Linux VPN Masquerade HOWTO − Version française

John D. Hardin <jhardin@wolfenet.com>, version française par Yann Hirou <hirou@linuxfr.org>

$Revision: 1.1.1.1 $ $Date: 2003/01/03 02:38:54 $

Ce document décrit comment configurer un pare−feu Linux pour masquer le trafic d'un réseau privé virtuel (NdT: Virtual Private Network, VPN) utilisant IPsec ou PPTP, vous permettant ainsi d'établir une connexion VPN sans perdre ni la sécurité ni la flexibilité apportées par la connexion internet de votre pare−feu Linux, et vous permettant de rendre accessible un serveur VPN qui n'a pas d'adresse IP publique. Des informations sur la configuration du client et du serveur VPN sont également fournies.

Table des matières

1. Introduction

1.1. Introduction

Ce document décrit comment configurer le masquage d'un trafic VPN de type IPsec ou PPTP. Les VPNs utilisant SSH (comme celui vendu par F−Secure, et référencé dans le VPN mini−HOWTO) sont fondés sur un trafic TCP standard, et ne nécessitent aucune modification particulière du noyau.

Le masquage de VPN vous permet d'établir une ou plusieurs sessions IPsec et/ou PPTP vers des serveurs VPN accessibles sur internet via votre pare−feu internet sans que vous deviez connecter la machine sur laquelle tourne le client VPN directement à votre FAI (Fournisseur d'Accès Internet) − donc en conservant tous les avantages de votre pare−feu internet sous Linux. Il vous est également possible de configurer un serveur VPN avec une adresse IP de réseau privé (voir le RFC1918) derrière un pare−feu Linux faisant du masquage, vous permettant ainsi de fournir de façon assez sécurisée un accès à un réseau privé via seulement une seule adresse IP référencée − y compris si cette adresse IP représente celle d'une connexion modem pouvant varier.

Il est très fortement recommandé que vous compreniez, configuriez et testiez le masquage IP avant de tenter de mettre en place du masquage VPN. Consultez le IP Masquerade HOWTO et la page de ressources sur le masquage IP à l'adresse http://ipmasq.cjb.net/ avant de commencer. La planification et la mise en place de votre VPN et de votre pare−feu dépassent le cadre de ce document. Voici quelques ressources :

- http://www.linux.org/help/ldp/howto/Firewall−HOWTO.html
- http://hal2000.hal.vein.hu/~mag/linux−security/VPN−HOWTO.html

Le patch pour les noyaux de la série 2.0.x fonctionne bien sur la version 2.0.36 du noyau Linux, et a été intégré dans la version 2.0.37. Il doit également fonctionner sur les versions antérieures à la 2.0.36, et devrait fonctionner sur les noyaux Linux jusqu'à la version 2.1.102. Le code du masquage IP se trouvant dans le noyau a été restructuré autour de la version 2.1.103, nécessitant un patch différent pour les séries de noyaux 2.1.105+ et 2.2.x.. Un patch est disponible pour les noyaux de 2.2.5 à 2.2.17, et il devrait fonctionner sur les noyaux antérieurs.

1.2. Avis, Crédits & Ressources

Le site où trouver les patchs du noyau pour le masquage VPN avec Linux est http://www.impsec.org/linux/masquerade/ip_masq_vpn.html

N'hésitez pas à m'envoyer votre avis ou des commentaires sur ce document à l'adresse <jhardin@wolfenet.com>. La version actuelle est disponible à l'adresse :

- HTML: ftp://ftp.rubyriver.com/pub/jhardin/masquerade/VPN−howto/VPN−Masquerade.html
- PostScript: ftp://ftp.rubyriver.com/pub/jhardin/masquerade/VPN−howto/VPN−Masquerade.ps.gz
- SGML source: ftp://ftp.rubyriver.com/pub/jhardin/masquerade/VPN−Masquerade.sgml

Si vous travaillez avec un noyau dont le numéro de version est supérieur à tous ceux mentionnés dans ce document, *merci* de regarder s'il n'y a pas une version à jour de ce HOWTO sur le site cité ci−dessus avant de me contacter directement.

Il peut également être trouvé via le répertoire HOWTO du Linux Documentation Project et le répertoire */usr/doc/HOWTO/* sur la machine Linux la plus proche. Ces copies ne sont pas directement mises à jour par moi, donc elles peuvent être un peu dépassées.

J'ai personnellement de l'expérience sur le masquage de clients IPsec et PPTP tournant sur MS W'98 et NT, sur la configuration d'un serveur PPTP avec une adresse IP publique, et sur l'utilisation de PPTP pour du routage inter−réseaux.

Les informations sur le masquage d'un serveur PPTP avec une adresse IP privée proviennent de discussions avec Len Bayles <len@isdi.com>, Simon Cocking <simon@ibs.com.au> et C. Scott Ananian <cananian@lcs.mit.edu>.

Le site pour le patch du noyau concernant uniquement le masquage PPTP pour les séries de noyaux 2.1.105+ et les premiers 2.2.x est http://bmrc.berkeley.edu/people/chaffee/linux_pptp.html.

Le site pour le patch du noyau concernant la redirection de port *ipportfw* et pour l'outil de configuration des noyaux 2.0.x est http://www.ox.compsoc.org.uk/~steve/portforwarding.html. La redirection de port est incluse dans les noyaux 2.2.x, et l'outil de configuration *ipmasqadm* contrôlant la redirection de port des 2.2.x peut être obtenu à l'adresse http://juanjox.kernelnotes.org/.

Le site pour le redirecteur IP générique *ipfwd* est http://www.pdos.lcs.mit.edu/~cananian/Projects/IPfwd/.

Pleins de remerciements à Gordon Chaffee <chaffee@cs.berkeley.edu> pour avoir codé et partagé un patch pour traceroute qui permet de tracer le trafic GRE. Il va se montrer d'une valeur inestimable pour la détection d'erreurs si votre trafic GRE se trouve bloqué quelque part. Le patch est disponible à l'adresse http://www.wolfenet.com/~jhardin/pptp−traceroute.patch.gz

Encore plus de remerciements à Steve Chinatti <chinatti@alumni.Princeton.EDU> pour avoir partagé sa modification du masquage IPsec, d'où j'ai récupéré sans vergogne quelques idées très importantes...

De plus amples informations sur comment installer des règles de pare−feu s'exécutant automatiquement − y compris comment utiliser automatiquement la bonne adresse IP dans un environnement d'adressage IP dynamique − peuvent se trouver à l'adresse http://www.wolfenet.com/~jhardin/ipfwadm/invocation.html

Le site pour Linux FreeS/WAN (IPsec pour Linux) est http://www.xs4all.nl/~freeswan/ − c'est la solution de VPN sous Linux conseillée.

Un serveur PPTP Linux natif appelé PoPToP est disponible à l'adresse http://www.moretonbay.com/vpn/pptp.html − pour les informations les plus à jour sur PPTP sous Linux, allez y.

Paul Cadach <paul@odt.east.telecom.kz> a écrit des patchs qui ajoutent au pppd de Linux le support MS−CHAP−v2, MPPE et Multilink. Allez voir ftp://ftp.east.telecom.kz/pub/src/networking/ppp/ppp−2.3.5−my.tgz pour MS−CHAP et MPPE, et ftp://ftp.east.telecom.kz/pub/src/networking/ppp/multilink/ppp−2.3.5−mp.tgz pour Multilink. Un autre ensemble de patchs (probablement intéressants) pour pppd est disponible sur le site de téléchargement de PoPToP à l'adresse http://www.moretonbay.com/vpn/download_pptp.html.

Le site du projet original PPTP pour Linux est http://www.pdos.lcs.mit.edu/~cananian/Projects/PPTP et un patch pour ajouter les fonctionnalités de serveur PPTP est disponible à l'adresse http://debs.fuller.edu/cgi−bin/display?list=pptp=222

Merci à Eric Raymond de maintenir Le fichier du Jargon (The Jargon File), et à Denis Howe de maintenir Le dictionnaire en ligne gratuit de l'informatique (The Free On−line Dictionary of Computing).

1.3. Copyright & mise en garde

Les informations fournies dans ce document sont correctes dans la limite de mon savoir. Le masquage IP est *expérimental*, et il est possible que j'aie fait des erreurs en écrivant ou testant le patch du noyau, ou encore en écrivant les instructions dans ce document ; à vous de décider si vous souhaitez effectuer les changements indiqués dans ce document.

```
L'AUTEUR NE PEUT ETRE TENU RESPONSABLE POUR DES DEGATS CAUSES PAR DES
ACTIONS BASEES SUR LES INFORMATIONS CONTENUES DANS CE DOCUMENT.
SAUVEGARDEZ TOUTES LES DONNEES CRITIQUES AVANT D'EFFECTUER LES
CHANGEMENTS INDIQUES DANS CE DOCUMENT. ASSUREZ VOUS D'AVOIR UN NOYAU
QUI MARCHE, SUR LEQUEL VOUS POUVEZ DEMARRER, AVANT DE PATCHER ET
DE RECOMPILER VOTRE NOYAU COMME INDIQUE DANS CE DOCUMENT.
```

En d'autres mots, prenez des précautions.

2. Connaissances requises

2.1. Qu'est−ce qu'un VPN ?

Un Réseau Privé Virtuel (Virtual Private Network), ou "VPN", est un tunnel qui véhicule le trafic d'un réseau privé d'un système terminal vers un autre, en empruntant un réseau public (comme l'internet), sans que les intermédiaires entre les deux machines terminales soient visibles du point de vue du trafic véhiculé, et sans que les équipements intermédiaires voient les paquets qui sont en train de transiter dans le tunnel. Le tunnel peut en option compresser et/ou crypter les données, fournissant des performances accrues et quelques mesures de sécurité.

La partie "Virtuelle" vient du fait que vous construisez une liaison privée au dessus d'un réseau public, plutôt que d'acheter une liaison en dur sur une ligne louée. Le VPN vous permet de considérer que vous utilisez une ligne louée ou une ligne téléphonique pour communiquer entre les deux points terminaux.

Pour information, vous pouvez trouver la FAQ sur le VPN à l'adresse http://kubarb.phsx.ukans.edu/~tbird/vpn/FAQ.html.

2.2. Qu'est−ce qu'IPsec ?

IPsec est un ensemble de protocoles standards pour implémenter des communications sécurisées ainsi que l'échange de clés de cryptage entre ordinateurs. Il peut être utilisé pour mettre en place un VPN.

Un réseau privé virtuel IPsec consiste généralement en deux canaux de communication entre les machines terminales : un canal d'échange de clés, par lequel les informations sur l'authentification et les clés de cryptage transitent, et un ou plusieurs canaux de données par lesquels le trafic du réseau privé est véhiculé.

Le canal d'échange de clés est une connexion UDP standard en provenance de et vers le port 500. Le canal de données transportant le trafic entre le client et le serveur utilise le protocole IP numéro 50 (ESP).

Vous pouvez trouver de plus amples informations dans la FAQ IPsec de F−Secure, à l'adresse http://www.Europe.F−Secure.com/support/vpn+/faq/techfaq.html, et dans les RFC2402 (le protocole AH, protocole IP numéro 51), RFC2406 (le protocole ESP, protocole IP numéro 50), et RFC2408 (le protocole d'échange de clés ISAKMP).

IPsec est un protocole de communication symétrique. Cependant, vu que la plupart des gens vont s'y trouver confronté uniquement sous la forme d'un client Windows accédant à une passerelle centrale de sécurité réseau, le terme "client" va être utilisé pour désigner la machine devant laquelle l'utilisateur est assis, et le terme "serveur" va être utilisé pour désigner la passerelle centrale de sécurité réseau.

Note importante : si votre VPN est basé sur le protocole AH (y compris AH+ESP), il ne peut pas être masqué. Le protocole AH utilise un contrôleur d'intégrité cryptographique sur des parties de l'entête IP, y compris l'adresse IP. Le masquage IP modifie l'adresse source pour les paquets sortants, et l'adresse destination pour les paquets entrants. La passerelle de masquage ne pouvant pas participer à l'échange de clés, elle ne peut pas régénérer correctement les contrôleurs d'intégrité cryptographiques pour les entêtes IP modifiés. Les paquets IP modifiés seront donc rejetés par le destinataire comme des paquets invalides, car ils ne passeront pas le test d'intégrité cryptographique.

2.3. Qu'est−ce que PPTP ?

PPTP signifie *P*oint−to−*P*oint *T*unnelling *P*rotocol. C'est un protocole proposé par Microsoft pour réaliser un VPN.

Le protocole VPN PPTP consiste en deux canaux de communication entre le client et le serveur : un canal de contrôle par lequel les informations de gestion du lien transitent, et un canal de données par lequel le trafic (éventuellement crypté) du réseau privé est véhiculé.

Le canal de contrôle est une connexion TCP standard vers le port 1723 du serveur. Le canal de données véhiculant le trafic du réseau privé utilise le protocole IP numéro 47, un protocole d'encapsulation générique décrit dans le RFC1701. La transmission transparente des données sur le canal de données est réalisée par la négociation d'une connexion PPP standard sur ce canal, simplement comme s'il s'agissait d'une connexion modem directement du client vers le serveur. Les options négociées sur le tunnel via le protocole PPP contrôlent si les données sont compressées et/ou cryptées, et donc PPTP n'a rien à voir avec le cryptage.

Les détails du protocole PPTP sont documentés dans le RFC2637.

L'implémentation du protocole PPTP par Microsoft n'est pas considérée comme très sécurisée. Si vous êtes intéressés par les détails, voici trois analyses différentes :

http://www.counterpane.com/pptp.html

http://www.geek−girl.com/bugtraq/1999_1/0664.html

http://oliver.efri.hr/~crv/security/bugs/NT/pptp2.html

2.4. Qu'est−ce que FWZ ?

FWZ est un protocole de cryptage propriétaire développé par Check Point Software Technologies. Il est utilisé dans les VPNs qui sont construits autour de leur produit Firewall−1.

Un pare−feu Checkpoint peut être configuré avec différents modes. Le mode d' "encapsulation FWZ" *ne peut pas* être masqué. Le mode "IKE", qui utilise les protocoles standards IPsec, peut être masqué avec des changements de configuration minimes sur la passerelle VPN.

