A lire en priorité

Cher client, merci d'acquérir/d'évaluer WinRoute Pro. Kerio Technologies, le leader en matière de technologie de parefeu (firewall) pour les réseaux de petites ou moyennes tailles, a fait beaucoup d'efforts et de recherches pour vous faire profiter d'un routeur/firewall puissant et facile à utiliser, pour les systèmes d'exploitation Windows.

WinRoute Pro est une application réseau qui, couplée à un PC, se substitue à des systèmes matériels de routeur et de firewall beaucoup plus coûteux. En tant que tel, il est nécessaire que le réseau soit correctement mis en place et configuré. Une certaine expérience avec les environements réseau est donc nécessaire.

Il est à noter (sur la base de nos statistiques) qu'environs 90% des problèmes que rencontrent nos clients pour connecter leur réseau à Internet, sont causés par une mauvaise configuration réseau. Ce manuel contient plusieurs exemples de configurations réseau, bien que chaque configuration peut présenter de nombreuses différences.

Nous vous recommandons fortement de lire avec attention et complètement cette documentation. Elle a été réalisée en tenant compte du fait que les utilisateurs possèdent quelques connaissances de base en matière de réseau et, en particulier, la mise en place de réseaux locaux (LAN).

Si de plus amples informations, recommandations ou corrections logicielles sont nécessaires, Kerio Technologies prie ses clients de vérifier en priorité les sections correspondantes de son support en ligne avant d'appeler le support technique.

Nous voulons vous remercier, une fois de plus, de faire l'aquisition/l'évaluation de WinRoute.

Merci,

KERIO TECHNOLOGIES, INC.

Guide de Référence

WinRoute Pro 4.2

Pour la version 4.1 (Build 22 et plus)

Kerio Technologies Inc.

Table des Matières

CHAPITRE 1

Administration dans WinRoute

Dans ce chapitre

Introduction à l'Administration

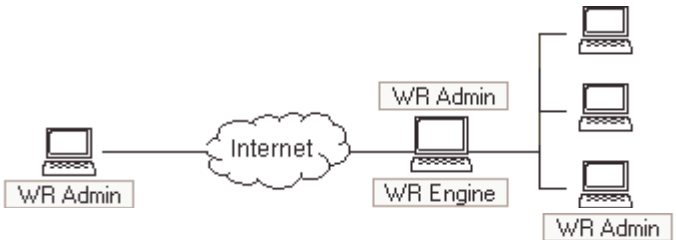
WinRoute Pro fournit aux utilisateurs les avantages de l'administration distante. Avec les réglages appropriés et les droits nécessaires, il est possible d'administrer en toute sécurité votre parefeu depuis n'importe quel endroit dans le monde. L'accès au Moteur est sécurisé par un fort cryptage et un mot de passe.

Composants de WinRoute Pro

WinRoute Pro 4.x est composé de trois modules:

Le Moteur WinRoute s'occupe de opérations de routage et d'analyse (translation d'adresses (NAT), filtrage des paquets, assignation de port (Port mapping) etc.). Vous pouvez Démarrer/Arrêter le Moteur WinRoute depuis le Moniteur du Moteur WinRoute ou si vous utilisez Windows NT, directement à partir du panneau de contrôle des services. Le Moteur WinRoute s'execute de manière invisible en tant que service sous Windows 2000/NT/98 or 95.

Le Moniteur du Moteur WinRoute est l'application de surveillance qui montre si le Moteur WinRoute est actif ou non. Il apparait en bas à droite de votre bureau sous la forme d'un petit icône bleu.

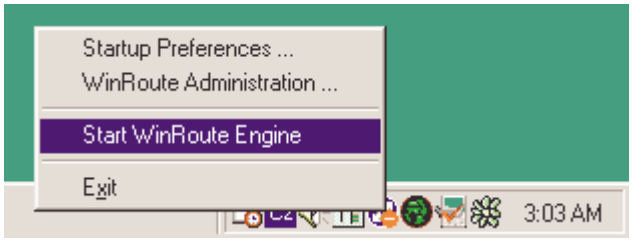


L'Administrateur WinRoute permet la configuration et le paramètrage du Moteur WinRoute. L'Administrateur WinRoute est une application autonome (wradmin.exe) qui peut être executée sur n'importe quel ordinateur et connectée via une connexion TCP/IP, à l'ordinateur executant le Moteur WinRoute. Pour les réglages nécessaires au Moteur WinRoute afin qu'il autorise les connexions distantes, veuillez consulter les autres chapitres de cette section.

Administration depuis le réseau local

Afin d'administrer WinRoute depuis un réseau local sur l'ordinateur executant WinRoute, vous devez procéder comme suit:

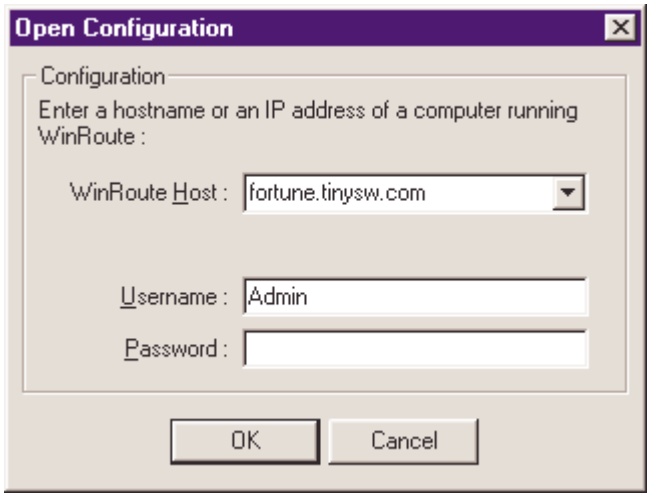
1. **Vérifiez que le Moteur WinRoute soit actif et qu'il s'execute correctement**
   Pour vérifier que WinRoute est bien démarré, il faut lancer le Moniteur du Moteur WinRoute à partir du menu programme WinRoute 4.0. Un petit icône rond, bleu et blanc, apparait alors dans les icônes systèmes de la barre des tâches (en bas à droite sur le bureau). Cela indique que l'application s'execute. Une croix rouge sur l'icône indique que WinRoute est arrêté. Pour démarrer le Moteur WinRoute, cliquez simplement sur l'icône **avec le bouton droit** et choisissez Démarrer le Moteur WinRoute à partir du menu contextuel qui vient d'apparaître.



2. Lancer l'Administrateur Winoute

Pour démarrer le module d'Administration WinRoute, lancez l'application à partir du menu Démarrer=>Programmes=>WinRoute 4.0 ou en cliquant avec le bouton droit sur l'icône du Moniteur du Moteur WinRoute et en choisissant Administrateur WinRoute dans le menu contextuel. Vous pouvez également copier le fichier WRAdmin.exe sur n'importe quel ordinateur sur votre réseau et le lancer depuis ce dernier.

Lorsque la fenêtre de l'Administrater apparait, vous pouvez laisser la préselection de la machine locale ou entrer l'adresse IP de l'ordinateur sur lequel s'execute WinRoute. Entrez le nom d'utilisateur et le mot de passe utilisés pour l'administration.



Note: Si vous vous connectez pour la première fois, vous devrez utiliser "Admin" comme nom d'utilisateur et laissez le mot de passe vide. Voir la section Configuration des utilisateurs pour plus de détails concernant la politique des noms d'utilisateur et des mots de passe pour l'administration.

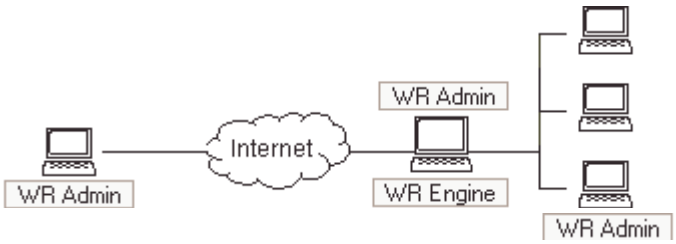
Vous devez obligatoirement vous connecter en tant qu'Administrateur au Moteur WinRoute afin de règler les différents paramètres.

Les raisons possibles de connexions infructueuse depuis un réseau local:

- Le Moteur WinRoute n'est pas actif ou ne s'execute pas
- Mavais nom d'utilisateur et mot de passe
- Mauvaise adresse IP utilisée pour se connecter au Moteur WinRoute
- Vous n'avez pas les droits nécessaires pour administrer WinRoute
- La translation d'adresses (NAT) est activée sur l'interface connectée au réseau local - voir le chapitre Liste de contrôle et Paramètrage du réseau pour plus d'aide

Administration depuis Internet

Vous pouvez administrer WinRoute Pro depuis n'importe quel ordinateur dans le monde du moment qu'une connexion TCP/IP est disponible. L'administration s'effectue en toute sécurité (transmissions cryptées) et son accès est contrôlé par un nom d'utilisateur et un mot de passe.



Afin d'administrer un ordinateur executant WinRoute depuis l'extérieur du réseau local (depuis Internet) le Port Mapping doit être activé et configuré sur l'ordinateur WinRoute. Il est nécessaire de comprendre qu'une fois la translation d'adresses (NAT) activée sur l'interface connectée à l'Internet (afin de partager la connexion Internet), l'intégralité de votre réseau (y compris la machine executant WinRoute) est completement protégée et que donc personne ne peut y accèder.

Pour configurer le Port Mapping pour l'administration distante, allez dans le menu Settings=>Advanced=>Port Mapping, selectionnez Add et paramètrez :

Protocol: TCP/UDP

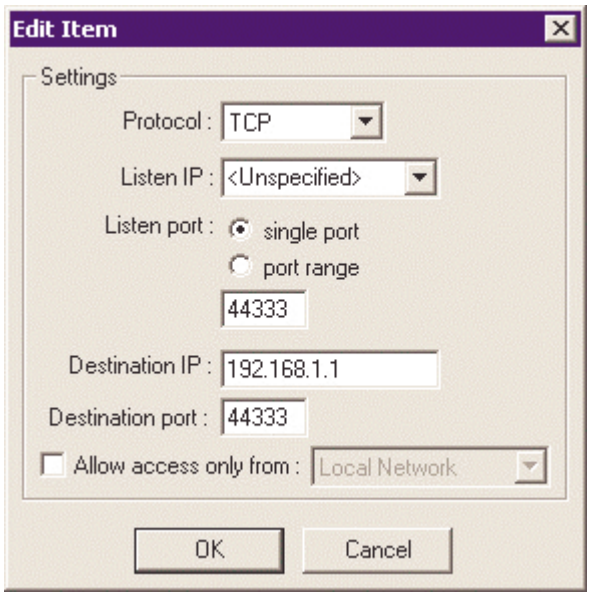
Listen IP: <unspecified> (recommendé) ou l'adresse IP de l'interface.

Listen Port: 44333

Destination IP: L'adresse IP de l'interface reliant l'ordinateur executant WinRoute au réseau local (adresse IP de classe privée).

Destination Port: 44333

Allow access only from: *Si vous cochez cette case, vous pouvez limiter l'accès au Moteur WinRoute. Vous devez alors prédéfinir les adresses IP autorisées à accèder au Moteur WinRoute dans le menu Settings=>Advanced=>Address Groups. Vous pouvez grouper des adresses IP séparées, des intervales d'adresses et des réseaux.*



Veuillez voir les exemples pour plus de détails concernant le Port Mapping. Si vous avez tout paramètré correctement, vous pouvez alors lancer le programme d'Administration de WinRoute depuis n'importe quel ordinateur et entrer l'adresse IP (registered - e.g. 206.86.181.25) de l'ordinateur executant WinRoute. Vous devrez également entrer le nom d'utilisateur et le mot de passe utilisés pour l'administration de cet ordinateur. Voir la configuration des utilisateurs pour plus de détails concernant les noms d'utilisateurs et les politiques de mots de passe pour l'administration.

Les raisons possibles de problèmes de connexions depuis Internet:

- Le Moteur WinRoute n'est pas actif ou ne s'execute pas
- Mavais nom d'utilisateur et mot de passe
- Mauvaise adresse IP utilisée pour se connecter au Moteur WinRoute
- Vous n'avez pas les droits nécessaires pour administrer WinRoute

- Il n'y a pas de Port Mapping de configuré sur l'ordinateur executant WinRoute ou le Port Mapping est mal paramètré.

Vous avez perdu le mot de passe d'administration

Si vous perdez le mot de passe d'administration, veuillez envoyer un e-mail à support@kerio.com pour de plus amples informations. Pour des raisons de sécurité, nous ne publions pas la solution de ce problème.

CHAPITRE 2

Mise en marche et utilisation

Dans ce chapitre

Système requis

Pour installer et executer WinRoute Pro 4.2 nous recommandons au moins:

- Un PC équipé de processeur Pentium (un ou deux processeurs)
- Système d'exploitation Windows 95/98/NT4.0/2000
- 32MB de mémoire vive
- 1MB d'espace disque libre
- au moins 2 interfaces disponibles. Cela peut être: Ethernet, RAS, TokenRing, DirecPC

Démarrage rapide

Pour tous les utilisateurs de WinRoute, il y a une liste de paramètres et de règles qui, si ils ne sont pas négligés, assurent une connexion réussie de leur réseau. Bien évidemment, une connexion Internet fonctionnant est obligatoire.

Vous allez devoir éffectuer les paramètrages décris ci-après si vous voulez bénéficier des avantages de la Translation d'adresse (NAT) pour partager votre accès à Internet. Si vous voulez utiliser un serveur Proxy (integré dans WinRoute) vous n'avez pas à effectuer ces paramètrages. Dans ce cas, vous devriez paramètrer vos navigateurs et vos applications pour qu'ils utilisent le serveur Proxy de WinRoute. Nous recommandons fortement l'utilisation de la translation d'adresses (NAT) dès que cela est possible. C'est plus rapide, plus sûr et plus fonctionnel.

Paramètrages et règles à suivre:

1 **Sur le PC WinRoute - Deux Interfaces (NIC)**
Vérifiez que l'ordinateur WinRoute possède (au moins) deux interfaces. Une pour la connexion internet et l'autre pour la connexion au réseau local. Cela peut être des adaptateurs réseau ou des lignes de connexions distantes. Une interface (Ethernet ou connexion distante) est utilisée pour la connexion à Internet pendant que l(es)'autre(s) interface(s) (Ethernet, token ring, ...) sert pour la connexion au(x) réseau(x).

2 **Il faut s'assurer que toutes les adresses IP sont joingnables !**

Afin que WinRoute fonctionne correctement, les machines clientes doivent être capables de joindre (en utilisant la commande ping) les adresses publiques ainsi que les adresse privées de la machine WinRoute.

Sur le PC WinRoute - Activez la translation d'adresse (NAT) sur l'interface Internet !
Assurez vous que la case NAT est cochée pour l'interface connectée à Internet (Ethernet, connexion distante). Vous pouvez faire cela depuis le menu Settings=>Interface table et allez dans les proprietés de l'interface désirée.

3 **Sur le PC WinRoute - Desactivez la translation d'adresses (NAT) sur l'interface interne !**
Vérifiez que la case NAT **N'EST PAS COCHEE** sur l'interface ou les interfaces connectées au(x) réseau(x) interne(s).
On peux noter que, dans des configurations très spéciales, la translation d'adresses (NAT) peut également être activée sur l'interface interne. Vous trouverez des examples ici dès qu'ils seront disponibles.

4 **Sur le PC WinRoute - Pas de passerelle sur l'interface interne !**
Assurez vous qui n'y a PAS de passerelle par défaut dans les proprietés de l'interface (carte réseau) connectée au réseau interne. Il est évident que la passerelle par défaut de l'interface connectée à Internet sera fixée en fonction des détails fournis par votre Fournisseur d'Accès Internet (FAI).

5 **Sur le PC WinRoute - Entrer les options de la configuration DHCP !**
Dans la plupart des cas vous utiliserez le serveur DHCP de WinRoute pour automatiser la configuration du réseau. Vérifier bien que vous avez défini un ou plusieurs intervalles d'adresses IP que vous voulez voir attribuées par le serveur DHCP. Dans les Options vous pouvez spécifier d'autres informations transmises à vos stations de travail, comme le serveur DNS, la passerelle par défaut, etc.

6 **Sur le PC client - L'adresse IP interne du PC WinRoute est la passerelle par defaut !**
Le PC WinRoute agit comme PASSERELLE PAR DEFAUT pour tous les ordinateur du réseau local (LAN). Ainsi, vous spécifiez l'adresse IP de l'interface interne de la machine WinRoute comme la passerelle sur chaque ordinateur interne/client. Vous devez spécifier cette adresse sur chaque ordinateur client OU spécifiez la une seule fois sur le serveur DHCP de WinRoute et il transmettra automatiquement cette adresse à vos stations de travail. Consultez les exemples de réseaux avancés pour voir si vous avez besoin d'utiliser une autre passerelle par défaut!

Dans les cas ou WinRoute est simplement utilisé comme un Firewall ou un Serveur de messagerie (c'est à dire quand il n'est pas nécessaire de partager un accès

Internet), il n'est PAS nécessaire d'activer la Translation d'adresse (NAT) sur quelque interface que ce soit.

Les interfaces sur l'ordinateur WinRoute doivent avoir des adresses IP différentes de réseaux différents. Il n'est pas possible d'assigner des adresses IP d'un même réseau à plusieurs interfaces (c'est à dire 207.181.216.23 sur l'une et 207.181.216.24 sur l'autre). Typiquement vous aurez une interface locale (LAN) et une interface Internet. Dans ce cas vous n'aurez pas de problème. Dans certains cas vous aurez trois interfaces (2 locales et 1 Internet) et vous devrez assigner des adresses de réseaux différents aux interfaces locales (une avec 192.168.1.1 et l'autre avec 192.168.2.1 par exemple).

Conflits logiciels

Il existe quelques solutions concernant les programmes présentant une incompatibilité:

Norton Antivirus

Désactivez le port 110 dans la configuration de Norton Antivirus si vous voulez utiliser le serveur de Mail WinRoute. Laisser le port 110 dans Norton empêchera l'ordinateur de démarrer.

WinGate

Désinstaller WinGate avant l'installation. Désinstaller le logiciel client ainsi que le logiciel serveur.

SyGate

Désinstaller SyGate avant l'installation. Désinstaller le logiciel client ainsi que le logiciel serveur.

MS Proxy Server

Désinstaller MS Proxy Server avant l'installation. Désinstaller le logiciel client ainsi que le logiciel serveur. Enlevez TCP/IP, redémarrer, et réinstallez le.

Microsoft Internet Connection Sharing (partage de connexion Internet)

Désinstallez MS ICS avant l'installation, enlevez le protocole TCP/IP, redémarrer et remettez le.

WinProxy d'Ositis

Désinstallez WinProxy avant l'installation, enlevez le protocole TCP/IP, redémarrer et remettez le.

Tous les logiciels mentionnes ci-dessus, utilisent des pilotes qui ne fonctionnent pas correctement avec les fonctions bas niveau du protocole réseau implémentées par WinRoute.

Résolution des problèmes de table de routage

Il peut arriver que vous ayez tous les composants correctement installes et que cela ne fonctionne toujours pas. En effet, les systèmes d'exploitation Windows 95/98/NT ne sont pas spécialement crées pour les réseaux. Même après avoir configuré WinRoute et les paramètres réseau correctement, vous pouvez vous rendre compte que cela ne fonctionne toujours pas. Si tel est le cas, vous devrez regarder la table de routage et faire l'une des choses suivantes:

- réparer les routes en les supprimant et en les ajoutant de nouveau - réservé aux utilisateurs expérimentes

ou

- enlever complètement le protocole TCP/IP, redémarrer l'ordinateur et ajouter de nouveau le protocole. L'effet est garanti.

Résolution des problèmes lies aux clients Proxy

Certains serveurs proxy ont besoin qu'un logiciel client soit installe sur toutes les machines clientes. Ce client force les applications de la machine a faire leurs requêtes sur le serveur proxy. Si le client proxy n'est pas enlevé, cette machine ne peut se connecter a Internet sachant que WinRoute n'est pas configuré comme un serveur proxy. Si après cela la machine ne peut toujours pas se connecter à Internet, réinstaller TCP/IP et ses paramètres et redémarrer l'ordinateur.

Résolution des problèmes lies aux pilotes de Cartes Réseaux

Essayez d'utiliser les interfaces réseaux les plus standard possible. Si vous avez une carte spécifiquement vieille ou un modèle dernier cri, son pilote peut comporter certaines instructions spéciales qui empêcheront WinRoute de communiquer avec lui. Essayer de trouver une carte Ethernet standard sur votre réseau et échangez la avec celle qui pose problème. Quelques rares utilisateurs "mécontents" ont retrouve le sourire en changeant de carte réseau ou en mettant à jour le pilote de celle ci.

WinRoute est un logiciel complètement neutre de routeur/firewall qui ne nécessite l'utilisation d'aucun logiciel client sur les machines du réseau. On notera que, pour l'administration distante, l'installation du programme "wradmin.exe" est nécessaire.

Configuration du réseau

L'utilisation du service DHCP peut simplifier considérablement la configuration des machines de votre réseau local. En utilisant le serveur DHCP, le seul parametrage à faire sur les machines clientes de votre réseau, est de leur indiquer de demander leur adresse IP dynamiquement au serveur DHCP. (C'est de plus le paramètre par défaut lors de l'installation du protocole TCP/IP dans les paramètres réseau.)

Vous pouvez utiliser le serveur DCHP inclus dans WinRoute ou un serveur DCHP tiers installé sur votre réseau. Faites attention à ce que plusieurs serveurs DHCP ne tournent pas en même temps sur votre réseau!

Réglage de la passerelle par défaut

WinRoute agit en tant que routeur. Il faut donc que deux paramètres simples soient vérifiés sur les machines de votre réseau:

- Spécifiez une adresse IP – manuellement ou en utilisant un serveur DHCP (celui de WinRoute par exemple)
- Configurez la passerelle par défaut

La passerelle par défaut sur chaque ordinateur désirant accéder à Internet en utilisant la machine WinRoute, doit être configurée en indiquant **l'adresse IP** de l'interface Ethernet reliant l'ordinateur WinRoute au réseau local.

Exemple:

Un ordinateur client a 10.10.10.23 comme adresse IP. Le PC WinRoute a deux interfaces, l'une d'elles le reliant au modem câble avec une adresse IP fournie par le FAI (Fournisseur d'acces Internet), et l'autre le reliant au réseau prive (10.10.10.1). La passerelle par défaut sur l'ordinateur 10.10.10.23 sera 10.10.10.1.

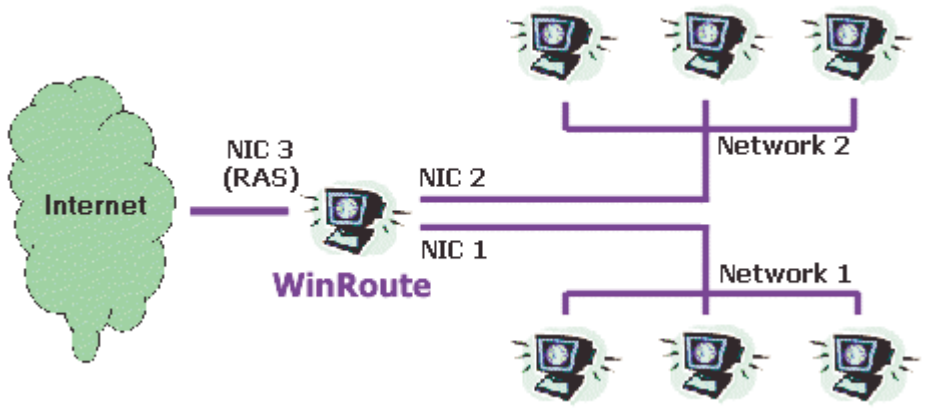
Remarque 1: Lorsque vous faites votre plan d'adressage IP sur votre réseau local, vous devez utiliser des adresses IP faisant partie d'un même sous réseau. C'est a dire que si votre masque de sous réseau est 255.255.255.0, alors toutes les adresses doivent être entre 10.10.10.1 et 10.10.10.255 (non comprise).

Remarque 2: Il est possible de connecter plusieurs réseaux a Internet grâce a WinRoute. Vous devez pour cela avoir plusieurs interfaces réseau dans l'ordinateur WinRoute; une pour chaque réseau. Chaque carte réseau (son adresse IP) représente la passerelle par défaut pour les machines appartenant au réseau connecté sur cette interface.

Choisir le bon ordinateur WinRoute

WinRoute **DOIT TOUJOURS** s'executer sur l'ordinateur connecte à Internet - à travers une carte réseau, modem câble, modem DSL, connexion distante ou un routeur.

WinRoute agit en permanence en tant que passerelle entre deux (ou plus) réseaux ou chaque réseau est représenté par une interface. Ces interfaces peuvent être des cartes Ethernet, des adaptateurs RAS (connexion réseau à distance), adaptateurs USB vers Ethernet, adaptateurs PPPoE, etc.



Configuration IP avec le serveur DHCP

Vérifiez bien que les stations de travail sont configurées pour demander une adresse IP au serveur DHCP (voir les propriétés TCP/IP->interface réseau properties de chaque ordinateur). Tous les autres paramètres doivent être laisses blancs (y compris les paramètres DNS).

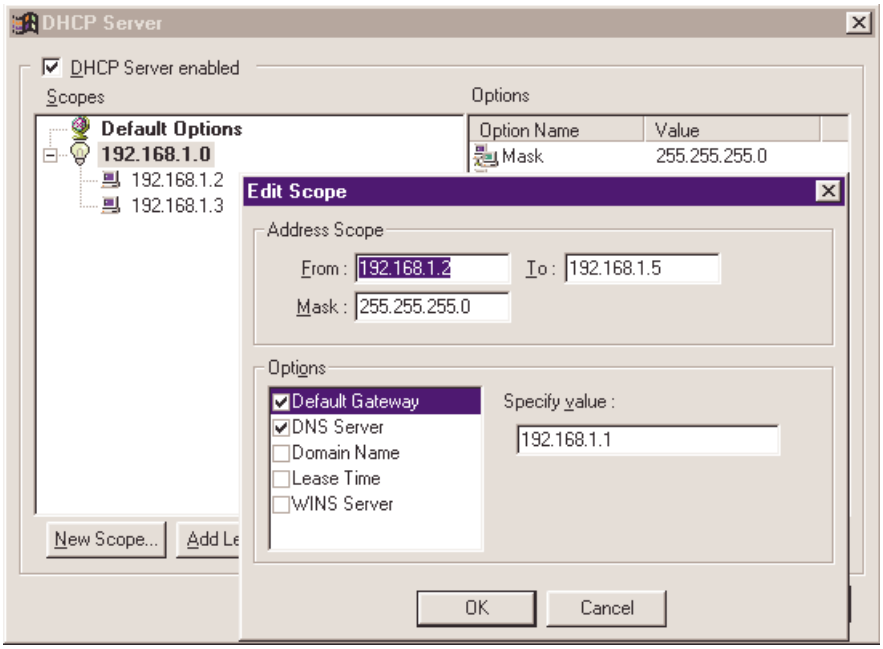
Vous pouvez alors lancer le programme d'administration de WinRoute:

1. *Aller dans le menu Settings=>DHCP server.*

2. Activez l'option DHCP server (placez une croix devant) et appuyez sur le bouton **New Scope**.

3. **Add Scope (ajouter une plage)**
   Vous indiquerez ici la plage d'adresses IP utilisées par le serveur DHCP et qui seront distribuées aux stations de travail. Souvenez vous qu'une adresse IP est déjà utilisée par l'ordinateur WinRoute, et qu'il ne faut donc pas l'utiliser. La plage d'adresses IP doit appartenir au même sous réseau. Voir l'image ci dessous pour exemple.

4. **Indiquez les options (important!)**
   Dans les Options vous spécifiez quelles informations supplémentaire seront transmises aux stations de travail (ex: Passerelle par défaut, serveur DNS, etc.). Cochez la case devant chaque composant et entrer les informations nécessaires. Entrer les informations pour la passerelle par défaut et pour le serveur DNS (vous utilisez normalement WinRoute comme serveur DNS) et vous utiliserez l'adresse IP de la machine WinRoute (ex: 192.168.1.1). Vous laisserez les autres en blanc.



