé. Si quiconque souhaite fournir ici des solutions *testées* pour d'autres démons de messagerie, j'accueille volontiers toute contribution.

7.3.1 Une solution utilisant Sendmail

Afin que les messages délivrés sur un hôte soient accessibles depuis toutes les machines, la solution la plus simple est d'exporter le répertoire de spool de la messagerie avec des droits de lecture/écriture sur l'ensemble du réseau privé. La passerelle de réseau privé se comportera comme un échangeur de messagerie pour celui-ci et doit donc avoir les droits de « root » en ce qui concerne l'écriture sur le disque du répertoire de spool de la messagerie. Les autres clients peuvent ou non rembarrer « root », à votre gré. Ma philosophie générale en matière de sécurité est de ne pas attribuer ces privilèges à moins qu'il n'y ait une bonne raison de le faire, ainsi j'interdis l'utilisateur « root » depuis toutes les machines sauf depuis la passerelle de réseau privé. Ceci a pour effet que root ne peut lire son courrier que depuis cette machine mais ce n'est pas vraiment un handicap sérieux. Notez que le répertoire réseau de spool peut être localisé sur la passerelle de réseau privé elle-même, exporté par NFS, ou qu'il peut être localisé sur l'un des serveurs internes, exporté sur l'ensemble du réseau privé. Si le répertoire de spool réside sur la passerelle de réseau privé, il n'y a pas intérêt à interdire « root » pour cette machine. Si le répertoire de spool est sur un autre serveur, notez que le courrier ne sera pas délivrable si ce serveur, la passerelle, ou le réseau les reliant sont hors-service.

Pour les machines Windows de votre réseau privé, vous pouvez soit mettre en place un serveur POP sur le serveur de mail ou bien utiliser Samba pour exporter le répertoire de spool sur ces machines. Les machines Windows doivent être configurées pour envoyer et recevoir les messages sous un nom d'utilisateur Linux tel que joeuser@example.com, ainsi l'adresse mél de l'hôte est le nom de domaine uniquement, pas un nom de machine tel que barney.example.com. Le serveur SMTP sortant doit être localisé sur la passerelle de réseau privé qui sera chargée de la redirection des messages et de toute réécriture d'adresse.

Ensuite vous devrez configurer Sendmail pour qu'il redirige les messages en provenance des machines du réseau privé et qu'il réécrive les adresses si nécessaire. Récupérez les sources les plus récents depuis le site web de Sendmail à l'adresse *http://www.sendmail.org* . Compilez les exécutables et ensuite allez dans le sous-répertoire `cf/domain` dans l'arborescence source de Sendmail et créez le nouveau fichier suivant : `example.com.m4`.

```
divert(-1)
#
# Copyright (c) 1998 Sendmail, Inc.  All rights reserved.
# Copyright (c) 1983 Eric P. Allman.  All rights reserved.
# Copyright (c) 1988, 1993
#       The Regents of the University of California.  All rights reserved.
#
# Par l'utilisation de ce fichier, vous acceptez les termes et conditions places
# dorenavant dans le fichier LICENCE qui peut etre trouve a la racine
# de la distribution de sendmail
#
#

#
# Ce qui suit est un fichier generique de domaine. Vous devriez pouvoir
# l'utiliser n'importe ou. Si vous voulez le personnaliser, copiez-le dans un fichier
# nomme comme votre domaine et faites les modifications; puis copiez les fichiers .mc
# appropries et changez `DOMAIN(generic)' pour qu'ils renvoient a vos fichiers
# de domaine modifies.
#
divert(0)
define(`confFORWARD_PATH', `$z/.forward.$w+$h:$z/.forward+$h:$z/.forward.$w:$z/.forward')dnl
FEATURE(redirect)dnl
MASQUERADE_AS(example.com)dnl
FEATURE(masquerade_envelope)dnl
```

Ceci définit le domaine example.com. Ensuite vous devez créer les fichiers `sendmail.cf` qui seront utilisés sur le serveur de messagerie (la passerelle de réseau privé), et sur les autres noeuds du réseau privé.

Créez le fichier suivant dans l'arborescence de Sendmail, sous `cf/cf` : `example.master.m4`

```
     divert(-1)
#
# Copyright (c) 1998 Sendmail, Inc.  All rights reserved.
# Copyright (c) 1983 Eric P. Allman.  All rights reserved.
```

```
# Copyright (c) 1988, 1993
#       The Regents of the University of California.  All rights reserved.
#
# Par l'utilisation de ce fichier, vous acceptez les termes et conditions places
# dorenavant dans le fichier LICENCE qui peut etre trouve a la racine
# de la distribution de sendmail
#

#
# Ceci est un fichier prototype pour une configuration qui ne supporte rien
# a part des connexions SMTP de base sur TCP.
#
# Vous devez changer la macro `OSTYPE' pour specifier le systeme d'exploitation
# sur lequel ca va marcher ; cela indiquera la localisation de fichiers de support
# divers pour l'environnement de votre systeme d'exploitation. Vous DEVEZ
# creer un fichier de domaine dans ../domain et le referencer en ajoutant une
# macro `DOMAIN' apres la macro `OSTYPE'. Je vous recommande de
# commencer  par copier ce fichier sous un autre nom de facon a ce que les mises
# a jour de sendmail n'ecrasent pas vos modifications.
#

divert(0)dnl
OSTYPE(linux)dnl
DOMAIN(example.com)dnl
FEATURE(nouucp)
FEATURE(relay_entire_domain)
FEATURE(`virtusertable', `hash /etc/sendmail/virtusertable')dnl
FEATURE(`genericstable', `hash /etc/sendmail/genericstable')dnl
define(`confPRIVACY_FLAGS', ``noexpn,novrfy'')dnl
MAILER(local)
MAILER(smtp)
Cw fred.example.com
Cw example.com
```

Dans cet exemple, on a désactivé les commandes « expn » et « vrfy ». Un agresseur pourrait tester en boucle avec « expn » des alias tels que « personnel » ou « employes » jusqu'à ce qu'il trouve un alias qui lui développe plusieurs noms d'utilisateurs. Il peut alors essayer certains mots de passe médiocres dans le but d'entrer (en supposant qu'il puisse obtenir une invite de login - les réglages de sécurité dans la section 8 (Sécuriser votre domaine) sont définis de façon à ce qu'aucune invite de login ne soit possible pour les attaquants de l'extérieur).