2.5. Pourquoi masquer un client VPN ?

La plupart des clients VPN actuels partent du principe que vous allez connecter l'ordinateur client directement à internet. Faire cela lorsque vous n'avez qu'une seule connexion d'accès internet contourne votre pare−feu Linux, la sécurité, ainsi que les capacités de partage d'accès qu'il fournit. Étendre le pare−feu Linux pour aussi masquer le trafic VPN vous permet de conserver la sécurité pare−feu fournie par le pare−feu Linux, ainsi que d'autoriser d'autres systèmes de votre réseau local à accéder à internet, sans avoir à prendre en compte le fait que la connexion VPN soit active ou non.

Si votre pare−feu est utilisé en environnement professionnel, vous pouvez également souhaiter imposer aux utilisateurs clients du VPN de traverser ce pare−feu pour des raisons de sécurité, plutôt que de leur fournir des modems pour qu'ils puissent se connecter tout seuls à l'extérieur quand ils ont besoin d'utiliser le VPN. Le masquage VPN vous permet de le faire même si les machines clientes n'ont pas des adresses IP publiques.

2.6. Plusieurs clients sur mon réseau local peuvent−ils utiliser IPsec simultanément ?

Oui, bien qu'il puisse y avoir parfois quelques problèmes mineurs.

Les protocoles IPsec définissent une méthode pour identifier les flux de trafic appelée *Index des Paramètres de Sécurité (Security Parameters Index)* ("SPI"). Malheureusement le SPI utilisé pour le trafic sortant est différent du SPI utilisé pour le trafic entrant, et il n'y a pas d'autre information permettant l'identification qui ne soit pas cryptée, donc l'association entre le flux entrant et le flux sortant est difficile et pas parfaitement fiable.

Le masquage IPsec tente d'associer les trafics ESP entrant et sortant en mettant en série les nouvelles connexions. Alors que ceci fonctionne bien pendant les tests, on ne peut pas garantir que ce soit parfaitement fiable, et la sérialisation des nouveaux trafics peut aboutir à des fins d'attente (timeouts) si la liaison est saturée ou si plusieurs machines locales faisant de l'IPsec tentent d'initier des communications ou de rééchanger leurs clés simultanément, avec la même machine distante faisant de l'IPsec.

Il est également reconnu que ce schéma associatif peut ne pas arriver à associer les flux de trafic correctement, les machines faisant de l'IPsec ne vont alors pas prendre en compte le trafic mal dirigé, car il aura de mauvaises valeurs SPI. Ce comportement est requis par le RFC sur IPsec.

Ces problèmes auraient pu être supprimés s'il y avait eu un moyen d'écouter les nouvelles valeurs SPI provenant de l'échange de clés ISAKMP avant que le moindre trafic ESP n'apparaisse, mais malheureusement cette partie de l'échange de clés est cryptée.

Afin de minimiser les problèmes associés à cela, il est recommandé d'ouvrir une fenêtre de commandes sur votre machine IPsec masquée, et de lancer le programme "ping" vers une machine du réseau distant pour maintenir le tunnel actif.

Regardez les notes techniques sur IPsec à la fin du document pour de plus amples détails.

2.7. Plusieurs clients sur mon réseau local peuvent−ils utiliser PPTP simultanément ?

Oui.

Vous devez mettre en place le masquage d'identifiant d'appel PPTP (PPTP Call ID) lors de la configuration de votre noyau, afin de distinguer les différents flux de données en provenance du même serveur. Le masquage PPTP avec le masquage d'identifiant d'appel activé va permettre d'avoir plusieurs sessions masquées simultanées sans restriction sur le choix du serveur que le client appelle.

Le RFC sur PPTP spécifie dans la section 3.1.3 qu'il ne peut y avoir qu'un seul canal de contrôle entre deux systèmes. Ceci *devrait* signifier que vous pouvez masquer seulement une session PPTP à la fois avec un serveur distant donné, mais dans la pratique l'implémentation PPTP de MS ne tient pas compte de ça, tout du moins pas dans le Service Pack 4 de NT 4.0. Si le serveur PPTP que vous cherchez à atteindre n'autorise qu'une seule connexion à la fois, il suit correctement le protocole. Notez que cela n'affecte pas un serveur masqué, mais seulement plusieurs clients masqués cherchant à se connecter au même serveur distant.

Pour d'autres alternatives, voir la question suivante...

2.8. Puis−je accéder au réseau distant depuis l'ensemble de mon réseau local ?

Oui. Cependant, votre client VPN doit pouvoir faire suivre un trafic IP (IP forwarding).

Ceci signifie que vous devrez utiliser soit un client VPN Linux ou un client VPN MS NT. La pile IP de W'95 et W'98 ne permet pas de faire suivre un trafic IP. NT Workstation le gère, et est moins cher que NT Server si vous ne l'utilisez que pour router un trafic crypté.

Si vous ne pouvez pas installer un client Linux ou NT, alors vous devrez activer le masquage d'identifiant d'appel PPTP si vous utilisez PPTP, et installer un logiciel client VPN sur toutes les machines auxquelles vous voulez fournir un accès. Ceci est peu efficace, esthétiquement révoltant, sécuritairement mauvais, et peut ne pas fonctionner si le serveur PPTP implémente correctement le protocole, mais c'est moins cher que d'acheter des licences NT.

Le routage réseau à réseau avec cette méthode fonctionne très bien. C'est comme ça que j'ai installé mon réseau à la maison. Cela requiert un petit peu plus de connaissances réseau que de simplement donner à tout le monde son client VPN.

De par mon expérience, le routage de réseau à réseau dans un environnement purement MS requiert l'installation de RRAS des deux côtés du tunnel.

2.9. Pourquoi masquer le serveur VPN ?

Si votre serveur VPN a une adresse IP publique, vous n'avez pas besoin de le masquer, configurez simplement votre pare−feu pour router le trafic VPN correctement, comme indiqué plus bas.

Si votre serveur VPN a une adresse IP de réseau privé, vous aurez besoin de rediriger vers lui le trafic entrant, et de masquer son trafic sortant. Le masquage vous permet de rendre le serveur VPN accessible depuis internet même si vous n'avez qu'une seule adresse IP publique. Ceci devrait aussi fonctionner même si votre adresse IP est assignée dynamiquement : rendez simplement publique l'adresse IP pour les clients au travers de l'utilisation d'un service de DNS dynamique externe, comme par exemple celui fourni par DDNS.ORG ou CJB.NET et configurez les clients pour se connecter à une machine appelée *notre−entreprise.ddns.org* ou quelque chose du genre. Notez que ceci est une faille de sécurité, car il est possible que le client récupère du serveur DNS dynamique une mauvaise adresse IP à cause d'une mauvaise synchronisation, suite à un problème lors de l'enregistrement de l'adresse IP actuelle, ou suite à l'enregistrement d'une adresse IP différente avec le même nom par une tierce partie.

2.10. Pourquoi patcher le noyau Linux ?

Le plus gros problème dans le masquage de trafic VPN vient du fait que le masquage IP Linux de base n'a aucune connaissance des protocoles IP autres que TCP, UDP et ICMP.

Tout le trafic peut être redirigé et filtré par adresse IP, mais le masquage de protocoles IP autres que TCP, UDP et ICMP nécessite une modification du noyau.

Le canal de contrôle PPTP est du TCP pur, et ne nécessite aucune configuration particulière autre que de le laisser passer au travers du pare−feu et de le masquer.

Masquer les canaux de données IPsec et PPTP nécessite une modification qui ajoute le support des protocoles ESP et GRE au code de masquage, et le masquage du protocole d'échange de clés ISAKMP nécessite une modification qui empêche l'opération de masquage de modifier le numéro de port UDP source et qui remplace le suivi des valeurs de cookies ISAKMP par le suivi du numéro de port.

2.11. État actuel

Le patch pour les noyaux 2.0.x fonctionne sur le noyau 2.0.36 et est inclus dans les versions standards des noyaux 2.0.37 et supérieurs. Il devrait fonctionner sur les noyaux antérieurs, mais je n'ai pas testé, et je vous recommande, si vous utilisez un noyau plus ancien, de passer au noyau 2.0.38 pour des questions de sécurité.

Le patch pour les noyaux 2.2.x fonctionne sur les noyaux de 2.2.5 à 2.2.17, et devrait fonctionner sur les noyaux plus récents, mais ça n'a pas été testé. Il a été soumis pour être inclus dans la version standard 2.2.18.

Je n'ai pas les moyens de suivre les noyaux de développement, donc actuellement aucun travail n'a été fait sur le masquage VPN pour les 2.3.x et 2.4.x. Si vous connaissez quelqu'un qui *travaille* dessus, merci de me le faire savoir.

Le patch pour les noyaux 2.0.x a été testé et fonctionne sur les machines à base de x86 et sparc, et le patch pour les noyaux 2.2.x a été testé et fonctionne sur les machines à base de x86 et PowerPC, mais il ne devrait pas y avoir de problème majeur pour le porter sur d'autres architectures. Je crois que les dépendances vis−à−vis des architectures proviennent seulement de la représentation interne des nombres dans la définition de l'entête GRE utilisé pour formater les messages du journal et de déboguage. Si quelqu'un porte ce patch pour une architecture autre qu'Intel, j'apprécierais d'en avoir un écho, afin que je puisse intégrer les changements à la version d'origine.

Un patch noyau spécifique à PPTP pour les noyaux 2.1.105+ et les premiers 2.2.x est disponible à l'adresse http://bmrc.berkeley.edu/people/chaffee/linux_pptp.html.

Allez voir le site sur le masquage VPN à l'adresse http://www.impsec.org/linux/masquerade/ip_masq_vpn.html pour l'état des patchs de masquage VPN, et http://bmrc.berkeley.edu/people/chaffee/linux_pptp.html pour l'état du patch de masquage spécifique pour PPTP s'appliquant aux 2.1.105+/2.2.x.

3. Configurer le pare−feu Linux

3.1. Exemple de réseau

Pour les exemples de configuration avec des adresses IP privées de ce document, nous allons utiliser cet exemple de réseau :

```
Internet-------- 200.200.200.*   ppp0 ou  200.200.200.200 eth1
                                 Pare-feu Linux à deux cartes
            .--- 10.0.0.1        eth0
            |
            |--- 10.0.0.2        Client ou serveur VPN
            |
```

Pour les exemples de configuration avec des adresses IP publiques de ce document, nous allons utiliser cet exemple de réseau :

```
Internet-------- 200.200.200.200 eth1
                                 Pare-feu Linux à deux cartes
            .--- 222.0.0.1       eth0
            |
            |--- 222.0.0.2       Client ou serveur VPN
            |
```

Le serveur VPN auquel les clients des exemples se connecteront sera *199.0.0.1*

Les clients VPN qui se connecteront au serveur des exemples seront *199.0.0.2* et *199.0.0.3*

3.2. Déterminer ce qui doit être fait sur le pare−feu

Si votre client ou serveur VPN a une adresse IP publique, vous n'avez *pas* besoin de faire du masquage ni de modifier votre noyau − le noyau de base va correctement router tout trafic VPN. Vous pouvez directement passer aux sections ci−dessous sur la mise en place avec adresse IP publique.

Si votre client ou serveur VPN a une adresse IP de réseau privé comme décrit dans le RFC1918 vous avez besoin de patcher votre noyau (à moins que ce ne soit un noyau 2.0.37 ou supérieur, dans la série 2.0.x).

Si vous installez un serveur VPN masqué, vous allez aussi devoir récupérer les deux paquetages suivants.

- Pour rediriger le trafic TCP/UDP entrant (le canal de contrôle PPTP 1723/tcp ou le canal ISAKMP 500/udp), vous avez besoin du patch noyau de redirection de port approprié *ipportfw* récupérable sur http://www.ox.compsoc.org.uk/~steve/portforwarding.html. La redirection de port a été incorporée dans les noyaux 2.2.x. Regardez *man ipmasqadm* pour les détails de configuration. Si *ipmasqadm* n'est pas inclus dans votre distribution, il peut être obtenu à l'adresse http://juanjox.kernelnotes.org/.
- Pour rediriger le tunnel contenant le trafic initial entrant (GRE pour PPTP et ESP pour IPsec), vous avez besoin du redirecteur IP générique *ipfwd*, qui se trouve sur http://www.pdos.lcs.mit.edu/~cananian/Projects/IPfwd/.

Vous n'avez *pas* besoin de redirection de port ni d'ipfwd si vous ne masquez que les clients.

3.3. Patcher et configurer le noyau 2.0.x pour le support de masquage VPN

1. Installez les sources du noyau (de préférence version 2.0.37), que vous pouvez obtenir sur http://www.kernel.org/ ou un site miroir. Les sources doivent se décompacter automatiquement dans le répertoire */usr/src/linux*.
2. Configurer et tester le masquage IP standard (regardez le IP Masquerade HOWTO). Ceci va vous permettre de vous familiariser avec la recompilation de votre noyau, et plus largement, vous faire aborder le masquage IP.
3. *Sauvegardez les sources de votre noyau.*
4. Récupérez le patch noyau si nécessaire.

   Si la version de votre noyau est 2.0.36 ou inférieure, récupérez le patch du masquage VPN pour noyau 2.0.x sur le site du masquage VPN listé dans la section "Ressources" plus haut.

   Si la version de votre noyau est 2.0.37 ou plus dans la série 2.0.x, vous n'avez pas besoin d'appliquer de patch. Le code du masquage VPN est inclus dans le noyau. Passez la discussion sur le le patch du noyau.

   Pour les besoins de ce document, nous supposerons que vous avez sauvegardé le patch approprié sous le chemin */usr/src/ip_masq_vpn.patch.gz*.
5. Appliquez le patch de masquage VPN à votre noyau, si nécessaire :

   - Allez dans le répertoire des sources du noyau :

     ```
     cd /usr/src/linux
     ```

   - Appliquez le patch :

     ```
     zcat ../ip_masq_vpn.patch.gz | patch −l −p0 > vpn−patch.log 2>&1
     ```

     ```
     Notez que les options sont "tiret L minuscule, tiret P minuscule
     zero".
     Vous pourriez avoir des résultats étranges si vous changez l'ordre des
     arguments, car la commande patch semble sensible à l'ordre dans lequel
     ils apparaissent sur la ligne de commande.
     ```

   - Vérifiez le contenu du fichier *vpn−patch.log* pour voir si certaines étapes ont échoué. Si certaines étapes n'ont pas fonctionné, alors vous avez sûrement oublié des options, ou lancé le programme patch depuis le mauvais répertoire. Utilisez votre sauvegarde pour récupérer votre noyau, et recommencez.
6. Si vous masquez un serveur VPN, récupérez et installez le patch *ipportfw* depuis le site indiqué plus haut.