Note: L'adresse IP de la carte Ethernet (reliée au LAN) sur l'ordinateur WinRoute doit être assignée et vous utiliserez cette adresse IP comme passerelle par défaut et (de manière optionnelle) comme serveur DNS ! Dans tous les cas, la passerelle par défaut pour cette interface ne sera pas renseignée.

Configuration IP avec un serveur DHCP tiers

L'utilisation d'un autre serveur DHCP que celui de WinRoute nécessite une attention particulière quant aux valeurs transmises aux stations de travail de votre réseau par un tel serveur.

Vérifier bien que votre serveur DHCP fournit des informations correctes à vos stations clientes. C'est à dire que vous devez faire que votre serveur DHCP fournisse l'adresse IP de la carte réseau de l'ordinateur WinRoute en tant que passerelle par défaut et (éventuellement) en tant que serveur DNS.

Veillez également à ce que les adresses IP transmises aux stations appartiennent au même sous réseau que celle de l'ordinateur WinRoute.

VÉRIFIEZ ABSOLUMENT (!!!) que la carte interne de l'ordinateur WinRoute possède une adresse IP fixe (par exemple 192.168.1.1) et que cette adresse soit indiquée comme passerelle par défaut à l'ensemble du réseau. Le serveur DHCP ne doit pas attribuer d'adresse IP à la machine WinRoute!

Exemple:

NT serveur avec le service DHCP tourne sur l'adresse 192.168.1.1 alors que WinRoute tourne sur l'adresse 192.168.1.5. La passerelle par défaut (et le DNS si vous utilisez celui de WinRoute) transmise aux stations clients sera 192.168.1.5.

Configuration IP - assignation manuelle

Dans certains cas, il est nécessaire d'assigner des adresses IP manuellement aux stations de travail. Lorsque c'est le cas, prenez en compte les règles suivantes:

Assignation des adresses IP

Assignez à chaque ordinateur une adresse IP de "type interne". Habituellement 192.168.x.x ou 10.x.x.x. Veillez à ce que les adresses appartiennent au même sous réseau. Par exemple, des que vous avez attribué l'adresse IP 192.168.1.1 à la machine WinRoute, vous devez continuer en suivant le même plan (ex: 192.168.1.2, 192.168.1.3, etc.)

Passerelle par défaut

Utilisez l'adresse IP de la machine WinRoute en tant que passerelle par défaut pour tous les PC clients. En d'autres termes, chaque ordinateur client utilisera l'adresse IP de Ia machine WinRoute (adresse IP interne) comme passerelle par défaut. Cela se paramètre dans les proprietes réseau de l'ordinateur (TCP/IP=>Ethernet_adapter).

Configuration DNS

Pour terminer, utilisez l'adresse IP de l'ordinateur WinRoute comme serveur DNS pour tous les ordinateurs (l'adresse IP interne,si vous utilisez le serveur DHCP de WinRoute). La seule exception peut être l'utilisation de l'adresse DNS de votre FAI ou d'une adresse d'un autre serveur DNS. Entrez alors les informations fournies par votre fournisseur d'accès (dans TCP/IP->NIC properties sur chaque station).

Important ! Consulter le chapitre des recommandations de ce manuel pour de plus amples informations concernant le parametrage DNS !

Connexion du réseau à Internet

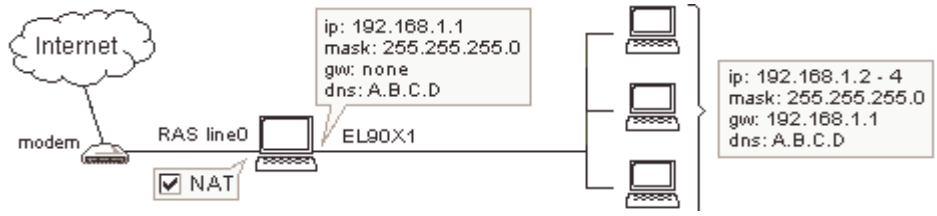
WinRoute Pro est l'ultime routeur Internet - Firewall qui vous permet, pratiquement sans effort, de partager une connexion Internet ! - Connectez vous à travers une connexion distante, une ligne DSL, un modem câble, une liaison spécialisée ou une connexion DirecPC.

Connexion modem ou RNIS (Numéris)

Connexion par accès réseau à distance ou RNIS (Numéris - ISDN)

Si vous avez une connexion distante a Internet (modem 56K ou RNIS) sur un PC avec Win95, Win98, WinNT or Win2000, vous avez tout ce qu'il faut pour utiliser WinRoute. WinRoute fonctionne sur un ordinateur possédant:

- un modem connecté sur un ligne téléphonique ou RNIS
- un carte réseau (NIC) connectée au réseau interne



Si vous possédez un modem RNIS connecte à votre ordinateur via une carte Ethernet, referez vous au chapitre Connexion DSL. Dans ce cas, vous aurez à configurer WinRoute pour qu'il fonctionne avec deux cartes Ethernet.

Avant la connexion

Avant de vous connecter à Internet, vérifier bien les points suivant:

- le protocole TCP/IP est correctement installé et configuré
- l'accès réseau à distance (Windows 95/98) ou le service d'accès distant (RAS service - WindowsNT) est correctement installé et configuré
- le modem est connecté au PC WinRoute

WinRoute utilise les connexions distantes ou RAS disponibles sur votre système d'exploitation pour se connecter à Internet.

Il est recommande de vous connecter à Internet sur l'ordinateur ou WinRoute doit être exécuté AVANT d'installer et de lancer WinRoute, pour être sûr que la connexion est correctement configurée et fonctionne correctement.

Configuration de WinRoute

1. Aller dans le menu Settings->Interface table - vous verrez alors normalement toutes les interfaces réseau disponibles sur votre ordinateur. Les accès distants sont appelés RAS dans WinRoute (sur tous les systèmes d'exploitation).
2. Aller dans les propriétés de l'interface RAS sélectionnée
3. Cochez alors "Perform NAT with IP address of this interface on all communication passing through"
4. Aller dans la table RAS dans la fenêtre Properties, choisissez ou créez votre connexion et configurer les paramètres selon vos besoins. Voir Table RAS pour plus de détails.

Attention ! La translation d'adresse (NAT) doit être activée sur l'interface RAS et désactivée sur le(s) interface(s) reliées au réseau interne.

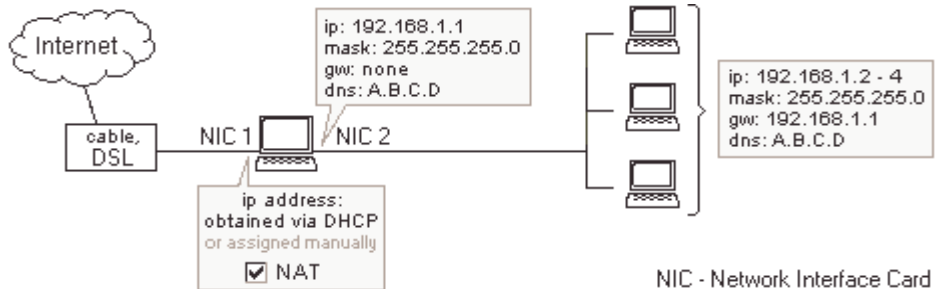
Configuration de l'interface Ethernet

1. La carte réseau reliée au réseau interne a une adresse IP fixe (appartenant à une classe privée) mais PAS de passerelle !
2. Les entrées DNS utilisées pour cette interface sont basées sur les données fournies par le fournisseur d'acces (FAI). Si vous n'avez pas ces données, contactez votre fournisseur.

Vous pouvez configurer WinRoute pour qu'il utilise l'option "dial on demand" qui permet de faire que la connexion soit automatiquement activée suivant le trafic (données) sortant de votre réseau local.

Connexion DSL

Les connexions DSL (ADSL, SDSL) nécessitent que deux interfaces réseau (NIC) soient installées dans l'ordinateur WinRoute. L'une des interfaces sera connectée à Internet (modem DSL) alors que l'autre sera connectée au réseau interne.



Configuration de WinRoute

Pour vous connecter à Internet

1. Aller dans le menu Settings->Interface Table
2. Choisissez l'interface connectée a Internet, cliquez sur Properties et cochez la fonction "Perform NAT with IP address of the interface on all communication passing through". Lorsque vous ouvrirez la fenêtre listant les interfaces, vous apercevrez NAT ON en fin de ligne.
3. Vérifiez que la fonction NAT n'est pas activée pour l'interface reliée au réseau local interne (aller dans les propriétés de l'interface dans la table d'Interfaces).
4. Vérifiez qu'il n'y a pas de passerelle dans les proprietes TCP/IP de la carte interne et que cette dernière a une adresse IP interne.
5. Vérifiez que l'interface reliée à Internet est paramètrée correctement avec les informations fournies par votre FAI (Fournisseur d'Accès Internet). Si vous avez une adresse IP assignée dynamiquement, laissez le champ vide.

Pour d'autres paramètres réseau, reportez vous sur les chapitres concernes, et en particulier sur le chapitre ***CheckList*** .

Connexion xDSL via PPPoE

PPPoE est une technologie récente utilisée par de nombreux abonnés DSL.. Bien qu'elle soit largement utilisée par de nombreux Fournisseurs d'Acces, elle fournit une connexion de piètre qualité et n'est pas (à l'heure actuelle) la meilleure solution pour connecter votre réseau à Internet. Les clients devront demander une solution DSL standard (sans PPPoE ni PPTP) le plus souvent possible.

Le déploiement de PPPoE avec WinRoute est identique à celui d'une connexion DSL standard en ce qui concerne les paramètres TCP/IP. WinRoute Pro doit être installé sur le même ordinateur que l'adaptateur PPPoE. WinRoute Pro reconnaîtra l'adaptateur PPPoE comme une carte réseau. Vous devez activer la translation d'adresse (NAT) sur cette interface. Vous devez également voir la carte Ethernet (connectée à votre modem) dans la table des interfaces de WinRoute Pro. Vous ne devez pas activer la translation d'adresse sur cette interface.

WinRoute Pro fonctionne avec tous les adaptateurs PPPoE présents sur le marche. Il arrive cependant que certains utilisateurs rencontre certains problèmes de performance en utilisant certains adaptateurs PPPoE :

Enternet 100, 300, 500 PPPoE client

WinRoute Pro 4.2 fonctionne bien avec l'adaptateur Enternet PPPoE de NTS si vous avez active le pilote au niveau protocole (protocole drivers) au lieu de l'option par défaut (Filter Driver). Pour faire cela, lancer le client Enternet PPPoE, aller dans le menu Settings->Advanced et faites la modification nécessaire.

Si vous rencontrer des problèmes de performance, vous pouvez également abaisser la MTU a 800 sur les machines clientes.

WinPoet d'Ivasion

WinRoute Pro 4.2 fonctionne bien avec WinPoet si la compression d'en-tête IP (dans les proprietes de votre connexion distante) est désactivée.

Abaisser la MTU:

Pour les utilisateurs de Windows 95/98 :

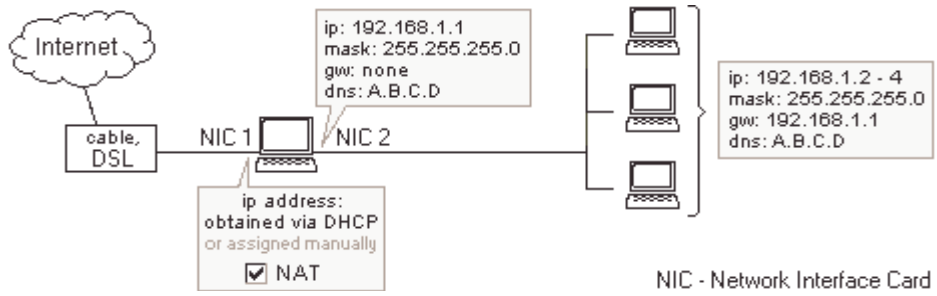
http://www.microsoft.com/support/kb/articles/Q158/4/74.asp

Pour les utilisateurs de Windows NT4/2000 :

http://www.microsoft.com/WINDOWS2000/library/resources/reskit/samplechapters/cnbd/cnbd_trb_vcfx.asp

Connexion (bi-directionnelle) par modem câble

Une connexion par modem câble nécessite que deux cartes réseau (NIC) soit inclues dans l'ordinateur exécutant WinRoute. Une interface doit être connectée à Internet (modem câble) et l'autre au réseau interne. Pour les modems câble sans voie de retour (connexion unidirectionnelle), aller au chapitre approprie.



Configuration de WinRoute

1. Aller dans le menu Settings->Interface Table
2. Choisissez l'interface connectée a Internet, cliquez sur Properties et cochez la fonction "Perform NAT with IP address of the interface on all communication passing through". Lorsque vous ouvrirez la fenêtre listant les interfaces, vous apercevrez NAT ON en fin de ligne.

3 Vérifiez que la fonction NAT n'est pas activée pour l'interface reliée au réseau local interne (aller dans les proprietes de l'interface dans la table d'Interfaces).

4 Vérifiez qu'il n'y a pas de passerelle dans les proprietes TCP/IP de la carte interne et que cette derniere a une adresse IP interne.

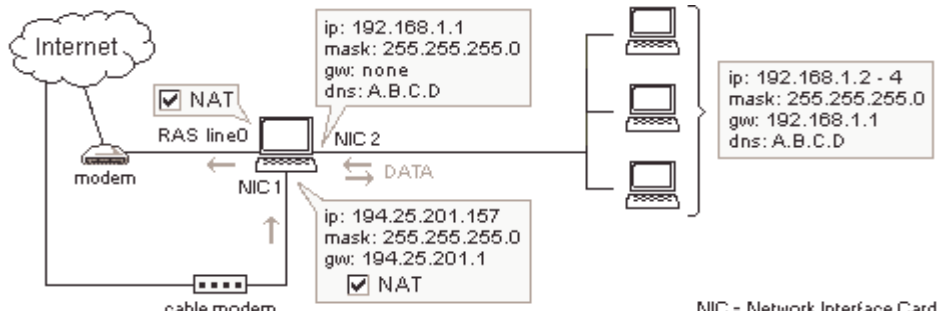
5 Vérifiez que l'interface reliée à Internet est parametree correctement avec les informations fournies par votre FAI (Fournisseur d'Acces Internet). Si vous avez une adresse IP assignée dynamiquement, laissez le champ vide.

Pour d'autres parametres réseau, reportez vous sur les chapitres concernes, et en particulier sur le chapitre ***checklist*** , ***configuration IP*** etc.

Connexion unidirectionnelle par modem câble et ligne modem

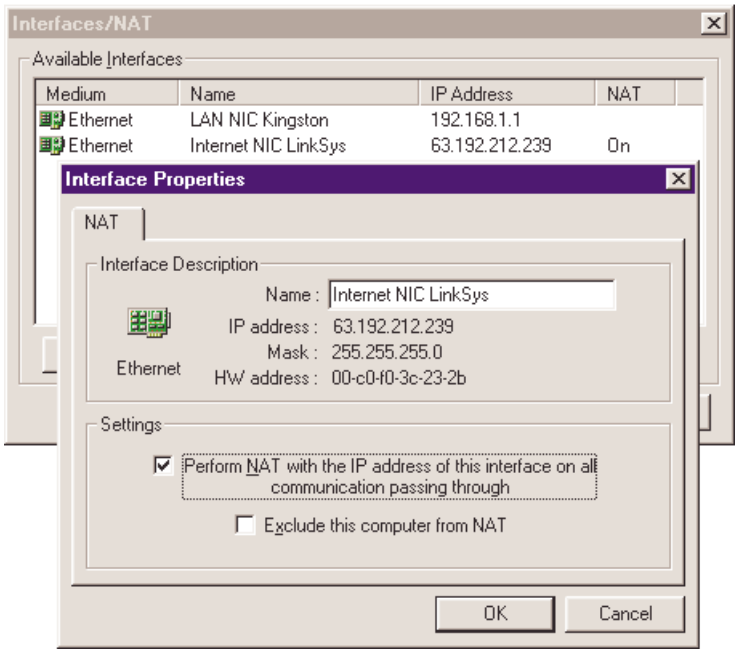
NOTE: Ce type de connexion à Internet **n'est pas une "configuration officiellement supportée"** de par le fait que les paramètrages **peuvent varier** d'un Fournisseur d'accès à un autre. Cependant, nous essayons de fournir le plus de scénarios de connexions possibles. Un grand nombre d'utilisateurs ont réussit leur connexion en utilisant les paramètres suivants :

En général le flux de données est **similaire à DirecPC**. Le flux de paquets sort à travers l'interface de **connexion distante**. Le flux entrant est quant à lui assuré **par le câble**. En fait, votre fournisseur d'accès Internet doit lier vos deux interfaces ensemble. Bien que cela puisse sembler étrange, c'est la seule manière d'établir une connexion. C'est pour cela que nous vous conseillons de faire toutes les vérifications nécessaires avec votre fournisseur d'accès avant d'acheter WinRoute.



*1. Aller dans le menu Settings->Interface Table. Vous verrez une ligne d'accès distant (**RAS line** - votre modem) ainsi que deux **cartes réseau** - une reliée à Internet et l'autre reliée au réseau local.*

2. Cliquez sur l'interface de la carte réseau reliée à Internet et aller ensuite dans "Properties." et cochez "Perform NAT with IP address of the interface on all communication passing through".



*3. Cliquez sur **RAS interface** et allez dans "Properties." et cochez "Perform NAT with IP address of the interface on all communication passing through". Dans **l'onglet RAS** sélectionnez la connexion que vous utiliserez pour vous connecter à votre fournisseur d'acces (FAI), entrez votre nom d'utilisateur et votre de passe.*

4. Vérifiez que la translation d'adresse (NAT) n'est **N'EST PAS ACTIVÉE** sur l'interface reliée au réseau interne (allez dans les propriétés de cette interface)

5. Vérifiez **qu'il n'y a pas de passerelle** dans les propriétés TCP/IP de la carte interne (aller dans les paramètres réseau) et que cette dernière a une adresse **IP interne** (ex:.10.10.1.1).

6. Vérifiez que l'interface reliée à Internet est paramètrée correctement avec les informations fournies par votre FAI (Fournisseur d'Acces Internet). Si vous avez une adresse IP assignée dynamiquement, laissez le champ vide.

En général la NAT doit être activée sur les deux interfaces reliées à Internet.

Connexion AOL

En utilisant WinRoute Pro vous pouvez connecter votre réseau à Internet via une simple connexion d'accès distant sur votre compte AOL. AOL ne supporte cependant que les ordinateur sous Win95/98. Pour vous connecter via AOL suivez les instructions suivantes :

1 Installez le client AOL (de préférence AOL 5.0 ou supérieur)

2 Connectez vous à Internet pour être sur du bon fonctionnement de votre connexion AOL

3 Installez WinRoute Pro

Dans l'administrateur WinRoute allez dans le menu Settings->Interface table

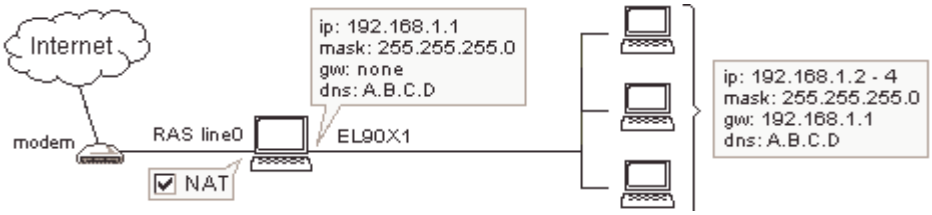
4 Vous verrez alors normalement l'AOL adapter parmi les interfaces disponibles. Allez dans les propriétés de cette interface et activez "perform NAT" dedans.

Configurez alors votre ordinateur WinRoute et les machines clientes comme indiqué dans le chapitre Démarrage rapide.

Attention ! La fonction "Dial on demand" ne fonctionnera pas. Vous devez activer votre connexion AOL manuellement.

Connexion T1 ou LAN

Une connexion T1 ou LAN nécessite que deux cartes réseau (NIC) soit inclues dans l'ordinateur exécutant WinRoute. Une interface doit être connectée à Internet (routeur) et l'autre au réseau interne.



Configuration de WinRoute

Pour vous connecter a Internet

1. Allez dans le menu Settings->Interface Table
2. Choisissez l'interface connectée à Internet, cliquez sur Properties et cochez la fonction "Perform NAT with IP address of the interface on all communication passing through". Lorsque vous ouvrirez la fenêtre listant les interfaces, vous apercevrez NAT ON en fin de ligne.
3. Vérifiez que la fonction NAT n'est pas activée pour l'interface reliée au réseau local interne (aller dans les propriétés de l'interface dans la table d'Interfaces).
4. Vérifiez qu'il n'y a pas de passerelle dans les propriétés TCP/IP de la carte interne et que cette dernière à une adresse IP interne.

5 Vérifiez que l'interface reliée à Internet est paramètrée correctement avec les informations fournies par votre FAI (Fournisseur d'Acces Internet). Si vous avez une adresse IP assignée dynamiquement, laissez le champ vide.

Pour d'autres paramètres réseau, reportez vous sur les chapitres concernes, et en particulier sur le chapitre ***CheckList*** .

Connexion DirecPC

DirecPC utilise un modem (analogique, RNIS, ...) ou une carte réseau (Ethernet, Token Ring) pour la voie montante tout en utilisant une connexion satellite pour la voie descendante. Votre connexion Internet est assurée par DirecPC ou vous pouvez utiliser votre Fournisseur actuel pour votre connexion distante.

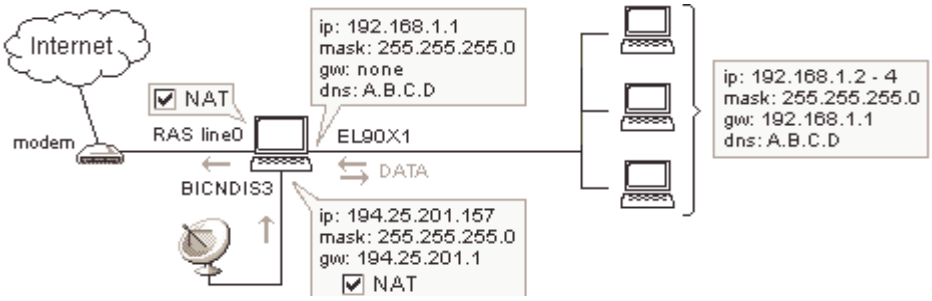
Les données vont de votre ordinateur au service DirecPC par modem, puis elles sont routées jusqu'à leur destination finale. Au retour, DirecPC, vos données sont jointes à d'autres et transitent par satellite.

Configuration de WinRoute

Tout d'abord, vous devez installer et configurer correctement tous les composants et les logiciels DirecPC. Ensuite configurez WinRoute selon les conditions nécessaires.

Vous pouvez utiliser soit le dialer DirecPC, soit la connexion RAS de WinRoute pour le voie montante. En utilisant WinRoute vous bénéficierez de la fonctionnalité de connexion à la demande (dial on demand) qui permet de faire des économies sur votre facture de téléphone.

1. Utilisation d'une ligne d'accès distant (RAS) pour la voie montante

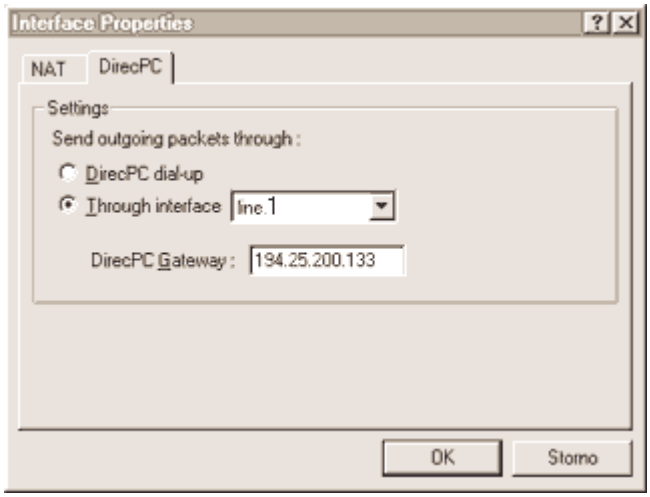


Aller dans le menu Settings->Interface Table. Vous verrez l'interface de votre ligne RAS (votre modem) et l'interface de votre carte DirecPC.

Cliquez sur l'interface DirecPC et aller dans ses Propriétés (Properties). Vous verrez alors deux onglets - **NAT** et **DirecPC**.

Dans l'onglet NAT cochez la case "Perform NAT with of the interface on all communication passing through".

Dans l'onglet DirecPC choisissez la ligne 0 (line0) pour la voie montante. Entrez l'adresse de la passerelle IP qui vous a été donnée par DirecPC.

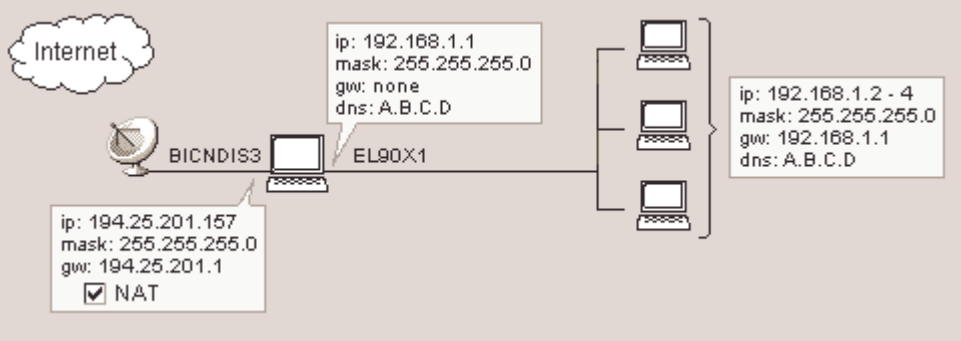


3. Cliquez sur l'interface RAS, allez dans ses propriétés (Properties) et cochez "Perform NAT with IP address of the interface on all communication passing through". Dans l'onglet RAS, sélectionnez la connexion que vous allez utiliser pour vous connecter à votre fournisseur d'accès Internet, et entrer votre nom d'utilisateur et votre mot de passe.

Attention ! Vous devez désélectionner l'option "Use default gateway on remote network" dans les propriétés de votre compte d'accès distant créé pour votre connexion à votre fournisseur d'accès distant. Sélectionnez cette option dans les propriétés TCP/IP de votre interface d'accès distant.

2. Utilisation du dialer DirecPC pour la voie montante

Vous pouvez utiliser le dialer intégré de DirecPC lorsqu'il est disponible. Cependant nous recommandons l'utilisation du dialer intégré dans WinRoute lorsque cela est possible.



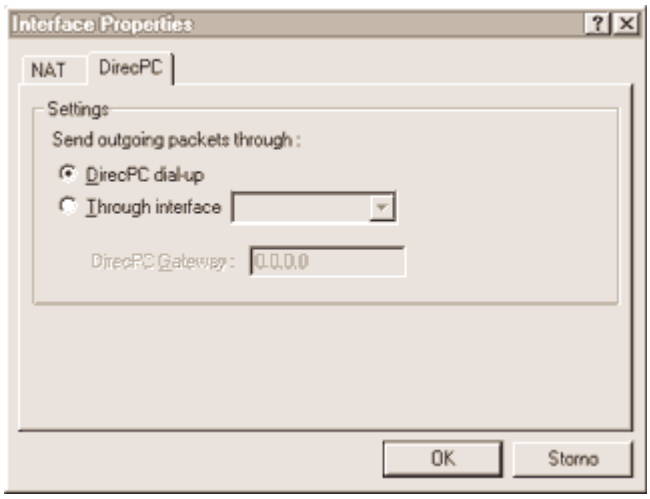
Pour utiliser le dialer (numéroteur) DirecPC:

Aller dans le menu Settings->Interface Table. Vous verrez l'interface de la ligne RAS (votre modem) et l'interface de la carte DirecPC

Cliquez sur l'interface DirecPC et aller dans ses proprietes (Properties). Vous verrez deux onglets - NAT et DirecPC.