L'autre fichier que vous devez créer définira le sendmail.cf pour les machines esclaves : `example.slave.m4`.

```
divert(-1)
#
# Copyright (c) 1998 Sendmail, Inc.  All rights reserved.
# Copyright (c) 1983 Eric P. Allman.  All rights reserved.
# Copyright (c) 1988, 1993
#       The Regents of the University of California.  All rights reserved.
#
# Par l'utilisation de ce fichier, vous acceptez les termes et conditions places
```

```
# dorenavant dans le fichier LICENCE qui peut etre trouve a la racine
# de la distribution de sendmail
#
#


#
#  Ceci est un prototype pour un << null-client >> -- c'est a dire un client qui
#  ne fait rien a part rediriger tout le courrier vers un echangeur de mail.
#  IL N'EST PAS UTILISABLE EN L'ETAT !!!
#
#  Pour l'utiliser, vous devez utiliser la fonction nullclient avec le nom de
#  de l'echangeur de mail comme argument. Vous DEVEZ egalement definir un
#  `OSTYPE' pour definir la localisation des repertoires de file d'attente et apparentes.
#  En plus, vous POUVEZ selectionner la fonction nocanonify. Cela entrainera
#  l'envoi d'adresses non qualifiees par la connection SMTP; normalement
#  elles sont qualifiees avec le nom de masquage, qui est par defaut le
#  nom de la machine de connexion.
#  A part ca, il ne devrait pas contenir d'autre ligne.
#

divert(0)dnl

OSTYPE(linux)
FEATURE(nullclient, fred.$m)
Cm example.com
```

Vous compilez les fichiers sendmail.cf qui vont bien avec la commande :

```
make example.master.cf example.slave.cf
```

et puis vous copiez les fichiers sur les machines appropriées sous le nom de `sendmail.cf`.

Cette configuration installe la plupart des fichiers de configuration de Sendmail dans le sous-répertoire `/etc/sendmail` et amène *sendmail* à analyser et à utiliser deux fichiers spécifiques, `virtusertable.db` et `genericstable.db`. Pour utiliser ces fichiers spécifiques, créez leurs fichiers source. D'abord, `virtusertable.db` :

```
John.Public@example.com              jpublic
Jane.Doe@example.com                 jdoe@somemachine.somedomain
abuse@example.com                    root
Pointyhaired.Boss@example.com        #phb#@hotmail.com
```

Ceci met en relation les adresses de messagerie du courrier entrant avec de nouvelles destinations. Les messages envoyés à John.Public@example.com sont délivrés localement sur le compte Linux jpublic. Les messages pour Jane.Doe@example.com sont redirigés vers un autre compte de messagerie, éventuellement, dans un domaine différent. Le courrier pour abuse@example.com est envoyé à root et ainsi de suite. L'autre fichier est `genericstable.src` :

```
jpublic                              John.Public@example.com
janedoe                              Jane.Doe@example.com
whgiii                               Pointyhaired.Boss@example.com
```

Ce fichier change le nom de l'expéditeur des courriers sortants provenant de la messagerie locale. Alors qu'il ne peut manifestement pas avoir d'incidence sur l'adresse de retour des messages envoyés directement par jdoe@somemachine.somedomain, il vous permet de réécrire l'adresse des expéditeurs en changeant leurs noms d'utilisateurs internes selon le « plan d'adressage mél » que vous avez choisi. En dernier ressort, créez le fichier `Makefile` suivant dans `/etc/sendmail` :

```
all : genericstable.db virtusertable.db

virtusertable.db : virtusertable.src
        makemap hash virtusertable < virtusertable.src

genericstable.db : genericstable.src
        makemap hash genericstable < genericstable.src
```

Exécutez *make* pour créer les fichiers compilés interprétables par *sendmail*, et n'oubliez pas de ré-exécuter *make* et de redémarrer *sendmail* (ou de lui envoyer un SIGHUP) après toute modification de chacun de ces fichiers « .src ».

7.3.2 Solutions utilisant d'autres MTA (Agents de transfert de mail)

Je n'ai d'expérience que sur Sendmail. Si quiconque souhaite écrire cette section, contactez-moi svp. Sinon, il est possible que j'essaye plus tard de donner moi-même des détails sur des MTA tels que *Postfix*, *Exim* ou *smail*. Je préférerais vraiment que quelqu'un d'autre, qui utilise ces programmes, écrive cette section.

7.4 Mettre en place le serveur web

Pour des raisons de sécurité, vous devriez mettre en place votre serveur web public sur une machine à l'extérieur du réseau privé et non sur la passerelle. Si le serveur web a besoin d'accéder à des bases de données ou à d'autres ressouces entreposées sur le réseau privé, la situation se complique tant du point de vue du réseau que du point de vue de la sécurité. Une telle configuration est hors du champ de ce document.

Les précisions sur l'installation du serveur en lui même peuvent être trouvés dans la documentation d'apache et dans le WWW-HOWTO de Linux à l'adresse *ftp://metalab.unc.edu/pub/Linux/docs/HOWTO/WWW-HOWTO* ou à l'adresse *http://www.freenix.org/unix/linux/HOWTO/WWW-HOWTO.html* en version française.

7.5 Mettre en place le serveur FTP

Une fois encore, votre serveur FTP devrait être localisé sur une des machines visibles depuis l'extérieur et non sur la passerelle de réseau privé. Suivez les indications qui sont fournies avec votre démon FTP. Assurez-vous d'avoir récupéré la version la plus récente car il existe des failles de sécurité dans les vieilles versions de beaucoup de serveurs. Si votre site FTP ne nécessite pas que des utilisateurs anonymes y transfèrent des fichiers, assurez-vous d'avoir désactivé cette fonction dans le démon. Je recommande que la « connexion-utilisateur » (non anonyme) ne soit pas autorisée sur le serveur, ceci impliquant que vos utilisateurs utilisent scp, la commande de copie à distance du shell sécurisé, pour toute mise à jour de fichier qu'ils seraient amenés à faire sur le serveur FTP. Cela donne également aux utilisateurs de bonnes habitudes de sécurité et protège du problème de « routeur hostile » décrit dans la section 8 (Sécuriser votre domaine).