   Il existe un conflit connu entre le patch de masquage VPN et deux autres patchs réseau : le patch de chaînes pare−feu IP (ipchains), et le patch ipportfw. Ils cherchent tous à ajouter des options au même endroit dans *net/ipv4/Config.in*, et les changements effectués par un patch altèrent le contexte recherché par les autres patchs.

Si vous appliquez le patch de masquage VPN et les patchs de chaînes pare−feu IP ou ipportfw sur votre noyau 2.0.x, vous allez devoir éditer à la main le fichier *net/ipv4/Config.in* et ajouter le bloc des options de configuration du fichier patch qui n'ont pas été appliquées. En regardant le fichier patch vous devez trouver où les nouvelles options doivent être ajoutées dans le fichier *net/ipv4/Config.in*.

La syntaxe des fichiers patch est simple. Pour chaque bloc de changements à effectuer, il y a 2 parties : la première indique l'état "avant" avec une indication des lignes devant être changées ou effacées ; la seconde indique l'état "après", avec une indications des lignes qui ont été changées ou ajoutées. Utilisez la première partie pour trouver où ajouter les lignes, et ajoutez les lignes qui sont indiquées dans la seconde partie.

Ceci ne devrait pas être un problème, ces patchs étant à jour pour les noyaux 2.0.37+.

7. Configurez votre noyau et sélectionnez les options suivantes − répondez *YES* à ce qui suit :

```
* Prompt for development and/or incomplete code/drivers
  CONFIG_EXPERIMENTAL
      - Vous devez l'activer pour voir les options de masquage VPN

* Networking support
  CONFIG_NET

* Network firewalls
  CONFIG_FIREWALL

* TCP/IP networking
  CONFIG_INET

* IP: forwarding/gatewaying
  CONFIG_IP_FORWARD

* IP: firewalling
  CONFIG_IP_FIREWALL

* IP: masquerading (EXPERIMENTAL)
  CONFIG_IP_MASQUERADE
      - Option nécessaire.

* IP: PPTP masq support (EXPERIMENTAL)
  CONFIG_IP_MASQUERADE_PPTP
      - Active le masquage de canal de données PPTP, si vous
        masquez un client ou un serveur PPTP.

* IP: PPTP Call ID masq support (EXPERIMENTAL)
  CONFIG_IP_MASQUERADE_PPTP_MULTICLIENT
      - Active le masquage d'identifiant d'appel PPTP; nécessaire
        uniquement si vous comptez masquer plusieurs clients
        se connectant au même serveur distant. N'activez PAS
        cette option si vous masquez un serveur PPTP.

* IP: IPsec ESP & ISAKMP masq support (EXPERIMENTAL)
  CONFIG_IP_MASQUERADE_IPSEC
      - Active le masquage IPsec, si vous masquez une machine
        IPsec.

* IP: IPSEC masq table lifetime (minutes)
      - Voyez avec votre administrateur réseau pour déterminer
        quel est "l'intervalle de renouvellement des clés"
        ou la "durée de validité d'une clé".
        La durée de validité par défaut pour les entrées de la
        table de masquage est de trente minutes.
        Si l'intervalle de renouvellement des clés est supérieur
```

```
          à trente minutes, vous devez alors augmenter la durée
          de validité jusqu'à une valeur légèrement supérieure
          à l'intervalle de renouvellement des clés.

  * IP: always defragment
    CONFIG_IP_ALWAYS_DEFRAG
        − Très fortement recommandé pour un pare−feu.
```

NOTE : ce ne sont que les éléments dont vous avez besoin pour le masquage. Sélectionnez également toutes les autres options dont vous avez besoin pour votre configuration spécifique.

8. Recompilez le noyau, et installez−le pour le tester. Ne remplacez pas un noyau qui marche par votre nouveau noyau tant que vous n'avez pas vérifié qu'il fonctionnait.

Pour déterminer si le noyau qui tourne inclut ou non le support du masquage VPN, lancez la commande suivante :

```
grep −i masq /proc/ksyms
```

...et cherchez les entrées suivantes :

- Masquage IPsec : *ip_masq_out_get_isakmp*, *ip_masq_in_get_isakmp*, *ip_fw_masq_esp* et *ip_fw_demasq_esp*
- Masquage PPTP : *ip_fw_masq_gre* et *ip_fw_demasq_gre*
- Masquage d'identifiant d'appel PPTP : *ip_masq_pptp*

Si vous ne trouvez pas ces entrées, le masquage VPN n'est probablement pas supporté. Si vous avez des messages d'erreurs sur l'indisponibilité de */proc/ksyms* ou de */proc*, assurez−vous d'avoir activé le système de fichiers */proc* dans la configuration de votre noyau.

Regardez le Kernel HOWTO pour plus de détails sur la configuration et la recompilation de votre noyau.

Si vous utilisez le masquage IPsec et que votre système génère des erreurs de protection générale (regardez */var/log/messages*) ou bien se bloque, regardez le site du masquage VPN pour une mise à jour. Ce patch est pour le noyau 2.0.38, mais devrait fonctionner sur les noyaux antérieurs. Il a été soumis à Alan Cox pour être inclus dans le noyau 2.0.39.

3.4. Patcher et configurer le noyau 2.2.x pour le support de masquage VPN

1. Installez les sources du noyau (de préférence version 2.2.17 ou plus), que vous pouvez obtenir sur http://www.kernel.org/ ou un miroir. Les sources doivent être automatiquement extraites dans le répertoire */usr/src/linux*.
2. Configurez et testez le masquage IP standard (regardez le IP Masquerade HOWTO). Ceci va vous permettre de vous familiariser avec la recompilation de votre noyau, et plus largement, vous faire aborder le masquage IP.
3. *Sauvegardez les sources de votre noyau.*
4. Récupérez le patch noyau depuis le site du masquage VPN indiqué dans la section "Ressources" plus haut.

Pour les besoins de ce document, nous supposerons que vous avez sauvegardé le patch approprié sous */usr/src/ip_masq_vpn.patch.gz*.

5. Appliquez le patch de masquage VPN à votre noyau, si nécessaire.

   ♦ Allez dans le répertoire des sources :

   ```
   cd /usr/src
   ```

   ♦ Appliquez le patch :

   ```
   zcat ip_masq_vpn.patch.gz | patch −l −p0 > vpn−patch.log 2>&1
   ```

   ```
   Notez que les options sont "tiret L minuscule, tiret P minuscule zéro".
   Vous pourriez avoir des résultats étranges si vous changez l'ordre des arguments,
   car la commande patch semble sensible à l'ordre dans lequel ils apparaissent sur
   la ligne de commande.
   ```

   ```
   Notez également que le répertoire depuis lequel vous lancez la commande
   patch est différent pour le patch noyau 2.2.x.
   ```

   ♦ Vérifiez le contenu du fichier *vpn−patch.log* pour voir si certaines étapes ont échoué. Si des étapes ont échoué, alors vous avez sûrement oublié des options, ou lancé la commande patch depuis le mauvais répertoire. Utilisez votre sauvegarde pour récupérer votre noyau, et recommencez.

6. Si vous masquez un serveur VPN, vous n'avez *pas* besoin du patch *ipportfw* car la redirection de port est maintenant de base. Regardez la page de manuel de *ipmasqadm* pour de plus amples détails. Si *ipmasqadm* n'est pas inclus dans votre distribution, vous pouvez l'obtenir à l'adresse http://juanjox.kernelnotes.org/.
7. Configurez votre noyau et sélectionnez les options suivantes − répondez *YES* à ce qui suit :

```
  * Prompt for development and/or incomplete code/drivers
    CONFIG_EXPERIMENTAL
        - Vous devez l'activer pour voir les options de masquage VPN.

  * Networking support
    CONFIG_NET

  * Network firewalls
    CONFIG_FIREWALL

  * TCP/IP networking
    CONFIG_INET

  * IP: firewalling
    CONFIG_IP_FIREWALL

  * IP: always defragment
    CONFIG_IP_ALWAYS_DEFRAG
        - Nécessaire pour le masquage. Cette option peut être
          ou ne pas être dans la configuration de votre
          noyau. Si elle n'est pas présente, vous
          devez exécuter ceci dans vos scripts de démarrage :
        echo 1 > /proc/sys/net/ipv4/ip_always_defrag
```

```
* IP: masquerading (EXPERIMENTAL)
  CONFIG_IP_MASQUERADE
      − Option nécessaire.

* IP: masquerading special modules support
  CONFIG_IP_MASQUERADE_MOD
      − Option nécessaire.

* IP: ipportfw masq support (EXPERIMENTAL)
  CONFIG_IP_MASQUERADE_IPPORTFW
      − Activer cette option va vous permettre de masquer un serveur VPN.

* IP: PPTP masq support
  CONFIG_IP_MASQUERADE_PPTP
      − Active le masquage de canal de données PPTP, si vous
        masquez un client ou un serveur PPTP. Cette option
        est maintenant disponible en module.
        Notez que vous n'avez plus besoin de spécifier
        le masquage d'identifiant d'appel.

* IP: IPsec ESP & ISAKMP masq support (EXPERIMENTAL)
  CONFIG_IP_MASQUERADE_IPSEC
      − Active le masquage IPsec, si vous masquez une machine
        IPsec. Cette option est maintenant disponible en module.

* IP: IPsec masq table lifetime (minutes)
      − Voyez avec votre administrateur réseau pour déterminer
        quel est "l'intervalle de renouvellement des clés"
        ou "la durée de validité d'une clé".
        La durée de validité par défaut pour les entrées de la
        table de masquage est de trente minutes.
        Si l'intervalle de renouvellement des clés est supérieur
        à trente minutes, vous devez alors augmenter la durée
        de validité jusqu'à une valeur légèrement supérieure
        à l'intervalle de renouvellement des clés.

* IP: Enable parallel sessions (possible security risk − see help)
  CONFIG_IP_MASQUERADE_IPSEC_PAROK
      − Regardez les notes techniques sur le masquage IPsec et
        la section spéciale sur les informations sur la sécurité de ce HOWTO
        pour être au courant des problèmes de sécurité lorsque
        vous faites du masquage. Si vous ne masquez qu'un seul client
        IPsec, cette option n'a aucun effet.
```

Répondez *NO* à ce qui suit :

```
* IP: GRE tunnels over IP
  CONFIG_NET_IPGRE
      − Cette option n'a, contrairement aux apparences,
        *RIEN* à voir avec PPTP. Elle active le support
        pour les tunnels GRE tels qu'ils sont utilisés
        par les routeurs Cisco. Le fait que vous voyiez
        cette option n'implique pas que le support de
        PPTP est disponible. Vous devez toujours appliquer
        le patch pour le masquage VPN si les options
        PPTP listées ci−dessus n'apparaissent pas lorsque
        vous configurez votre noyau. N'activez PAS cette
        option, sauf si vous implémentez un tunnel GRE
        vers un routeur Cisco.
```

NOTE : ce ne sont que les options dont vous avez besoin pour faire du masquage. Sélectionnez également toutes les autres options dont vous avez besoin pour votre configuration spécifique.

8. Recompilez le noyau et installez−le pour le tester. Ne remplacez jamais un noyau qui fonctionne par votre nouveau noyau tant que vous n'avez pas la preuve qu'il fonctionne.

Pour savoir si le noyau qui tourne contient le support de masquage VPN, lancez la commande suivante :

```
grep −i masq /proc/ksyms
```

...et cherchez les entrées suivantes :

- Masquage IPsec : *ip_masq_esp* et *ip_demasq_esp*
- Masquage PPTP : *ip_masq_pptp_tcp* et *ip_demasq_pptp_tcp*

Ou lancez :

```
lsmod
```

...et cherchez les entrées suivantes :

- Masquage IPsec : *ip_masq_ipsec*
- Masquage PPTP : *ip_masq_pptp*

Si vous ne voyez pas ces entrées, le support de masquage VPN n'est probablement pas activé − avez−vous bien tapé *modprobe ip_masq_pptp.o* ou *modprobe ip_masq_ipsec.o* si vous les avez compilés en modules ? Si le masquage VPN ne fonctionne plus après le redémarrage de la machine, avez−vous inséré les commandes *modprobe* dans votre fichier de démarrage */etc/rc.d/rc.local* ?

Si vous avez des messages d'erreur sur l'indisponibilité de */proc/ksyms* ou de */proc*, assurez−vous d'avoir activé le système de fichiers */proc* lors de la configuration de votre noyau.

Allez voir le Kernel HOWTO pour de plus amples informations sur la configuration et la recompilation de votre noyau.

3.5. Paramétrage de ipfwadm pour un client ou un serveur VPN avec une adresse IP privée

Le pare−feu doit maintenant être configuré pour masquer le trafic VPN sortant. Vous pouvez souhaiter jeter un coup d'oeil sur http://www.wolfenet.com/~jhardin/ipfwadm.html pour voir une interface graphique pour la commande ipfwadm qui automatise une grande partie du paramétrage du filtrage de paquets au niveau de la sécurité.

Les règles pare−feu minimales sont :

```
# Met la politique par défaut de transmission des paquets à REFUS
ipfwadm −F −p deny
# Autorise le trafic sur le réseau local
ipfwadm −I −a accept    −S 10.0.0.0/8 −D 0.0.0.0/0  −W eth0
ipfwadm −O −a accept    −S 0.0.0.0/0  −D 10.0.0.0/8 −W eth0
# Masque le trafic pour les adresses internet et autorise le trafic internet
ipfwadm −F −a accept −m −S 10.0.0.0/8 −D 0.0.0.0/0  −W ppp0
ipfwadm −O −a accept    −S 0.0.0.0/0  −D 0.0.0.0/0  −W ppp0
ipfwadm −I −a accept    −S 0.0.0.0/0  −D 0.0.0.0/0  −W ppp0
ou, si vous avez une connexion permanente,
ipfwadm −F −a accept −m −S 10.0.0.0/8 −D 0.0.0.0/0  −W eth1
ipfwadm −O −a accept    −S 0.0.0.0/0  −D 0.0.0.0/0  −W eth1
ipfwadm −I −a accept    −S 0.0.0.0/0  −D 0.0.0.0/0  −W eth1
```

Mais ce paramétrage est complètement ouvert. Il va permettre de masquer *tous* les trafics en provenance de *toutes* les machines du réseau interne destiné à *n'importe quelle* machine sur internet, et ne met en place absolument *aucune* sécurité.