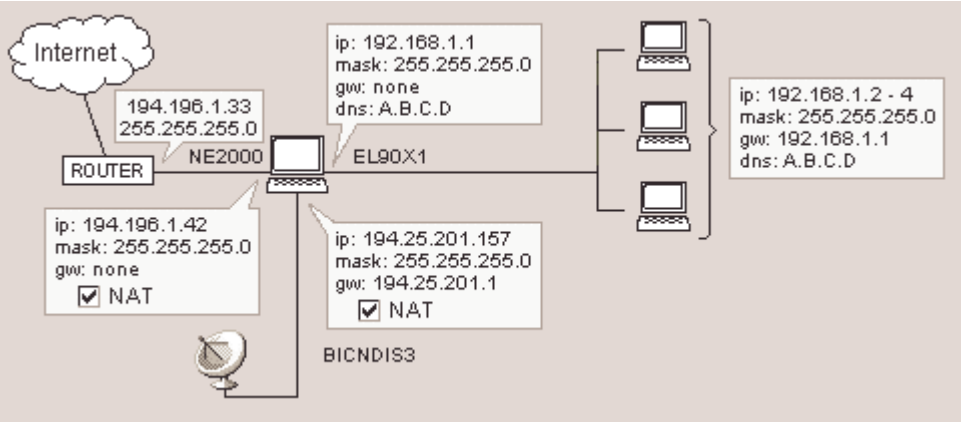
Dans l'onglet NAT, sélectionnez "Perform NAT with IP address of the interface on all communication passing through".

Dans l'onglet DirecPC sélectionnez "Use DirecPC dialer for uplink".

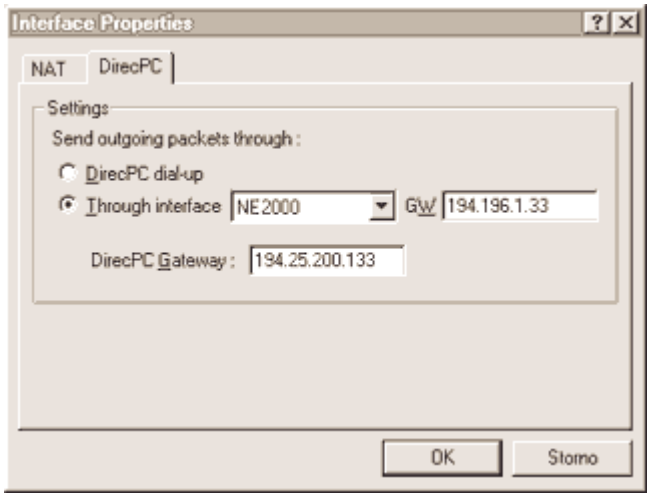


3. Utilisation d'une interface Ethernet pour la voie montante

Parfois vous devrez utiliser une interface Ethernet pour la voie montante. Cela arrivera si votre lien montant (uplink) est assuré par une connexion RNIS (et que vous avez un routeur RNIS ou un modem) ou une connexion V-SAT (via une carte Ethernet).



Allez dans les propriétés de l'interface de la carte DirecPC.



Dans l'onglet NAT, activez "Perform NAT with IP address of the interface on all communication passing through".

Dans l'onglet DirecPC choisissez "Through interface" et selectionnez l'interface reliée a Internet. Entrer alors l'adresse de la passerelle par défaut de votre fournisseur d'accès dans le champ "GW" (ex: 194.196.1.33).

Augmenter le débit

Pour obtenir un débit maximum lorsque vous êtes connecte à Internet en utilisant DirecPC, réduire la valeur **TCP receive window** sur tous les ordinateurs utilisant DirecPC:

Sur Windows NT:

1. Aller dans le registre HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
2. Ajouter (si cela existe deja, éditer simplement) une entrée nommée "TcpWindowSize" (de type DWORD) dans le registre. Configurez sa valeur a 0xBB80.

Sur Windows 95:

1. Aller dans le registre HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP .
2. Ajouter (si cela existe deja, éditer simplement) une entrée nommée "DefaultRcvWindow" (de type STRING) dans le registre. Configurez sa valeur a "0xBB80".

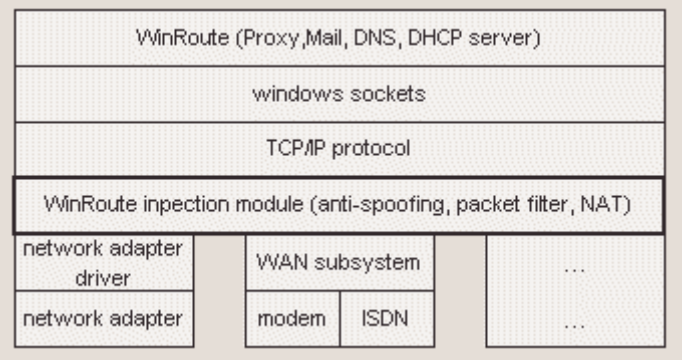
CHAPITRE 3

Configurer la sécurité

Dans ce chapitre

La sécurité NAT

WinRoute réalise les opérations de translation d'adresse (NAT) au niveau de la couche protocole réseau (niveau le plus bas). WinRoute contrôle le trafic entre les pilotes des interfaces et la pile TCP. WinRoute a un contrôle total sur tout le trafic Internet, en capturant aussi bien les paquets sortants que les paquets entrant, limitant ainsi tous les risques. C'est une fonctionnalité unique de l'implémentation WinRoute de la translation d'adresse (NAT). De plus, cela procure d'avantage de fonctionnalités en ce qui concerne la sécurité, comme l'antispoofing et le filtrage de paquets. Avec la translation d'adresse (NAT) de WinRoute, le réseau tout entier (ainsi que l'ordinateur WinRoute lui même) bénéficie d'une protection complète.



Options de la sécurité NAT

Dans les paramètres avancés de WinRoute (build 20 et plus), il y a un menu d'options concernant la sécurité NAT et qui comprend un **mode silence** (**silent mode**). Ce mode permet de faire que WinRoute, pour certains types de requêtes, ignore les paquets et rende ainsi votre réseau invisible du monde extérieur.

Requête écho ICMP entrante (Incoming ICMP echo request):

Internet Control Message Protocol (ICMP) est le protocole d'information qui permet de faire des requêtes simples sur l'état du réseau (UN ping, par exemple - ping 206.86.211.32). Lorsqu'un ordinateur essaye de **pinger** l'ordinateur WinRoute, les **options de sécurité NAT** proposent deux comportements possibles :

Si vous sélectionnez l'option "send ICMP echo reply" l'ordinateur ayant fait la requête recevra une réponse.

Si vous sélectionnez l'option "drop request (silent mode)" le datagramme sera saute, comme s'il avait été perdu pendant le transite. L'ordinateur ayant fait la requête recevra alors le message "destination host unreachable." (l'ordinateur distant ne peut être atteint).

Paquets entrant non identifiés dans la table de NAT (Incoming packets with no entry in the NAT table):

WinRoute inspecte tout le trafic entrant et sortant du réseau. Si WinRoute doit appliquer la translation d'adresse (NAT) sur un paquet, il l'examinera et enregistrera certaines informations comme le numéro de port et l'adresse IP dans la table de NAT. Ainsi, lorsque le paquet revient, WinRoute peut le comparer avec les entrées de la table de NAT, et ainsi déterminer vers qui router le paquet. Si le paquet n'est pas un paquet de retour (paquet non initialisé), WinRoute le comparera avec la table de NAT et déterminera qu'il n'est pas initialisé. Si aucun port mapping n'est créé, WinRoute sera incapable de router le paquet vers qui que ce soit à l'intérieur du LAN.

- L'option “send denying packet” renverra simplement le paquet à l'envoyeur en indiquant que la connexion n'a pu être établie.
- L'option “drop packet (silent mode)" éliminera simplement le paquet sans envoyer de paquet en retour. De cette manière, l'ordinateur WinRoute, ainsi que tout le réseau derrière lui, seront invisibles et sembleront inexistants.

Paquet entrant UDP:

Certaines applications qui utilisent le protocole UDP (**User Datagram Protocol**) ont besoin d'envoyer des paquets UDP à un serveur central. WinRoute enregistre la source et la destination de tous les paquets UDP sortants vers le serveur choisi par l'application envoyant le paquet. Dans certains cas, le serveur peut passer votre adresse IP et votre numéro de port a un autre serveur qui vous enverra alors un paquet UDP contenant les informations que vous avez demandées. Bien que cet ordinateur aléatoire possède une adresse IP différente de celle du serveur, il peut cependant envoyer des paquets UDP parce qu'il connaît l'adresse IP et le port à utiliser.

En utilisant cet exemple, si vous sélectionnez “can pass through NAT with any source IP address” le paquet UDP passera à travers WinRoute.

Pour augmenter le niveau de sécurité, vous pouvez sélectionner “can pass through NAT only if it comes from source IP address that was recorded when first outgoing packet from LAN was sent.” Cela indiquera à WinRoute de seulement laisser passer les paquets UDP en provenance du serveur central.

Options d'audit de NAT (logging options):

Dans les options avancées de sécurité, vous avez la possibilité d'enregistrer des informations sur les paquets arrivant sur le réseau sans avoir êtes demandés par quelqu'un à l'intérieur du LAN. Cela concerne typiquement les réseaux comportant des serveurs Web, FTP, DNS ou autres, derrière WinRoute. Cela aide à déterminer la source d'un problème.

Auditer les paquets entrant sans référence dans la table de translation (NAT table):

WinRoute propose deux options pour auditer les paquets TCP non présents dans la table de NAT.

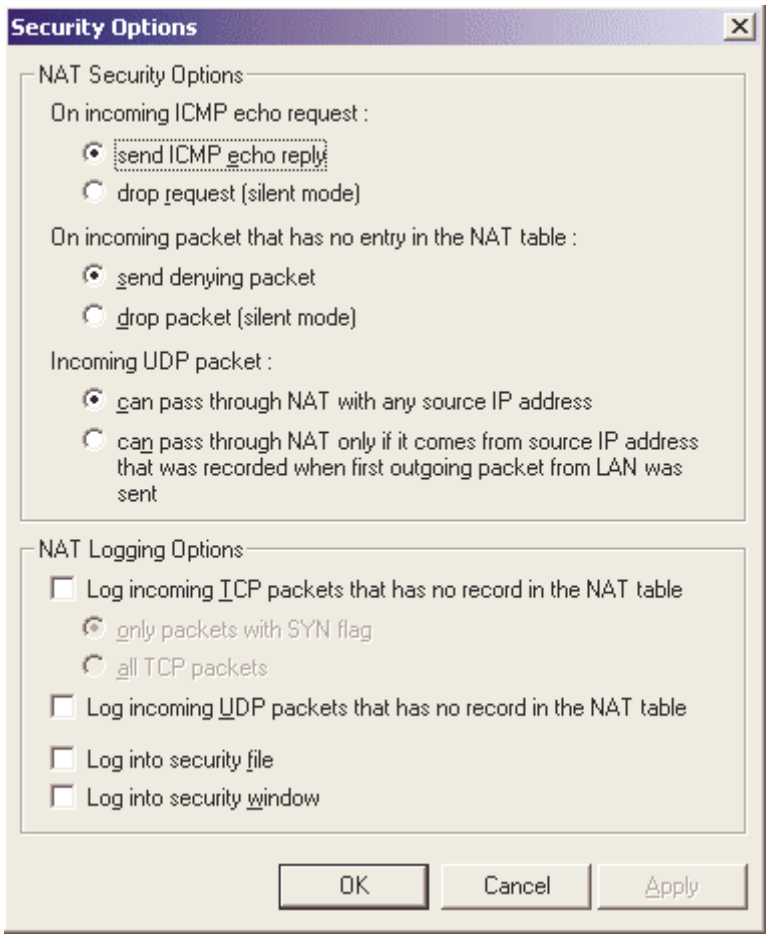
Si vous choisissez d'auditer "only packets with SYN flag" (synchronize), le paquet TCP sera audité seulement si une connexion à été établie entre l'émetteur et le destinataire.

L'option "all TCP packets" audite tous les paquets TCP entrant, sans se préoccuper de la connexion. Comme les paquets UDP n'utilise pas de flags, tous les paquets UDP non initialisés seront audités si vous avez choisi d'auditer les paquets UDP.

Auditer dans un fichier ou dans une fenêtre (Logging to a file or window):

Si vous sélectionnez “log into security window” vous pouvez voir les information d'audit depuis l'application d'administration de WinRoute en affichant les audits de sécurité (view-logs-security log).

Si vous choisissez "log to a file", WinRoute enregistrera toutes les informations d'audit dans le fichier d'audit de sécurité situé dans le répertoire logs de WinRoute Pro (typiquement C:\Program Files\WinRoute Pro\Logs)


Security Options
NAT Security Options
On incoming ICMP echo request :
send ICMP echo reply
drop request (silent mode)
On incoming packet that has no entry in the NAT table :
send denying packet
drop packet (silent mode)
Incoming UDP packet :
can pass through NAT with any source IP address
can pass through NAT only if it comes from source IP address that was recorded when first outgoing packet from LAN was sent
NAT Logging Options
Log incoming TCP packets that has no record in the NAT table
only packets with SYN flag
all TCP packets
Log incoming UDP packets that has no record in the NAT table
Log into security file
Log into security window
OK
Cancel
Apply

Configuration du filtrage de paquets

La configuration de la partie "filtre de paquet" du firewall WinRoute Pro est très simple. Cela demande une bonne compréhension des fonctionnalites de filtrage des paquets effectue par WinRoute.

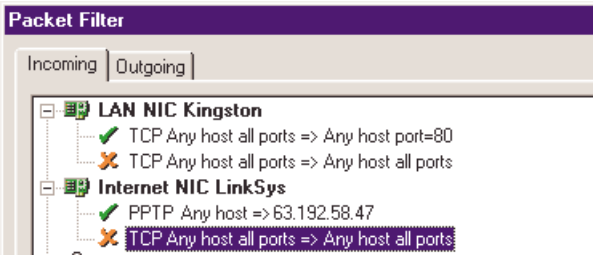
Règles définies par Interface

Les utilisateurs peuvent définir des règles de sécurité sur chaque interface de l'ordinateur, de manière individuelle. Cette fonctionnalité est très importante lorsque l'on administre des réseaux multi segments.

Exemple: l'image suivante montre un exemple de réseau qui:

autorise l'accès au serveur web interne à tout le monde depuis Internet

autorise l'accès au serveur PPTP interne seulement a certains individu appartenant au Groupe d'Adresses Travellers défini auparavant



Séparer les règles pour le paquets entrant et sortant

WinRoute applique des règles spécifiques aux paquets sortant et aux paquets entrant. Une table est créée par WinRoute pour chaque interface. Dans cette table, les deux types de paquets sont enregistrés (paquets sortants et paquets entrants). En d'autres termes, chaque paquet a deux entrées, une pour la sortie et une pour l'entrée.

Qu'est-ce qu'un paquet ENTRANT/SORTANT ?

WinRoute considère toujours son moteur comme le centre du système. Cela veut dire que tous les paquets partant de WinRoute sont des paquets SORTANT, qu'ils aillent vers le LAN ou vers Internet. De la même manière, tout les paquets arrivant sur le PC WinRoute sont des paquets ENTRANT, peu importe d'ou ils viennent. Il est important de bien considérer cela lors de la création des règles de sécurité.

APPLICATION DES REGLES:

Du HAUT vers le BAS

Les règles sont définies dans une liste et appliquées de haut en bas. Lorsque le paquet arrivent sur l'interface, il est vérifie suivant la liste des critères définis. La première règle est alors vérifiée puis les suivantes jusqu'à la règle la plus basse qui est vérifiée en dernière. Lorsque le paquet correspond à un critère, la règle correspondante est appliquée et les autres règles sont ignorées.

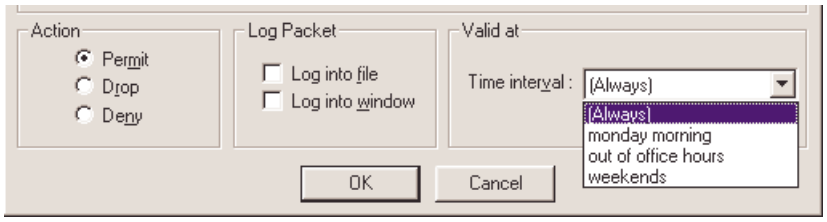
Les règles peuvent être appliquées à:

- des utilisateurs autonomes
- un intervalle d'adresses IP
- un groupe d'adresses IP défini par l'utilisateur (pour définir un groupe d'adresses IP, referez vous à la partie référence de ce manuel)

- tout le sous-réseau ou réseau

Les règles peuvent être appliquées dans une zone de temps prédéfinie

Dans certains cas, il peut être utile d'appliquer des règles spécifiques pendant les heures de bureau, et d'appliquer ensuite d'autres critères. Vous pouvez également autoriser certains utilisateurs du web pendant la période de déjeuner, et limiter l'accès à certaines ressources pendant les heures de travail.



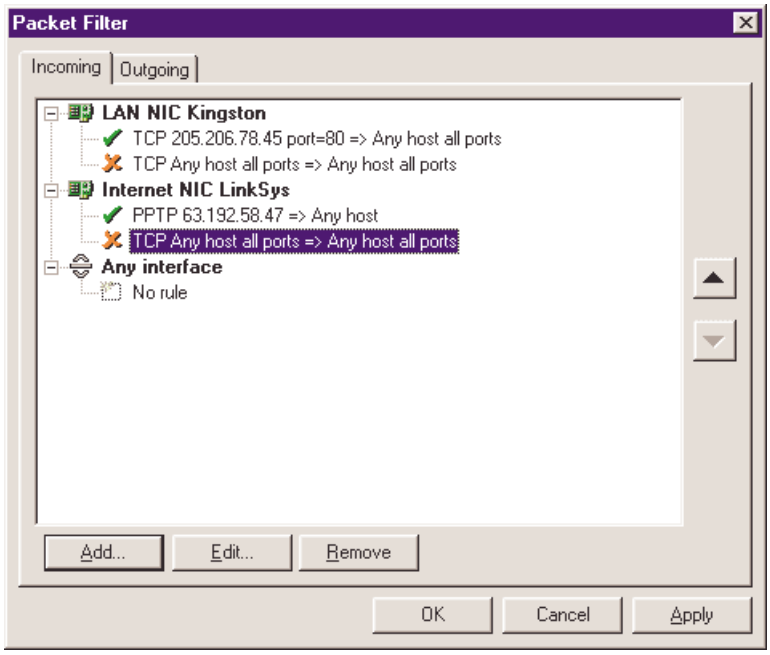
Exemple:

Contrôle total des accès utilisateurs: L'administrateur du réseau veut autoriser l'accès au réseau aux utilisateurs autorisés. En plus, un accès public au serveurs Web et FTP situés derrière WinRoute est nécessaire.

Dans ce cas, les règles sont entrées dans l'ordre suivant pour les paquets entrants:

1. autoriser les paquets provenant de n'importe quelle machine allant sur le port 80
2. autoriser les paquets provenant de n'importe quelle machine allant sur le port 21
3. rejeter tout les paquets

Si le paquet entrant est concerne par la règle 1 ou la règle 2, il pourra passer et la règle 3 ne sera pas appliquée. Si ce n'est pas le cas, alors la règle 3 s'applique et le paquet est rejeté.



CHAPITRE 4

Description de WinRoute

Dans ce chapitre

Sommaire des fonctionalités de WinRoute

WinRoute Pro est l'ultime **Routeur Internet - Firewall** qui vous permet, pratiquement sans effort, de partager une connexion Internet ! - Connectez vous a travers une connexion distante, une ligne DSL, un modem câble, une liaison spécialisée, LAN, T1, Radio ou une connexion DirecPC. C'est aussi facile que ca !

Administration distante

L'administrateur WinRoute fournit la configuration et les paramètres au Moteur WinRoute. L'administrateur WinRoute est une application séparée (wradmin.exe) qui peut être exécutée depuis n'importe quelle ordinateur avec une connexion sur le Moteur de la machine WinRoute. L'accès au Moteur WinRoute est sécurisé par un chiffrage puissant et un mot de passe.

Audit (logging)

WinRoute Pro fournit à l'administrateur du firewall un contrôle total sur le trafic traversant l'ordinateur exécutant WinRoute. Il est alors possible d'analyser et d'auditer les flux TCP, UDP, ICMP, ARP, les requêtes DNS, les informations du drivers et encore plus. Toutes les opérations ont une indication de temps.

Routeur IP avec Translation d'Adresse (NAT)

WinRoute inclus (la meilleure) implémentation de la technologie "Network Address Translation (NAT)" (qui signifie Translation d'Adresse) disponible a ce jour. Cela a été conçu pour fournir aux utilisateurs le meilleur en terme de routage et de protection réseau. Le driver NAT écrit exclusivement pour WinRoute offre, à un coût réduit, une sécurité comparable à celle des produits les plus chers.

Routage NAT Avance (Advanced NAT Routing)

Le routage NAT Avance permet de changer l'adresse IP source des paquets sortant suivant de nombreux critères. Cela permet une intégration facile de réseau(x) derrière WinRoute dans un environnement WAN. WinRoute permet la mise en place de plusieurs segments, de Réseaux Prives Virtuels (VPN), de Zone Démilitarisée (DMZ), etc.

Hébergement de Serveurs derrière WinRoute

Par défaut, WinRoute ferme tous les ports pour une sécurité maximum. Ainsi, tous les paquets non initialisés sont rejetés, à moins qu'un port mapping existe. La technologie Port Mapping permet aux utilisateurs de décider de comment ils veulent laisser passer les paquets IP à travers n'importe quelle interface gérée par WinRoute. Cela leur permet d'exécuter un serveur Web, Mail, FTP, VPN ou encore virtuellement tous les types de serveurs, derrière le firewall.

Sécurité Firewall

WinRoute fournit aux utilisateurs un niveau de sécurité firewall, comparable à celui de solutions beaucoup plus chères, à travers une combinaison de son architecture NAT et de sa capacité à opérer au plus bas niveau. Cela permet à WinRoute de capturer aussi bien les paquets entrants que les paquets sortants, ce qui le rend indétournable. L'Anti-spoofing est un module du filtre de paquet de WinRoute, pour une plus grande protection contre les attaques du réseau dans lesquelles les pirates falsifient leur adresse IP source.

Configuration Simple du Réseau (Simple Network Configuration)

Le serveur DHCP et le relayeur DNS (DNS forwarder), inclus dans WinRoute Pro, simplifient l'administration et la configuration du réseau. Les deux composants sont à la pointe de leur technologie et ainsi, le serveur DHCP de WinRoute remplace sans problème le serveur DHCP inclus dans Windows NT/2000 Serveur.

Serveur De Messagerie (Mail Server)

Le serveur de messagerie de WinRoute, complètement compatible avec les protocoles SMTP et POP3, permettent virtuellement une infinité de création d'alias et d'automatisation du tri de courrier. Les utilisateurs peuvent avoir une ou plusieures adresses email et peuvent réellement travailler en groupe (ex: ventes, support, relations clients, etc.) et chaque groupe peut désigner plusieurs utilisateurs. Toutes ces fonctionalités sont indépendantes du type de connexion à Internet dont vous disposez.

Cache HTTP

L'architecture de WinRoute inclue un moteur de cache tres innovant. A l'inverse des serveurs Proxy utilisant un système de cache, le cache WinRoute stocke les données dans un fichier d'un taille prédefinie au lieu d'utiliser un fichier pour chaque objet stocké. Cela permet de sauvegarder une place importante du disque dur, et spécialement sûr les environnements disposant d'un système de fichiers FAT16 (comme la plupart des systèmes utilisant Windows 95).

Routeur NAT

NAT -Translation d'Adresse

La Translation d'adresse, ou encore NAT, est l'une des fonctions de sécurité de WinRoute parmi les plus puissantes. La NAT est une technologies standard d'Internet permettant de "cacher" des adresses réseau privées derrière une ou plusieurs adresses publiques. Une version de la NAT appelée "IP Masquerading" à été très populaire pendant un grand nombre d'années dans la communauté Linux, et WinRoute et l'un des programmes peu nombreux tournant sous Windows et proposant une solution de NAT.

La NAT peut être implémentée de plusieurs manières, mais elle crée essentiellement un espace contenant un nombre pratiquement illimité d'adresses privées pour le réseau interne. Ces adresses sont "translatées" par WinRoute et ainsi, les communications peuvent "passer" vers et depuis le réseau public sans réveler les informations concernant le réseau privé. Il est donc impossible de produire une attaque directe contre une machine interne dont l'adresse IP est translatée par le firewall WinRoute.

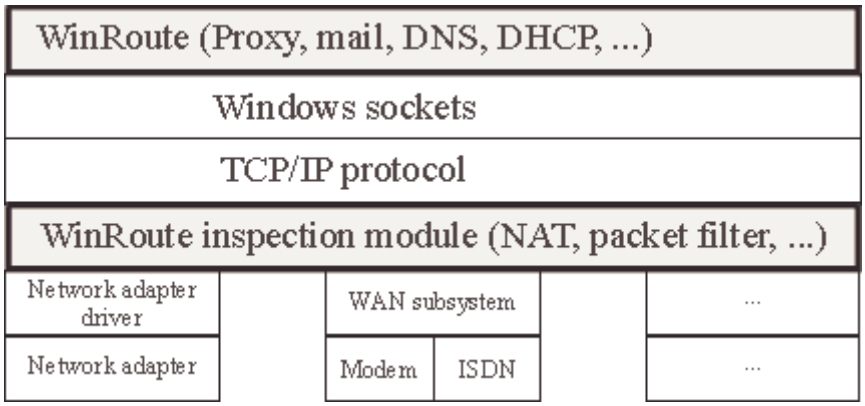
Architecture de WinRoute

Architecture de WinRoute

Pour réaliser des configurations de réseaux avances, il est important de bien comprendre comment WinRoute fonctionne. En considérant les explications et les exemples suivant, WinRoute prouve qu'il est une solution d'excellence pour pratiquement tous les types de configuration réseau.

1. **Sécurité Totale**
   WinRoute agit **en dessous de la pile TCP** au niveau IPSEC. En d'autres termes, il capture aussi bien les paquets **sortants** et **entrants AVANT** qu'ils aient une chance d'entrer dans l'ordinateur.

Cette conception avancée rend la sécurité de WinRoute pratiquement **incassable**



2. **Support Total des Protocoles**
   WinRoute est un ROUTEUR logiciel. En tant que tel, à l'inverse de serveur Proxy comme WinGate ou WinProxy, WinRoute peut transmettre pratiquement tous les types de protocoles Internet. En même temps, WinRoute vérifie chaque paquet en utilisant ses fonctionalites de firewall et de sécurité avancée. Sur les systèmes Windows 95 et 98, WinRoute se charge du routage des paquets. Sur les systèmes Windows NT, le systeme NT se charge du routage et WinRoute s'occupe des fonctionalités de NAT (entre autres).

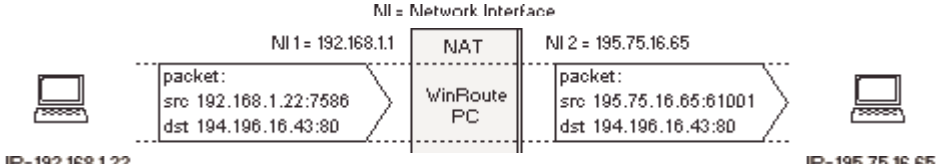
3. **Flexibilité Totale**
   WinRoute réalise la Translation d'Adresses (NAT - Network Address Translation) sur les interfaces de votre choix. WinRoute réalise également toutes les règles de sécurité prédéfinies par l'utilisateur sur les interfaces de son choix. Cela donne à l'utilisateur un grand champ d'action lors de la création et de la configuration des règles de sécurité.

Fonctionnement de la Translation d'Adresse (NAT)

La Translation d'adresse (NAT) est un procédé qui modifie les paquets envoyés depuis/vers le réseau local vers/depuis Internet ou d'autres réseaux bases sur le protocole IP.

En sortant ...
Les paquets passant à travers le moteur de translation **depuis le** LAN sont changés ou tranlatés pour sembler provenir de l'ordinateur se chargeant de la translation (cet ordinateur est directement relié à Internet). Ce qui se passe réellement, c'est que l'adresse IP "source" dans l'en-tête du paquet est remplacée par l'adresse IP (publique) de l'ordinateur se chargeant de la translation (ordinateur NAT).