7.6 Mettre en place le filtrage de paquets

Ce sujet est présenté en détail dans la section 8.1 (Configurer votre Pare-feu).

8 Sécuriser votre domaine

Cette section traite de la sécurisation de votre domaine. L'accent est mis sur l'importance de la transparence de cette dernière vis à vis des utilisateurs. Si votre sécurité est trop contraignante et dérange trop les activités de vos utilisateurs, ceux-ci développeront leurs propres procédures de contournement qui peuvent nuire à l'ensemble du domaine. Le meilleur moyen d'éviter ceci est de rendre la sécurité aussi peu contraignante que possible et d'encourager les utilisateurs à vous contacter en premier lieu quand ils ont des difficultés qui pourraient être imputables aux mesures de sécurité du site. Une certaine tolérance est importante. Je sais, d'expérience personnelle, que si le règlement de sécurité est trop rigide, les utilisateurs mettront en place leurs propres tunnels à travers le firewall de façon à pouvoir se loguer depuis l'extérieur du domaine. Il est préférable que les procédures de connexion à distance, ou n'importe quoi d'autre que tentent de faire les utilisateurs soient installées, contrôlées et approuvées par vous.

Cette section traite de la sécurisation de votre réseau contre les agressions extérieures et contre un espionnage factuel depuis l'intérieur. Sécuriser votre site contre une attaque déterminée de la part d'utilisateurs légitimes à l'intérieur du réseau est une tâche beaucoup plus difficile et compliquée et reste hors du champ de ce document.

Un des points de sécurité sur lesquels se base cette section est la protection contre le « routeur hostile ». Le routeur fourni par votre ISP peut constituer à lui seul un ordinateur contrôlable à distance dont le mot de passe est détenu par votre FAI. Il y a eu, dans le passé, des problèmes de sécurité quand les mots de passe constructeur (ceux qui sont utilisés quand le FAI oublie le mot de passe qu'il a attribué) ont été connus par des « pirates ». Si possible, vous devriez planifier votre sécurité en prenant comme hypothèse que le routeur est potentiellement hostile. C'est à dire qu'il pourrait utiliser n'importe quelle adresse dans vos plages publique *ou privée*, qu'il pourrait rediriger les paquets sortants vers un autre site ou qu'il pourrait enregistrer tout ce qui lui passe au travers.

8.1 Configurer votre pare-feu (firewall)

Cette section traite de la configuration d'un routeur de filtrage, de masquage et de transport basé sur *ipchains*. Vous devriez certainement lire d'abord le IPCHAINS-HOWTO (à l'adresse *ftp://metalab.unc.edu/pub/Linux/docs/HOWTO/IPCHAINS-HOWTO* ; *http://www.freenix.org/unix/linux/HOWTO/IPCHAINS-HOWTO.html* en version française) puis chercher ici des conseils additionnels. Ce HOWTO décrit les étapes pour configurer un noyau avec support de masquage (masquerading) et décrit en détail l'utilisation de l'exécutable. Vous devriez activer le pare-feu sur toutes les machines ayant une IP exposée.

Vérifiez vos scripts de démarrage afin de vous assurer que leur enchaînement est comme suit sur la passerelle de réseau privé :

1. la carte Ethernet est initialisée
2. les règles de pare-feu sont passées en revue par ipchains
3. le transport est activé
4. les démons des services réseau sont démarrés

Ainsi, à titre d'exemple, sur un système basé sur la Slackware, la configuration du pare-feu devrait intervenir entre l'exécution du `rc.inet1` et du `rc.inet2`. En outre, si un quelconque problème apparaît au cours des étapes de démarrage du pare-feu, un avertissement devrait être affiché et la carte réseau externe désactivée avant que les services réseau ne soient lancés.