Un paramétrage de pare−feu rigoureux n'autoriserait que le trafic entre le client et le serveur, et bloquerait tout le reste :

```
# Met la politique par défaut à REFUS :
ipfwadm -I -p deny
ipfwadm -O -p deny
ipfwadm -F -p deny
# Autorise le trafic sur le réseau local
ipfwadm -I -a accept -S 10.0.0.0/8 -D 0.0.0.0/0  -W eth0
ipfwadm -O -a accept -S 0.0.0.0/0  -D 10.0.0.0/8 -W eth0
# Masque uniquement le trafic VPN entre le client VPN et le serveur VPN
ipfwadm -F -a accept -m -P udp -S 10.0.0.2/32 500 -D 199.0.0.1/32 500  -W ppp0
ipfwadm -F -a accept -m -P tcp -S 10.0.0.2/32     -D 199.0.0.1/32 1723 -W ppp0
ipfwadm -F -a deny      -P tcp -S 10.0.0.2/32     -D 199.0.0.1/32      -W ppp0
ipfwadm -F -a deny      -P udp -S 10.0.0.2/32     -D 199.0.0.1/32      -W ppp0
ipfwadm -F -a accept -m -P all -S 10.0.0.2/32     -D 199.0.0.1/32      -W ppp0
ipfwadm -O -a accept    -P udp -S 200.200.200.0/24 500 -D 199.0.0.1/32 500  -W ppp0
ipfwadm -O -a accept    -P tcp -S 200.200.200.0/24     -D 199.0.0.1/32 1723 -W ppp0
ipfwadm -O -a deny      -P tcp -S 200.200.200.0/24     -D 199.0.0.1/32      -W ppp0
ipfwadm -O -a deny      -P udp -S 200.200.200.0/24     -D 199.0.0.1/32      -W ppp0
ipfwadm -O -a accept    -P all -S 200.200.200.0/24     -D 199.0.0.1/32      -W ppp0
ipfwadm -I -a accept    -P udp -S 199.0.0.1/32 500     -D 200.200.200.0/24 500 -W ppp0
ipfwadm -I -a accept    -P tcp -S 199.0.0.1/32 1723    -D 200.200.200.0/24     -W ppp0
ipfwadm -I -a deny      -P tcp -S 199.0.0.1/32         -D 200.200.200.0/24     -W ppp0
ipfwadm -I -a deny      -P udp -S 199.0.0.1/32         -D 200.200.200.0/24     -W ppp0
ipfwadm -I -a accept    -P all -S 199.0.0.1/32         -D 200.200.200.0/24     -W ppp0
ou, si vous avez une connexion permanente
ipfwadm -F -a accept -m -P udp -S 10.0.0.2/32 500 -D 199.0.0.1/32 500  -W eth1
ipfwadm -F -a accept -m -P tcp -S 10.0.0.2/32     -D 199.0.0.1/32 1723 -W eth1
ipfwadm -F -a deny      -P tcp -S 10.0.0.2/32     -D 199.0.0.1/32      -W eth1
ipfwadm -F -a deny      -P udp -S 10.0.0.2/32     -D 199.0.0.1/32      -W eth1
ipfwadm -F -a accept -m -P all -S 10.0.0.2/32     -D 199.0.0.1/32      -W eth1
ipfwadm -O -a accept    -P udp -S 200.200.200.200/32 500 -D 199.0.0.1/32 500  -W eth1
ipfwadm -O -a accept    -P tcp -S 200.200.200.200/32     -D 199.0.0.1/32 1723 -W eth1
ipfwadm -O -a deny      -P tcp -S 200.200.200.200/32     -D 199.0.0.1/32      -W eth1
ipfwadm -O -a deny      -P udp -S 200.200.200.200/32     -D 199.0.0.1/32      -W eth1
ipfwadm -O -a accept    -P all -S 200.200.200.200/32     -D 199.0.0.1/32      -W eth1
ipfwadm -I -a accept    -P udp -S 199.0.0.1/32 500  -D 200.200.200.200/32 500 -W eth1
ipfwadm -I -a accept    -P tcp -S 199.0.0.1/32 1723 -D 200.200.200.200/32     -W eth1
ipfwadm -I -a deny      -P tcp -S 199.0.0.1/32      -D 200.200.200.200/32     -W eth1
ipfwadm -I -a deny      -P udp -S 199.0.0.1/32      -D 200.200.200.200/32     -W eth1
ipfwadm -I -a accept    -P all -S 199.0.0.1/32      -D 200.200.200.200/32     -W eth1
```

Note : ces règles n'autorisent que le trafic VPN et bloquent *tout le reste*. Vous devez ajouter des règles pour tous les autres flux que vous voulez autoriser, comme par exemple DNS, HTTP, POP, IMAP, etc...

3.6. Paramétrage d'ipchains pour un client ou serveur VPN avec une adresse IP privée

Les règles pare−feu ipchains minimales sont :

```
# Met la politique par défaut de transmission des paquets à REFUS
ipchains -P forward DENY
# Autorise le trafic sur le réseau local
ipchains -A input   -j ACCEPT -s 10.0.0.0/8 -d 0.0.0.0/0  -i eth0
ipchains -A output  -j ACCEPT -s 0.0.0.0/0  -d 10.0.0.0/8 -i eth0
# Masque le trafic vers les adresses internet et autorise le trafic internet
```

```
ipchains −A forward −j MASQ   −s 10.0.0.0/8 −d 0.0.0.0/0  −i ppp0
ipchains −A output  −j ACCEPT −s 0.0.0.0/0  −d 0.0.0.0/0  −i ppp0
ipchains −A input   −j ACCEPT −s 0.0.0.0/0  −d 0.0.0.0/0  −i ppp0
ou, si vous avez une connexion permanente,
ipchains −A forward −j MASQ   −s 10.0.0.0/8 −d 0.0.0.0/0  −i eth1
ipchains −A output  −j ACCEPT −s 0.0.0.0/0  −d 0.0.0.0/0  −i eth1
ipchains −A input   −j ACCEPT −s 0.0.0.0/0  −d 0.0.0.0/0  −i eth1
```

Mais ce paramétrage est complètement ouvert. Il va permettre de masquer *tous* les trafics en provenance de *toutes* les machines du réseau interne destiné à *n'importe quelle* machine sur internet, et ne met en place absolument *aucune* sécurité.

Un paramétrage de pare−feu rigoureux n'autoriserait que le trafic entre le client et le serveur, et bloquerait tout le reste :

```
# Met la politique par défaut à REFUS :
ipchains −P input   DENY
ipchains −P output  DENY
ipchains −P forward DENY
# Autorise le trafic sur le réseau local
ipchains −A input  −j ACCEPT −s 10.0.0.0/8 −d 0.0.0.0/0  −i eth0
ipchains −A output −j ACCEPT −s 0.0.0.0/0  −d 10.0.0.0/8 −i eth0
# Masque uniquement le trafic VPN entre le client VPN et le serveur VPN
# IPsec
ipchains −A forward −j MASQ   −p udp −s 10.0.0.2/32 500      −d 199.0.0.1/32 500     −i ppp0
ipchains −A output  −j ACCEPT −p udp −s 200.200.200.0/24 500 −d 199.0.0.1/32 500     −i ppp0
ipchains −A input   −j ACCEPT −p udp −s 199.0.0.1/32 500     −d 200.200.200.0/24 500 −i ppp0
ipchains −A forward −j MASQ   −p 50  −s 10.0.0.2/32          −d 199.0.0.1/32         −i ppp0
ipchains −A output  −j ACCEPT −p 50  −s 200.200.200.0/24     −d 199.0.0.1/32         −i ppp0
ipchains −A input   −j ACCEPT −p 50  −s 199.0.0.1/32         −d 200.200.200.0/24     −i ppp0
# PPTP
ipchains −A forward −j MASQ   −p tcp −s 10.0.0.2/32       −d 199.0.0.1/32 1723 −i ppp0
ipchains −A output  −j ACCEPT −p tcp −s 200.200.200.0/24  −d 199.0.0.1/32 1723 −i ppp0
ipchains −A input   −j ACCEPT −p tcp −s 199.0.0.1/32 1723 −d 200.200.200.0/24  −i ppp0
ipchains −A forward −j MASQ   −p 47  −s 10.0.0.2/32       −d 199.0.0.1/32      −i ppp0
ipchains −A output  −j ACCEPT −p 47  −s 200.200.200.0/24  −d 199.0.0.1/32      −i ppp0
ipchains −A input   −j ACCEPT −p 47  −s 199.0.0.1/32      −d 200.200.200.0/24  −i ppp0
ou, si vous avez une connexion permanente,
# IPsec
ipchains −A forward −j MASQ   −p udp −s 10.0.0.2/32 500        −d 199.0.0.1/32 500       −i eth1
ipchains −A output  −j ACCEPT −p udp −s 200.200.200.200/32 500 −d 199.0.0.1/32 500       −i eth1
ipchains −A input   −j ACCEPT −p udp −s 199.0.0.1/32 500       −d 200.200.200.200/32 500 −i eth1
ipchains −A forward −j MASQ   −p 50  −s 10.0.0.2/32            −d 199.0.0.1/32           −i eth1
ipchains −A output  −j ACCEPT −p 50  −s 200.200.200.200/32     −d 199.0.0.1/32           −i eth1
ipchains −A input   −j ACCEPT −p 50  −s 199.0.0.1/32           −d 200.200.200.200/32     −i eth1
# PPTP
ipchains −A forward −j MASQ   −p tcp −s 10.0.0.2/32        −d 199.0.0.1/32 1723  −i eth1
ipchains −A output  −j ACCEPT −p tcp −s 200.200.200.200/32 −d 199.0.0.1/32 1723  −i eth1
ipchains −A input   −j ACCEPT −p tcp −s 199.0.0.1/32 1723  −d 200.200.200.200/32 −i eth1
ipchains −A forward −j MASQ   −p 47  −s 10.0.0.2/32        −d 199.0.0.1/32       −i eth1
ipchains −A output  −j ACCEPT −p 47  −s 200.200.200.200/32 −d 199.0.0.1/32       −i eth1
ipchains −A input   −j ACCEPT −p 47  −s 199.0.0.1/32       −d 200.200.200.200/32 −i eth1
```

Note : ces règles n'autorisent que le trafic VPN. Vous devrez ajouter des règles pour tous les autres flux que vous souhaitez autoriser, comme par exemple DNS, HTTP, POP, IMAP, etc...

Notez également combien ces règles sont plus propres et plus faciles à comprendre que les règles ipfwadm équivalentes. C'est parce que ipchains autorise la spécification de tous les protocoles IP, et pas seulement TCP, UDP, ICMP, ou ALL.

3.7. Une note sur l'adressage IP dynamique

Si votre pare−feu se voit attribuer une adresse IP dynamique par votre FAI (les comptes modems fonctionnent comme ça, ainsi que certains cablo−opérateurs), alors vous devez ajouter ce qui suit au script de démarrage */etc/rc.d/rc.local*:

```
echo 7 > /proc/sys/net/ipv4/ip_dynaddr
```

Ceci active le suivi d'adresse IP dynamique, ce qui signifie que si votre connexion tombe et remonte, toutes les sessions actives seront mises à jour avec la nouvelle adresse IP plutôt que de continuer à essayer d'utiliser l'ancienne adresse IP. Cela ne veut pas dire que les sessions resteront actives malgré l'interruption, mais plutôt qu'elles se fermeront rapidement.

Si vous ne le faites pas, il peut y avoir une "période de latence" après la reconnexion et avant l'expiration des anciennes entrées de la table de masquage pendant laquelle vous serez masqué avec la mauvaise adresse IP, ce qui vous empêchera d'établir une connexion.

Ceci est particulièrement utile si vous utilisez un démon de demande de connexion comme *diald* pour gérer votre connexion modem.

Regardez le fichier */usr/src/linux/Documentation/networking/ip_dynaddr.txt* pour de plus amples détails.

3.8. Paramétrages additionnels pour un serveur VPN avec une adresse IP privée

Si vous mettez en place le masquage VPN pour un serveur VPN avec une adresse IP privée (c'est à dire que vous voulez faire du masquage aussi bien pour les connexions *entrantes* que *sortantes*), vous avez également besoin d'installer deux outils de transmission de paquets. L'un(*ipportfw*) fait suivre le trafic TCP ou UDP entrant adressé à un port spécifique du pare−feu vers une machine sur le réseau local derrière le pare−feu. Il est utilisé pour rediriger le canal de contrôle PPTP initial 1723/tcp en entrée, ou le trafic ISAKMP 500/udp vers le serveur VPN. L'autre (*ipfwd*) est un outil de transmission de paquets plus générique, qui peut être utilisé pour tous les protocoles IP. Il est utilisé pour faire suivre le trafic entrant initial 47/ip (GRE) ou 50/ip (ESP) du canal de données vers le serveur VPN.

Les sorties en réponse au trafic entrant 1723/tcp ou 500/udp sont masquées grâce aux fonctionnalités standard de masquage IP du noyau Linux. Le trafic sortant 47/ip ou 50/ip est masqué grâce au patch du noyau pour le masquage VPN que vous avez installé précédemment.

Une fois que ces outils sont installés, vous devez les configurer pour faire suivre le trafic vers le serveur VPN.