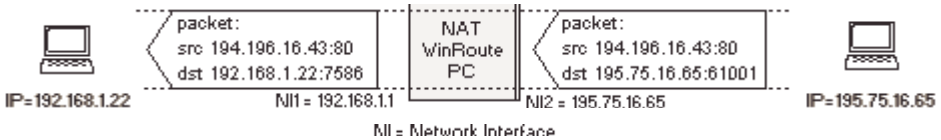
Le Moteur NAT gère également une table d'enregistrements des informations concernant chaque paquet en transit vers Internet.



En revenant ...

Les paquets passant à travers le moteur de translation **vers** le LAN sont recherchés dans la table de NAT gérée par le moteur de translation. C'est à cet endroit que l'adresse IP de destination est changée (suivant les informations stockées dans la table de NAT) pour redevenir l'adresse IP privée spécifique permettant d'atteindre l'ordinateur dans le réseau interne.

Souvenez vous que le paquet est revenu avec l'adresse IP publique de l'ordinateur NAT (en tant qu'adresse de destination dans son en-tête IP). Le Moteur NAT doit donc changer cette information pour que le paquet parvienne à son destinataire réel, situé dans le réseau local interne.



Configurer la NAT sur les deux interfaces

Vous pouvez vouloir utiliser WinRoute seulement comme un **routeur d'accès neutre** pour le trafic (paquets) provenant **d'Internet** vers un **réseau local**. Dans ce cas, vous avez déjà une solution de partage d'accès Internet; si cette solution ne vous permet pas d'exécuter dans votre réseau privé des serveurs et des applications qui doivent être accessibles depuis Internet, alors WinRoute peut être la bonne solution, s'il est configuré spécifiquement.

Voici des exemples de services qui peuvent avoir besoin d'être accessibles depuis Internet:

- serveur TELNET (ex: AS400)
- serveur WWW
- serveur MAIL
- serveur FTP
- PC Anywhere

- … et tous les autres serveurs (services) qui sont accessibles sur un certain port.

WinRoute fournira à vos utilisateurs/clients un accès fiable et sécurisé à ces différents services. La configuration de WinRoute pour ces services est décrite dans d'autres chapitres. Les paramètres suivants devront être configurés différement:

Fonction	Configuration normale	Dans ce cas
NAT sur l'interface Internet	ON	ON
NAT sur l'interface interne (LAN)	OFF	ON
Adresse IP de l'interface interne de WinRoute en tant que passerelle par défaut pour les ordinateurs du réseau	OUI (OBLIGATOIREMENT)	NON (pas nécessairement)

En d'autres termes, WinRoute permettra de rendre certains services accessibles depuis Internet SANS DEVOIR changer la configuration réseau.

Attention ! Activer la Translation d'Adresse (NAT) sur les deux interfaces ne vous PERMET PAS d'utiliser WinRoute pour partager votre connexion Internet !

Le paramètrage de la passerelle par défaut comme dans cette exemple vous laisse un grande liberté. Vous pouvez laisser inchangé tout votre environnement réseau existant. Tout en laissant les routeurs et les routes déjà établis dans votre réseau, et en ajoutant des ordinateurs exécutant WinRoute, vous pouvez permettre à des utilisateurs extérieurs d'accéder à des serveurs dans votre réseau local.

C'est une fonctionalité très puissante, lorsque vous avez un réseau étendu existant (WAN) et que vous voulez permettre à des utilisateurs extérieurs d'accéder a votre AS400 (serveur TELNET) ou à votre réseau interne via PPTP.

Pour faire cela, vous devez suivre les instructions suivantes:

1. Ajoutez un ordinateur possédant deux interfaces à votre réseau. Une Interface (externe) sera reliée à Internet alors que l'autre interface (interne) sera reliée à votre réseau existant.
2. Assignez à l'interface externe une adresse IP qui sera utilisée pour accéder à vos serveurs/services que vous voulez rendre accessibles depuis Internet.
3. Assignez une adresse IP manuellement ou dynamiquement (via serveur DHCP) à l'interface interne.
4. Configurez WinRoute pour réaliser la Translation d'Adresse (NAT) sur les deux interfaces.
5. Activez un Port Mapping pour chaque services que vous voulez activer sur votre réseau.

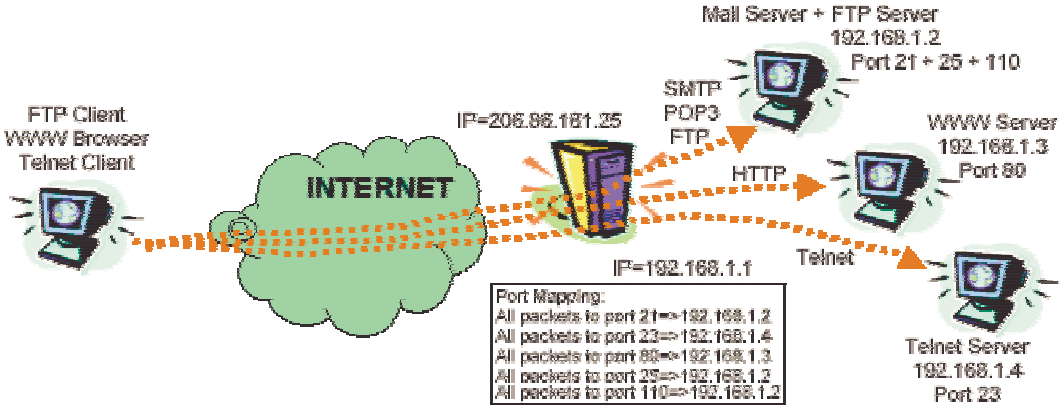
Après cette configuration, les utilisateurs externes pourront accéder, depuis Internet, à vos services internes s'exécutant sur les ports spécifiques. La sécurité de ces processus est garantie par le firewall de WinRoute.

Port Mapping - Transmission de Paquet

WinRoute fait de la Translation d'adresse (NAT), ce qui rend le réseau protégé inaccessible depuis l'extérieur. En utilisant le port mapping (ou Translation d'adresse de port - Port Address Translation - PAT) les services publics, comme les serveurs WEB ou FTP, peuvent être rendu accessibles depuis Internet.

Fonctionnement du Port Mapping

Chaque paquet arrivant du réseau extérieur (Internet) est comparé, suivant ses attributs (protocole, port de destination et adresse IP de destination), a une entrée de la table de port mapping (protocole, port d'écoute, adresse IP d'écoute). Si le paquet arrivant réponds aux critères désirés, le paquet est modifié et envoyé à l'adresse IP du réseau protégé définie en tant qu'adresse IP de destination (Destination IP) dans les entrées de la table et vers le port défini (Destination port).



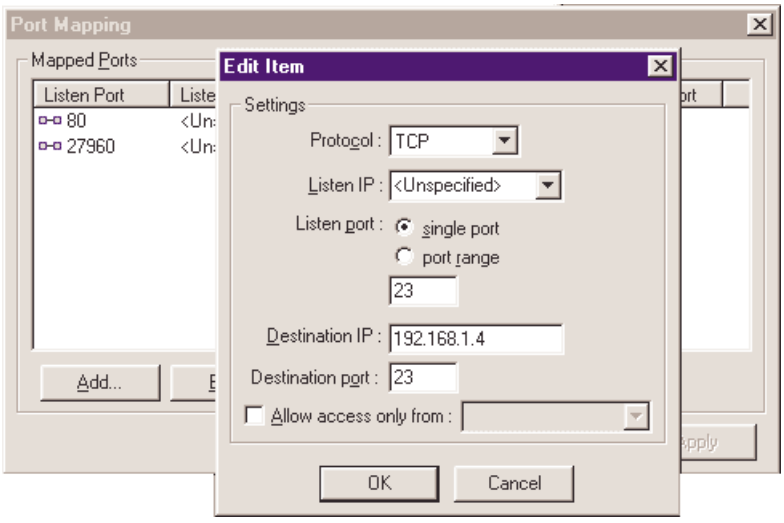
Par exemple, vous exécutez un serveur Web sur l'adresse interne 192.168.1.3 et vous voulez permettre à des utilisateurs extérieurs d'y accéder. Il y aura des requêtes arrivant depuis Internet sur l'adresse IP extérieure de votre ordinateur WinRoute (cette adresse IP correspond à l'entrée DNS correspondant à www.votre-domaine.com). Comme toutes les requêtes arrivant sur un serveur Web arrivent sur le port 80, vous allez configurer un port mapping qui indiquera que toutes les communications TCP sur le port 80 seront déviées vers l'adresse IP interne 192.168.1.3.

Configuration du Port Mapping

Pour configurer le Port Mapping

Aller dans le menu Settings->Advanced->Port mapping

6 Ajouter un nouveau port mapping (Bouton Add)



Protocole (Protocol)

Sélectionnez le protocole utilisé par le service ou l'application. Certains services (ou applications) utilisent TCP et UDP en même temps. Comme le module d'administration de WinRoute par exemple.

Adresse IP d'écoute (Listen IP)

C'est l'adresse IP où arrivent les paquets entrant. C'est normalement l'adresse IP associée à votre interface Internet. A noter: vous pouvez avoir plusieurs adresses IP associées a l'interface (si vous avez plusieurs serveurs Web par exemple).

Port d'écoute (Listen Port)

Le numéro du port sur lequel arrivent les paquets.

Adresse IP de destination (Destination IP)

L'adresse IP dans votre réseau local sur laquelle tourne le serveur (le service ou l'application) répondant aux paquets entrant (serveurs Web, serveur FTP, etc.).

Port de destination (Destination Port)

Le port sur lequel le service ou l'application écoute. C'est normalement le même numéro que celui du port d'écoute.

Autoriser seulement les accès depuis ... (Allow access only from)

Vous pouvez specifier des adresses IP depuis lesquelles vous souhaitez autoriser les accès. Cela est très important pour augmenter le niveau de securité dans le cas d'utilisation du port mapping vers des applications d'administration ou de management telles que l'administrateur WinRoute, PC Anywhere, etc. Vous pouvez spécifier une adresse seule ou un groupe d'adresses IP. Dans ce dernier cas, vous devrez préalablement créer un groupe d'adresse dans la fenêtre "Address Groups".

Port Mapping pour systèmes d'hébergement multiples (plusieurs adresses IP)

Il se peut que vous ayez plusieurs adresses IP assignées à votre interface Internet, et que vous ayez plusieurs serveurs (à l'intérieur de votre réseau) que vous voulez rendre accessibles depuis Internet.

Scénario comportant 5 serveurs Web

Considérons que vous vouliez faire tourner 5 serveurs Web correspondant chacun a un nom de domaine et une adresse IP différents.

Dans ce cas, vous aller assigner 5 adresses IP à votre interface externe (reliée à Internet) et installer les serveurs Web sur les ordinateurs dans votre réseau interne.

Chaque serveur Web peut s'exécuter sur un ordinateur différent, ou vous pouvez assigner plusieurs adresses IP sur un ordinateur de votre réseau local et exécuter tous les serveurs Web sur cet ordinateur.

Vous aller ensuite définir 5 port mappings dans la fenêtre Port Mapping. Pour chaque serveur Web (chaque domaine) il faudra définir:

- Une adresse IP d'écoute (adresse IP publique associée à votre domaine).
- Un port d'écoute: 80 dans ce scénario.
- Une adresse IP de destination: l'adresse IP interne du serveur Web correspondant.
- Un port de destination: 80 (pour le Web).

Pour plus d'exemples à propos de "Advanced Port Mapping", voir le chapitre des réseaux avancés.

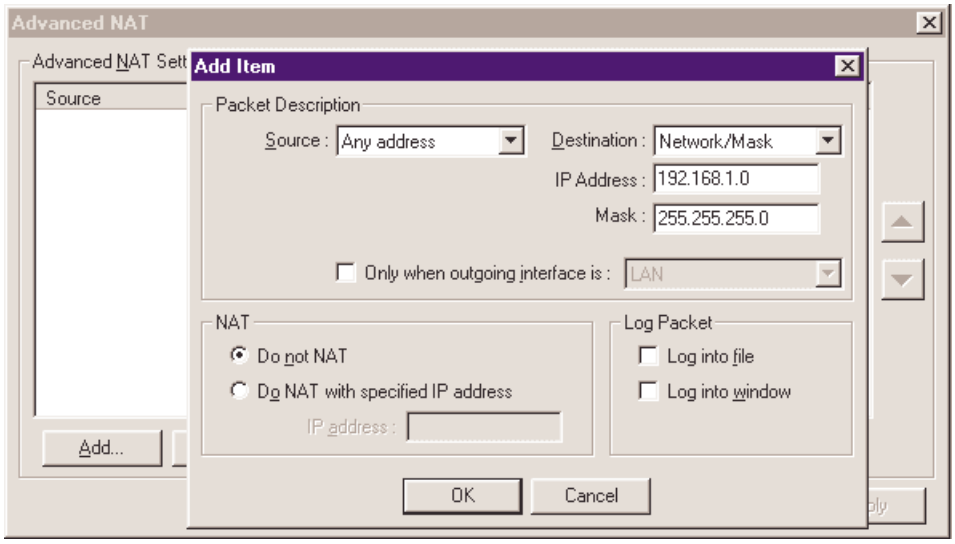
NAT Multiple

WinRoute permet la simple Translation d'adresse **(NAT)** (Network Address Translation) mais également des configurations bien plus évoluées. Vous pouvez spécifier, selon l'adresse IP **source** ou **destination** du paquet, que l'opération de NAT soit effectuée avec une **autre adresse IP** (c'est à dire que les paquets sembleront provenir d'une autre adresse IP) ou même spécifier que l'opération de **NAT** ne se fasse pas du tout.

De telles configurations sont d'une grande importance avec des réseaux plus compliques où:

- certains ordinateurs doivent apparaître comme une **autre** adresse IP que celle utilisée par le **reste** du réseau
- vous avez des bureaux extérieurs connectes via **WAN** avec un espace d'adresses privées, et que vous voulez partager **un** accès Internet à tout les bureaux
- vous avez plusieurs segments derrière WinRoute dont un (ou plus) segment est une zone DMZ avec des adresses IP publiques
- vous voulez avoir des adresses IP publiques à l'intérieur de votre réseau privé (Souvenez vous! Vous devez confirmer à votre Fournisseur d'accès que toutes ces adresses IP seront routées sur l'adresse IP principale)

Vous trouverez quelques exemples dans le chapitre des réseaux avancés.



Adresse IP Source, Adresse IP de Destination

Vous pouvez paramètrer la NAT avancée selon l'adresse IP depuis laquelle les paquets sont envoyés (source) ou vers laquelle ils sont envoyés (destination). Comme source vous pouvez entrer l'adresse IP d'une machine, un réseau entier (défini pour le masque de sous-réseau) ou un groupe d'adresses IP créé auparavant dans le menu Settings->Advanced->Address Groups.

Ne pas faire la Translation (Do not NAT)

Si cette option est sélectionnée, les paquets passant à travers l'interface Internet ne seront pas modifiés.

Faire la Translation (NAT) avec une adresse IP spécifique (Do NAT with specified IP address)

Si cette option est sélectionnée, les paquets seront modifiés pour sembler provenir de l'adresse IP spécifiée.

Table des Interfaces

La table des interfaces est une fenêtre dans laquelle WinRoute affiche toutes les interfaces disponibles dans l'ordinateur qu'il peut reconnaître. Si vous pensez disposer de plus d'interfaces que WinRoute n'en affiche, c'est que les drivers de ces interfaces ne sont pas correctement chargés par le système d'exploitation et que WinRoute ne peut pas les lire.

Vous pouvez voir:

Le nom de l'interface

Vous pouvez changer le nom en sélectionnant “properties” et en changeant le nom.

Adresse IP

La valeur entrée dans les propriétés TCP/IP de l'interface. Si l'interface est configurée pour obtenir une adresse IP depuis un serveur DHCP, vous verrez alors l'adresse IP actuelle assignée à cette interface.

NAT “On” ou “Off”

Si la Translation d'adresse (NAT) est activée sur l'interface, alors "On" est affiché dans la colonne.

Support VPN

Comme cela a été évoqué auparavant, WinRoute est totalement capable de faire passer le trafic des protocoles VPN les plus répandus: Le Protocole de Sécurité IP (IPSec) proposé par l'IETF, et le PPTP (Point-to-Point Tunneling protocol), rendu populaire ces dernières années par la percée des systèmes d'exploitation Microsoft Windows.

Serveur DHCP

Dans un réseau, chaque ordinateur doit avoir ses propriétés TCP/IP configurées correctement. Cela veut dire qu'il faut indiquer l'adresse IP, le masque réseau, la passerelle par défaut, l'adresse du serveur DNS, etc. sur chaque ordinateur. Si le responsable réseau doit effectuer ce parametrage sur un grand nombre d'ordinateurs, cela peut induire des erreurs (ex: double utilisation d'une même adresse IP) ce qui peut perturber le réseau tout entier.

DHCP (Dynamic Host Configuration Protocol) est implanté dans WinRoute pour simplifier l'administration du réseau. Ce protocole est utilisé pour configurer dynamiquement la pile TCP/IP des ordinateurs présents sur le réseau. Lors de leur démarrage, les ordinateur utilisant DHCP envoient une requête. Lorsque le serveur DHCP reçoit cette requête, il choisit les parametres TCP/IP pour le client et les lui transmet. Les parametres ainsi envoyés sont l'adresse IP, le masque de sous-réseau, la passerelle par défaut, l'adresse du serveur DNS, le nom de domaine du client, etc.

Le serveur peut assigner une configuration au client pour une période limitée (appelée la durée du bail). Le serveur assigne toujours les adresses IP de manière a ce qu'il n'y ait pas de collision entre les adresses IP des clients utilisant DHCP.

Lorsqu'un serveur DHCP est disponible, il suffit d'activer la fonction "Obtenir une adresse IP automatiquement" et le serveur prend alors en charge la bonne configuration du protocole TCP/IP sur les stations clientes. Cela permet de réduire considérablement la maintenance du réseau et les coûts de management.

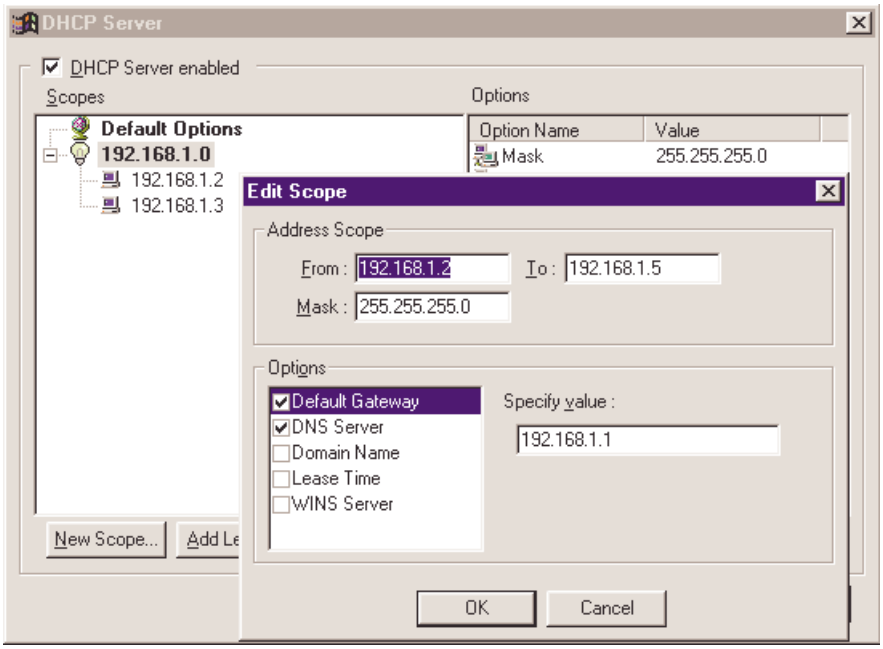
Si certains ordinateurs de votre réseau ne sont pas configurés dynamiquement par DHCP, mais ont une adresse IP fixe à la place, vous devez vous assurer que les adresses IP utilisées par le serveur DHCP ne rentrent pas en conflit avec des adresses fixes du réseau.

Configuration DHCP

Tout d'abord, vérifiez bien que les stations de travail sont configurées pour obtenir automatiquement une adresse IP depuis un serveur DHCP (voir les propriétés TCP/IP de chaque ordinateur) et que toutes les autres propriétés TCP/IP sont laissées vide, et ceci même pour les informations DNS.

Lancez alors le programme d'Administration de WinRoute:

1. Aller dans le menu Settings=>DHCP server.
2. Activez le service DHCP (cochez la case) et cliquez sur le bouton Add **New Scope**.
3. **Ajouter un intervalle (Add Scope)**
   Vous aller spécifier ici l'intervalle d'adresses IP utilisées par le serveur DHCP pour être transmises aux stations. N'oubliez pas que WinRoute utilise déjà une adresse qui ne doit pas être transmise aux stations. L'intervalle d'adresses IP doit être dans le même sous réseau. Voir l'exemple ci-dessous.
4. **Spécifiez des options (Specify Options) (ceci est important!)**
   Dans les options vous spécifiez quelles autres informations seront transmises aux stations de travail (ex: passerelle par défaut, serveur DNS, etc.). Cochez la case devant chaque composant dans la fenêtre et entrer les informations appropriées. Habituellement, on entre la passerelle par défaut et le serveur DNS (vous utiliserez normalement WinRoute comme serveur DNS) en indiquant l'adresse IP de WinRoute (ex: 192.168.1.1). Vous pouvez laisser les autres options vides.



A Noter: L'adresse IP de l'interface Ethernet (reliée au LAN) doit être assignée manuellement! La passerelle par défaut pour cette interface ne sera pas renseignée (laissez-la vide).

Firewall - Filtrage des Paquets

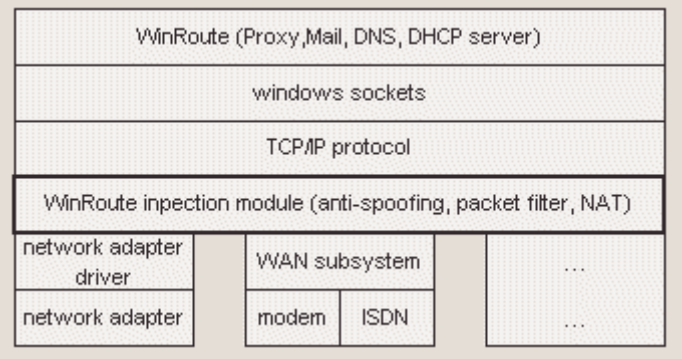
Le coeur de tout mécanismes de contrôle d'accès d'un firewall est, bien avidement, la technologie qu'il utilise pour permettre ou non la transmission des paquets destinés au réseau protégé. WinRoute implémente une des technologies les plus répandues pour le contrôle des accès réseau: le filtrage des paquets. Bien que WinRoute implémente d'autres mécanismes de contrôle d'acces, comme un Proxy de cache intégré pour les protocole HTTP, FTP et Gopher, cela est fait dans le but d'augmenter les performances et non la sécurité.

Le filtrage des paquets est une grande tradition dans la communauté de la sécurité réseau, et c'est une technologie bien implémentée dans des produits répandus comme le système d'exploitation IOS de CISCO. Lorsqu'ils sont bien configurés, les filtres de paquets peuvent être très sûrs, et particulièrement adaptés pour les sites Internet de gros volumes du fait de leurs grandes performances.

Architecture

Les Firewalls sont habituellement construits sur une base matérielle, mais une partie logicielle peut difficilement être évitée. Cependant, la faiblesse majeure dans la plupart des outils de sécurité réseau se manifeste pendant la courte période durant laquelle le matériel est capable de router le trafic et où le logiciel prend le contrôle des interfaces réseau. Pendant cette jonction, le sécurité peut être totalement compromise.

Le pilote de WinRoute, aussi appelé le Moteur de WinRoute, s'active au moment où les fichiers du noyau de Windows se chargent en mémoire; plus spécifiquement, le Moteur se charge avant les modules NDIS (Network Device Interface Specification), ce qui empêche toutes les communications réseau avant que WinRoute ne soit activé. Ainsi, la protection est activée sur toutes les interfaces avant que des attaques puissent être menées contre la machine protégée. Cela donne un grand avantage a WinRoute si on le compare ou programmes autonomes qui tournent en tant que service et qui ne sont pas activés avant que le système ait démarré.



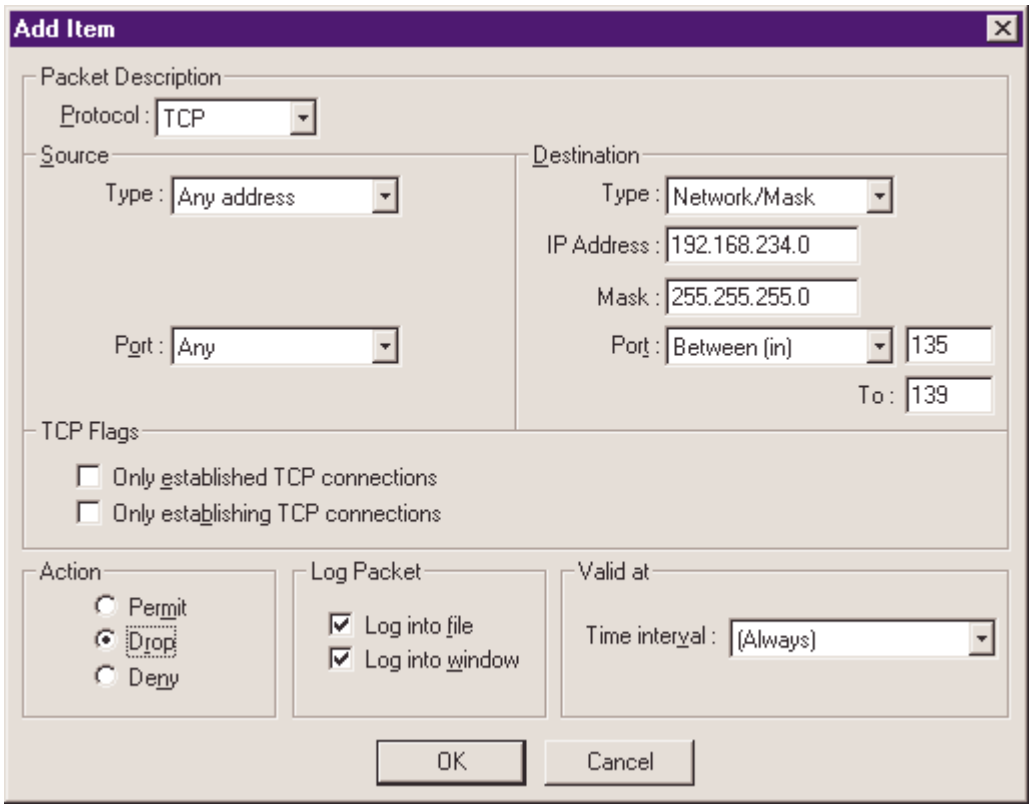
WinRoute "enveloppe" les drivers réseau en utilisant une technologie propriétaire pour que tout le trafic TCP/IP soit récupéré depuis le driver de la carte réseau par le Moteur avant qu'il soit transmis à la couche de communication du système d'exploitation.

Cette insertion du Moteur de WinRoute dans les couches basses de système d'exploitation permet à WinRoute d'avoir une perspective unique sur tout le trafic réseau d'une interface réseau quelconque (trafic entrant et trafic sortant). Comme de nombreux produits firewall pour Entreprise, comme Firewall-1 de Check Point, WinRoute peut prendre la première décision concernant un paquet. Encore une fois, cela prévient le système d'exploitation et les applications contre les attaques qui pourraient contourner la sécurité d'un firewall. Cela est préférable pour des passerelle Internet, mais cela peut également apporter une solution pour les machines indépendantes ayant de gros besoins en terme de sécurité ou d'anonymat, comme des systèmes de détection d'intrusion. Les programmes de détection d'intrusion comme Real Secure de la compagnie Internet Security Systems (ISS) seraient pratiquement invisibles sur une machine protégée par WinRoute.