Un problème courant avec les pare-feu basés sur ipchains est de s'assurer que les règles sont correctement positionnées selon que les paquets arrivent sur l'interface de loopback, ou depuis l'une des deux interfaces, interne ou externe. Les paquets d'origine locale peuvent être bloqués par le pare-feu. Trop souvent, ceci est réglé par une espèce de débogage bricolé rapidement où les règles du pare-feu sont manipulées jusqu'à ce que l'application semble fonctionner à nouveau correctement sur le pare-feu. Malheureusement, ceci peut parfois aboutir à un dispositif qui a des trous de sécurité involontaires. Avec ipchains, il est possible d'écrire un script de firewall qui peut être facilement débogué et peut éviter beaucoup de problèmes. Voici un script d'exemple `/sbin/firewall.sh` :

```
#! /bin/sh
#
# Nouveau script de firewalling utilisant IP chains. Cree un routeur filtrant
# avec masquage de reseau
#

# definition de quelques variables

IPCHAINS=/sbin/ipchains

LOCALNET="192.168.1.0/24"       # le reseau prive
ETHINSIDE="192.168.1.1"         # IP privee de fred.example.com #
ETHOUTSIDE="10.1.1.9"           # IP publique de fred.example.com #
LOOPBACK="127.0.0.1/8"
ANYWHERE="0/0"
OUTSIDEIF=eth1                  # interface privee de fred.example.com

FORWARD_PROCENTRY=/proc/sys/net/ipv4/ip_forward

#
# Ces deux commandes retourneront des codes d'erreur si les regles
# existent deja (ce qui se produit si vous executez le script
# de pare-feu plus d'une fois). On met ces commandes avant << set -e >>
# comme ca, dans ce cas le script n'est pas interrompu.

$IPCHAINS -N outside
$IPCHAINS -N portmap

set -e                  # Abandonne immediatement si des erreurs se produisent
                        # lors de l'installation des regles.

#
# Arrete la redirection de ports et initialise les tables

echo "0" > ${FORWARD_PROCENTRY}

$IPCHAINS -F forward
```

```
$IPCHAINS -F input
$IPCHAINS -F output
$IPCHAINS -F outside
$IPCHAINS -F portmap

#
# Masque les paquets en provenance de notre reseau local
# a destination du monde exterieur. Ne masque pas les
# paquets locaux a destination locale.

$IPCHAINS -A forward -s $LOCALNET -d $LOCALNET -j ACCEPT
$IPCHAINS -A forward -s $ETHOUTSIDE -d $ANYWHERE -j ACCEPT
$IPCHAINS -A forward -s $LOCALNET -d $ANYWHERE -j MASQ

#
# Positionne les signaux de priorite. Delais minimum
# de connexion pour www, telnet, ftp et ssh (paquets sortants
# uniquement).

$IPCHAINS -A output -p tcp -d $ANYWHERE www -t 0x01 0x10
$IPCHAINS -A output -p tcp -d $ANYWHERE telnet -t 0x01 0x10
$IPCHAINS -A output -p tcp -d $ANYWHERE ftp -t 0x01 0x10
$IPCHAINS -A output -p tcp -d $ANYWHERE ssh -t 0x01 0x10

#
# n'importe quel paquet venant de notre classe C locale doit
# etre accepte comme le sont les paquets provenant de l'interface
# de loopback  et l'interface externe de fred

$IPCHAINS -A input -s $LOCALNET -j ACCEPT
$IPCHAINS -A input -s $LOOPBACK -j ACCEPT
$IPCHAINS -A input -s $ETHOUTSIDE -j ACCEPT

#
# On va creer un jeu de regles pour les paquets provenant du grand,
# mechant monde exterieur, et puis y attacher toutes les interfaces
# externes. Ces regles seront appelees << outside >>.
#
# On cree egalement une chaîne << portmap >>. Les sockets utilisees
# par les demons references par le portmapper RPC ne sont pas
# fixes, il est donc un peu difficile de leur attribuer des
# regles de filtrage. La chaîne portmap est configuree dans un
# script a part.

#
# Paquets envoyes depuis n'importe quelle interface exterieure
# a la chaîne << outside >>. Ceci inclut l'interface $OUTSIDEIF
# et toute interface ppp utilisee pour se connecter (ou fournir
# une connexion).
```

```
$IPCHAINS -A input -i ${OUTSIDEIF} -j outside
$IPCHAINS -A input -i ppp+ -j outside

###################################################
#
#  installe les regles de la chaîne << outside >>  #
#
###################################################

#
# Personne de l'exterieur ne devrait pouvoir se faire
# passer comme venant de l'interieur ou du loopback.

$IPCHAINS -A outside -s $LOCALNET -j DENY
$IPCHAINS -A outside -s $LOOPBACK -j DENY

#
# Aucun des paquets routes vers notre reseau local
# ne peut venir de l'exterieur car l'exterieur
# n'est pas cense connaître nos adresses IP privees.

$IPCHAINS -A outside -d $LOCALNET -j DENY

#
# Bloque les connexions entrantes sur les ports X. Bloque 6000 a 6010.

$IPCHAINS -l -A outside -p TCP -s $ANYWHERE -d $ANYWHERE 6000:6010 -j DENY

#
# Bloque les ports NFS 111 et 2049.

$IPCHAINS -l -A outside -p TCP -s $ANYWHERE -d $ANYWHERE 111 -j DENY
$IPCHAINS -l -A outside -p TCP -s $ANYWHERE -d $ANYWHERE 2049 -j DENY
$IPCHAINS -l -A outside -p UDP -s $ANYWHERE -d $ANYWHERE 111 -j DENY
$IPCHAINS -l -A outside -p UDP -s $ANYWHERE -d $ANYWHERE 2049 -j DENY

#
# Bloque les paquets xdm venant de l'exterieur, port UDP 177.

$IPCHAINS -l -A outside -p UDP -s $ANYWHERE -d $ANYWHERE 177 -j DENY

#
# Bloque le port 653 YP/NIS .

$IPCHAINS -l -A outside -p TCP -s $ANYWHERE -d $ANYWHERE 653 -j DENY

#
# On ne va pas s'embeter avec des logins sur le port TCP 80, le port www.

$IPCHAINS -A outside -p TCP -s $ANYWHERE -d $ANYWHERE 80 -j DENY
```

```
#
# Accepte des connexions donnees et controle FTP.

$IPCHAINS -A outside -p TCP -s $ANYWHERE 20:21 -d $ANYWHERE 1024: -j ACCEPT

#
# Accepte les paquets ssh.

$IPCHAINS -A outside -p TCP -s $ANYWHERE -d $ANYWHERE ssh -j ACCEPT

#
# Accepte les paquets DNS depuis l'exterieur.

$IPCHAINS -A outside -p TCP -s $ANYWHERE -d $ANYWHERE 53 -j ACCEPT
$IPCHAINS -A outside -p UDP -s $ANYWHERE -d $ANYWHERE 53 -j ACCEPT

#
# Accepte SMTP depuis partout.

$IPCHAINS -A outside -p TCP -s $ANYWHERE -d $ANYWHERE 25 -j ACCEPT

#
# Accepte les paquets NTP.

$IPCHAINS -A outside -p UDP -s $ANYWHERE -d $ANYWHERE 123 -j ACCEPT

#
# N'accepte pas les paquets d'indentification, on ne les utilise pas.

$IPCHAINS -A outside -p TCP -s $ANYWHERE -d $ANYWHERE 113 -j DENY

#
# Desactive et journalise tous les autres paquets entrants,
# TCP ou UDP, sur les ports privilegies.

$IPCHAINS -l -A outside -p TCP -s $ANYWHERE -d $ANYWHERE :1023 -y -j DENY
$IPCHAINS -l -A outside -p UDP -s $ANYWHERE -d $ANYWHERE :1023 -j DENY

#
# Controle base sur les regles de portmapper.

$IPCHAINS -A outside -j portmap

##############################################
#
#  Fin des regles de la chaîne << outside >>   #
#
##############################################
```

```
#
# Bloque les paquets rwho sortants.

$IPCHAINS -A output -p UDP -i $OUTSIDEIF -s $ANYWHERE 513 -d $ANYWHERE -j DENY

#
# Empeche les paquets netbios de s'echapper.

$IPCHAINS -A output -p UDP -i $OUTSIDEIF -s $ANYWHERE 137 -d $ANYWHERE -j DENY

#
# Active le routage.

echo "1" > ${FORWARD_PROCENTRY}
```

Remarquez que le pare-feu peut être utilisé non seulement pour les paquets entrants mais aussi pour les paquets sortants qui pourraient dévoiler des informations sur votre réseau privé tels que des paquets « rwho » ou « netbios ».