- Paramétrer *ipportfw* pour les noyaux 2.0.x

  Les commandes suivantes vont paramétrer *ipportfw* pour faire suivre le trafic 500/udp entrant vers le serveur IPsec :

  ```
  # Paramétrage d'ipportfw pour IPsec avec une adresse IP statique
  # Vide la table de redirection d'ipportfw
  /sbin/ipportfw −C
  # Fait suivre le trafic adressé au port 500/udp du pare−feu
  # au port 500/udp du serveur IPsec
  /sbin/ipportfw −A −u 200.200.200.200/500 −R 10.0.0.2/500
  ```

Les commandes suivantes vont paramétrer *ipportfw* pour faire suivre le trafic entrant 1723/tcp initial vers le serveur PPTP :

```
# Paramétrage d'ipportfw pour PPTP avec une adresse IP statique
# Vide la table de redirection d'ipportfw
/sbin/ipportfw −C
# Fait suivre le trafic adressé au port 1723/tcp du pare−feu
# vers le port 1723/tcp du serveur PPTP
/sbin/ipportfw −A −t 200.200.200.200/1723 −R 10.0.0.2/1723
```

Notez que les paramètres d'ipportfw contiennent l'adresse IP internet du pare−feu, et que vous ne pouvez pas spécifier l'interface (par exemple *ppp0*) contrairement à ipfwadm. Ceci veut dire que dans le cas d'une connexion IP dynamique (comme pour une connexion PPP par modem) vous devez lancer ces commandes à chaque fois que vous vous connectez à internet, et qu'une nouvelle adresse IP vous est attribuée. Vous pouvez le faire assez facilement − ajoutez simplement les lignes suivantes à votre script */etc/ppp/ip−up* ou */etc/ppp/ip−up.local* :

```
# Paramétrage d'ippportfw pour IPsec avec une adresse IP dynamique
# Vide la table de redirection d'ipportfw
/sbin/ipportfw −C
# Fait suivre le trafic adressé au port 500/udp du pare−feu
# vers le port 500/udp du serveur IPsec
/sbin/ipportfw −A −u ${4}/500 −R 10.0.0.2/500
```

ou :

```
# Paramétrage d'ipportfw pour PPTP avec une adresse IP dynamique
# Vide la table de redirection d'ipportfw
/sbin/ipportfw −C
# Fait suivre le trafic adressé au port 1723/tcp du pare−feu
# vers le port 1723 du serveur PPTP
/sbin/ipportfw −A −t ${4}/1723 −R 10.0.0.2/1723
```

Allez voir http://www.wolfenet.com/~jhardin/ipfwadm/invocation.html pour de plus amples détails sur la mise en place d'un pare−feu avec une adresse IP dynamique.

- Configurer *ipfwd* pour les noyaux 2.0.x et 2.2.x

  La commande suivante va paramétrer *ipfwd* pour faire suivre le trafic entrant 50/ip initial au le serveur IPsec :

  ```
  /sbin/ipfwd --masq 10.0.0.2 50 &
  ```

  La commande suivante va paramétrer *ipfwd* pour faire suivre le trafic entrant 47/ip initial au serveur PPTP :

  ```
  /sbin/ipfwd --masq 10.0.0.2 47 &
  ```

  Cette commande n'a besoin d'être exécutée qu'une seule fois, depuis votre script */etc/rc.d/rc.local*.

Les techniques décrites ici peuvent être généralisées pour autoriser le masquage de la plupart des serveurs − HTTP, FTP, SMTP, etc. Les serveurs qui sont basés uniquement sur TCP ou UDP n'ont pas besoin de *ipfwd*.

Si vous masquez un serveur PPTP, vous avez aussi besoin de vous assurer que vous n'avez *pas* activé le masquage d'identifiant d'appel PPTP dans le noyau. L'activation du masquage d'identifiant d'appel PPTP fait croire que vous masquez uniquement des clients PPTP, l'activer risque donc de vous empêcher de masquer correctement le trafic du serveur PPTP. Cela signifie également qu'avec la version 2.0.x du patch, vous ne pouvez pas masquer simultanément un serveur PPTP et des clients PPTP.

3.9. Paramétrage d'ipfwadm pour un serveur VPN avec une adresse IP publique

Mettre en place un serveur VPN avec une adresse IP publique se trouvant derrière un pare−feu Linux est un simple problème de routage et de filtrage de paquets. Le masquage n'est pas nécessaire.

Malheureusement les noyaux 2.0.x ne nous permettent pas de préciser le protocole IP 47 ou 50, donc ce pare−feu est moins sûr que ce qu'il aurait pu être. Si cela vous pose un problème, alors installez le patch noyau pour les chaînes pare−feu IP ou passez à un noyau de la série 2.1.x ou 2.2.x, avec lesquels vous pouvez faire du filtrage par protocole IP.

Les règles pare−feu vont avoir un peu cette tête là :

```
# Cette section doit se trouver après vos autres règles pare−feu

# Précisez explicitement les clients potentiels pour plus de sécurité
# Autorise le trafic ISAKMP IPsec entrant et sortant.
ipfwadm −I −a accept −W eth1 −V 200.200.200.200 −P udp −S 199.0.0.2/32 500 −D 222.0.0.2/32 500
ipfwadm −O −a accept −W eth1 −V 200.200.200.200 −P udp −D 199.0.0.2/32 500 −S 222.0.0.2/32 500
ipfwadm −I −a accept −W eth1 −V 200.200.200.200 −P udp −S 199.0.0.3/32 500 −D 222.0.0.2/32 500
ipfwadm −O −a accept −W eth1 −V 200.200.200.200 −P udp −D 199.0.0.3/32 500 −S 222.0.0.2/32 500
# Autorise le canal de contrôle PPTP en entrée et en sortie
ipfwadm −I −a accept −W eth1 −V 200.200.200.200 −P tcp −S 199.0.0.2/32 −D 222.0.0.2/32 1723
ipfwadm −O −a accept −W eth1 −V 200.200.200.200 −P tcp −D 199.0.0.2/32 −S 222.0.0.2/32 1723
ipfwadm −I −a accept −W eth1 −V 200.200.200.200 −P tcp −S 199.0.0.3/32 −D 222.0.0.2/32 1723
ipfwadm −O −a accept −W eth1 −V 200.200.200.200 −P tcp −D 199.0.0.3/32 −S 222.0.0.2/32 1723

# Bloque tous les autres trafics TCP et UDP en provenance d'internet
# Ceci est principalement une règle "défaut refus TCP/UDP" qui
# ne s'applique qu'à l'interface internet.
ipfwadm −I −a deny −W eth1 −V 200.200.200.200 −P tcp
ipfwadm −I −a deny −W eth1 −V 200.200.200.200 −P udp

# Précisez explicitement les clients potentiels pour plus de sécurité
# Notez que ce paramétrage est trop large, car nous sommes
# obligés de préciser "−P all" au lieu de "−P 47" ou "−P 50"...
# Autorise le canal de données PPTP et le trafic ESP IPsec entrant et sortant.
ipfwadm −I −a accept −W eth1 −V 200.200.200.200 −P all −S 199.0.0.2/32 −D 222.0.0.2/32
ipfwadm −0 −a accept −W eth1 −V 200.200.200.200 −P all −D 199.0.0.2/32 −S 222.0.0.2/32
ipfwadm −I −a accept −W eth1 −V 200.200.200.200 −P all −S 199.0.0.3/32 −D 222.0.0.2/32
ipfwadm −O −a accept −W eth1 −V 200.200.200.200 −P all −D 199.0.0.3/32 −S 222.0.0.2/32

# Bloque tous les autres trafics en provenance d'internet.
# Ceci est principalement une règle du type "par défaut, refus"
# qui ne s'applique qu'à l'interface internet.
ipfwadm −I −a deny −W eth1 −V 200.200.200.200
```

Si vous installez des règles pare−feu ou des règle de transmission de paquets sur l'interface interne, vous aurez à faire quelque chose de semblable. L'exemple ci−dessus ne concerne que le trafic VPN ; il vous faut l'insérer dans votre paramétrage pare−feu actuel pour autoriser les autres trafics dont vous avez besoin.

3.10. Paramétrage d'ipfwadm pour un client VPN avec une adresse IP publique

La mise en place d'un client VPN avec une adresse IP publique derrière un pare−feu Linux est similaire à celle d'un serveur VPN avec une adresse IP publique.

Les règles pare−feu auront cette allure :

```
# Autorise le trafic ISAKMP IPsec entrant et sortant.
ipfwadm -O -a accept -W eth1 -V 200.200.200.200 -P udp -S 222.0.0.2/32 500 -D 199.0.0.1/32 500
ipfwadm -I -a accept -W eth1 -V 200.200.200.200 -P udp -D 222.0.0.2/32 500 -S 199.0.0.1/32 500
# Autorise le canal de contrôle PPTP en entrée et en sortie.
ipfwadm -O -a accept -W eth1 -V 200.200.200.200 -P tcp -S 222.0.0.2/32 -D 199.0.0.1/32 1723
ipfwadm -I -a accept -W eth1 -V 200.200.200.200 -P tcp -D 222.0.0.2/32 -S 199.0.0.1/32 1723

# Bloque tous les autres trafics TCP et UDP en provenance d'internet.
# Ceci est principalement une règle "par défaut, refus de TCP/UDP" qui
# ne s'applique qu'à l'interface internet.
ipfwadm -I -a deny -W eth1 -V 200.200.200.200 -P tcp
ipfwadm -I -a deny -W eth1 -V 200.200.200.200 -P udp

# Notez que ce paramétrage est trop large, car nous sommes
# obligés de préciser "-P all" au lieu de "-P 47" ou "-P 50"...
# Autorise le canal de données PPTP et le trafic ESP IPsec entrant et sortant.
ipfwadm -O -a accept -W eth1 -V 200.200.200.200 -P all -S 222.0.0.2/32 -D 199.0.0.1/32
ipfwadm -I -a accept -W eth1 -V 200.200.200.200 -P all -D 222.0.0.2/32 -S 199.0.0.1/32

# Bloque tous les autres trafics en provenance d'internet.
# Ceci est principalement une règle du type "par défaut, refus"
# qui ne s'applique qu'à l'interface internet.
ipfwadm -I -a deny -W eth1 -V 200.200.200.200
```

3.11. Paramétrage d'ipchains pour un serveur VPN avec une adresse IP publique

Mettre en place un serveur VPN avec une adresse IP publique derrière un pare−feu Linux correspond à vérifier que les commandes de routage et de filtrage de paquet appropriées sont bien en place. Le masquage n'est pas nécessaire.

Les règles pare−feu auront cette allure :

```
# Spécifiez explicitement les clients potentiels pour plus de sécurité.
# Autorise le trafic ISAKMP IPsec entrant et sortant.
ipchains -A input  -j ACCEPT -p udp -s 199.0.0.2/32 500 -d 222.0.0.2/32 500 -i eth1
ipchains -A output -j ACCEPT -p udp -d 199.0.0.2/32 500 -s 222.0.0.2/32 500 -i eth1
ipchains -A input  -j ACCEPT -p udp -s 199.0.0.3/32 500 -d 222.0.0.2/32 500 -i eth1
ipchains -A output -j ACCEPT -p udp -d 199.0.0.3/32 500 -s 222.0.0.2/32 500 -i eth1
# Autorise le trafic ESP IPsec entrant et sortant.
ipchains -A input  -j ACCEPT -p 50  -s 199.0.0.2/32     -d 222.0.0.2/32     -i eth1
ipchains -A output -j ACCEPT -p 50  -d 199.0.0.2/32     -s 222.0.0.2/32     -i eth1
ipchains -A input  -j ACCEPT -p 50  -s 199.0.0.3/32     -d 222.0.0.2/32     -i eth1
ipchains -A output -j ACCEPT -p 50  -d 199.0.0.3/32     -s 222.0.0.2/32     -i eth1
# Autorise le canal de contrôle PPTP en entrée et en sortie.
ipchains -A input  -j ACCEPT -p tcp -s 199.0.0.2/32 -d 222.0.0.2/32 1723 -i eth1
ipchains -A output -j ACCEPT -p tcp -d 199.0.0.2/32 -s 222.0.0.2/32 1723 -i eth1
ipchains -A input  -j ACCEPT -p tcp -s 199.0.0.3/32 -d 222.0.0.2/32 1723 -i eth1
ipchains -A output -j ACCEPT -p tcp -d 199.0.0.3/32 -s 222.0.0.2/32 1723 -i eth1
# Autorise le tunnel PPTP en entrée et en sortie.
ipchains -A input  -j ACCEPT -p 47  -s 199.0.0.2/32 -d 222.0.0.2/32      -i eth1
ipchains -A output -j ACCEPT -p 47  -d 199.0.0.2/32 -s 222.0.0.2/32      -i eth1
ipchains -A input  -j ACCEPT -p 47  -s 199.0.0.3/32 -d 222.0.0.2/32      -i eth1
ipchains -A output -j ACCEPT -p 47  -d 199.0.0.3/32 -s 222.0.0.2/32      -i eth1
```

Si vous installez des règles pare−feu ou des règles de transmission de paquets sur l'interface interne, vous aurez à faire quelque chose de semblable. L'exemple ci−dessus ne concerne que le trafic VPN ; il vous faut l'insérer dans votre paramétrage pare−feu actuel pour autoriser les autres trafics dont vous avez besoin.

3.12. Paramétrage d'ipchains pour un client VPN avec une adresse IP publique

La mise en place d'un client VPN avec une adresse IP publique derrière un pare−feu Linux est identique à celle d'un serveur VPN avec une adresse IP publique.

Les règles pare−feu auront cette allure :

```
# Autorise le trafic ISAKMP IPsec entrant et sortant.
ipchains −A output −j ACCEPT −p udp −s 222.0.0.2/32 500 −d 199.0.0.1/32 500 −i eth1
ipchains −A input  −j ACCEPT −p udp −d 222.0.0.2/32 500 −s 199.0.0.1/32 500 −i eth1
# Autorise le trafic ESP IPsec entrant et sortant.
ipchains −A output −j ACCEPT −p 50  −s 222.0.0.2/32     −d 199.0.0.1/32     −i eth1
ipchains −A input  −j ACCEPT −p 50  −d 222.0.0.2/32     −s 199.0.0.1/32     −i eth1
# Autorise le canal de contrôle PPTP en entrée et en sortie.
ipchains −A output −j ACCEPT −p tcp −s 222.0.0.2/32 −d 199.0.0.1/32 1723 −i eth1
ipchains −A input  −j ACCEPT −p tcp −d 222.0.0.2/32 −s 199.0.0.1/32 1723 −i eth1
# Autorise le tunnel PPTP en entrée et en sortie.
ipchains −A output −j ACCEPT −p 47  −s 222.0.0.2/32 −d 199.0.0.1/32      −i eth1
ipchains −A input  −j ACCEPT −p 47  −d 222.0.0.2/32 −s 199.0.0.1/32      −i eth1
```

3.13. Masquage VPN et LRP

Le projet de routeur Linux (Linux Router Project), qui se trouve à l'adresse http://www.linuxrouter.org/, fournit un kit pare−feu−sur−disquette basé sur Linux. Avec un PC '386, deux cartes réseaux, et un lecteur de disquette, vous pouvez mettre en place un pare−feu masquant avec toutes les fonctionnalités. Aucun disque dur n'est nécessaire.