Enfin, le Moteur de WinRoute prend à sa charge toutes les fonctionnalités de routage de Windows (que ce soit Windows 9x, NT, ou 2000). Cela permet de s'assurer que si, pour une raison ou une autre, le Moteur WinRoute devait tomber, aucun trafic réseau ne serait plus routé entre les différents réseaux. Cette fonctionnalité est utilisée par de nombreux firewall depuis de nombreuses années.

Règles

Despite theoretical issues surrounding packet filtering, the primary point of failure for modern firewall systems is misconfiguration, especially by inexperienced administrative staff. WinRoute makes configuration of filters simple and yet flexible enough so that even the novice network administrators can implement a secure configuration with a little knowledge of TCP/IP and a few mouse clicks, as illustrated in the following screen capture.



Filter rules may be applied on a per-interface basis to all of the following entities:

- a single IP address
- an administrator-defined list of IP addresses
- an entire network or subnet

It is also important to note here that filters can be set for both incoming and outgoing traffic.

These capabilities allow granular tailoring of access rules to the security needs of almost any organization. For example, a group of Web developers could be granted access to specific external resources such as anonymous FTP staging servers, or a specified list of internal addresses can be designated accessible to external partner networks for drop-off of electronic files. The inbound/outbound configuration allows protection from malicious "inside-out" attacks such as Back Orifice (BO) or distributed denial of service (DDOS) servlets that attempt to communicate over unreliable protocols back out through the firewall with external attackers.

Rules can either Permit, Drop, or Deny the specified traffic; the "Drop" action gives away the least information about the firewall to potential attackers, as it does not send an ICMP Administrative Prohobited Filter or a TCP Reset/Acknowledge response to a TCP SYN packet (the 1st step in the standard three-way TCP handshake sequence).

Rules may be prioritized to act in a specific, user-defined order upon incoming or outgoing packets. The most popular use of this capability is to add so-called "cleanup rules" to filter lists that block all traffic not specifically allowed by previous rules that have higher priority in the list (for an example of a clean-up rule, see the Sample Basic packet Filter Rule sets, later in this document).

Protocoles

Les protocoles supportés par le filtre de paquet de WinRoute sont:

- IP
- 7 types ICMP (ou tous)
- TCP
- UDP
- PPTP.

La capacité de laisser passer ou de bloquer des types ICMP inconnu, ou des protocoles IP inconnus, est inestimable pour les administrateurs réseau qui doivent faire face à une liste toujours grandissante de spécifications d'applications à gérer et à supporter. En particulier les relativement nouveaux protocoles VPN, comme IPSec, transitent sur les protocoles IP inconnus 51 et 52, ce qui est impossible a filtrer en utilisant des firewalls limités disponibles sur le marché qui sont incapables de filtrer autre chose que des protocoles basés sur TCP ou UDP.

Anti-Spoofing

En plus, WinRoute propose des fonctionnalités d'anti-spoofing, qui empechent des paquets avec des adresses IP source non valides de sortir. L'Anti-spoofing aurait pu eviter l'attaque smurf ICMP rapportée en Février 2000 et ayant causée des interruptions de service sur des sites Web majeurs comme ceux de Yahoo et Buy.com. Les utilisateurs de WinRoute peuvent etre rassurés de savoir qu'aucune attaque de ce type ne peut provenir de leur réseau s'ils ont activé cette fonctionnalité.

Exemple de règles de base pour le filtrage des paquets

Règles d'entrée (l'ordre est important)

Protocole	Source	Destination	Types ICMP	Action	Log	Desc
UDP	Any Address, Port = 53	Any Address, Port > 1023		Permit		Perm requ
TCP	Any Address, Any Ports	Any Address, Port > 1023		Permitestablished TCP		Perm paqu local
ICMP	Any Address	Any Address	Echo Reply	Permit		Cela ping ping
IP	Any Address	Any Address		Drop	To window	Règl tous non l

A Noter: Cette dernière règle interférera avec tous les outils de capture de paquet utilisés sur cette machine.

Exemple de règles de base pour les connexions entrantes HTTP et FTP

Protocol	Source	Destination	ICMP Types	Action	Log	Descript
TCP	Any Address, Any port	[this host], Port = 80		Permit	(optionnel)	Permet HTTP su
TCP	Any address, Any port	[this host], Port = 21		Permit	(optionnel)	Permet l le canal cet ordin
TCP	Any address, Any port	[this host], Port = 20		Permit	(optionnel)	Permet l le canal cet ordin le FTP a FTP a ouvrir to

Relayeur DNS

Chaque ordinateur connecté à Internet est identifié par une adresse IP numérique unique. Pour établir une connexion avec un ordinateur sur Internet, son adresse doit être connue de l'ordinateur qui établit la connexion. Comme les adresses IP sont difficiles à mémoriser, le Service de Nom de Domaine (DNS) a été créé.

Le DNS est une base de données de noms qui sont plus faciles à mémoriser. Ainsi, un utilisateur n'a pas à se souvenir ou à connaître l'adresse IP d'un serveur pour communiquer avec lui. Il suffit d'entrer le nom approprié (ex: www.yahoo.com) et DNS trouvera l'adresse IP actuelle de la machine.

Le raleyeur DNS de WinRoute

WinRoute est équipé d'un module DNS qui est capable de transférer les requêtes DNS vers un autre serveur DNS choisi sur Internet. Le module DNS stocke également les résultats des requêtes dans une mémoire cache, et ceci pendant un certain temps. Ainsi, les requêtes répétitives sont renseignées via la mémoire cache, sans avoir à attendre la réponse depuis Internet.

Le module DNS de WinRoute est capable de répondre aux requêtes selon des entrées stockées dans un fichier HOSTS défini par l'utilisateur. Lorsqu'une requête DNS arrive, WinRoute regarde en premier lieu dans le fichier HOSTS avant de transmettre la requête sur Internet. Si aucun enregistrement correspondant n'est trouvé dans ce fichier, alors la requête est transmise sur Internet.

Configuration du raleyeur DNS

Le raleyeur DNS est configuré via le menu: Settings => DNS raleyeur.

"Enable DNS forwarding"

Cette option détermine si le raleyeur est actif ou non.

"Forward DNS queries to the server automatically selected from the DNS servers known to operating system."

Si cette option est sélectionnée, les requêtes DNS sont transmises au serveur DNS indiqué par la configuration TCP/IP de l'interface Internet ou de l'accès réseau à distance.

"Enable lookup in HOST file"

Lorsque cette option est validée, le serveur DNS répond aux requêtes DNS en utilisant les entrées spécifiées dans le fichier HOSTS.

"Edit HOSTS file..."

Ce bouton démarre un programme externe qui permet d'editer le fichier HOSTS (vous devez vous trouver sur la machine WinRoute pour cela).

"DNS domain"

Entrer votre nom de domaine (ex: "acme.com") ici. Lors d'une réponse DNS, le nom de domaine est ajouté au nom d'hote recupéré dans le fichier HOSTS ou depuis la table de bail du service DHCP.

"Forward DNS queries to"

Entrer l'adresse du raleyuer DNS vers lequel vous souhaitez rediriger les requêtes DNS. Choisissez l'adresse du raleyuer DNS de votre Fournisseur d'acces ou d'un raleyuer DNS rapidement accessible depuis votre connexion.

"Enable DNS cache"

Cela permet aux requêtes DNS d'être stockées en mémoire cache. De cette manière, les requêtes récurrentes sont traitées plus rapidement sans devoir établir de connexion sur Internet.

"When resolving name from HOSTS file or leased table combine it with DNS domain"

Pour comprendre cette fonctionnalité, voyons l'exemple suivant - vous voulez résoudre le nom de l'ordinateur JOHN. Dans le fichier HOSTS vous avez entré que JOHN.OFFICE est associé à une adresse IP. Alors les requêtes pour JOHN et JOHN.OFFICE seront correctement traitées.

Notez que la mémoire cache ne stocke que les requêtes du type "Nom => adresse IP". Les réponses sont stockées jusqu'à ce qu'elles arrivent à expiration. Le temps d'expiration d'un nom est fixé par le raleyuer DNS pour chaque requête.

Comptes Utilisateurs

WinRoute - Comptes Utilisateurs

WinRoute peut être configuré avec plusieurs comptes utilisateurs qui peuvent être regroupés (configurés dans Settings | Accounts… | onglet Users). Les utilisateurs existant dans Windows NT/2000 peuvent être importés via l'onglet Advanced dans le menu Settings | Accounts.

Définition d'un utilisateur

En tant qu'utilisateur de WinRoute vous pouvez participer à l'administration, avoir une boite aux lettres électronique et participer aux règles de restriction d'accès du Proxy WinRoute.

Les utilisateurs peuvent créer des groupes et leur appliquer les privilèges ou restrictions mentionnés ci-dessus.

A Noter: Vous pouvez également configurer des restrictions d'accès au niveau du routeur en configurant le filtrage des paquets sur le firewall.

Ajouter un utilisateur

Pour ajouter un utilisateur:

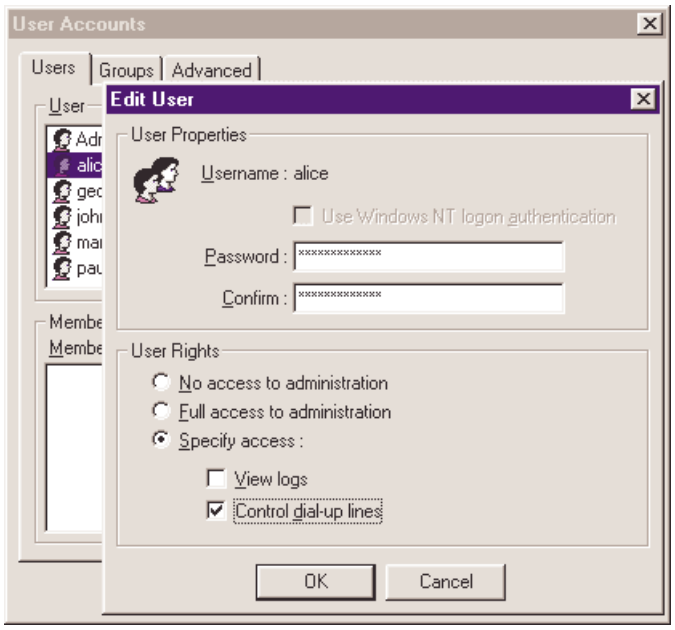
1. Allez dans le menu **Settings->Accounts**
2. Appuyez sur le bouton **Add**
3. Définissez un **nom d'utilisateur (user name)** et un **mot de passe (password)**
4. Assigner des **droits** à l'utilisateur:

   L'utilisateur n'a aucun droit pour administrer WinRoute.

   L'utilisateur a tous les droits pour administrer WinRoute

   - **View logs:** L'utilisateur a le droit de se connecter avec l'administrateur WinRoute pour voir les logs (les audits) dans la fenêtre réservée à cet effet. L'utilisateur n'a aucun droit pour changer les paramètres.

- **Control Dial-up lines:** L'utilisateur a le droit de se connecter avec l'administrateur WinRoute pour établir ou déconnecter une connexion Internet. L'utilisateur n'a aucun droit pour changer les paramètres.



Groupes d'utilisateurs

Dans WinRoute, vous pouvez classer les utilisateurs dans différents groupes. Un utilisateur peut être membre de plusieurs groupes simultanément.

Vous pouvez attribuer des **droits** aux différents groupes.

A Noter: les droits assignés à un groupe "surpassent" les droits assignés à un utilisateur.

Les membres d'un groupe peuvent avoir les **droits** suivants:

L'utilisateur n'a aucun droit d'administration WinRoute.

L'utilisateur a tous les droits d'administration.

- **View logs:** L'utilisateur a le droit de se connecter avec l'administrateur WinRoute pour voir les logs (les audits) dans la fenêtre réservée à cet effet. L'utilisateur n'a aucun droit pour changer les paramètres.
- **Control Dial-up lines:** L'utilisateur a le droit de se connecter avec l'administrateur WinRoute pour établir ou déconnecter une connexion Internet. L'utilisateur n'a aucun droit pour changer les paramètres.

Serveur de messagerie

Dans WinRoute est inclut un serveur de messagerie SMTP/POP3 complètement fonctionnel. Vous pouvez l'utiliser de la même manière que vous utilisez le serveur de messagerie de votre Fournisseur d'accès. Le serveur de messagerie de WinRoute vous permet d'envoyer des e-mails vers Internet ainsi qu'aux utilisateurs de votre réseau local (utilisateurs LAN). Il vous permet également de recevoir des e-mails et de les stocker dans les boites aux lettres des utilisateurs de WinRoute. WinRoute inclut également un planificateur qui vous permet de planifier vos échanges de courrier électronique.

Si vous n'utiliser pas le serveur de messagerie

Il n'est pas nécessaire d'utiliser le serveur de messagerie de WinRoute. Vous pouvez très bien conserver le serveur de messagerie de votre FAI ou d'un tiers. Dans ce cas, WinRoute sera votre routeur/firewall qui permettra à votre logiciel de messagerie de communiquer avec le serveur de courrier de votre Fournisseur d'accès.

A Noter! Ne paramétrer pas votre logiciel de messagerie pour qu'il utilise le Proxy! Vous devez utiliser la Translation d'adresse (NAT) de WinRoute pour accéder à Internet, et indiquer à votre logiciel de messagerie d'acceder directement à Internet. Si vous ne parvenez pas à récupérer vos messages, cela vient du fait que la Translation d'Adresse (NAT) n'est pas configurée correctement.

Utilisateurs de la Messagerie

Il y a quelques règles de base à propos des utilisateurs, des adresses e-mail et des boites aux lettres électroniques dans WinRoute.

Un utilisateur = une boite aux lettres

Chaque utilisateur de WinRoute a une **boite aux lettres** de créée. La boite aux lettres prend le nom de l'utilisateur. Au cas où vous auriez un nom de domaine enregistré sur Internet et configuré dans WinRoute l'adresse de l'utilisateur devient automatiquement utilisateur@nomdedomaine.com.

Un utilisateur = Plus d'adresses

Pour utiliser des adresses e-mail différentes et pour créer des adresses générales comme ventes@..., support@...., info@... vous devrez définir des alias. Le nombre de combinaisons possibles est virtuellement infini..

Pour ajouter des utilisateurs:

1. Aller dans le menu **Settings=>Accounts**
2. Ajouter des **Utilisateurs**
3. Grouper les utilisateurs dans des **Groupes** si nécessaire

Exemple:

Une compagnie a le domaine brutus.com. L'utilisateur John aura l'adresse john@brutus.com. Pour plus d'options d'adressage, voir les Alias.

A Noter: Les boites aux lettres sont stockées dans des répertoires différents. Typiquement dans C:\Program files\WinRoute\Mail. Les boites aux lettres sont physiquement créées APRES que le premier message soit arrivé.

Envoyer des e-mails aux autres utilisateurs de WinRoute sur votre réseau

Pour envoyer un message à d'autres utilisateurs **à l'intérieur** de votre LAN, utiliser le **nom d'utilisateur WinRoute** de votre correspondant à la place de son **adresse Internet** complète.

Exemple: Le nom d'utilisateur de votre correspondant est John et son adresse e-mail Internet est john@compagnie.com. Vous pouvez entrer john dans le champ To: de votre message.

Configuration avec Alias

Si vous utilisez **l'adresse email complète** d'un utilisateur local, le message partira sur Internet vers le serveur SMTP de relais et retournera ensuite vers WinRoute. Pour éviter cela, vous pouvez spécifier des alias.

N'oubliez pas! Vous devez spécifier le PC WinRoute en tant que votre serveur de courrier sortant (SMTP).

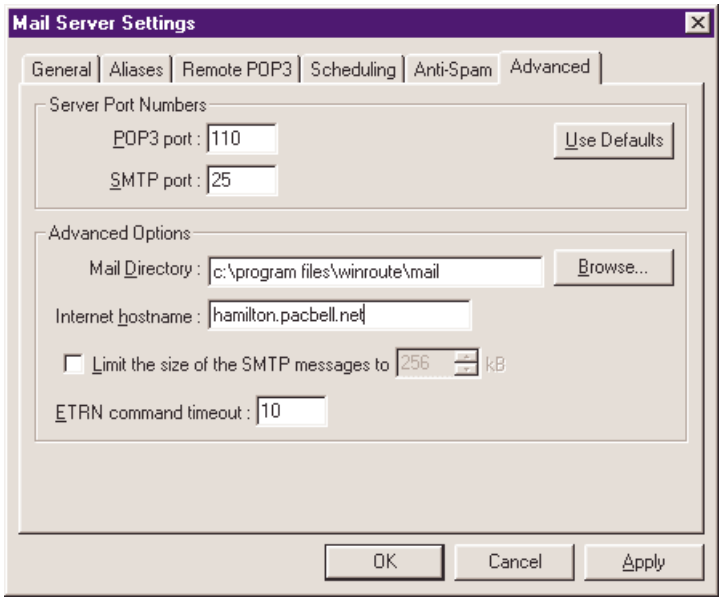
Authentification

Authentification

Certains Fournisseurs d'accès demandent une authentification pour les messages sortants pour éviter le spamming. Pour faire cela avec WinRoute:

1. Aller dans la fenêtre Mail Server->onglet Advanced

2. Entrer **le nom d'hote** désiré dans le champ Internet host name (mail.isp.com)



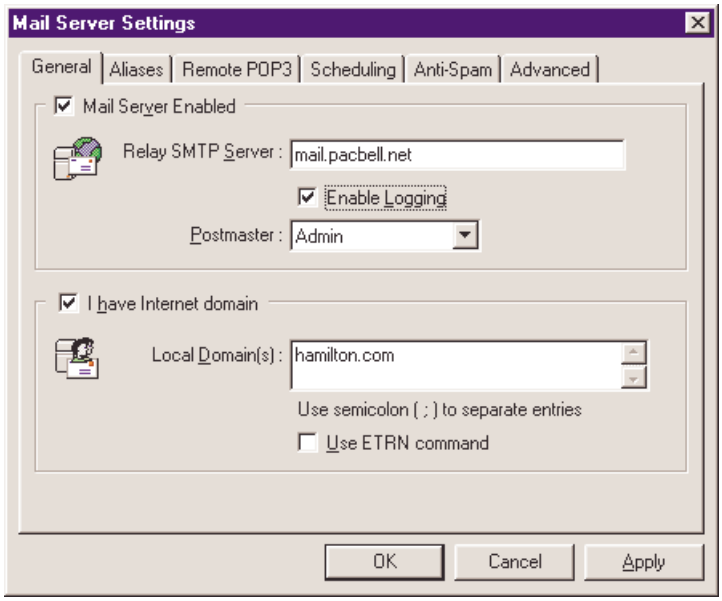
Envoyer des Emails sur Internet

Vous pouvez utiliser WinRoute en tant que **serveur SMTP** pour le courrier sortant. WinRoute utilise un **serveur SMTP relais** (le serveur SMTP de votre Fournisseur d'accès) pour envoyer vos messages, au lieu d'utiliser les MX records. En d'autres termes - tous les messages sortant seront envoyés à travers le serveur que vous avez specifié. Vos logiciels de messagerie utiliseront WinRoute en tant que serveur de courrier sortant (serveur SMTP).

Pour configurer le serveur SMTP de relais pour le courrier sortant:

Aller dans le menu Settings=>Mail Server

Entrer le nom du serveur de courrier sortant (SMTP) de votre Fournisseur d'Accès dans le champ Relay SMTP Server

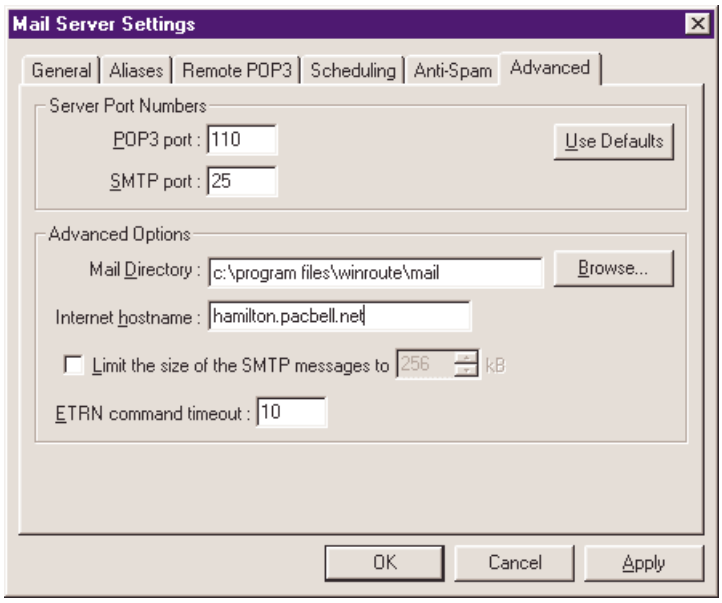


Authentification

Certains Fournisseurs d'accès demandent une authentification pour les messages sortants pour éviter le spamming. Pour faire cela avec WinRoute:

1. Aller dans la fenêtre Mail Server->onglet Advanced

2. Entrer **le nom d'hote** désiré dans le champ Internet host name (mail.isp.com)



Recevoir du courrier

Vous avez un nom de domaine

Le serveur de messagerie de WinRoute est totalement compatible avec les protocoles ***SMTP***[1] et ***POP3***[2]. Vous avez peut être enregistré votre propre **nom de domaine Internet** et recevez peut être du courrier via SMTP. WinRoute peut récupérer automatiquement vos e-mails sur le compte POP3 de votre Fournisseur d'Accès.

---

[1] Le protocole **SMTP** (Simple Mail Transfer Protocol) est utilisé pour les communications directes entre les serveurs de messagerie (comme le serveur de messagerie de WinRoute et le serveur de messagerie de votre FAI) et pour envoyer des messages depuis votre logiciel client de courrier électronique. SMTP est un protocole unidirectionnel - c'est à dire que votre message peut être envoyé via ce protocole, mais ne peut être récupéré. Vous devez utilisé les protocole POP3 pour cela.

SMTP est un protocole basé sur TCP et travaillant sur le **port 25**. Si vous voulez placer un serveur SMTP derrière une machine WinRoute, vous devez faire un port mapping sur le port TCP 25 et le diriger vers l'adresse privée de votre serveur SMTP à l'intérieur de votre réseau privé.

[2] Le protocole **POP3** est principalement utilisé par les logiciels clients de messagerie pour récupérer les messages contenues dans des boites aux lettres électroniques compatibles POP3. Le serveur de messagerie de WinRoute à cette fonctionalité. Il peut, par exemple, récupérer les messages contenus dans plusieurs boites aux lettres chez votre FAI, et les distribuer localement dans les boites aux lettres des utilisateurs WinRoute.

POP3 est un protocole basé sur le protocole **TCP** et utilisant le **port 110**. Si vous voulez accéder à un serveur de messagerie POP3 situé derrière une machine WinRoute exécutant le module de NAT, vous devez créer un **Port Mapping** pour le protocole TCP sur le port 110 et l'envoyer vers l'adresse **privée** de la machine exécutant le serveur de messagerie.

Si vous avez un nom de domaine enregistré sur une adresse IP externe (publique), WinRoute peut recevoir le courrier directement via le protocole SMTP. Dans l'onglet "general" dans le fenêtre de configuration du serveur de messagerie de WinRoute, entrez le nom de domaine que vous avez enregistré.

N'oubliez pas de configurer un port mapping sur le port 25 vers l'adresse IP privée de votre PC WinRoute! Sinon, le protocole SMTP ne sera pas autorisé à passer la Translation d'Adresse de WinRoute (NAT)!

Suivant votre type de connexion Internet, veuillez considérer les points suivant:

1 Vous avez une connexion Internet permanente

Aucun paramètre spécifique n'est requis. Entrez juste le(s) nom(s) de domaine.

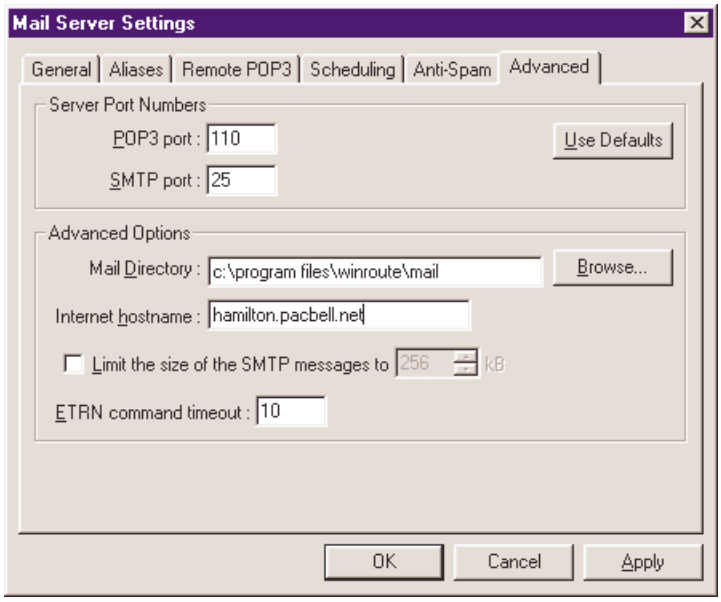
2 Vous avez une connexion modem ou Numeris (commande ETRN)

Dans le cas d'une connexion Internet non permanente, votre Email est stocké temporairement chez votre Fournisseur d'Accès. Cet Email est transféré lorsque vous êtes connecté. Certains Fournisseurs d'Accès demandent l'utilisation d'une commande **ETRN**[3] *pour demander les messages. Le serveur de messagerie de WinRoute supporte la commande ETRN. Vous pouvez cocher cette option dans l'onglet General dans le fenêtre de configuration du* ***Serveur de Messagerie.***

[3] ETRN est une commande utilisée par les serveurs SMTP pour récupérer du courrier SMTP.

La commande ETRN est utilisée lorsqu'un serveur SMTP n'est pas en ligne 24h/24 et que les emails envoyés sur ce serveur doivent être stockés temporairement sur un autre serveur SMTP. La commande permet ainsi de récupérer les messages sur le serveur temporaire.

Si besoin est, vous pouvez spécifier un temps d'attente maximale pour ETRN (aller dans l'onglet Advanced).



Temps d'attente maximale pour ETRN (time out)

Cette entrée indique la période, après l'établissement d'une connexion, pendant laquelle le serveur SMTP de WinRoute doit essayer de faire une requête pour le courrier SMTP.

Domaines multiples

Domaines multiples

Vous pouvez disposer de plusieurs domaines assignés sur votre connexion Internet. Si c'est le cas, entrez tous vos noms de domaine dans l'onglet Settings=>Mail Server=>General et séparez les par des points virgules.

Configuration avec plusieurs domaines

Il y a deux manières pour configurer plusieurs domaines sur votre réseau:

1 Chaque domaine dispose de sa propre adresse IP

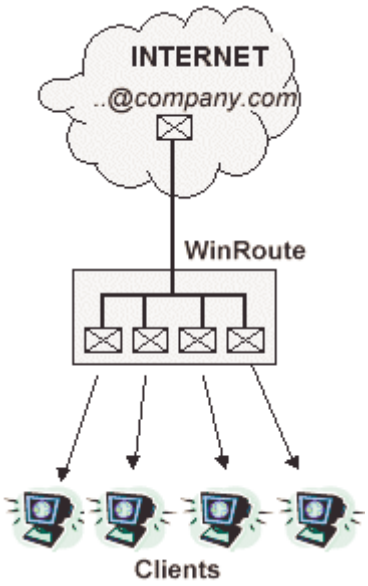
Dans ce cas, vous devez avoir plusieurs adresse IP publiques configurées sur votre interface Internet. Il faut alors faire plusieurs ports mapping, un pour chaque adresse, avec la même adresse de destination: celle de l'interface interne du PC WinRoute.

2 Tous les domaines sont associés à une même adresse IP

Il n'y a pas de configuration spécifique autre que la mise en place d'un port mapping sur le port 25 vers l'adresse IP interne de la machine WinRoute.

Vous avez un domaine assigné à un compte POP3

Vous pouvez faire en sorte, avec le concours de votre Fournisseur d'Accès, que tous les emails de votre domaine arrivent dans un seul compte. WinRoute peut alors vérifier ce compte via POP3, récupérer les messages et les redistribuer dans les différentes boites aux lettres locales des utilisateurs.