Comme noté plus haut, les règles du portmapper sont légèrement différentes car les démons portmap s'abonnent eux-mêmes au portmapper et sont renseignés sur les ports à écouter. Les ports utilisés par un démon quelconque peuvent changer si vous modifiez les services RPC utilisés ou si vous changez leur ordre de démarrage. Le script suivant, `/sbin/firewall.portmap.sh`, génère les règles pour le démon portmap.

```
#! /bin/sh
#
ANYWHERE=0/0

IPCHAINS=/sbin/ipchains

$IPCHAINS -F portmap

# Regles pour empecher l'acces aux services portmappes aux personnes de l'exterieur.
#
/usr/bin/rpcinfo -p | tail +2 | \
        { while read program vers proto port remainder
          do
             prot=`echo $proto | tr "a-z" "A-Z"`
             $IPCHAINS -l -A portmap -p $prot -s $ANYWHERE -d $ANYWHERE $port -j DENY || exit 1
          done
             }
```

Nous n'avons pas à nous soucier du fait que les paquets entrants sont des paquets « légitimes » en provenance du réseau privé ou non, la chaîne portmap n'est vérifiée que quand les paquets proviennent de l'extérieur.

Cette configuration de pare-feu note la plupart des paquets suspects par l'intermédiaire de klogd avec la priorité kern.info. Elle notera les essais de connexion normaux aussi bien que tous les scans furtifs connus.

Maintenant on assemble le tout. On aimerait s'assurer qu'il n'existe pas de petite fenêtre de vulnérabilité au démarrage du système, en conséquence on configure la séquence de démarrage comme suit :

```
#! /bin/sh
```

```
#
# Demarrer le reseau de facon securisee
#
#
/etc/rc.d/rc.inet1              # configure les interfaces reseau
                                # et active le routage.
/sbin/firewall.sh || { echo "la configuration du pare-feu a echoue"
                       /sbin/ifconfig eth1 down }

/sbin/ipchains -I outside 1 -j DENY     # interdit tous les paquets entrants

/etc/rc.d/rc.inet2              # demarre les demons reseau

sleep 5                         # les laisse se stabiliser

# securise les service portmappes
/sbin/firewall.portmap.sh || { echo "la configuration du pare-feu de portmap a echoue"
                               /sbin/ifconfig eth1 down }

/sbin/ipchains -D outside 1       # autorise les paquets entrants
```

Ceci suppose que eth1 est l'interface ayant l'adresse IP visible. Si la moindre erreur a lieu lors de l'installation d'une des règles d'ipchains, un avertissement est produit et cette interface est désactivée. La chaine « outside » est positionnée de manière à refuser tous les paquets avant que les démons de service réseau ne soient démarrés, parce que les règles de pare-feu ne sont pas encore en place pour les services portmappés. Une fois que ces services sont protégés par le pare-feu, la chaîne « outside » est rendue à son comportement normal.

8.2 Configurer OpenSSH ou SSH1

à l'heure où j'écris, Open SSH, aussi bien que SSH1, offre désormais des possibilités de configuration permettant d'intégrer *scp*, *ssh* et *slogin* comme des exécutables sous les noms *rcp*, *rsh* et *rlogin* avec un retour transparent, dans les programmes clients ssh, aux *rsh*, *rcp* ou *rlogin* d'origine quand le site distant n'exécute pas *sshd*. Faire en sorte que l'invocation de *rsh* exécute à sa place le client *ssh* est, à mon avis, important pour conserver une sécurité facile à utiliser et pour en décharger les utilisateurs. Les scripts de tout le monde, les configurations de *rdist*, etc. continueront à fonctionner sans modification si le site distant exécute *sshd*, mais les données seront envoyées chiffrées avec une forte certification de l'hôte. La réciproque n'est pas toujours vraie. Tout spécialement si la machine distante n'exécute pas sshd, le programme *rsh* enverra un message à l'écran, avertissant que la connexion n'est pas chiffrée. Ce message provoque une erreur avec *rdist* et probablement avec d'autres programmes. Il ne peut être supprimé par des options en ligne de commande ou de compilation. Pour *rdist*, une solution est d'appeler le programme avec `-p /usr/lib/rsh/rsh`.

Récupérez ssh1 depuis le site de ssh (à : *http://www.ssh.org*), ou OpenSSH depuis son site (à : *http://www.openssh.org*), et compilez-le pour remplacer les « programmes en r » (*rsh*, *rlogin* et *rcp*) non chiffrés. D'abord, copiez ces trois fichiers dans `/usr/lib/rsh`, puis configurez le paquet ssh avec :

```
./configure --with-rsh=/usr/lib/rsh/rsh --program-transform-name='s/^s/r/' --prefix=/usr
```

Installez les exécutables et configurez-les en fonction des directives. Sur la passerelle de réseau privé, assurez-vous que la configuration de sshd comprend bien les entrées suivantes :

```
ListenAddress 192.168.1.1       # l'adresse interne de fred
```

```
IgnoreRhosts no
X11Forwarding yes
X11DisplayOffset 10
RhostsAuthentication no
RhostsRSAAuthentication yes
RSAAuthentication yes
PasswordAuthentication yes
```

Vous serez amené à effectuer des réglages supplémentaires dans le fichier `/etc/sshd_config`, mais essayez de ne pas changer ces champs. Une fois que vous avez réglé toutes les entrées du fichier sur les valeurs qui vous conviennent, copiez le fichier vers un nouveau fichier,`/etc/sshd_config.ext`, pour le réseau externe. Changez deux entrées dans le nouveau fichier : la valeur de « ListenAdress » doit être remplacée par l'adresse IP de la passerelle de réseau privé (10.1.1.9 dans notre exemple de fred.example.com) et « PasswordAuthentication » doit être positionné sur « no » dans `/etc/sshd_config.ext`. Dans vos scripts de démarrage des services réseau, faites démarrer sshd deux fois, une fois avec

```
/usr/sbin/sshd
```

et une fois avec

```
 /usr/sbin/sshd -f /etc/sshd_config.ext
```

Ceci lancera deux démons sshd. Celui opérant sur l'interface interne autorisera les connexions avec mot de passe, mais l'interface externe exigera la validation d'une clé RSA avant que quiconque puisse se loguer.