Le masquage VPN est censé être inclus dans la version 2.2.9 de LRP − pour vérifier s'il est disponible, regardez si *ip_masq_ipsec* ou *ip_masq_pptp* sont dans la liste des modules chargeables dans *Package Settings −> Modules*, ou faites un grep sur */proc/ksyms* comme décrit plus haut. Si vous voulez ajouter le masquage VPN à une version antérieure du LRP, alors quelqu'un sur la liste de diffusion du LRP pourra vous fournir une image de disquette, ou bien vous pouvez faire votre propre noyau en utilisant les instructions qui se trouvent sur la page du LRP.

Les règles pare−feu seront ajoutées au script de démarrage dans *Network Settings −> Direct Network Setup*.

3.14. Masquage VPN sur un système tournant avec FreeS/WAN ou PoPToP

Si vous souhaitez utiliser le pare−feu en tant que passerelle IPsec avec FreeS/WAN, vous *ne devez pas* activer le masquage IPsec. Si vous souhaitez utiliser le pare−feu comme serveur PPTP avec PoPToP, ou comme client PPTP en utilisant le logiciel client PPTP pour Linux, vous *ne devez pas* activer le masquage PPTP.

Le masquage VPN et le client ou serveur VPN utilisant les mêmes protocoles, ils ne peuvent pas cohabiter sur le même ordinateur.

Votre pare−feu *peut*, cependant, être une passerelle VPN IPsec FreeS/WAN et faire du masquage PPTP, ou vice−versa.

4. Configurer le client VPN

4.1. Configurer un client MS W'95

1. Configurez votre routage pour que votre pare−feu Linux soit votre passerelle par défaut :

    a. Ouvrez *Panneau de configuration/Réseau* ou faites un clic droit sur "Voisinage Réseau" et cliquez sur *Propriétés*.
    b. Cliquez sur l'onglet *Configuration*.
    c. Dans la liste des composants réseaux installés, faites un double−clic sur la ligne "TCP/IP −> votre−carte−réseau".
    d. Cliquez sur l'onglet *Passerelle*.
    e. Entrez l'adresse IP locale de votre pare−feu Linux. Enlevez les autres passerelles.
    f. Cliquez sur le bouton "OK".
2. Testez le masquage. Par exemple, lancez "*telnet le.serveur.de.mail.de.mon.fai smtp*" et vous devriez voir la bannière d'accueil du serveur de mail.
3. Installez et configurez le logiciel de VPN. Pour le logiciel IPsec, suivez les instructions de l'éditeur. Pour PPTP de MS :

    a. Ouvrez *Panneau de Configuration/Réseau* ou faites un clic droit sur "Voisinage Réseau" et cliquez sur *Propriétés*.
    b. Cliquez sur l'onglet *Configuration*.
    c. Cliquez sur le bouton "Ajouter", et cliquez ensuite sur la ligne "Carte".
    d. Sélectionnez "Microsoft" comme constructeur, et ajoutez l'adaptateur "Carte de Réseau Privé Virtuel Microsoft".
    e. Redémarrez lorsque l'ordinateur vous le demande.
    f. Si vous avez besoin de cryptage fort (128 bits), téléchargez la mise à jour pour cryptage fort de DUN 1.3 sur le site sécurisé de MS à l'adresse http://mssecure.www.conxion.com/cgi−bin/ntitar.pl et installez la, redémarrez ensuite quand l'ordinateur vous le demande.
    g. Créez une nouvelle entrée dans votre carnet d'adresse d'appel distant pour votre serveur PPTP.
    h. Sélectionnez l'adaptateur VPN comme périphérique à utiliser, et entrez l'adresse IP internet du serveur PPTP comme numéro de téléphone.
    i. Sélectionnez l'onglet *Types de Serveur*, et cochez les cases *Activer la compression logicielle* et *Demander un mot de passe crypté*.
    j. Cliquez sur le bouton "Paramétrages TCP/IP".
    k. Renseignez les informations concernant l'adresse IP dynamique/statique de votre client comme précisé par l'administrateur de votre serveur PPTP.
    l. Si vous souhaitez avoir accès à votre réseau local pendant que votre connexion PPTP est active, décochez la case "Utiliser la passerelle par défaut pour le réseau distant".
    m. Redémarrez encore quelques fois, juste par habitude... :−)

4.2. Configurer un client MS W'98

1. Configurez le routage pour que le pare−feu Linux soit votre passerelle par défaut, et testez le masquage comme indiqué plus haut.

2. Installez et configurez le logiciel de VPN. Pour un logiciel IPsec, suivez les instructions de l'éditeur. Pour PPTP de MS :

   a. Ouvrez *Panneau de Configuration/Ajout/Suppression de programme* et cliquez sur l'onglet*Installation de Windows*.
   b. Cliquez sur l'option *Communications* et cliquez sur le bouton "Détails...".
   c. Assurez vous que l'option "Réseau Privé Virtuel (VPN)" est cochée. Cliquez alors sur le bouton "OK".
   d. Redémarrez la machine lorsqu'on vous le demande.
   e. Si vous avez besoin d'utiliser du cryptage fort (128 bits), téléchargez la mise à jour sécurité pour le cryptage fort VPN sur le site sécurisé de MS à l'adresse : http://mssecure.www.conxion.com/cgi−bin/ntitar.pl et installez−la, et ensuite redémarrez encore lorsqu'on vous le demande.

3. Créez et testez une nouvelle entrée pour votre serveur VPN dans votre carnet d'adresse d'appel distant, comme décrit plus haut.

4.3. Configurer un client MS W'ME

Je n'en ai pas vu pour l'instant. Je suppose que la procédure est très proche de celle pour W'98. Quelqu'un pourrait−il me dire quelles sont les différences, s'il y en a ? Merci.

4.4. Configurer un client MS NT

```
Note: cette section peut être incomplète car ça fait
un petit moment que je n'ai pas installé PPTP sur un système NT.
```

1. Configurez votre routage pour que le pare−feu Linux soit votre passerelle par défaut :

   a. Ouvrez *Panneau de Configuration/Réseau* ou faites un clic droit sur "Voisinage Réseau" et cliquez sur *Propriétés*.
   b. Cliquez sur l'onglet *Protocoles* et faites un double−clic sur la ligne "Protocole TCP/IP".
   c. Entrez l'adresse IP locale de votre pare−feu Linux dans la zone de dialogue "Passerelle par défaut".
   d. Cliquez sur le bouton "OK".

2. Testez le masquage. Par exemple, lancez "*telnet le.serveur.de.mail.de.mon.fai smtp*" et vous devriez voir apparaître la bannière d'accueil du serveur de mails.
3. Installez et configurez le logiciel VPN. Pour un logiciel IPsec, suivez les instructions de l'éditeur. Pour PPTP de MS :

   a. Ouvrez *Panneau de Configuration/Réseau* ou faites un clic droit sur "Voisinage Réseau" et cliquez sur *Propriétés*.
   b. Cliquez sur l'onglet *Protocoles*.
   c. Cliquez sur le bouton "Ajouter", et faites ensuite un double−clic sur la ligne "Point to Point Tunneling Protocol".
   d. Quand on vous demande les numéros de Réseaux Virtuels Privés, entrez les numéros des serveurs PPTP que vous pouvez potentiellement joindre.
   e. Redémarrez lorsqu'on vous le demande.

f. Si vous avez besoin d'utiliser du cryptage fort (128 bits), téléchargez la mise à jour de PPTP pour cryptage fort sur le site sécurisé de MS à l'adresse http://mssecure.www.conxion.com/cgi−bin/ntitar.pl et installez la, puis redémarrez lorsqu'on vous le demande.
g. Créez une nouvelle entrée dans votre carnet d'adresse d'appel distant pour votre serveur PPTP.
h. Sélectionnez l'adaptateur VPN comme périphérique à utiliser, et entrez l'adresse IP internet du serveur PPTP comme numéro de téléphone.
i. Sélectionnez l'onglet *Types de Serveur* et cochez les cases *Activer la compression logicielle* et *Demander un mot de passe crypté*.
j. Cliquez sur le bouton "Paramètres TCP/IP".
k. Renseignez les informations concernant l'adresse IP dynamique/statique de votre client comme précisé par l'administrateur de votre serveur PPTP.
l. Si vous souhaitez avoir accès à votre réseau local pendant que la connexion PPTP est active, regardez L'article de la Base de Connaissances MS Q143168 pour modifier la base de registres. (*Hum.*)
m. Assurez vous d'avoir ré−appliqué le dernier Service Pack, pour être sûr que les librairies RAS et PPTP sont à jour en ce qui concerne la sécurité et les performances.

4.5. Configuration pour du routage réseau à réseau

A écrire.

Vous devriez vraiment jeter un oeil sur FreeS/WAN (IPsec pour Linux) à l'adresse http://www.xs4all.nl/~freeswan/ plutôt que de faire du masquage.

4.6. Masquer des VPNs basés sur SecuRemote de CheckPoint

Il est possible de masquer le trafic VPN basé sur SecuRemote de Checkpoint à certaines conditions.

Pour commencer, vous devez configurer le pare−feu SecuRemote pour autoriser les sessions masquées. Sur le pare−feu SecuRemote, faites ce qui suit.

1. Exécutez *fwstop*
2. Éditez *$FWDIR/conf/objects.C* et après la ligne "*:props (*", ajoutez ou modifiez les lignes suivantes pour avoir

```
:userc_NAT (true)
:userc_IKE_NAT (true)
```

3. Exécutez *fwstart*
4. Réinstallez votre politique de sécurité.
5. Vérifiez que les changements ont été pris en compte en vérifiant *$FWDIR/conf/objects.C* et *$FWDIR/database/objects.C*

Si vous utilisez les protocoles IPsec (appelés "IKE" par CheckPoint) vous n'avez pas besoin de faire autre chose pour masquer le trafic VPN. Configurez simplement votre passerelle de masquage pour masquer le trafic IPsec comme décrit plus haut.

Le protocole propriétaire FWZ de CheckPoint est plus compliqué. Il y a deux modes dans lesquels FWZ peut être utilisé : le mode encapsulé, et le mode de transport. En mode encapsulé, la vérification d'intégrité est faite sur l'ensemble du paquet IP, comme avec le protocole AH d'IPsec. Changer l'adresse IP casse cette garantie d'intégrité, donc les tunnels FWZ encapsulés *ne peuvent pas* être masqués.

En mode transport, seule la portion du paquet contenant les données est cryptée, et les entêtes IP ne sont pas vérifiés pour voir s'ils ont été modifiés. Dans ce mode, le masquage doit fonctionner avec les modifications indiquées plus haut.

La configuration pour choisir entre le mode encapsulé ou le mode transport se fait via l'IHM FireWall−1. Dans l'objet réseau correspondant au pare−feu, sur l'onglet VPN, éditez les propriétés FWZ. Le troisième onglet dans les propriétés FWZ vous permet de choisir le mode encapsulé.

Vous ne pourrez masquer qu'un seul client à la fois.

Vous trouverez de plus amples informations aux adresses :

- http://www.phoneboy.com/fw1/nat.html,
- http://www.phoneboy.com/fw1/faq/0141.html
- http://www.phoneboy.com/fw1/faq/0372.html

---

5. Dépannage

5.1. Tests

Pour tester le masquage VPN :

1. Activez la connexion à votre FAI depuis votre machine Linux, et vérifiez qu'elle fonctionne correctement.
2. Vérifiez que le masquage fonctionne correctement, par exemple en utilisant une machine de votre réseau local masquée pour aller surfer sur un site web, ou pour accéder à un serveur FTP.
3. PPTP : vérifiez que vous avez correctement configuré le masquage du canal de contrôle PPTP : essayez de faire un telnet depuis la machine cliente PPTP vers le port 1723 de votre serveur PPTP. Ne vous attendez pas à voir quelque chose, mais si vous avez une erreur disant que la connexion a échoué ou si vous n'avez pas de réponse, jetez un coup d'oeil aux règles de masquage sur votre machine Linux, pour vous assurer que vous masquez bien le trafic en provenance du poste client PPTP vers le port TCP 1723 du serveur PPTP.
4. PPTP : essayez d'établir une connexion PPTP. Je vous recommande de lancer également *RASMON* s'il est disponible, car il va vous donner un minimum d'informations sur l'état de la connexion. Si vous établissez une connexion PPTP lors de votre première tentative, félicitations ! Vous avez réussi !
5. IPsec : essayez d'établir une connexion IPsec.

5.2. Problèmes possibles

Il y a plusieurs éléments qui peuvent empêcher d'établir une session VPN. Nous allons les considérer en partant du client vers le serveur, puis dans l'autre sens. Pour les exemples, nous partirons du principe que le client est un client Windows, ce qui correspond au cas le plus courant.

1. Information sur la connexion : le "numéro de téléphone" dans l'écran de configuration VPN distant doit être l'adresse IP internet du serveur VPN, ou l'adresse du pare−feu si le serveur est masqué.
2. PPTP et cryptage fort : si le client et le serveur n'ont pas le fichier *NDISWAN.SYS* ou le logiciel PPTP pour W'95/'98 128 bits, vous n'arriverez pas à établir une session avec cryptage fort. Malheureusement, au cours de mon expérience j'ai constaté que ce problème ne génère pas de message d'erreur, et que le client cherche à se connecter sans cesse... Vous pouvez récupérer la mise à jour pour le cryptage fort sur le site sécurisé de Microsoft dont l'URL est donnée dans la section"Configurer un client MS".

   Ceci va également affecter les clients IPsec, s'ils utilisent les librairies de cryptage fournies par MS plutôt que leurs propres librairies.
3. Routage : vérifiez que la route par défaut sur votre client VPN pointe bien vers la machine de masquage Linux. Lancez la commande *route print* et cherchez l'entrée *0.0.0.0*.