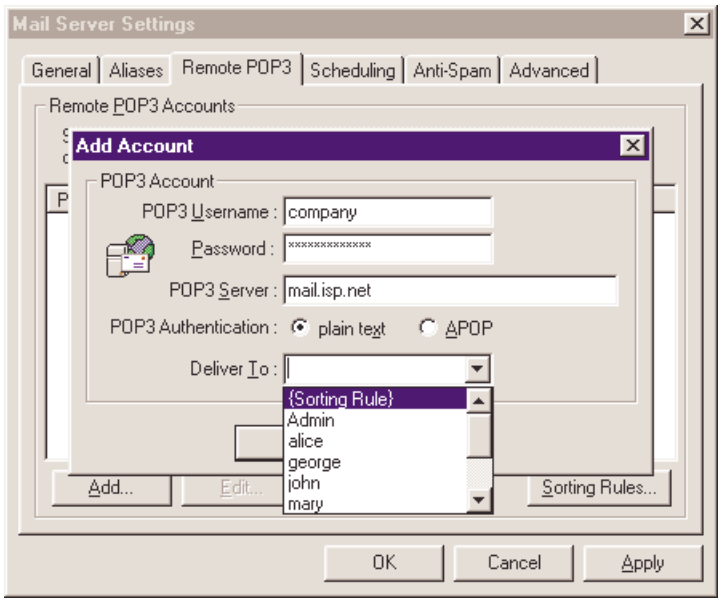


Exemple

Votre Fournisseur d'Accès a configuré la boite aux lettres compagnie@mail.isp.net. Vous avez le domaine compagnie.com, mais tous les messages pour ce domaine (ex: john@compagnie.com, support@compagnie.com, etc.) arrivent dans la boite compagnie@mail.isp.net chez votre FAI.

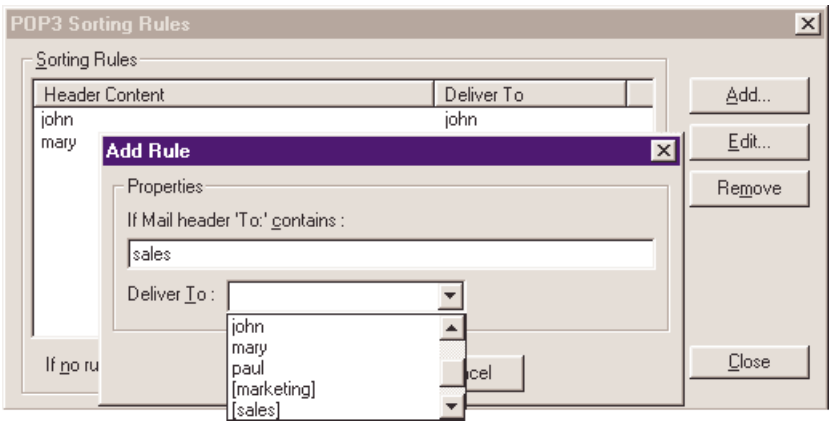
Allez dans le menu Settings=>Mail Server=>Remote POP3, ajoutez un nouveau compte et entrez ses détails.

3 Dans le champ "Deliver to:" sélectionnez "Sorting Rules"



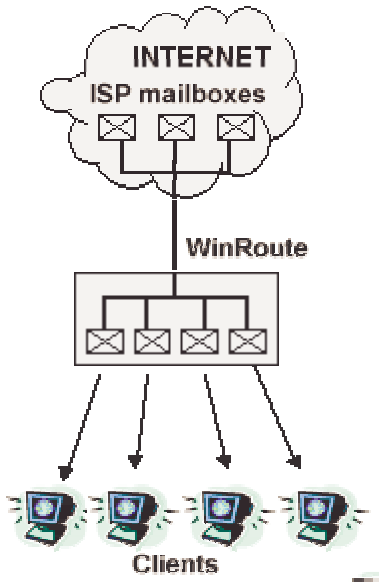
4 Appuyer sur le bouton [Sorting Rules] et ajouter un nouveau critère. WinRoute délivrera le message suivant l'adresse email du destinataire ou de l'expéditeur ou enfin suivant le sujet du message.

5 Dans la même fenêtre, sélectionnez un utilisateur ou un groupe d'utilisateurs à qui le message doit être transmis.


POP3 Sorting Rules
Sorting Rules
Header Content
Deliver To
john
john
mary
Add...
Edit...
Remove
Close
Add Rule
Properties
If Mail header 'To:' contains :
sales
Deliver To :
john
mary
paul
[marketing]
[sales]

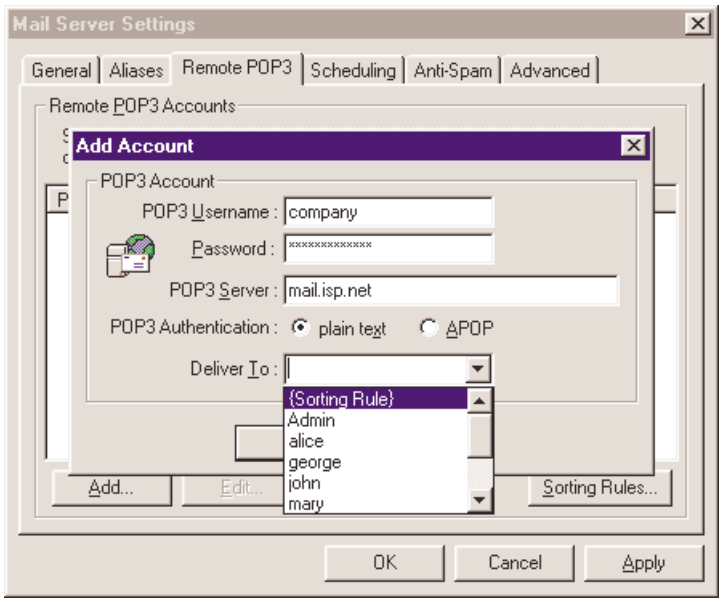
Recevoir des emails - Vous avez plusieurs comptes chez le Fournisseur d'Accès

WinRoute peut vérifier plusieurs comptes email chez votre FAI et délivrer automatiquement les messages s'y trouvant dans des boites aux lettres locales.



Allez dans le menu Settings=>Mail Server=>Remote POP3, ajoutez un nouveau compte et entrez ses détails.

6 Dans le champ "Deliver to:" sélectionnez les destinataire ou le groupe de destinataires.


Mail Server Settings
General
Aliases
Remote POP3
Scheduling
Anti-Spam
Advanced
Remote POP3 Accounts
Add Account
POP3 Account
POP3 Username :
company
Password :
POP3 Server :
mail.isp.net
POP3 Authentication :
plain text
APOP
Deliver To :
{Sorting Rule}
Admin
alice
george
john
mary
Add...
Edit...
Sorting Rules...
OK
Cancel
Apply

Configuration du logiciel de messagerie

Utiliser le Serveur de Messagerie de WinRoute

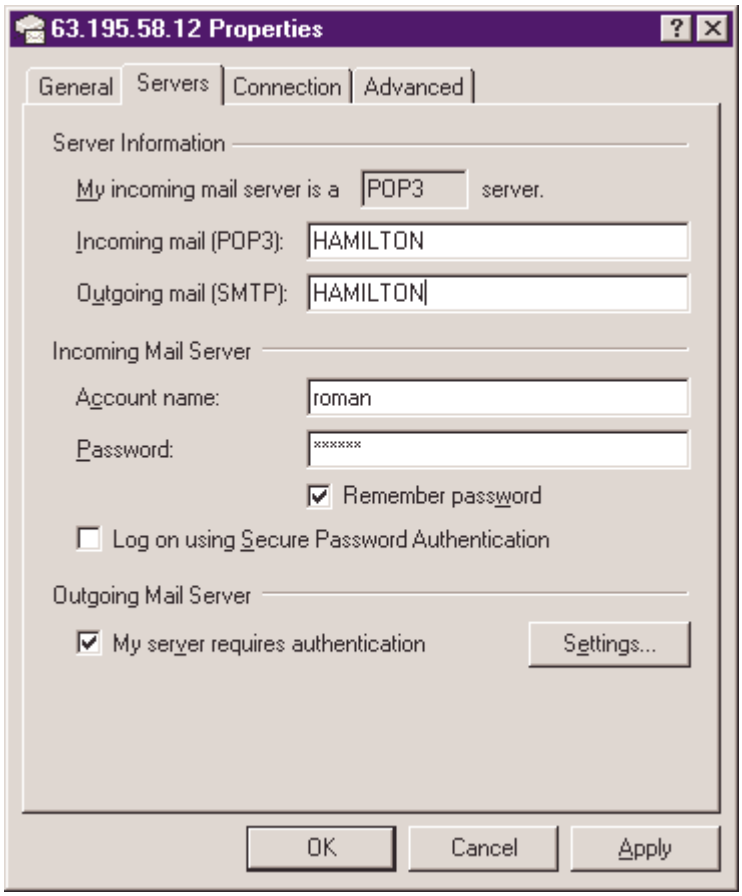
Email à travers le Serveur de Messagerie de WinRoute

Pour que vous utilisiez bien le serveur de messagerie de WinRoute, vous devez configurer votre **logiciel de messagerie**. L'ordinateur WinRoute sera le serveur de Messagerie **Entrant** et **Sortant**. Pour cela, vous devez entrer le nom (ou l'adresse IP) de l'ordinateur WinRoute dans les champs appropriés dans votre logiciel de messagerie. Si vous rencontrez des problèmes pour envoyer ou recevoir des emails, mieux vos alors entrer l'adresse IP à la place du nom de l'ordinateur, avant de chercher plus loin. Il peut en effet y avoir des problèmes de résolution DNS dans votre réseau local et vous n'utilisez peut être pas le serveur DNS de WinRoute.

Exemple:

Le serveur de Messagerie WinRoute tourne sur un ordinateur ayant une adresse IP attribuée dynamiquement et une adresse IP privée 192.168.1.1. Le nom de l'ordinateur est Hamilton (voir les parametres réseau dans le panneau de configuration).

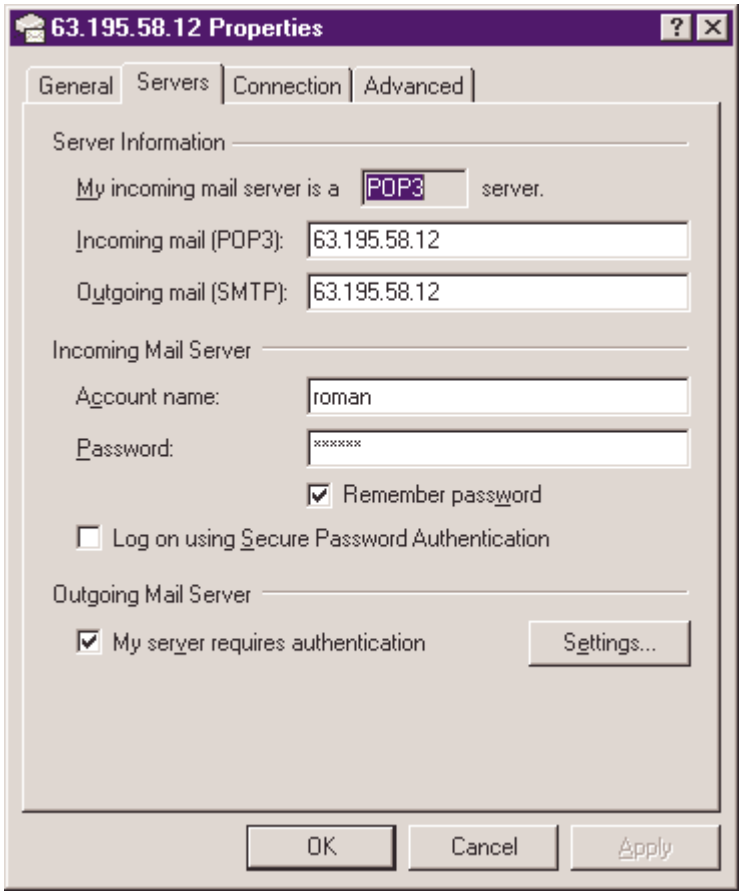
Vous pouvez aussi bien entrer HAMILTON ou 192.168.1.1 dans les champs pour les serveurs POP3 et SMTP de votre logiciel de Messagerie.


63.195.58.12 Properties
General
Servers
Connection
Advanced
Server Information
My incoming mail server is a
POP3
server.
Incoming mail (POP3):
HAMILTON
Outgoing mail (SMTP):
HAMILTON
Incoming Mail Server
Account name:
roman
Password:
******
Remember password
Log on using Secure Password Authentication
Outgoing Mail Server
My server requires authentication
Settings...
OK
Cancel
Apply

Ne pas utiliser le Serveur de Messagerie de WinRoute

Il se peut que vous vouliez ne pas utiliser le serveur de messagerie de WinRoute, et que vous vouliez recevoir et envoyer vos messages directement via le serveur de messagerie de votre FAI.

Dans ce cas, veuillez renseigner les champs pour le serveur sortant et le serveur entrant avec le nom du serveur de messagerie de votre Fournisseur d'Accès (FAI).



A Noter! Ne parametrez pas votre logiciel de messagerie pour qu'il utilise le Proxy! Vous devez utiliser la Translation d'Adresse (NAT) de WinRoute pour accéder à Internet et permettre à votre logiciel de messagerie d'accéder directement à Internet et au serveur de messagerie de votre FAI. Si vous ne parvenez pas à établir une connexion pour échanger vos messages, cela veut dire que la NAT est mal configurée.

Alias

Les **Alias** dans WinRoute sont utilisés pour **ajouter** des adresses aux utilisateurs de WinRoute ou pour **substituer** l'adresse email.

Grace aux **Alias** vous pouvez:

- assigner plusieurs adresses à un utilisateur
- assigner une adresse à plusieurs utilisateurs
- assigner une adresse à un groupe d'utilisateurs
- assigner plusieurs adresses à un groupe

Exemple:

Cet exemple montre que les possibilités sont pratiquement infinies.

La compagnie a 2 domaines:

- compagnie.com
- scociete.fr

L'utilisateur John doit recevoir des emails pour:

john_speaker@compagnie.com

john@societe.fr

ventes@compagnie.com

support@compagnie.com

Les Emails pour ventes@compagnie.com doivent aussi etre delivrés au groupe [Ventes].

Solution:

1. Aller dans le menu Settings=>Mail server=>onglet Aliases.

2. Ajouter les alias suivant:

john vers John -*

cela delivrera tous les emails provenant d'Internet dans lesquels il y a john comme destinataire. Par exemple, john_presentation@compagnie.com ainsi que john@compagnie2.com sera delivrés à l'utilisateur John. Cela permettra aussi d'éviter que les messages envoyés depuis le reseau local à john@compagnie.com passe par Internet. Le message ira en effet directement dans la boite aux lettres WinRoute de l'utilisateur.

ventes vers John -

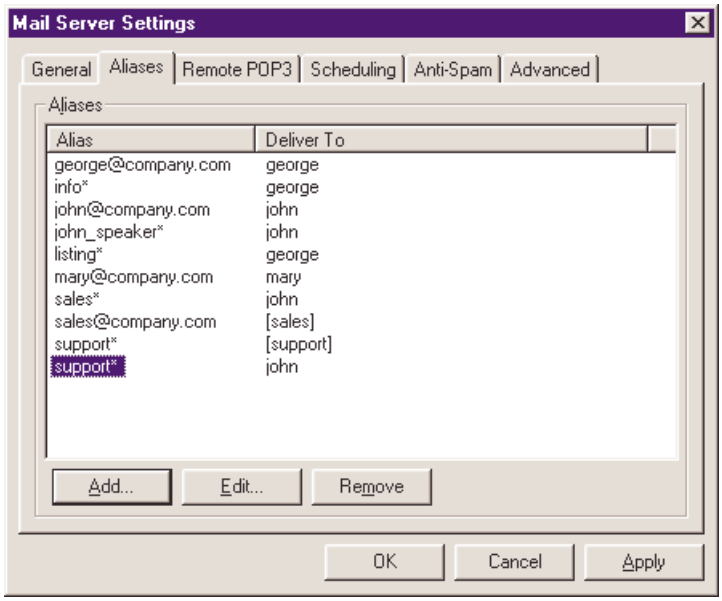
cela delivrera tous les emails pour ventes@…….. à l'utilisateur John

Support vers John -

cela delivrera tous les emails pour support@…… à John

Ventes vers [Ventes] -

cela delivrera tous les emails pour ventes@…. à tous les membres du groupe [Ventes]



Planification des échanges de courrier électronique

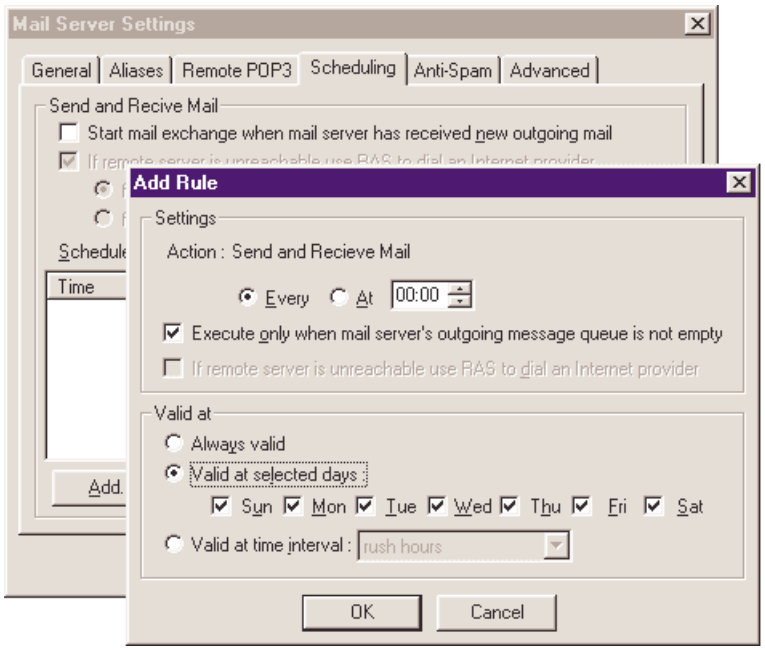
Le planificateur dans les paramètres du serveur de messagerie vous permet de régler ces options:

- les intervalles réguliers pour vérifier les emails chez votre FAI (que ce soit via POP3 ou SMTP par ETRN)
- règles pour envoyer le courrier sortant

les intervalles de temps pendant lesquels les règles sont valides. Vous pouvez pré-définir ces intervalles de temps dans le menu Settings->Advanced->Time intervals

Vous pouvez choisir entre envoyer les nouveaux emails dès qu'ils arrivent, et les envoyer à des périodes pré-définies.

Vous pouvez également choisir si le serveur doit appeler dans le cas de nouveaux emails. Si vous sélectionnez cette option, le serveur de messagerie de WinRoute établira une connexion à chaque fois que les utilisateurs enverront de nouveaux messages.



Pour recevoir des emails, vous pouvez configurer le calendrier en lui indiquant exactement à quel moment vous voulez récupérer votre courrier. Vous pouvez combiner plusieurs règles pour rendre votre planification de récupération du courrier aussi efficace que possible.

Aller dans le menu Settings->Mail Server->Scheduling

7 Spécifiez les options de votre choix et ajouter de nouvelles règles pour vérifier les emails.

A Noter! les règles "d'intervalles de temps" doivent être configurées dans le menu Settings->Advanced->Time Intervals

Serveur Proxy

L'objectif premier d'un serveur proxy est de **sauver** la **bande passante** de votre connexion Internet. Si les utilisateurs accèdent à Internet à travers un serveur Proxy, ce dernier peut **stocker** les objets des différentes requêtes (comme les pages HTML, les images, et les autres types de fichiers) dans sa mémoire **cache**.

Si les pages ou les images sont demandées une nouvelle fois par le même utilisateur ou quelqu'un d'autre, le serveur proxy répondra à l'utilisateur en utilisant l'objet stocké dans sa mémoire cache. Cela **réduit** la charge de la connexion Internet et les opérations sont beaucoup plus rapides.

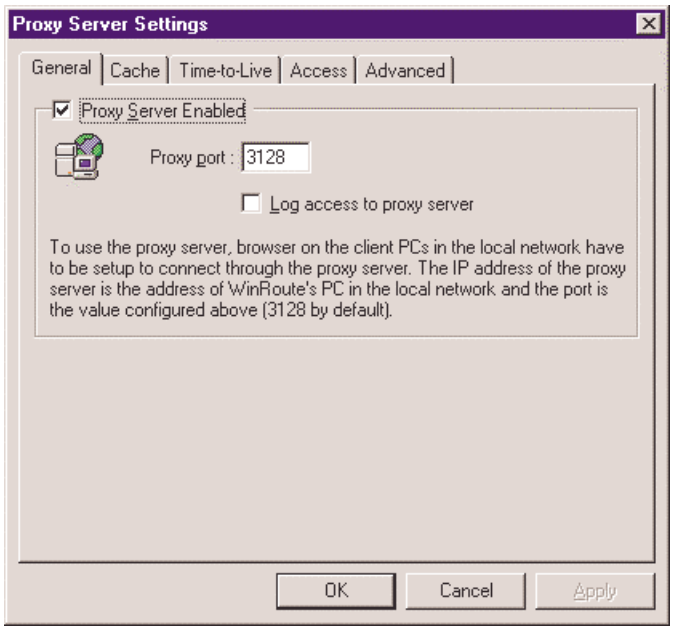
Cependant, les objets stockés dans la mémoire cache peuvent être périmés. Vous devez alors régler la valeur **TTL** (Time-To-Live) d'un document pour éviter d'avoir les nouvelles du jour précédent si vous êtes sur le site de CNN news - par exemple.

Configuration rapide

Avant tout - avec WinRoute vous **n'avez pas besoin** du Serveur Proxy pour accéder à Internet. Votre connexion Internet est assurée par un **routeur NAT** inclus dans WinRoute. La Translation d'Adresse est largement meilleure que la technologie Proxy pour le partage d'un accès Internet. Néanmoins, WinRoute inclus également un serveur Proxy pour vous permettre de bénéficier des fonctionalités de mise en mémoire cache.

Pour utiliser le serveur Proxy de WinRoute, suivez les étapes suivantes:

Dans l'outil d'Administration de WinRoute, sélectionnez l'onglet Settings -> Proxy Settings -> General. Cochez la case "Proxy Server Enabled". Laisser le numéro de port à 3128.



8 Dans votre navigateur Internet (Explorer, Netscape Navigator, Opera...), allez dans les paramètres proxy, et choisissez une configuration manuelle du proxy et entrez l'adresse de l'ordinateur WinRoute comme serveur proxy pour les protocoles HTTP, FTP, et Gopher. Entrez 3128 comme port de serveur proxy pour tous les protocoles mentionnés précédemment.

9 Testez cette configuration en accédant à une page Web sur Internet en utilisant votre navigateur Web.

Onglet General Properties

Proxy Server Enabled

Utilisez cela pour activer ou désactiver le Serveur Proxy.

Port number

C'est le numéro de port sur lequel le Serveur Proxy écoutera les requêtes. Habituellement, il n'y a pas de raison de changer la valeur par défaut, 3128.

Log access to proxy server

En activant cette option, toutes les URL demandées au proxy seront enregistrées dans un fichier de log.

Serveur Proxy - Contrôle des accès utilisateurs

Le serveur Proxy de WinRoute permet aux administrateurs de contrôler les accès aux pages Web. L'administrateur peut décider que les accès à certaines pages ou certains domaines seront seulement permis à certains utilisateurs et/ou groupes d'utilisateurs.

Forcer les utilisateurs à utiliser le serveur Proxy

Si vous décidez d'utiliser le contrôle du serveur Proxy, vous devrez également bloquer les accès directs aux pages Web, pour que seul les accès via le proxy ne soient possibles. Pour bloquer les accès directs, il faut définir des règles dans le ***Filtrage des paquets*** (see "Forcer les utilisateurs à utiliser le Serveur Proxy" on page 145) (voir la section correspondante dans le manuel WinRoute).

Configuration du contrôle d'accès du serveur Proxy

Pour configurer le contrôle d'accès du Proxy de WinRoute, allez dans l'onglet "Access" dans les paramètres du Serveur Proxy.

Access List

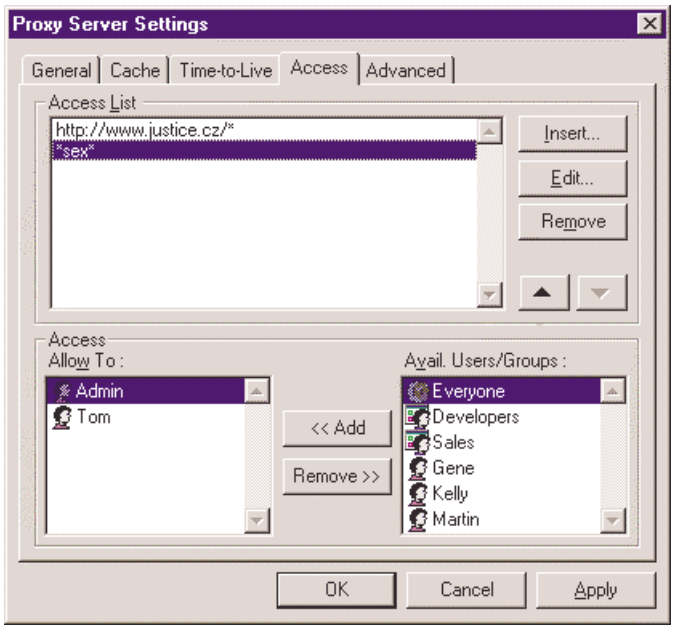
La liste des URL à accès restreint. Vous pouvez utiliser l'étoile comme caractère de remplacement pour n'importe quelle chaîne de caractère. Par exemple, pour indiquer tous les ordinateurs d'un domaine.com, utilisez la chaîne "*.domaine.com". WinRoute 4.0 utilise également des sous-chaîne pour vérifier une URL. Par exemple "sexe" identifie les mêmes URL que la chaîne "*sexe*".

Allow To

La liste des utilisateurs et/ou groupes d'utilisateurs qui ont accès à une URL particulière.

Avail. Users/Groups

La liste des utilisateurs et de groupes définis dans WinRoute.



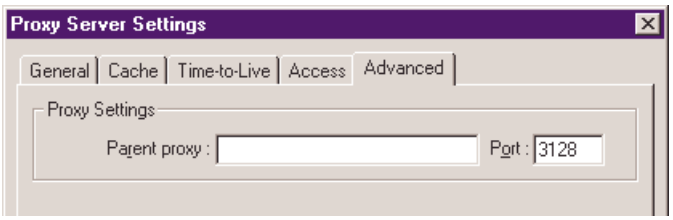
Si un utilisateur essaye d'accéder à une page Web qui est dans la catégorie des pages à accès restreint, l'utilisateur se verra demander une authentification par son navigateur Web. WinRoute vérifiera alors le nom d'utilisateur ainsi que le mot de passe pour déterminer si l'utilisateur peut accéder à la page en question.

Le navigateur garde le nom d'utilisateur et le mot de passe en mémoire. Toutes les requêtes suivantes seront alors automatiquement transmises avec le nom et le mot de passe de l'utilisateur. Ce qui fait que l'utilisateur n'a pas à s'authentifier encore et encore, à chaque requête.

Cependant, les utilisateurs doivent bien comprendre qu'une fois authentifié sur leur navigateur, ils ne doivent pas laisser l'ordinateur sans surveillance avant que le navigateur soit déchargé de la mémoire.

Propriétés avancées

Dans l'onglet "Advanced" des paramètres du Serveur Proxy, vous pouvez indiquer à WinRoute d'utiliser un serveur Proxy parent.



Parfois, vous pouvez avoir accès à un serveur Proxy disposant d'une **mémoire cache considérable** et/ou une **connexion Internet ultra rapide**. Si votre connectivité sur ce serveur est bonne, vous pouvez utiliser ce serveur en tant que serveur Proxy parent.

Pour cela, il suffit d'indiquer à WinRoute de transférer toutes les requêtes vers ce serveur Parent. Entrez simplement le nom du serveur Proxy parent et son numéro de port dans les champs correspondant dans l'onglet "**Advanced**".