Ensuite, désactivez les services telnet et shell dans le fichier de configuration de inetd (notez que la configuration proposée dans la section 8.1 (Configurer votre pare-feu) empêche déjà les accès depuis l'extérieur, mais il est préférable de se défendre en profondeur, ne vous en remettez pas au fait que tout fonctionne correctement).

Les personnes qui veulent pouvoir se connecter depuis leur domicile ou depuis un lieu de déplacement auront besoin une clé RSA. Assurez-vous qu'elles savent comment procéder de façon à ce qu'elles ne gaspillent pas leur énergie à essayer de mettre en place un autre moyen de se connecter comme, par exemple, exécuter un telnetd sur un port sans privilège sur la machine pare-feu.

Une clé RSA est générée par la commande suivante :

```
ssh-keygen -b 1024 -f new_rsa_key
```

Vous serez invité à entrer une phrase-clé (passphrase). Celle-ci ne doit *pas* être vide. Une personne ayant un accès au fichier `new_rsa_key` et connaissant la phrase-clé a tout ce qu'il lui faut pour réussir un défi d'authentification RSA. La phrase-clé peut être un mot de passe « introuvable » ou une phrase longue, mais choisissez quelque chose de pas banal. Le fichier `new_rsa_key` peut être copié sur une disquette ou sur un portable et, en association avec la phrase-clé, peut être utilisé pour se connecter sous les comptes paramétrés pour accorder l'accès à cette clé RSA précise.

Pour configurer un compte de façon à ce qu'il soit accessible par une clé RSA, créez simplement un répertoire `$HOME/.ssh` pour cet utilisateur sur la passerelle de réseau privé (c'est à dire la machine qui recevra la demande de connexion), et copiez le fichier `new_rsa_key.pub` qui a été créé par la commande « ssh-keygen » dans le fichier `$HOME/.ssh/authorized_keys`. Pour des détails sur les autres options que vous pouvez ajouter à la clé, telles qu'obliger la demande de connexion à provenir d'une certaine adresse IP ou d'un certain nom d'hôte, ou bien permettre à la clé de n'autoriser l'invocation à distance que de certaines commandes seulement (par exemple une clé RSA qui ne fait que commander le début d'une sauvegarde ou l'envoi par mail à l'extérieur du site d'un rapport d'état), reportez-vous à la section « AUTHORIZED_KEYS FILE FORMAT » dans la page de manuel de sshd.

Il reste une seule chose à faire pour rendre le mécanisme de chiffrement RSA aussi simple que possible pour les utilisateurs. Si l'utilisateur est obligé d'entrer la phrase-clé plus d'une fois ou deux au cours de sa session, il va vraisemblablement finir par être gêné et par prendre en main les questions de sécurité. Sous Linux, faites en sorte que son shell de login soit invoqué sous *ssh-agent*. Par exemple si les portables de société utilisés en déplacement exécutent *xdm* et basculent les utilisateurs sous une session X, allez dans le fichier `/var/X11R6/lib/xdm/Xsession_0` et modifiez les lignes qui lancent le démarrage et qui sont probablement du type :

```
exec "$startup"
```

par des lignes du type :

```
exec ssh-agent "$startup"
```

Dans mon paramétrage de xdm il y a trois lignes dans ce fichier qui ont dû être modifiées. Maintenant, quand l'utilisateur ouvre une session sur le portable, il saisit la commande

```
ssh-add new_rsa_key
```

sous n'importe quel prompt, il saisit la phrase-clé quand il y est invité et toutes les fenêtres auront accès sans phrase-clé au compte sur la passerelle de réseau privé jusqu'à ce que l'utilisateur déconnecte la session X sur le portable.

Exécutez sshd sur toutes les machines de votre réseau privé, autant que sur vos hôtes exposés. Pour les autres machines que la passerelle, l'entrée ListenAdress dans le fichier `/etc/sshd_config` peut-être positionnée sur « 0.0.0.0 ». Vous devez mettre en place les clés des hôtes avec la commande :

```
ssh-keygen -b 1024 -f /etc/ssh_host_key -N ""
```

puis exécuter *make-ssh-known-hosts* et distribuer le fichier `/etc/ssh_know_hosts` sur toutes les machines du réseau privé.

Désactivez le telnet entrant et les « services en r » non chiffrés. Ne supprimez pas l'exécutable *telnet*, il est utile pour d'autres choses que de simples connexions telnet sur le port 23. Vous pouvez autoriser l'identification par mot de passe sur le réseau privé et la désactiver sur les machines exposées, en imposant une clé RSA pour la connexion sur les hôtes exposés.

Il est pratique pour les utilisateurs que les hôtes du réseau se répertorient les uns les autres dans le fichier `/etc/hosts.equiv`. Les démons sshd prendront ceci en compte et permettront aux personnes de se connecter à distance ou d'exécuter des shells à distance entre machines sans mot de passe ou phrase-clé. À chacune des connexions, les machines vérifieront leurs identités respectives avec des clés RSA au niveau machine.

Une difficulté apparaît quand un utilisateur connecté sur une machine du réseau privé veut se connecter sur une machine ayant une adresse IP publique. Vous ne pouvez pas utiliser `/etc/hosts.equiv` ou `$HOME/.shosts` pour permettre une identification sans mot de passe parce que l'utilisateur est sur une machine dont l'adresse IP ne peut être déterminée - elle semblera venir du pare-feu, mais les clés-machine ne fonctionneront pas. Il y a deux solutions à cela. D'abord, si vous voulez vraiment utiliser les méthodes `/etc/hosts.equiv` ou `$HOME/.shosts`, l'utilisateur devra se connecter à la passerelle de réseau privé (fred.example.com dans notre exemple actuel) et ensuite se connecter sur la machine exposée depuis cet endroit. L'autre technique consiste à utiliser l'authentification RSA qui fonctionne toujours indépendamment des fantaisies du mécanisme de résolution et d'adresses IP occasionnées par votre configuration.