   Si d'autres services masqués (comme HTTP, FTP, IRC, etc...) fonctionnent sur votre machine cliente VPN, alors ce n'est pas un problème de routage.
4. Masquage : il y a deux parties dans la session VPN.

   Pour IPsec, le service d'authentification et d'échange de clés (ISAKMP), qui est une session UDP sur le port 500 de la machine IPsec distante, le pare−feu doit être configuré pour le masquage comme pour tout autre service UDP (par exemple DNS).

   Pour PPTP, le canal de contrôle, qui est une session TCP normale vers le port 1723 du serveur PPTP, le pare−feu doit être configuré pour le masquage comme pour tout autre service TCP (par exemple HTTP).

   Le canal de données crypté avec IPsec est transporté au dessus d'ESP, le protocole IP 50. Le canal de données crypté avec PPTP est transporté au dessus de GRE, le protocole IP 47. (Notez que ce ne sont *pas* des numéros de ports TCP ou UDP !) Le noyau Linux 2.0 ne vous permettant de préciser que les protocoles IP *TCP*, *UDP*, *ICMP* et *ALL* lors de la création des règles de masquage, vous devez masquer le trafic du protocole *ALL* même si vous masquez uniquement des services spécifiques. Si vous masquez tout, ne vous en inquiétez pas.

   Afin d'isoler les problèmes issus des règles du pare−feu de ceux provenant du code de masquage du noyau, essayez d'établir une connexion VPN avec votre pare−feu complètement ouvert, et si ça marche, resserrez alors les règles du pare−feu.

   Pare−feu complètement ouvert avec ipfwadm et un noyau 2.0.x :

   ```
   ipfwadm −I −p accept
   ipfwadm −O −p accept
   ipfwadm −F −a accept −m
   ```

   Pare−feu complètement ouvert avec ipchains et un noyau 2.2.x :

   ```
   ipchains −P input   ACCEPT
   ipchains −P output  ACCEPT
   ```

```
ipchains −P forward MASQ
```

Ne laissez *pas* votre pare−feu complètement ouvert plus de temps qu'il n'en faut pour prouver qu'une connexion VPN masquée peut être établie !

5. Équipements intermédiaires et Internet : Tous les routeurs entre votre pare−feu Linux et la machine IPsec distante doivent autoriser le passage des paquets porteurs du protocole IP 50. Tous les routeurs entre votre pare−feu Linux et le serveur PPTP doivent autoriser le passage des paquets porteurs du protocole IP 47. Si IPsec ou PPTP fonctionne lorsque votre client VPN est directement connecté à votre FAI, alors le problème ne vient probablement pas de là.

   Pour savoir si un équipement intermédiaire bloque le trafic GRE, utilisez un *traceroute* patché pour suivre la progression des paquets GRE. Regardez la section des ressources pour de plus amples informations sur le patch de traceroute. Un patch similaire pour ESP est en cours de codage.
6. Le pare−feu distant : le pare−feu du côté du serveur doit autoriser une machine ayant la même adresse IP que celle attribuée à votre machine Linux par votre FAI à se connecter au port 500/udp de la machine IPsec ou sur le port 1723/tcp du serveur PPTP. Si le VPN fonctionne lorsque votre client VPN est connecté directement à votre FAI, alors le problème ne vient probablement pas de là.
7. Le pare−feu côté serveur et ESP : les données cryptées IPsec sont transportées au dessus du protocole IP 50. Si le pare−feu derrière lequel se trouve la machine IPsec distante ne fait pas suivre le trafic ESP dans les deux sens, IPsec ne pourra pas marcher. Une fois de plus, si IPsec fonctionne lorsque votre client IPsec est connecté directement à votre FAI, alors le problème ne vient probablement pas de là.
8. Le pare−feu côté serveur et GRE : le canal de données PPTP est transporté comme une session PPP encapsulée dans GRE (protocole IP 47). Si le pare−feu derrière lequel votre serveur PPTP se trouve ne fait pas suivre le trafic GRE dans les deux sens, PPTP ne pourra pas fonctionner. Une fois de plus, si PPTP fonctionne lorsque votre client IPsec est connecté directement à votre FAI, alors le problème ne vient probablement pas de là.
9. Le patch : si votre client IPsec s'authentifie correctement mais ne peut pas établir de connexion réseau, le patch peut ne pas masquer le trafic ESP correctement. Si votre client PPTP établit le canal de contrôle (RASMON bipe et le petit téléphone clignote) et qu'un trafic GRE est généré (la lumière en haut de RASMON clignote) mais qu'il n'y a pas de trafic GRE en retour (la lumière en bas de RASMON ne clignote pas en réponse), le patch peut ne pas masquer le trafic GRE correctement.

   Regardez dans */var/log/messages* pour trouver les entrées des journaux qui montrent que le trafic VPN a été vu. Activez le déboguage du VPN pour vous aider à déterminer si le patch est responsable ou non. Faites aussi tourner un sniffeur sur votre connexion internet en cherchant le trafic VPN sortant *(voir plus bas)*.
10. Clients multiples : l'ancien patch PPTP ne supporte PAS le masquage de plusieurs clients PPTP cherchant à accéder au *même* serveur PPTP. Si vous essayez de le faire, vous devriez reconsidérer votre architecture réseau et voir si vous ne devriez pas installer un routeur PPTP pour vos clients locaux. Le patch 2.0 inclus le masquage d'identifiant d'appel, qui permet plusieurs sessions simultanées. *Note :* n'activez pas le masquage d'identifiant d'appel PPTP si vous masquez un serveur PPTP. Cela empêcherait le trafic sortant en provenance du serveur d'être masqué.

5.3. Dépannage

La plupart des problèmes peuvent être identifiés en faisant tourner un sniffeur de paquets (par exemple *tcpdump* avec l'option *−v*) sur votre pare−feu passerelle VPN. Si tout fonctionne correctement, vous allez voir le trafic suivant.

- Réseau local du client :

IPsec : le trafic UDP (destination UDP port 500) et ESP (protocole IP 50) en provenance de votre client local IPsec à destination de l'adresse IP internet de la machine IPsec distante. Si vous ne le voyez pas, votre client IPsec est mal configuré.

PPTP : le trafic TCP (destination TCP port 1723) et GRE (protocole IP 47) en provenance de votre client local PPTP à destination de l'adresse IP internet du serveur PPTP. Si vous ne le voyez pas, votre client PPTP est mal configuré.

- Du côté FAI de votre pare−feu client : un trafic UDP et ESP ou TCP et GRE en provenance de l'adresse IP internet du pare−feu client (souvenez vous, on fait du masquage) vers l'adresse IP internet du serveur VPN. Si vous ne le voyez pas, votre masquage est mal configuré, ou bien le patch ne fonctionne pas.
- Du côté FAI de votre pare−feu serveur : un trafic UDP et ESP ou TCP et GRE en provenance de l'adresse IP internet de votre client vers l'adresse IP internet du serveur VPN. Si vous ne le voyez pas, internet ne marche pas *:)* ou des équipements intermédiaires bloquent le trafic ESP ou GRE.
- Du côté DMZ de votre pare−feu serveur : un trafic UDP et ESP ou TCP et GRE en provenance de l'adresse IP internet du client vers l'adresse IP du serveur. Si vous ne le voyez pas, vérifiez les règles pare−feu concernant le suivi de paquets UDP port 500 ainsi que ceux porteurs du protocole IP 50 ou TCP port 1723 et protocole IP 47, ainsi que la configuration d'*ipportfw* et de *ipfwd* si vous masquez le serveur.
- Du côté interne du pare−feu serveur : un trafic UDP (port source 500) et ESP ou TCP (port source 1723) et GRE en provenance de l'adresse IP du serveur VPN et à destination de l'adresse IP internet du client. Si vous ne le voyez pas, vérifiez la configuration du serveur VPN, y compris les règles de filtrage de paquets sur le serveur VPN.
- Du côté FAI du pare−feu serveur : un trafic UDP et ESP ou TCP et GRE en provenance de l'adresse IP du serveur VPN (ou l'adresse IP du pare−feu si le serveur est masqué) vers l'adresse IP internet du client. Si vous ne le voyez pas, vérifiez les règles de votre pare−feu concernant la transmission de paquets UDP port 500 ainsi que de ceux porteurs du protocole IP 50 ou TCP port 1723 et protocole IP 47.
- Du côté FAI de votre pare−feu client : un trafic UDP et ESP ou TCP et GRE en provenance de l'adresse IP du serveur VPN et à destination de l'adresse IP internet du pare−feu client. Si vous ne le voyez pas, internet se révolte encore.
- Du côté réseau local client : un trafic UDP et ESP ou TCP et GRE en provenance de l'adresse IP internet du serveur VPN à destination de l'adresse IP sur le réseau local du client VPN. Si vous voyez le trafic UDP mais pas le trafic ESP, ou bien le trafic TCP mais pas le trafic GRE, le patch ne fonctionne pas ou n'a pas été installé correctement.

Vous pouvez trouver utile d'activer le déboguage du VPN et de recompiler votre noyau. Ajoutez ce qui suit au fichier */etc/syslog.conf*

```
# déboguage
*.=debug           /var/log/debug
```

et regardez */var/log/messages* et */var/log/debug* pour les messages concernant le trafic VPN. Notez que l'enregistrement − particulièrement l'enregistrement bavard (verbose log) − va engendrer une grande activité disque et va faire grossir très rapidement les journaux. N'activez pas le déboguage si vous n'en avez pas besoin, et coupez le quand vous avez fini.

5.4. Clients MS PTPP et noms de domaines

Merci à Charles Curley <ccurley@trib.com> pour ce qui suit :

```
Si vous utilisez PPTP (Point to Point Tunneling Protocol)
pour accéder à un environnement Réseau Microsoft (SMB) et que
```

```
vous avez votre propre environnement Réseau Microsoft sur votre
réseau local (Samba ou Windows), donnez à votre groupe de travail
local un nom qui n'est pas connu dans l'environnement distant.
La raison est que tant que votre client PPTP est connecté
à l'environnement distant, il va voir les serveurs de noms de
domaine de l'environnement distant, et il ne va voir que les machines
distantes appartenant à ce groupe de travail.
```

Vous devez éviter l'option paresseuse. Microsoft livre Windows pré−configuré pour un groupe de travail par défaut nommé WORKGROUP. Il y a des gens paresseux qui vont garder ce nom pour leur groupe de travail quand ils installeront leurs ordinateurs. Donc il y a une bonne chance pour que l'environnement distant ait un groupe de travail appelé WORKGROUP, que cela plaise ou non aux administrateurs.

Je pense que ceci s'applique indépendamment de l'utilisation du VPN, car les services de nommage sont indépendants du transport. Si votre (ou vos) client peut voir les serveurs WINS sur le réseau distant, vous aurez le problème, avec ou sans PPTP.

5.5. Clients PPTP MS et IPX Novell

Si vous avez des problèmes avec le trafic IPX sur votre liaison PPTP, lisez les sections 3.5 et 5.2 de cet article de la base de connaissances MS :
http://microsoft.com/ntserver/nts/downloads/recommended/dun13win95/ReleaseNotes.asp

Les mêmes considérations s'appliquent probablement également à W'98.

Merci à David Griswold <dgriswol@ix.netcom.com>

5.6. Problèmes de mots de passe réseau MS

Lorsque vous utilisez un VPN pour accéder à un réseau MS, souvenez−vous qu'il vous faut fournir deux jetons d'authentification différents − un pour se connecter au serveur VPN (le mot de passe VPN) et l'autre pour accéder aux ressources du réseau distant une fois que la connexion est établie (le mot de passe réseau).

Le mot de passe VPN − le nom d'utilisateur et le mot de passe que vous avez entré dans votre client VPN lorsque vous avez initié la connexion au serveur VPN − n'est utilisé que par le serveur VPN pour vous autoriser à vous connecter au réseau via le VPN. Il n'est utilisé pour rien d'autre une fois que vous êtes connecté.

Le mot de passe VPN n'est *pas* utilisé pour prouver votre identité aux autres ordinateurs du réseau distant. Pour cela vous devez fournir une autre paire nom d'utilisateur/mot de passe − votre mot de passe réseau.

Il y a deux méthodes pour fournir un mot de passe réseau. Votre mot de passe réseau peut provenir de la même paire nom d'utilisateur/mot de passe que celle que vous utilisez lorsque vous vous connectez sur le réseau local en allumant votre ordinateur. S'il est différent, vous pouvez configurer votre client VPN pour vous demander votre mot de passe pour le réseau distant une fois que la connexion VPN est établie.

Si vous arrivez à vous connecter au serveur VPN sans pouvoir accéder aux ressources disponibles sur le réseau distant, alors vous n'avez pas fourni une paire nom d'utilisateur/mot de passe valide sur le réseau distant. Vérifiez que le nom d'utilisateur et le mot de passe pour votre réseau local fonctionnent aussi sur le réseau distant, ou configurez votre client VPN pour vous demander un nom d'utilisateur et un mot de passe à utiliser sur le réseau distant, et pour vous "enregistrer" sur le réseau distant une fois que la connexion VPN est établie.

5.7. Si votre session IPsec meurt automatiquement après un certain laps de temps

Si vous avez des problèmes avec votre tunnel IPsec qui meurt régulièrement, plus particulièrement si une vérification des enregistrements sur le pare−feu montrent que des paquets ISAKMP avec des valeurs "zero cookie" passent, voici ce qui arrive.

Les versions antérieures du patch pour le masquage IPsec ne changeaient pas le délai de fin d'attente (timeout) pour les entrées de la table de masquage des paquets ISAKMP UDP. Les entrées de la table de masquage pour le trafic ISAKMP UDP vont arriver en fin d'attente assez rapidement (comparativement au canal de données) et vont être supprimées ; si l'hôte IPsec distant décide alors d'initialiser un renouvellement des clés avant que la machine IPsec locale ne le fasse, le trafic ISAKMP entrant pour le renouvellement des clés ne pourra alors pas être routé vers la machine masquée. Le trafic de renouvellement des clés sera rejeté, l'hôte IPsec distant pensera que le lien est tombé, et que la connexion va être terminée.

Le patch 2.0.x a été modifié depuis sa version initiale pour augmenter le délai de fin d'attente des entrées de la table de masquage concernant les paquets ISAKMP UDP. Récupérez la version actuelle du patch, disponible sur les sites indiqués dans la section Ressources, ré−appliquez le patch et recompilez votre noyau.