A propos de la mémoire cache

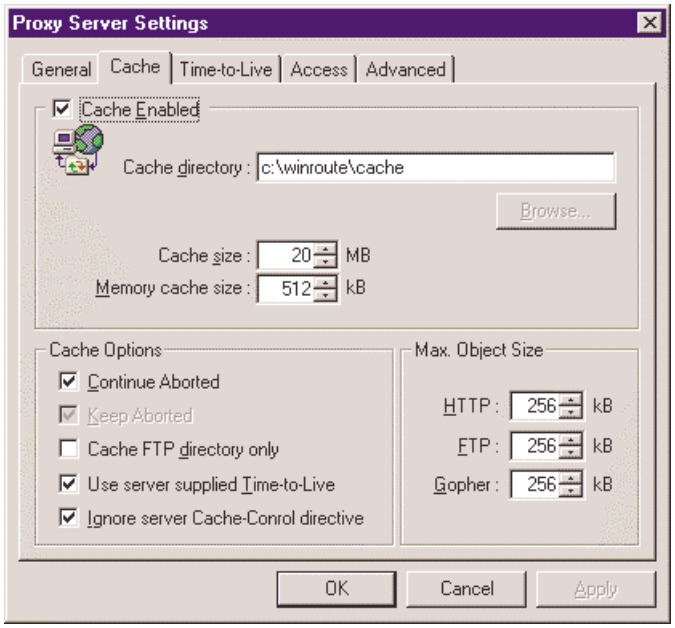
Le serveur Proxy de WinRoute utilise un moyen **très économique** pour stocker les donnés. Tous les objets mis en cache sont stockés dans **un seul fichier d'une taille fixe**. Cela à l'inverse de nombreux serveurs Proxy qui stockent chaque objet dans un fichier séparé.

Si le disque utilise une taille d'allocation importante (comme FAT16), cette méthode gaspille un espace disque très important, parce que les contenus Web son composés de nombreux fichiers de petites tailles. Habituellement, 50% de ces objets sont plus petits que 6 kilo octets, alors que la taille d'allocation sur les gros disques est de 32 KB (avec le système de fichier FAT).

Le fait que la mémoire cache de WinRoute stocke les donnés dans un seul fichier, sauve un grand pourcentage d'espace disque. Cela veut dire que vous aurez besoin de moins d'espace disque ou que vous utiliserez le même espace plus efficacement.

Le fichier de taille fixe permet également à WinRoute d'utiliser des techniques d'indexation qui rendent la mémoire cache de WinRoute très rapide.

Paramètres de la mémoire cache



Cache Enabled

Active ou désactive la mémoire cache. Si cette option est désactivée, toutes les requêtes sont envoyées, à chaque fois, sur Internet.

Cache Directory

Le répertoire contenant la mémoire cache.

Cache size

L'espace disque utilisé par le mémoire cache du Proxy. Lorsque vous devez choisir la taille de la mémoire cache, il faut considérer le nombre de vos utilisateurs, le trafic qu'ils génèrent, etc. Si vous avez beaucoup d'espace disque, vous pouvez configurer un grand fichier de cache. La taille maximum est de 3072 mega octets (3 GO).

Continue Aborted

Si cette option est activée, le serveur Proxy finira toujours de télécharger un objet depuis Internet, même si le navigateur ayant généré la requête arrête le téléchargement (lorsque l'utilisateur appuie sur le bouton stop). Ainsi les autres requêtes pour ce même objets bénéficieront de la fonction de mise en mémoire cache et seront donc plus rapides.

Keep Aborted

Cette option indique au serveur Proxy de WinRoute de mettre en mémoire cache les fichiers incomplets (pages web, images). Cela permet un gain de temps partiel lors d'une prochaine requête de l'objet ainsi mis en mémoire cache. Si "Continue Aborted" est activé, cette option est ignorée.

Cache FTP directory only

Lorsque vous naviguer dans un serveur FTP, utilisez cette option pour seulement mettre en mémoire cache la liste des répertoires. Si vous voulez aussi mettre en mémoire cache les fichiers téléchargés sur les serveurs FTP, désactivez cette option. La décision à prendre concernant la mise en cache ou non d'un fichier dépend aussi de sa taille. Voir l'option "Max. Object Size" ci-dessous.

Use server supplied Time-to-Live

Le "Time-to-Live" ou "Temps-de-vie" est la période pendant laquelle un objet sera considéré comme valide. Après, la page web sera considérée comme obsolète et son contenu sera téléchargé de nouveau sur le serveur web. Cette option indique donc au serveur Proxy de WinRoute d'obéïr au Time-to-Live (TTL) fournit par le serveur web de chaque page web. Si une page n'a pas de TTL, le TTL par défaut du serveur Proxy est utilisé.

Ignore server Cache-Control directive

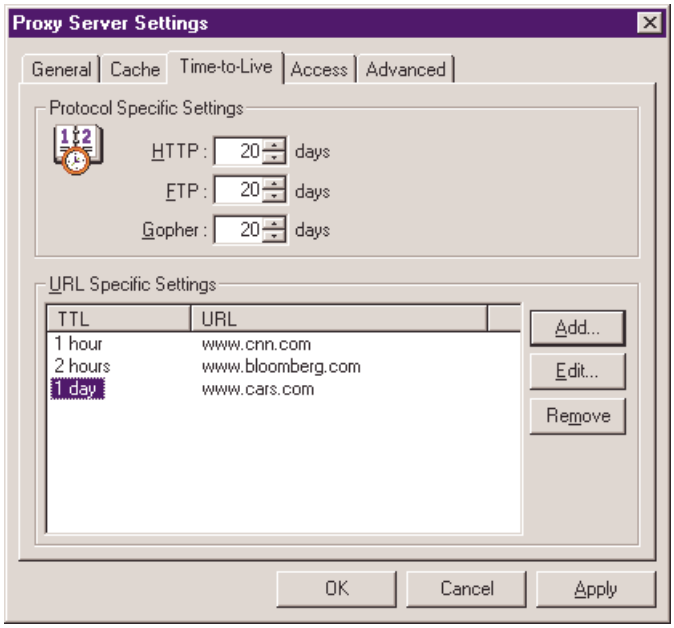
Si le contenu d'une page Web change très souvent, l'auteur de cette page peut décider de mettre une direction de "non-cache" pour celle-ci. C'est une fonction très utile, mais certains sites utilisent mal, car trop souvent, cette option. Cela perturbe alors l'efficacité des serveur Proxy. Vous pouvez alors ignorer ces directives de "non-cache" en activant cette option.

Max. Object Size

La taille maximum des objets mis en mémoire cache. Les objets plus gros seront passés au navigateur, mais ne sont pas mis en mémoire cache. En général, vous n'avez pas besoin de mettre en cache les gros fichiers (comme les fichiers archives), car vous ne les téléchargez pas régulièrement.

Temps de vie (TTL)

Vous pouvez définir des valeurs par défaut pour les Temps-De-Vie (TTL) utilisés si une page web n'a pas de TTL défini ou si vous voulez ne pas utiliser son TTL (voir l'option "Use server supplied Time-to-Live" dans l'onglet Cache).



Paramètres spécifiques aux protocoles

Vous pouvez définir ici les TTL par défaut pour les protocoles HTTP, FTP, et Gopher.

Paramètres spécifiques aux URL

Si vous avez besoin de définir des TTL individuels pour quelques domaines, serveurs web ou pages web individuelle, ajouter ici des valeurs de TTL pour les URL spécifiques. Vous pouvez spécifier le TTL en jours et/ou heures.

Vous pouvez utiliser le caractère étoile (*) dans les URL. Vous pouvez également mettre une sous chaîne et faire que, par exemple, toutes les URL contenant "ftp" dans leur nom soit considérées si vous indiquez "ftp" comme sous chaîne. C'est une nouvelle fonctionalité de WinRoute 4. il fallait avant entrer "*ftp*" pour couvrir ce cas).

Il est à noter que si vous avez activé l'option "Use server supplied Time-to-Live" dans l'onglet Cache, le TTL fourni par le serveur est prioritaire sur le TTL indiqué dans "URL Specific Settings".

Comment forcer les utilisateurs à utiliser le Proxy et non la NAT?

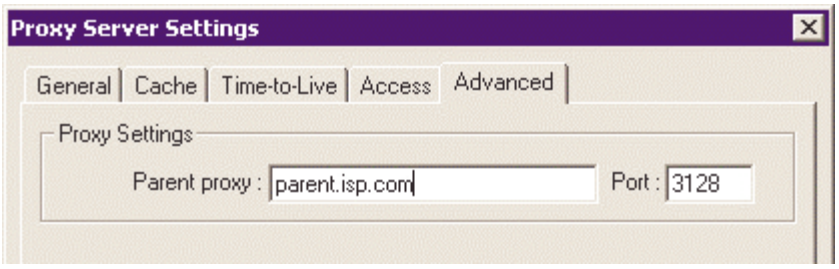
Bien que la **Translation d'Adresse (NAT)** donne d'excellents résultats, il se peut que vous ayez besoin de forcer les utilisateurs à utiliser le **Serveur Proxy** pour leurs accès au **World Wide Web**. Habituellement, c'est lorsque vous avez une connexion à 56K partagée pour toute la compagnie que l'utilisation de la mémoire cache devient très utile. C'est également une bonne solution si vous voulez mettre en place une solution de **contrôle d'accès utilisateur** basé sur un **filtre URL**.

Pour utiliser le Proxy pour accéder au Web, vous devez configurer tous les navigateurs pour qu'ils utilisent le serveur proxy sur le port **3128**. Vous pouvez changer le port si nécessaire. Les utilisateurs pourront cependant contourner le proxy et accédant directement à Internet à travers la NAT. Pour éviter cela, il est nécessaire de configurer le Firewall. Aller voir le chapitre correspondant dans le manuel: ***Configuration du Firewall*** (see "Forcer les utilisateurs à utiliser le Serveur Proxy" on page 145).

Utiliser un Serveur Proxy parent

Serveur Proxy Parent

Dans certains cas, vous aurez besoin de connecter le serveur Proxy de WinRoute à un serveur proxy de "plus haut niveau", également appelé ***proxy parent****. Aller dans le menu Settings / Proxy Server, choisissez l'onglet Advanced et entrez l'adresse IP (ou le nom) du serveur proxy parent ainsi que son numéro de port d'écoute.*



Nom d'utilisateur et mot de passe du Serveur Proxy parent

Le serveur proxy parent peut demander un authentification pour accéder à certains (ou tous) sites web, comme WinRoute le fait (voir le chapitre traitant du contrôle des accès Proxy, pour plus de détails). WinRoute Pro 4.2 inclut une telle fonctionalité depuis la build 22.

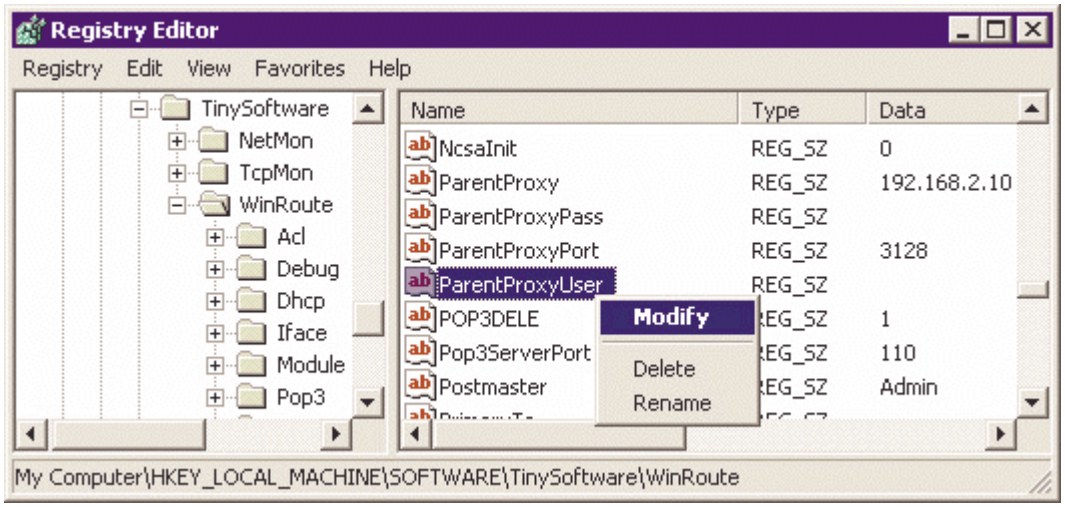
Pour configurer l'authentification:

- Arrêter le Moteur WinRoute (depuis les Services Windows ou en utilisant le Moniteur WinRoute)
- Lancer l'éditeur de registre Windows (regedit.exe)

Trouver la clé HKEY_LOCAL_MACHINE\Software\Kerio\WinRoute

- Trouver les entrées **ParentProxyUser** et **ParentProxyPass** et changer leur valeur en indiquant les nom d'utilisateur et mot de passe nécessaires.
- Fermer l'éditeur de registre et démarrer le Moteur WinRoute.

Après cette procédure, le serveur proxy de WinRoute s'authentifiera lui même auprès du serveur proxy parent.



Analyse des audits (log) et des paquets

Une fonction cruciale d'un outil de sécurité est la possibilité d'enregistrer avec précision tous les événements à tous moments. WinRoute enregistre six types d'audits différents en rapport avec le firewall, les paquets passant à travers, l'activité des utilisateurs, actions des différents filtres, etc. Une description de chaque audit est indiquée dans la table suivante:

HTTP Log	Montre les requêtes HTTP passant à travers le serveur Proxy de WinRoute; on y trouve les adresses IP source et les noms d'utilisateurs, les date et heure, et les requêtes HTTP.
Mail Log	Enregistre toutes les opérations du serveur de messagerie intégré dans WinRoute. On y trouve les activités entrantes et sortantes (POP3 et SMTP).
Security Log	Montre toutes les activités définies par "Log to window/file" dans les règles du filtre de paquets (voir plus loin pour la description des éléments enregistrés).
Dial Log	Enregistre les informations d'activité des lignes d'accès distants gérées par WinRoute.
Debug Log	Configuration "à la carte" de la visualisation des paquets ARP, ICMP, UDP, TCP, et/ou DNS qui transitent physiquement sur une des interfaces du routeur WinRoute; configuration précise dans Settings | Advanced | Debug Info, onglet Debug.
Error Log	Affiche toutes les opérations ayant généré une erreur dans l'un des modules de WinRoute.

Les audits peuvent s'afficher dans l'administrateur WinRoute ou être écrits dans un fichier (ou les deux). Les fichiers d'audits sont stockés dans le répertoire \%installroot%\Logs, qui est accessible des seuls comptes Administrateurs, Opérateurs, SYSTEME, et le créateur propriétaire ayant installé WinRoute.

Les informations d'audits de sécurité de WinRoute sont robustes et inclues toutes les informations nécessaires pour pouvoir mener une investigation en cas de problème de securité:

- Date
- Heure
- Règle du Filtre de Paquets concernée
- Interface
- Action (Permit: Autoriser, Drop: Ignorer, Deny: Refuser)
- Protocole
- Adresse IP Source et port TCP
- Adresse IP Destination et port TCP

Les tests d'audits avec des très gros trafics n'affectent pas les capacité d'audit de WinRoute. Ceci est très important pour éviter des pertes en cas de tentatives d'attaques ayant pour but d'interrompre le service du firewall en surchargeant sa capacité d'audit.

Audit de debug (Debug log)

L'audit de debug ou Debug log est l'audit le plus important dans WinRoute. Il vous permet de voir **tous les paquets IP** (TCP, UDP, ICMP, ARP, DNS) qui transittent physiquement sur n'importe quelle interface presente dans l'ordinateur WinRoute.

Dans la fenetre **Debug Events** vous pouvez voir les configurations d'evenements que vous voulez afficher.

Comment lire les audits ?

Depuis la gauche vous devez voir:

Time stamp - La date et l'heure identifiant exactement le moment de l'evenement.

The protocol - Le type de protocole du paquet.

From/To Interface name - le nom de l'interface et la direction du paquet.

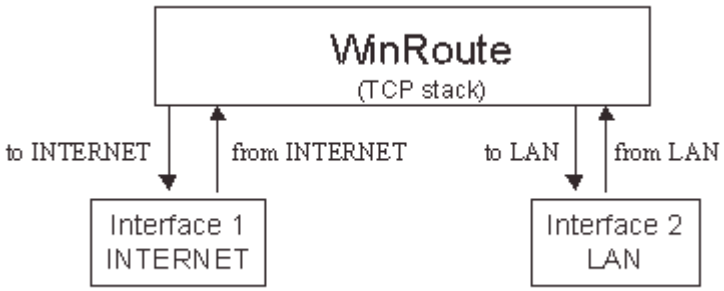
Source IP -> Destination IP address - les adresses IP source et destination presentes dans le paquet.

The flags - d'autres informations concernant l'action.

Exemple:

```
[10/Nov/1999 09:32:38] TCP: packet 511464, from lan,
length 1514, 192.168.1.7:2442 -> 192.168.1.1:25, flags:
ACK

[10/Nov/1999 09:32:38] TCP: packet 511465, to lan,
length 54, 192.168.1.1:25 -> 192.168.1.7:2442, flags:
ACK
```


WinRoute
(TCP stack)
to INTERNET
from INTERNET
to LAN
from LAN
Interface 1
INTERNET
Interface 2
LAN

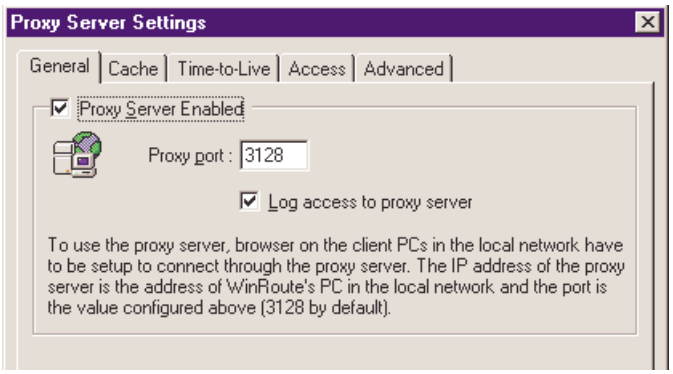
Audit HTTP (Proxy)

L'audit HTTP (Proxy) est un outil puissant qui vous permet de suivre les activités Internet des utilisateurs. Il fournit des informations plus compréhensives pour l'utilisateur que celles fournies dans l'audit de debug.

Quand est-ce que l'audit fonctionne ?

L'audit HTTP (Proxy) n'affiche que les informations concernant les données transitant via le serveur Proxy de WinRoute. Cela veut dire que si vous voulez recevoir es informations du serveur Proxy, vous devez forcer vos utilisateurs à utiliser le serveur Proxy. Voir le chapitres des exemples de Firewall ou le chapitre concernant le serveur Proxy, pour plus d'informations à ce sujet.

Egalement - vous devez activer l'option d'audit (log access to proxy server) dans la configuration du serveur Proxy



Comment lire l'audit HTTP (Proxy) ?

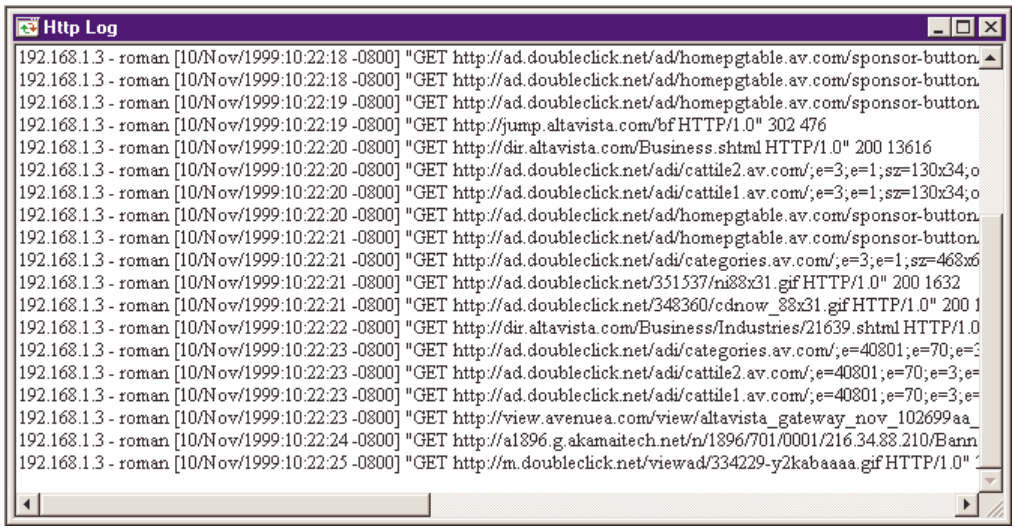
```
192.168.1.3 - roman [10/Nov/1999:10:22:20 -0800] "GET
http://dir.altavista.com/Business.shtml HTTP/1.0" 200
13616
```

De la gauche vers la droite:

Adresse IP - nom d'utilisateur : l'adresse IP et le nom de l'utilisateur effectuant la requete.

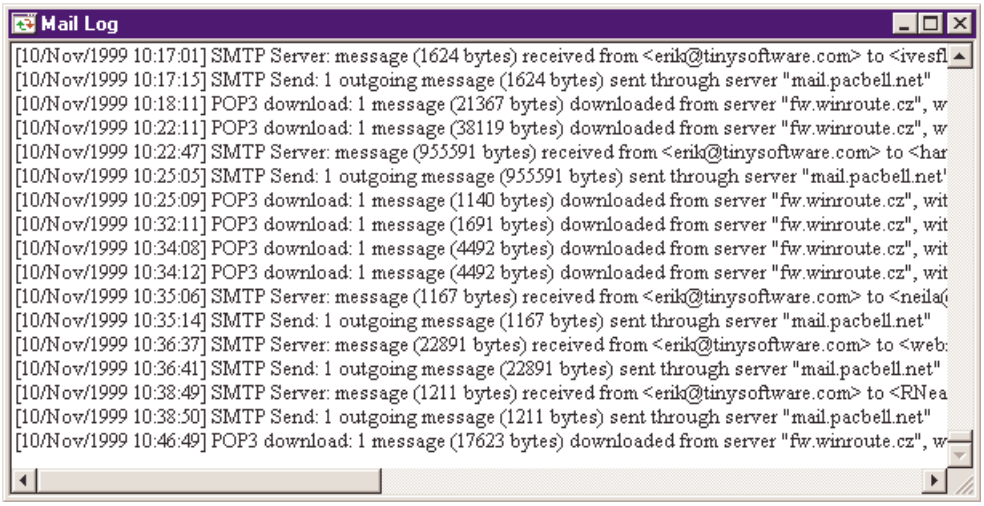
Time Stamp : la date et l'heure de la requete

GET "http..." : la requete en elle meme.



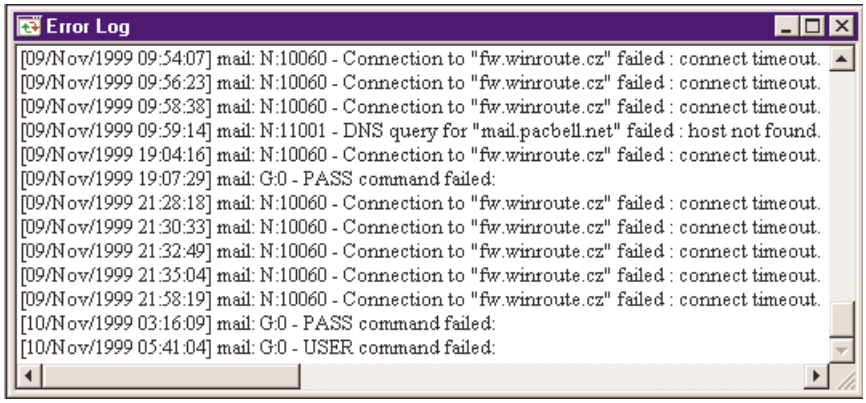
Audit de messagerie

L'audit de messagerie enregistre toutes les opérations concernant le serveur de messagerie incorporé dans WinRoute. Vous pouvez voir combien de messages sont envoyés, reçus, vers qui ils sont envoyés, etc. Toutes les opérations contiennent une indication de date et d'heure.



Audit d'erreur

L'audit d'erreur affiche les opérations sans succès ou ayant généré une erreur dans l'un des modules de WinRoute qui sont activés. vous pouvez par exemple voir une erreur s'étant produite lors d'un échange de messages ou dans le serveur DNS, etc.

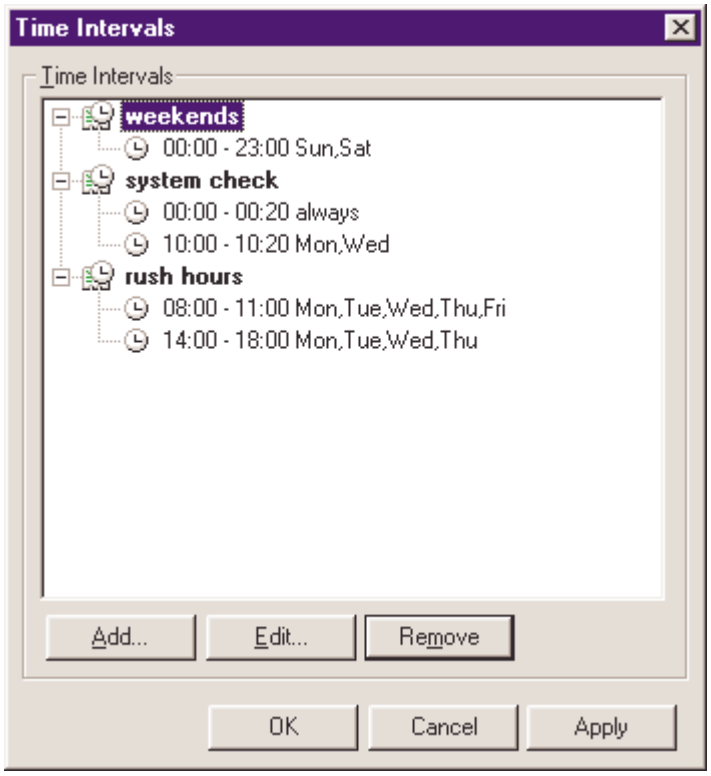


Intervales de Temps

Vous pouvez definir des Zones de Temps - intervales de temps prédéfinis - dans le but de faire certaines actions. Ces actions peuvent être:

- Filtre de paquets
- Echanges de messages (entrant et sortant)
- Connexion à Internet
- Configuration NAT avancée

Une Zone de Temps est un regroupement d'intervales. Vous pouvez ainsi créer des espaces des temps non homogènes consitués de plusieurs intervales de temps.



Par exemple: Vous pouvez définir une Zone de Temps appelé "Weekend" qui sera définir par: Vendredi de 17H00 à 19H00, Samedi et Dimanche.

Pour définir une Zone de temps:

- Aller dans le menu Settings=>Advanced=>Time Intervals
- Nommer la Zone de Temps
- Ajouter le nouvel intervale de temps
-

CHAPITRE 5

Exemples de Configuration

Dans ce chapitre

Solutions pour les VPN IPSEC, NOVELL et PPTP

VPN IPSEC

WinRoute Pro 4.2 supporte le mode IPSEC appelé "**Mode tunnel**". Le "**Mode tunnel**" devrait supporter n'importe quel client IPSEC qui permet que l'adresse IP du transport soit changée.

Configurations de WinRoute:

Créer le port mapping pour ESP:

Protocol: Other 50

Listen IP: <unspecified>

Destination IP: l'adresse IP privée du PC du client

Nous suggérons également de créer un port mapping pour IKE. Ce n'est pas nécessaire dans les cas où la transmission est initialisée de DERRIERE WinRoute vers l'Internet, toutefois certaines implémentation d'IPSEC peuvent exiger cette configuration:

Port mapping IKE:

Protocol: UDP

Listen IP: <Unspecified>

Listen port: 500

Destination IP: l'adresse IP privée du PC du client

Destination port: 500

Lancer plusieurs sessions IPSEC simultanément

S'il y a plusieurs clients IPSEC vous devez utiliser une adresse IP différente pour chaque client. Note - Le NAT de WinRoute laissera passer autant de clients simultanés que vous le voulez, du moment que la connexion est initialisé A PARTIR DU réseau local et que chaque client "utilise" une adresse IP attribuée à l'interface externe de WinRoute.