8.3 Configurer X

La quête perpétuelle de l'utilisateur pour prouver qu'il privilégie la facilité d'utilisation par rapport à la sécurité, a rendu commun l'usage de la commande

```
xhost +
```

dans ses scripts d'initialisation de X. Ceci permet l'accès au serveur X à n'importe qui dans le monde. Maintenant, n'importe quel intrus peut remplacer votre fond d'écran par quelque chose d'embarassant juste au moment où votre chef fait visiter votre bureau à sa mère. Cet intrus peut également tranquillement surveiller tout ce que vous tapez au clavier et capturer le contenu de votre écran sur sa machine. Inutile de dire que ceci ne sied pas très bien aux mots de passe que vous utilisez pour vous connecter sur d'autres sites ou à d'autres documents sensibles affichés à l'écran. Le protocole xhost lui même a des limitations inhérentes au fait qu'il n'est pas possible d'accorder la permission d'utiliser l'affichage sur une « base utilisateur » mais seulement sur une « base machine ».

Optez pour l'identification *xauth*. Si vous avez *xdm*, vous exécutez déjà probablement l'identification *xauth* mais *xhost* fonctionne toujours et peut continuer à être utilisé par les gens pour exécuter des processus X entre machines. Une fois encore, le but est de rendre la sécurité suffisamment facile à utiliser de manière à ce que les utilisateurs ne soient plus tentés d'utiliser la commande *xhost*.

Le paramétrage de sshd décrit dans la section 8.2 (Configurer SSH1), avec l'indicateur « X11Forwarding » positionné, est actuellement plus simple d'utilisation que la technique *xhos*t. Une fois que vous vous êtes connecté sur votre terminal, vous pouvez simplement vous « rloguer » sur une machine distante et exécuter *netscape*, *xv* ou ou ce que vous voulez sans avoir à positionner la variable $DISPLAY ou à accorder des permissions explicites. Au cours du login *ssh*, le système est configuré d'une manière transparente pour l'utilisateur final, et même, tous les paquets sont chiffrés avant de partir sur le réseau.

Si vous n'avez pas la possibilité d'utiliser le transfert X11 sshd pour une raison ou pour une autre, vous devrez utiliser *xauth* quand vous voudrez autoriser les autres machines à se connecter sur votre serveur X. Documentez ceci pour vos utilisateurs ou bien créez des scripts shell spécialisés pour les aider. La commande adéquate pour permettre une identification, « jpublic » sur la machine « barney » de façon à avoir accès au serveur est :

```
/usr/X11/bin/xauth extract - $DISPLAY | rsh -l jpublic barney /usr/X11/bin/xauth merge -
```

Cette séquence n'est pas nécessaire pour autoriser les connexions X depuis les machines qui partagent un répertoire commun de montage NFS. La clé xauth sera immédiatement disponible aux utilisateurs de toutes les machines qui montent le même répertoire racine.

Je serais tenté d'effacer purement et simplement *xhost* de toutes les machines. Si ceci cause des problèmes pour quelques programmes, vous saurez au moins que ces programmes avaient une sécurité mal conçue. Il est suffisamment aisé d'écrire un script-shell qui utilise la séquence *xauth* décrite plus haut comme solution de remplacement pour *xhost*.

Notez que, si *rsh* n'est pas le programme de chiffrement de ssh, la clé xauth est envoyée sous forme de texte. Quiconque s'empare du texte de la clé peut accéder à votre serveur, ainsi vous ne gagnez pas beaucoup de sécurisation si vous n'utilisez pas ssh pour ces transactions. Notez également que si les répertoires home des utilisateurs sont exportés via NFS (Network File System) la clé xauth est disponible en clair pour n'importe quelle personne en mesure d'espionner ces paquets NFS, indépendamment du fait que vous exécutez ssh sur vos systèmes.

8.4 Configurer le partage de fichiers

Avec la messagerie arrivant sur une machine centralisée, les procédures de lecture et d'expédition depuis n'importe quel hôte décrites ici sont très pratiques, mais des précautions doivent être prises contre le furetage de la part d'utilisateurs locaux qui s'ennuient. NFS sans implémentation de AUTH_DES manque foncièrement de sécurité. NFS s'en remet à la machine cliente pour certifier l'accès, il n'y a pas de vérification de mot de passe sur le serveur pour s'assurer que le client est autorisé à accéder à tel fichier privé d'un utilisateur particulier. Une machine Windows peut être configurée pour lire les volumes exportés par NFS sous n'importe quel identifiant numérique en outrepassant complètement les permissions de fichiers UNIX. En conséquence, les exports NFS ne devraient être mis en place que sur les machines qui sont toujours sous Linux (ou UNIX), sous votre contrôle direct, et jamais sur celles qui ont un boot multiple avec Windows. Si vous voulez exporter le répertoire de spool de votre messagerie, ou n'importe quel autre répertoire, vers des machines qui peuvent être à l'occasion utilisées sous Windows, exportez-les avec Samba en mettant le mode d'identification sur « security=USER ». Le fait de connecter les machines sur votre réseau à l'aide d'un commutateur plutôt qu'un hub sera également bénéfique et donnera peu d'intérêt à la mise en place de renifleurs sur les machines Windows. Cependant, et en dernier lieu, il est très difficile de sécuriser un partage de fichier à travers les réseaux au moment de son écriture.

Pourquoi vous inquiéter si vous ne pouvez réellement sécuriser les disques réseau ? C'est avant tout un moyen de rendre l'ensemble de la sécurisation crédible. Si vous laissez une feuille de papier avec des informations confidentielles sur votre bureau et que quelqu'un la lit, il pourra arguer du fait qu'il n'avait pas réalisé la nature du document, sa curiosité naturelle venant juste de l'emporter quand il l'a vu posée là. Si la feuille de papier est dans un classeur ou dans un tiroir du bureau, c'est une histoire totalement différente. L'objet des mesures de sécurité en interne est surtout de s'assurer que personne ne peut accidentellement compromettre la sécurité générale.