Vérifiez également que votre paramètre *Durée de vie de la table de masquage IPsec (IPsec Masq Table Lifetime)* est configuré pour être égal, ou légèrement supérieur, à votre intervalle de renouvellement des clés.

5.8. Si le masquage VPN ne fonctionne pas après le redémarrage

Vous souvenez−vous d'avoir mis les commandes *modprobe ip_masq_pptp.o* ou *modprobe ip_masq_ipsec.o* dans votre script de démarrage */etc/rc.d/rc.local* au cas où vous avez compilé le support de masquage VPN en modules ?

5.9. Si votre seconde session PPTP tue votre première session

La RFC de PPTP précise qu'il ne peut y avoir qu'un seul canal de contrôle entre deux systèmes. Cela peut vouloir dire qu'un seul client masqué est capable de contacter un serveur PPTP donné à un instant donné. Regardez pour de plus amples détails.

---

6. Notes techniques sur le masquage IPsec et considérations spéciales sur la sécurité

6.1. Limites et faiblesses du masquage IPsec

Le trafic utilisant le protocole AH *ne peut pas* être masqué. Le protocole AH inclut un contrôleur d'intégrité cryptographique qui couvre les adresses IP, et que la passerelle de masquage ne peut pas régénérer correctement. Donc tout le trafic AH masqué va être rejeté car il aura des contrôleurs d'intégrité non valides.

Le trafic IPsec utilisant le mode de transport ESP ne peut pas non plus être correctement masqué. Le mode de transport ESP crypte tout ce qui se trouve après l'entête IP. Or, par exemple, les contrôleurs d'intégrité de TCP et UDP incluent les adresses IP source et destination, ils se trouvent dans la partie cryptée, et ne peuvent donc pas être recalculés après que la passerelle de masquage ait modifié les adresses IP. L'entête TCP/UDP ne va donc pas passer les contrôles d'intégrité sur la passerelle distante, et le paquet va être rejeté. Les protocoles n'incluant pas les informations sur les adresses IP source ou destination peuvent utiliser le masquage du mode de transport.

Ces limites mises à part, le masquage IPsec est sûr et fiable à condition qu'un seul hôte IPsec soit masqué à un instant donné, ou que chaque hôte masqué communique avec un serveur distant différent. Lorsque plusieurs machines masquées communiquent avec la même machine distante, quelques faiblesses apparaissent :

- Les communications du mode transport sont sujettes à collisions.

  Si deux machines masquées ou plus utilisent le mode transport pour communiquer avec le même hôte distant, et si la politique de sécurité sur l'hôte distant permet plusieurs sessions de mode transport avec la même machine, il est possible que les sessions aient des collisions. Ceci arrive parce que l'adresse IP de la *passerelle de masquage* va être utilisée pour identifier les sessions, et que les autres informations d'identification ne pourront pas être masquées puisqu'elles sont dans la portion cryptée du paquet.

  Si la politique de sécurité de l'hôte distant n'autorise pas plusieurs sessions simultanées en mode transport avec la même machine, la situation est pire : la session en mode transport négociée en dernier va écraser *tout* le trafic de la session précédente, entraînant sa "mort". Alors que les sessions établies via l'ancienne session IPsec en mode transport vont être rapidement réinitialisées si l'hôte distant n'attend pas de trafic, au moins un paquet de données va être envoyé à la mauvaise machine. Ce paquet va probablement être ignoré par le destinataire, mais il va tout de même être envoyé.

  Donc une collision du mode transport peut avoir comme conséquence une fuite d'information entre les deux sessions ou bien la fin de l'une des deux sessions. L'utilisation d'IPsec en mode transport via une passerelle de masquage *n'est pas recommandée* s'il y a une possibilité que d'autres sessions IPsec en mode transport soient initialisées via la même passerelle de masquage vers le même hôte IPsec distant.

  IPsec en mode tunnel avec une adresse de réseau externe (l'hôte IPsec masqué se voit attribuer une adresse IP du réseau de l'hôte distant) n'est *pas* sujet à ces problèmes, car l'adresse IP fournie par le réseau distant sera utilisée pour identifier les sessions plutôt que l'adresse IP de la machine masquante.
- Les communications ISAKMP sont sujettes à des collisions de cookies.

  Si deux ou plusieurs machines masquées établissant une session avec la même machine distante utilisent le même cookie lors de l'initialisation du trafic ISAKMP, la passerelle de masquage va router tout le trafic ISAKMP vers la seconde machine. Il y a une chance sur 2^64 (ie. très petite) pour que cette collision ait lieu lorsque la connexion ISAKMP initiale est établie.

  Pour corriger cela, il faut inclure le cookie de réponse dans la clé utilisée pour router le trafic ISAKMP entrant. Cette modification est incluse dans le code de masquage IPsec des noyaux 2.2.x, et la courte période entre le moment où l'hôte masqué initialise l'échange ISAKMP et la réponse de l'hôte distant est protégée par le bloquage de tout nouveau trafic ISAKMP qui pourrait entrer en collision avec le trafic actuel. Cette modification va bientôt être portée sur le code des 2.0.x.
- Il peut y avoir une collision entre les valeurs SPI du trafic entrant.

  Deux ou plusieurs hôtes IPsec masqués communiquant avec la même machine IPsec distante peuvent négocier pour utiliser la même valeur SPI pour le trafic entrant. Si cela arrive, la passerelle de masquage va router tout le trafic entrant vers la première machine qui va recevoir tout le trafic entrant avec ce SPI. La probabilité est de 1 sur 2^32 pour chaque session ESP, et le cas peut se présenter à chaque renouvellement de clés.

  Les valeurs SPI sont rattachées à différents SA ayant différentes clés de cryptage, le premier hôte ne sera donc pas capable de décrire les données destinées aux autres machines, donc il n'y aura aucune

fuite de données. Il n'y a aucun moyen pour la passerelle de masquage de détecter ou d'empêcher cette collision. La seule façon d'empêcher cette collision est que l'hôte IPsec distant vérifie la valeur SPI proposée par la machine masquée pour voir si cette valeur SPI est déjà utilisée par un autre SA depuis la même adresse IP. Il est peu probable que ceci soit implémenté un jour, car cela imposerait une charge supplémentaire à une opération déjà coûteuse (le renouvellement des clés) pour un bénéfice concernant un nombre réduit de personnes et un type d'évènement assez rare.
- Les valeurs SPI entrantes et sortantes peuvent être dissociées.

  Ceci sera vu en détail dans la section suivante.

Pour éviter ces problèmes, le code des noyaux 2.2.x empêche par défaut l'établissement de plusieurs connexions vers la même machine distante. Si vous estimez que la faiblesse liée à plusieurs connexions vers la même machine distante est acceptable, vous pouvez activer les "sessions parallèles".

Il peut être gênant de bloquer pour des raisons de sécurité les sessions parallèles : il n'y a aucun moyen pour le code de masquage IPsec de sniffer la session et de voir quand elle se termine, donc les entrées de la table de masquage vont être conservées pendant leur durée de vie standard, même si la session se termine juste après qu'elle ait été établie. Si l'on empêche les sessions parallèles, cela signifie que le serveur n'acceptera pas d'autre client tant que l'entrée de la table de masquage la plus récente sera présente. Cela peut prendre plusieurs heures.

6.2. Routage correct du trafic crypté entrant

La partie de l'échange de clés ISAKMP où les valeurs SPI d'ESP sont communiquées est cryptée, donc les valeurs SPI d'ESP doivent être déterminées en étudiant le trafic ESP actuel. Le trafic ESP sortant ne contient aucune indication sur ce que sera le SPI entrant. Cela signifie qu'il n'y a aucune méthode fiable pour associer le trafic ESP entrant avec le trafic ESP sortant.

Le masquage IPsec tente d'associer le trafic ESP entrant et sortant en sérialisant le trafic ESP par machine distante. Concrètement :

- Si un paquet ESP sortant avec une valeur SPI qui n'a pas encore été vue (ou dont l'entrée dans la table de masquage a expiré) est reçu (il sera appelé par la suite un "paquet initial"), une entrée dans la table de masquage est créée pour cette combinaison AdresseSource+SPI+AdresseDest. Elle est marquée comme "en attente", ce qui signifie qu'aucun trafic correspondant à cette entrée n'a été pour l'instant reçu. Le marquage se fait en mettant la valeur "SPI entrant" dans l'entrée de la table de masquage à zéro, qui est une valeur réservée pour cela. Ceci arrivera lors de l'initialisation d'une nouvelle connexion ESP et à intervalles réguliers lors du renouvellement de clés d'une connexion ESP existante.
- Tant que l'entrée de la table de masquage est en attente, aucun autre paquet ESP initial à destination du *même hôte distant* n'est traité. Les paquets sont immédiatement rejetés, et une entrée du journal système est ajoutée, précisant que le trafic est temporairement bloqué. Ceci s'applique également au trafic initial en provenance de la même machine masquée à destination du même hôte distant, si les valeurs SPI sont différentes. Le trafic vers d'autres hôtes distants, et le trafic où les deux valeurs SPI sont connues (trafic déjà "établi") n'est pas affecté.
- Ceci peut facilement mener à un déni de service sur la machine distante, c'est pour cela que la durée de vie de cette entrée en attente de la table de masquage ESP est faible, et que seul un nombre limité de tentatives pour le même trafic est autorisé. Ceci permet de faire un accès via round−robin à la machine distante si plusieurs machines masquées tentent d'initialiser simultanément la connexion et que les réponses n'arrivent pas très vite, par exemple à cause d'une congestion réseau, ou d'une

machine distante lente. Le décompte des tentatives commence dès qu'il y a une collision, donc l'hôte IPsec masqué peut attendre une réponse aussi longtemps qu'il le faut jusqu'à ce qu'il soit nécessaire de faire une mise en série des connexions.
- Quand un paquet ESP est reçu en provenance de l'hôte distant en attente, et que la valeur SPI n'apparaît dans aucune entrée de la table de masquage, il est supposé que le paquet est la réponse au paquet en attente initial. La valeur SPI est stockée dans l'entrée courante de la table de masquage associant les valeurs SPI, et le trafic ESP entrant est alors routé vers la machine masquée. A ce point un autre paquet initial destiné au serveur distant peut être traité.
- Tout trafic ESP avec une valeur SPI de zéro est rejeté comme étant invalide, conformément au RFC.

Il y a plusieurs possibilités pour que l'association de trafic ne se fasse pas proprement :

- La latence du réseau ou la lenteur d'une machine distante peuvent retarder suffisamment la réponse au paquet initial pour que l'entrée de la table de masquage ait expiré, et qu'une autre machine masquée ait eu sa chance d'initialiser un trafic. Ceci peut faire que la réponse sera associée au mauvais SPI sortant, et donc le trafic entrant sera routé vers la mauvaise machine masquée. Si cela arrive, la machine masquée recevant le trafic par erreur le rejettera parce qu'il n'aura pas la valeur SPI attendue, et tout le monde risque de patienter jusqu'à la fin du temps d'attente pour faire un nouvel échange de clés, et réessayer. On peut y remédier en éditant */usr/src/linux/net/ipv4/ip_masq.c* (*ip_masq_ipsec.c* dans le 2.2.x) et en augmentant la durée de vie d'INIT ou le nombre de tentatives INIT autorisées, avec pour coût l'agrandissement de la fenêtre de bloquage (et de déni de service).
- Les sessions inactives ou semi−inactives (avec un trafic entrant peu fréquent et aucun trafic sortant) sur une longue période peuvent le rester suffisamment longtemps pour que l'entrée de la table de masquage expire. Si la machine distante envoie du trafic d'une session ayant déjà expiré au niveau de la table de masquage pendant qu'une initialisation est en cours vers la même machine, le trafic peut être incorrectement routé, pour la même raison que plus haut. On peut y remédier en s'assurant que le paramètre de configuration du noyau *IPsec Masq Table Lifetime* est légèrement plus grand que l'intervalle de renouvellement des clés, qui est la durée la plus longue que les paires SPI peuvent utiliser. Le problème ici est que vous ne pouvez pas connaître tous les intervalles de renouvellement des clés si vous masquez plusieurs serveurs distants, ou que certains peuvent avoir leurs intervalles de renouvellement des clés positionnés à des valeurs déraisonnablement élevées, comme plusieurs heures.
- S'il y a un délai entre un renouvellement de clés et la transmission du trafic ESP sortant utilisant le nouveau SPI, et si durant ce délai un trafic ESP entrant utilisant ce nouveau SPI est reçu, il n'y a pas d'entrée de la table de masquage décrivant comment router le trafic entrant. Si une autre machine masquée a une initialisation en attente avec le même hôte distant, le trafic va être dissocié. Notez que la sérialisation du trafic ESP initial n'affecte *pas* le trafic de renouvellement des clés ISAKMP.

La meilleure solution est d'avoir un moyen de pré−charger la table de masquage avec les bonnes paires SPI−sortie/SPI−entrée, ou une autre forme d'association machine_distante + SPI_entrée avec la machine_masquée. Cela ne peut pas être fait en suivant l'échange de clés ISAKMP, car il est crypté. Il peut être possible d'utiliser RSIP (également connu en tant que Translation d'Adresse Réseau pour un hôte (NdT : Host−NAT)) pour communiquer avec l'hôte IPsec masqué et demander une notification sur les informations SPI une fois que la négociation a eu lieu. Ce point est à étudier. Si quelque chose est fait pour l'implémenter, ce ne sera pas fait avant les séries 2.3.x, car RSIP est un protocole NAT client/serveur assez complexe.

Quand un paquet ESP entrant avec un nouveau SPI est reçu, le pare−feu de masquage tente de deviner à quel(s) hôte(s) masqué(s) ce trafic entrant est destiné. Si le trafic ESP entrant ne correspond pas à une session établie, ou à une session en cours d'initialisation, alors le paquet est envoyé à la (aux) machine(s) masquée(s) qui a (ont) renouvelé en dernier ses (leurs) clés avec cet hôte distant. Les machines masquées "incorrectement" vont rejeter le trafic comme n'étant pas correctement crypté, et la machine "correctement" masquée va recevoir des données. Lorsque la machine "correctement" masquée répond, le processus normal de sérialisation de l'initialisation ESP a lieu.