9 Remerciements

Ce document a été écrit comme documentation interne pour le projet DYNACAN, intégré au au projet de développement continu sous le contrôle du Développement des ressources humaines Canada.

Ce document a considérablement bénéficié des suggestions de

- Rod Smith (rodsmith@rodsbooks.com), qui a suggéré que je fournisse des détails sur la manière d'enregistrer un nom de domaine, sur la configuration avec des adresses IP dynamiques et qui m'a orienté sur les divers services d'hébergement d'IP dynamiques et sur Granite Canyon.
- Greg Leblanc (gleblanc@my-deja.com) pour des suggestions utiles pour améliorer la lisibilité du document.
- Sami Yousif (syousif@iname.com).
- Marc-André Dumas (m_a_dumas@hotmail.com), qui m'a suggéré la section concernant la transposition du domaine sur de nouvelles adresses IP.
- Osamu Aoki (aoki@pacbell.net).
- Joao Ribeiro <(url url="mailto:sena@decoy.ath.cx"name="sena@decoy.ath.cx">).

10 Glossaire des termes utilisés

Voici une liste de la signification de certains des mots ou acronymes utilisés dans le document.

Adresse IP

L'adresse d'une certaine interface réseau. Sous le standard actuel, nommé ipv4, cette adresse consiste en une série de 4 valeurs codées sur 8 bits généralement écrites en base 10 et séparés par des points. La communication entre ordinateurs sur internet est basée sur l'envoi de paquets d'information entre adresses IP.

Adresse IP dynamique

Adresse IP qui est attribuée périodiquement ou sur la base d'une session. Aucune garantie n'est donnée sur le fait que l'adresse IP restera la même. Une adresse IP dynamique n'est susceptible de changer que quand votre connexion réseau tombe et se reconnecte, ou bien périodiquement lors d'une négociation DHCP. Certains services basés sur la session tels que *telnet* ou *ssh* s'arrêteront si l'adresse IP de l'une ou l'autre des deux machines connectées change pendant la session.

Adresse IP statique

Une adresse IP qui vous a été attribuée ou louée de manière permanente. Sauf annulation de la convention qui vous attribue cette adresse IP, elle sera toujours disponible pour votre utilisation, et aucune autre machine sur internet n'est autorisée à utiliser cette adresse. S'oppose à Adresse IP dynamique.

DHCP

Dynamic Host Configuration Protocol. Un standard, défini dans la RFC 1531, pour que des ordinateurs sur réseau TCP/IP puissent obtenir de serveurs des informations telles que l'adresse IP qu'ils doivent utiliser, le masque de réseau, la passerelle, etc. Plutôt que ses informations soient paramétrées par un administrateur, la machine les demande simplement au serveur quand elle se connecte au réseau.

DNS

Domain name service. Un standard pour convertir les noms de domaine en adresses IP ou vice-versa, en recherchant l'information dans des bases de données centrales.

DSL

Digital Subscriber Line. Une connexion réseau relativement rapide, habituellement fournie sur un câblage téléphonique spécialisé.

FAI

Fournisseur d'accès à internet. La société qui vous fournit la connexion à internet, y compris la connexion physique, l'hébergement de services, et l'attribution d'adresses IP qu'elle contrôle.

Fournisseur d'accès Internet

voir 10 (FAI)

FTP

File Transfert Protocol. Un protocole pour envoyer des fichiers entre machines à travers internet.

ftpd

Le démon (serveur) chargé de fournir le service FTP sur un hôte. Il répond aux requêtes faites par un client distant.

IP

voir 10 (adresse IP)

ISP

Internet Service Provider, équivalent anglais pour 10 (FAI)

Masquage (ou camouflage)

Un type de filtrage dans lequel les paquets émanant d'une machine vers le monde extérieur ont leur en-tête réécrit de façon à ce qu'ils semblent provenir d'une machine intermédiaire. La machine intermédiaire transmet alors les réponses à la machine d'origine. Le résultat, en termes de réseau, est qu'un réseau entier de machines peut sembler n'utiliser qu'une seule adresse IP, celle de la machine qui assure le masquage, en ce qui concerne les connexions extérieures.

Masquerading

voir 10 (masquage)

named

Le serveur de noms. C'est le démon qui répond aux requêtes DNS. Il est distribué dans le paquet BIND.

Network Time Protocol

voir 10 (NTP)

NTP

Network Time Protocol. Un standard pour synchroniser votre horloge système avec « l'heure officielle », défini comme la référence de beaucoup d'horloges de précision à travers le monde.

OS

Operating System. voir 10 (SE)

PHB

Pointy Haired Boss (voir : *http://www.unitedmedia.com/comics/dilbert/about/html/boss.html* ou *http://www.cplus.fr/html/samedicomedie/dilbert/personnages.html#3*). Un personnage de Scott Adams, dans la série Dilbert.

Provider

voir 10 (FAI)

Requête DNS directe

(forward DNS) Une requête DNS qui convertit un nom de domaine en une adresse IP.

Requête DNS inversé

(reverse DNS) Une requête DNS qui convertit une adresse IP en un nom de domaine.

Routeur

Une machine spécialisée qui met à exécution les règles concernant l'endroit où envoyer les paquets sur la base de leur adresse IP, les ponts entre vos machines Ethernet et n'importe quel média de communication qui vous connecte avec votre FAI.

Script CGI

Common Gateway Interface. C'est un programme qui est exécuté à la demande pour générer le contenu d'une page web. Si une page web doit faire autre chose que d'envoyer des informations (textes et graphiques) fixes au navigateur, vous aurez probablement besoin d'un programme quelconque de génération d'affichage dynamique tel qu'un script CGI. Les applications peuvent être des forums de dicussion, des formulaires interactifs, des cartes de crédit e-commerce, etc.

SE

Système d'exploitation. Linux, Windows, FreeBSD, BeOS, HP-UX, MacOS, etc.

ssh

Le shell sécurisé. Une substitution chiffrée pour *rlogin*, *telnet*, *ftp* et autres programmes. Protège contre l'usurpation d'adresse, l'attaque de l'intercepteur, et le reniflage de paquets.