Informations générales au sujet d'IPSEC

IPSec ou security encryption protocol est utilisé pour la communication sécurisée entre deux ordinateurs.

IPSec utilise soit l'AH (Authentification Header) soit l'ESP (Encapsulating Security Payload). L'AH vérifie seulement l'identité de l'expéditeur et le contenue du paquet. Les données ne sont pas cryptées.

L'ESP crypte les données. L'ESP permet l'utilisation du surnommé "mode tunnel" qui est semblable au protocole PPTP. Le paquet comprend alors l'en-tête d'IP (nécessaire pour le transport) qui n'est pas crypté et la partie des données qui comprennent le paquet initial totalement crypté.

Le protocole IKE (parfois appelé ISAKMP) est utilisé pour l'authentification (échange de clefs de sécurisée). IKE utilise le protocole UDP sur le port 500 . Ce port est utilisé comme source et destination.

L'AH utilise le port 51, l'ESP le port 50. IPSec peut aussi communiquer en utilisant d'autres protocoles qui ne gênent pas le NAT en maintenant le niveau de certification.

Nous incorporerons automatiquement le protocole 50 à WinRoute de sorte qu'il n'y ait pas besoin de port mapping. La seule condition pour établir la connexion automatique est l'initialisation de la connexion DEPUIS le réseau local.

La plupart des implémentation d'IPSec utilisent l'algorithme MD5 et SHA1 pour l'authentification et DES, 3DES et Blowfish pour le cryptage. IPSec n'est étroitement connecté à aucun algorithme spécifique, ainsi les implémentations de différents logiciels peuvent être incompatibles.

VPN Novell Border Manager

Utilisation de WinRoute Pro avec le VPN Novell BorderManager (IPSEC)

Ce document décrit les procédures d'installation qui rendent possible la connection d'un réseau local, qui utilise le NAT pour partager une adresse IP unique fournie par un ISP, à un réseau distant qui utilise le logiciel Novell BorderManager Enterprise Server for VPN.

Selon le fichier de README.TXT fourni sur la disquette d'installation du client de Novell BorderManager VPN,

" vous ne pouvez pas utiliser le NAT entre un client VPN et un serveur VPN.Cela vient du fait que lorsque les paquets IP et IPX sont encapsulés et cryptés chez le client VPN, l'adresse IP de la source utilisée pour l'encapsulation est l'adresse du client VPN. Le calcul d'authentification d'en-tête IPSEC du paquet est basé sur cette adresse et l'adresse de destination du serveur VPN. Par conséquent, si l'une ou l'autre des adresses (celle du client VPN ou celle du serveur VPN) est modifiée par le NAT, quand il arrivera à destination, au serveur VPN, le calcul échouera et le paquet sera rejeté. Cependant, il est très probable, que le NAT ignore tout bonnement les paquets IPSEC parce qu'il gère seulement que TCP, UDP, et les paquets Internet Control Message Protocol (ICMP).

Quand vous avez des postes de travail dans un intranet qui doivent beaucoup communiquer avec des réseaux protégés par un serveur VPN via l'Internet, nous suggérons que vous utilisiez l'option site-to-site VPN de Novell BorderManager Enterprise Edition (au lieu de l'option client-to-site VPN)."

Cependant, le logiciel Novell BorderManager Enterprise Server est très cher pour un utilisateur à domicile. De plus, il exige la configuration de routes statiques sur le réseau distant consulté. La solution suggérée ci-dessus par Novell est donc inadaptée pour la personne qui voudrait connecter son réseau local qui utilise le NAT à un réseau distant par l'intermédiaire de Novell BorderManager VPN.

Étonnamment, il est possible de connecter un réseau local utilisant le NAT à un réseau distant en se servant de WinRoute pro et de Novell BorderManager VPN Client. Cette solution permet à n'importe quel ordinateur sur le réseau local d'accéder aux ressources sur le réseau distant lorsque le tunnel VPN est établi sur l'ordinateur routeur. Aucune configuration du réseau distant n'est exigée.

Ci dessous les phases de configuration pour le réseau local.

Étape 1: Installer et configurer le logiciel Novell BorderManager VPN Client sur l'ordinateur qui va être utilisé comme routeur. S'assurer que la connexion VPN vers le réseau à distance peut être établie avec succès et que les ressources sur le réseau distant peuvent être consultées.

Étape 2: Installer WinRoute pro sur l'ordinateur routeur. Suivre les instructions trouvées dans le guide d'administration pour configurer WinRoute pro et configurer les ordinateurs sur le réseau local pour marcher avec WinRoute Pro. Utilisez la configuration standard pour le partage d'adresse IP unique. S'assurer que les ressources Internet peuvent être consultées à partir de n'importe quel ordinateur sur le réseau local.

Étape 3: Quand vous voulez accéder aux ressources sur le réseau distant, exécuter Novell BorderManager VPN client sur l'ordinateur routeur puis la procédure de connexion au réseau à distance.

Cette solution est rendue possible grâce l'architecture de WinRoute pro. Puisqu'il travaille au niveau IPSEC, la translation d'adresses est effectuée avant que le paquet ne soit dirigé vers le virtual network adapter. Par conséquent les paquets envoyés au serveur VPN ont la véritable adresse IP de la source. Dans le sens inverse les paquets reçus par virtual network adapter traversent la couche de translation d'adresses et sont dirigés vers l'ordinateur concerné sur le réseau local.

Les limitations de cette installation sont que la procédure de connexion VPN doit être faite manuellement sur l'ordinateur routeur, et que la connexion VPN verra son délai d'attente dépassé après une certaine période d'inactivité, réglée sur le serveur VPN. En outre, les paquets IPX ne vont pas être routés même si le tunnel VPN supporte le protocole IPX. Par conséquent, le tunnel IPX sera disponible seulement sur l'ordinateur routeur.

D'une façon générale, cette installation est un moyen rentable et simple de connecter un réseau local qui utilise le NAT à un réseau distant en se servant de Novell BorderManager VPN.

Lancer un serveur PPTP derrière NAT

Pour avoir un serveur PPTP sur le réseau derrière WinRoute (même sur l'ordinateur sur lequel WinRoute fonctionne) vous devez configurer un port mapping.

Pour la connexion de contrôle:

- Protocol: TCP
- Listen IP:
- Listen Port: 1723
- Destination IP: Adresse IP de votre serveur PPTP (par exemple 192.168.1.12)
- Destination Port: 1723

Pour les paquets GRE (PPTP):

- Protocol: PPTP

- Listen IP:
- Destination IP: Adresse IP de votre serveur PPTP (par exemple 192.168.1.12)

Après configuration du Port Mapping comme indiqué ci-dessus vous pourrez placer votre serveur PPTP n'importe où derrière WinRoute Y COMPRIS l'ordinateur qui EXECUTE WinRoute. Les utilisateurs accéderont à votre serveur PPTP par "appel " à l'adresse IP externe (public) de votre réseau. Quand les paquets arriveront à l'ordinateur de WinRoute, ils seront automatiquement redirigés vers l'ordinateur approprié derrière le firewall.

Exemple de solution PPTP

WinRoute vous donne une manière très rentable de créer votre propre WAN entre diverses succursales connectées à l'Internet. Nous supposons que les lecteurs de ce document ont une connaissance minimale sur la gestion des réseaux et de WindowsNT.

Il est possible de créer un tel WAN en plusieurs étapes faciles:

1. Contrôler l'environnement:

   NT Serveur aux deux extrémités

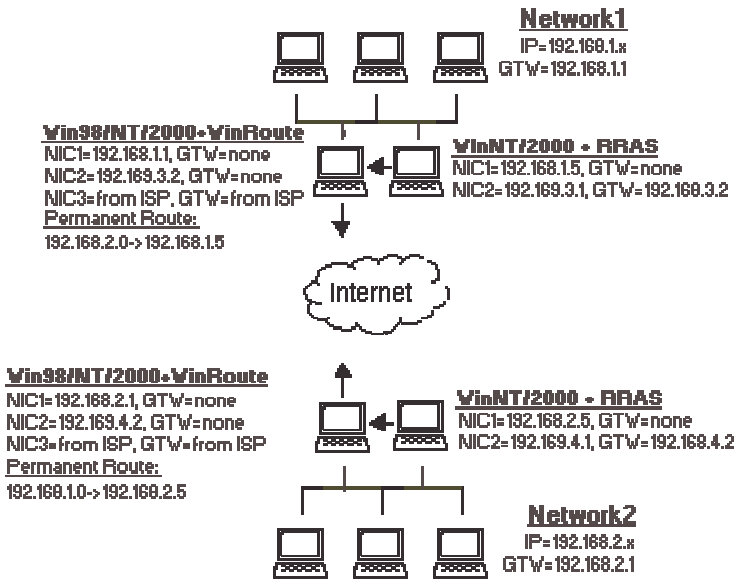
   WinRoute Pro installé aux deux extrémités

   RRAS (Stealhead) installé sur les deux NT Serveur

2. Créer une route statique sur les deux serveurs NT en indiquant que les paquets allant aux réseaux opposés passent par l'interface RRAS. Alors - si vous affichez des propriétés TCP dans le debug log de WinRoute Administrator vous devriez voir une interface dial-in parmi les interfaces disponibles.
3. Dans WinRoute Administrator aller dans l’Interface Table et afficher les propriétés de l'interface RAS utilisée pour la liaison PPTP. Assurez vous que le NAT est désactivé sur cette interface.

Dans l'onglet RAS de RAS interface properties, sélectionner la connexion PPTP parmi les entrées RAS. Si vous ne voyez pas la connexion RAS parmi des entrées RAS assurez vous que vous avez configuré l'annuaire téléphonique correctement. Aller au menu Settings->Advanced->Misc.Options et sélectionner l'annuaire téléphonique RAS à utiliser.

4 Tester la connexion - vous devriez pouvoir pinger le réseau opposé; de même vous devriez pouvoir accéder a l'Internet.



Lancer un client PPTP derrière NAT

Aucune configuration n'est exigée pour exécuter des clients PPTP derrière WinRoute (NAT) qui accédent a un serveur PPTP à l'exterieur sur l'Internet. Vous pouvez établir autant de connexions simultanées que nécessaire.

Exemples de configurations Firewall

Forcer les utilisateurs à utiliser le Serveur Proxy

Parfois vous pourriez trouver utile d'utiliser le **Server Proxy intégré** à WinRoute. Cela peut s'avérer utile si vous voulez **contrôler** l'activité d'utilisateur accédant à des pages webs, si vous voulez **restreindre** l'accès des clients à certains sites web, ou encore si vous vouliez qu'ils utilisent le **cache**.

Note! Vous pouvez utiliser **filtre de paquets** pour contrôler le trafic web; toutefois l'utilisation du **filtre d'URL intégré au proxy** est plus facile parce qu'il résout des noms de domaine ce qui veux dire que vous devez seulement entrer l'URL au lieu de l'adresse IP associée.

Configurations:

Vous devez créer deux règles de sécurité pour les paquets sortants:

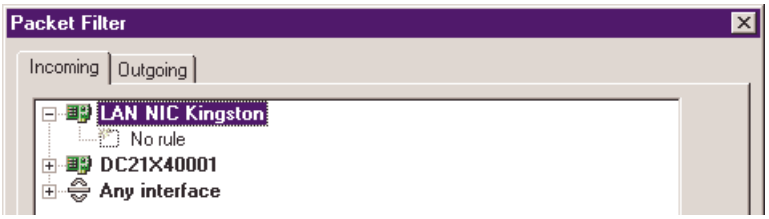
*1. **Permettre** aux paquets sortants qui ont comme port de destination le port 80 et comme IP source celle du serveur WinRoute*
*2. **Refuser** tous les paquets sortants qui ont comme port de destination le port 80*

Les règles doivent être définies exactement dans l'ordre indiqué ci-dessus. WinRoute applique les règles du **haut-vers-le bas**. Les règles sont appliquées sur le principe du premier arrivé premier-servit, c'est à-dire Le paquet entrant est recherché dans les règles en partant de la première, en haut, jusqu'à la dernière, en bas. La première règle correspondant à la description du paquet est appliquée et le reste des règles sera omis.

Pour configurer des règles:

1. Dans l'Administration de WinRoute allez dans le menu Configuration=>Avancée=>Filtre de paquets. Aller dans l'onglet Sortant.

2. Double cliquez sur votre interface externe (Internet). La liste des règles ou "Aucune règle" apparaît.



3. Cliquez sur le bouton Ajouter pour ajouter une nouvelle règle qui permettra à l'hôte WinRoute d'établir des connexions avec des serveurs web sur le port 80.

Sélectionner Le Protocole: TCP

Type De Source: Hôte

Adresse IP: adresse externe de votre Firewall WinRoute (par exemple 204.23.43.26)

Port De Destination: Égale (=) à 80, sous Action: sélectionner Autoriser.

4. Re-cliquez sur le bouton Ajouter pour ajouter la deuxième règle qui refusera toutes autres connexions TCP sur le port 80.

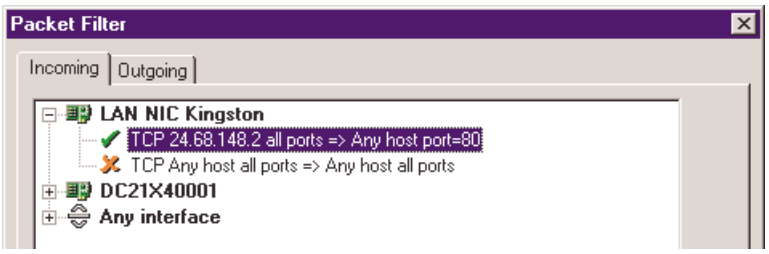
Sélectionner Le Protocole: TCP

Type De Source: Toutes

Port De Destination: Égale (=) à 80

Action: Refuser

Si vous voulez auditer les tentatives sectionnez l'option Auditer dans un fichier.



NOTE: En configurant des règles supplémentaires, se rappeler de les définir du HAUT vers le BAS.

Permettre la communication sur certain ports

Vous voulez avoir les règles suivantes:

- sécurité maximum
- permettre l'accès à votre serveur web
- permettre la communication avec votre serveur SMTP
- permettre aux emails d'être rapatrier depuis l'Internet vers votre serveur de courrier
- permettre l'accès à votre serveur FTP

Sécurité Maximum:

Onglet Entrant

Protocole: TCP, Refuser tous les paquets entrant

IP Source - Tous	IP de Destination - Tous
Port Source - Tous	Port de Destination - Tous

Cette règle sera toujours la plus basse des règles disponibles sur l'interface.

Permettre l'accès à votre serveur web depuis l'Internet:

Onglet Entrant

Protocole: TCP

IP Source - Tous	IP de Destination - Adresse IP du serveur web
Port Source - Tous	Port de Destination - 80

Permettre l'accès à votre serveur FTP de certaines adresses Internet:

Onglet Entrant

Protocole: TCP

IP Source - Tous	IP de Destination - Adresse IP du serveur FTP
Port Source - Tous	Port de Destination - 21

IP Source - Tous	IP de Destination - Adresse IP du serveur FTP
Port Source - Tous	Port de Destination - 20

Permettre a votre serveur SMTP de ne communiquer que via serveur relais SMTP (celui votre ISP):

Onglet Entrant

Protocole: TCP

IP Source - Le serveur SMTP relais de vote ISP	IP de Destination - Adresse IP du serveur SMTP sur votre LAN
Port Source Port - Tous	Port de Destination - 25

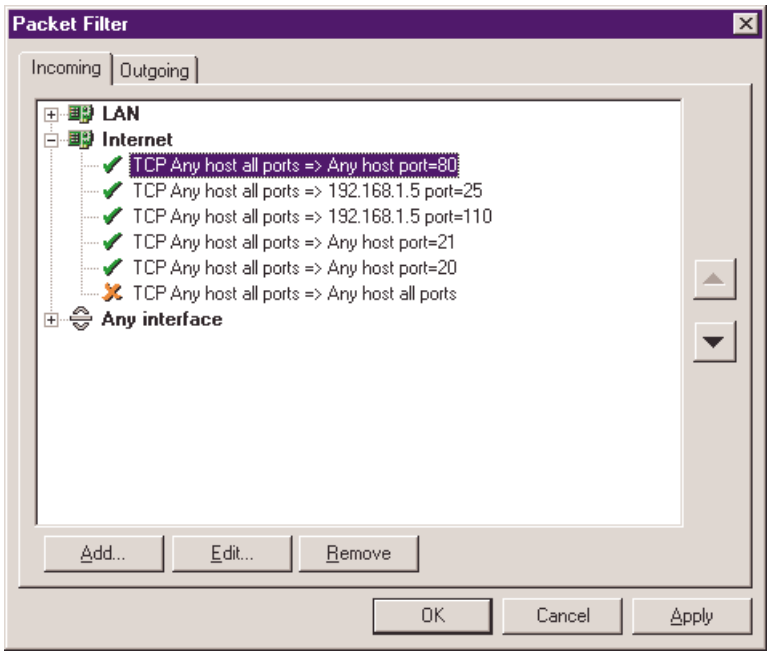
Onglet Sortant

IP Source - Votre serveur SMTP	IP de Destination -Adresse IP du serveur SMTP chez votre ISP
Port Source - Tous	Port de Destination - 25

Allows you to pick-up email from the Internet at your Mail Server

Onglet Entrant

IP Source - your SMTP server	IP de Destination - Adresse IP du serveur SMTP sur votre LAN
Port Source Port - Tous	Port de Destination - 110


Packet Filter
Incoming
Outgoing
LAN
Internet
TCP Any host all ports => Any host port=80
TCP Any host all ports => 192.168.1.5 port=25
TCP Any host all ports => 192.168.1.5 port=110
TCP Any host all ports => Any host port=21
TCP Any host all ports => Any host port=20
TCP Any host all ports => Any host all ports
Any interface
Add...
Edit...
Remove
OK
Cancel
Apply

Lancer ICQ, voix sur IP, vidéo conférence derrière WinRoute

Lancer ICQ derrière NAT

ICQ est le système de chat en ligne qui établit soit une connexion directe entre deux utilisateurs soit une inter-communication via l'intermédiaire du serveur ICQ. WinRoute Pro 4.2 est la première solution du commerce qui offre le support total de tous les services ICQ, en incluant le chat direct et de transfert de fichiers, à tous les utilisateurs à l'intérieur du réseau local sans aucune configuration.

Sur les postes de travails ICQ doit être configuré comme s’il avait un accès direct à l'Internet.

H.323 - NetMeeting 3.0

WinRoute intègre le support du protocole H.323. Cela signifie que toutes les applications voix-sur-ip (voice-over-ip) peuvent communiquer via WinRoute. Cela inclus des applications comme Microsoft NetMeeting, CuSeeMee, la téléphonie Internet (vous pouvez utiliser le téléphone Siemens IP phone a travers WinRoute par exemple) et d'autres.

Si la communication est initialisée de derrière WinRoute

Dans ce cas il n'y a aucune configuration exigée. WinRoute supportera un nombre de connexions simultanées pratiquement illimitées.

Si la communication est établie depuis Internet vers un PC derrière WinRoute

Dans ce cas il est nécessaire de créer un Port Mapping, en d'autres termes de dire à WinRoute où router les paquets H.323 entrants. Vous devez configurer le Port Mapping suivant:

Protocole:	TCP
IP d'écoute:	<non spécifiée> ou l'adresse IP utilisé pour les communications H.323 en cas de système multihome
Port d'écoute:	1723
IP de destination:	L'adress IP LAN de l'application H.323
Port de destination:	1723

Le protocole H.323 ne fonctionne pas que sur le port 1723 - WinRoute ajoutera automatiquement les autres connexions. En raison de limitations du protocole H.323 il ne peut y avoir, simultanément, qu'un seul poste de travail qui utilise une telle communication.

IRC - Internet Relay Chat

Aucune configuration spéciale n'est exigée pour exécuter un client IRC. Même les DCC (Direct Chat/Send(Receive) des fichiers) fonctionneront automatiquement si vous utilisez le port standard 6667 dans votre client IRC.

Pour exécuter un serveur IRC derrière NAT il faut mapper les ports suivants:

Protocole: TCP

IP d'écoute: <non spécifiée> ou IP que vous voulez utiliser pour le serveur IRC

Port d'écoute: 6667

IP de destination: adresse IP du PC qui exécute le serveur IRC

Port de destination: 6667

L'utilisation de n'importe quel autre port que le port standard entraînera comme conséquence que les DCC ne marcheront plus.

CITRIX Metaframe

WinRoute supporte totalement le protocole **CITRIX Metaframe** aussi bien que le protocole **MS Terminal Server**. Pour accéder à un serveur CITRIX Metaframe ou à un MS Terminal serveur qui fonctionne à l'intérieur du réseau de WinRoute depuis l'Internet vous devrez exécuter le Port Mapping suivant:

Pour MS Terminal Server:

Protocole: TCP

IP d'écoute: <non spécifiée> ou IP public que vous voulez que le serveur utilise

Port d'écoute: 3389

IP de destination: adresse IP privée du serveur à l'intérieur du réseau

Port de destination: 3389

Pour Citrix Metaframe:

Protocole: TCP

IP d'écoute: <non spécifiée> ou IP public que vous voulez que le serveur utilise

Port d'écoute: 1494

Destination IP: adresse IP privée du serveur à l'intérieur du réseau

Port de destination: 1494

Vous pouvez créer plus de ports mappés et ainsi accéder à plus de serveurs simultanément. Pour cela vous devrez pré-définir sur les ordinateurs clients quel port utiliser pour accéder au serveur. Ceci peut être indiqué dans le fichier .ini du client - quand vous créez l'icone de connexion.

Téléphonie Internet - BuddyPhone

GameRouter est devenue le premier logiciel de routage/firewall qui a amené la téléphonie sur Internet à un niveau sérieux. Avec l'application BuddyPhone (www.buddyphone.com) GameRouter vous permet de faire passer des appels par l'Internet d'un réseau à un autre.

BuddyPhone fonctionne très bien avec ICQ. Enregistrez-vous sur ce logiciel gratuit de messagerie instantané et vous apprécierez "la pression d'un seul bouton" pour appeler vos amis.

Tous les utilisateurs actifs dans votre liste de copain ICQ apparaîtront sur votre annuaire téléphonique BuddyPhone et le lancement d'un appel est aussi facile à utiliser que sélectionner un utilisateur dans la liste.

Aucune configuration n'est exigée du moment que vous utilisez BuddyPhone et ICQ ensembles.

Utilisation de BuddyPhone sans ICQ

GameRouter permet de détourner les appels venant d'Internet vers le bon récipient sur le réseau local en se basant sur le port.

Utiliser les ports 710 et suivants pour assigner aux utilisateurs locaux leur port respectif.

Exemple:

Vous avez trois utilisateurs dans votre réseau local qui utilisent BuddyPhone.

Nom de l'utilisateur	IP de l'utilisateur adresse IP interne	Port assigné à l'utilisateur
John	192.168.1.2	710
Quido	192.168.1.3	711

Bob	192.168.1.4	712

Alors vous configurerez les Port Mapping suivants:

Port d’écoute	IP de destination	Port de destination
710	192.168.1.2	700
711	192.168.1.3	700
712	192.168.1.4	700

Le lancement de l'appel téléphonique pour l'utilisateur sera facile, il suffira d’entrer company.com:port# dans la boite de dialogue direct dial de BuddyPhone. Par exemple sales.gamerouter.com:711.

Note! Ce n'est pas une erreur dans notre documentation! Le port de destination est vraiment 700. C'est le numéro de port employé par BuddyPhone. GameRouter fera le routage en se basant sur le port d'écoute.

CU-SeeMe

Les Ports Mappings suivant sont nécessaires pour recevoir des appels **CU-SeeMe** à travers le NAT:

Protocole: UDP

IP d’écoute: <non spécifiée>

Port d’écoute: 7648

IP de destination: l'adresse IP du poste de travail qui exécute le client CU-SeeMe

Port de destination: 7648

Protocole: UDP

IP d’écoute: <non spécifiée>

Port d’écoute: 7649

IP de destination: l'adresse IP du poste de travail qui exécute le client CU-SeeMe

Port de destination: 7649

Limitations:

- Actuellement, IL n'est pas possible d'exécuter plus d'un client CU-SeeMe sur un réseau local
- Il n'est pas possible de connecter à un "reflector" protégé par un mot de passe.

D'autres applications

Regardez sur www.kerio.com régulièrement pour les dernières mises à jour et ajouts à la liste croissante d'applications supportées. WinRoute supporte probablement votre application même si elle n'est pas énumérée, mais jusqu'à ce qu'elle soit documentée sur le site web vous devrez trouver par vous-même le port mapping si nécessaire.

Accès Distant - PC Anywhere

PC Anywhere

WinRoute inclut le meilleur support du marché pour Symantec's PC AnyWhere. PC AnyWhere permet aux utilisateurs d'accéder et de gérer des ordinateurs à l'intérieur du réseau. Pour cela vous devez appliquer le scénario suivant:

1. L'ordinateur à gérer exécutera PC AnyWhere Host.
2. L'ordinateur distant exécutera PC AnyWhere Remote
3. Le Port Mapping sur l'ordinateur de WinRoute sera configuré de cette façon:

   Protocole: TCP/UDP

   IP d’écoute: <non spécifiée>

   Port d’écoute (intervalle): 5631-5632

   Port de destination: L'adresse IP du PC AnyWhere Host à l'intérieur de votre réseau (e.g.192.168.1.12)

   Destination Port: 5631-5632

Question concernant la sécurité

Pour augmenter la sécurité et pour éviter d'ouvrir votre réseau au monde extérieur, WinRoute permet aux utilisateurs de choisir une adresse IP spécifique pour l'accès à certains ports spécifiques. Cette configuration permet que seulement certains ordinateurs ou réseaux puissent accéder votre système depuis l'Internet.

Pour définir les ordinateurs qui ont accès a votre réseau, vous devez d'abord définir un groupe d'adresses (même si vous n'entrez qu'un seul ordinateur). Pour configurer ceci aller dans le menu Configuration=>Avancée=>Groupe d'Adresses.

Changer l'accès vers un ordinateur différent

Vous pouvez configurer les droits d'Administration dans WinRoute pour permettre une connexion directe au serveur WinRoute. Lorsque vous êtes connecté, vous pouvez changer l'IP de destination du Port Mapping et accéder directement au PC que vous choisissez. Stupéfiant!

Passerelle PC Anywhere

Lancer PC AnyWhere en mode passerelle sur le PC de WinRoute permettra au client distant de rapatrier une liste des hôtes PC AnyWhere disponibles derrière le firewall. A partir de cette liste vous pourrez accéder et gérer n'importe lequel des hôtes PC AnyWhere derrière le firewall de WinRoute.

Ces étapes supposent que vous utilisez le PC AnyWhere 9.0 et que vous ne filtrez aucun paquet entrant/sortant sur le firewall de WinRoute

- Les ordinateurs gérés derrière le firewall de WinRoute exécuteront PC AnyWhere Host en utilisant le protocole TCP/IP
- L'ordinateur à distance exécutera PC AnyWhere Remote en utilisant aussi TCP/IP
- PC AnyWhere est installé sur le firewall de WinRoute en mode passerelle. En configurant le mode passerelle les dispositifs d'entrée et de sortie devront être réglés sur TCP/IP
- Sur le firewall de WinRoute, PC AnyWhere doit être configuré pour écouter le NIC interne (e.g.192.168.1.1). Des instructions sur la façon dont doit être configuré PC AnyWhere pour écouter sur une adresse IP/NIC spécifique peuvent être trouvées sur le site web de Symantec
- Ajouter les adresses IP des ordinateurs à gérer dans des options réseau de PC AnyWhere. Pour scanner l'intégralité du sous réseau utiliser 255 en tant que dernier octet (192.168.1.255).
- Configurer le port mapping suivant sur WinRoute:

  Protocole: TCP/UDP

  IP d’écoute: NIC externe (206.86.181.25)

  Port d’écoute: INTERVALLE (5631-5632)

  IP de destination: NIC interne (192.168.1.1)

  Port de destination: 5631-5632

Section Jeux

A propos du lancement de jeux derrière le NAT

Jouer à des Jeux

Beaucoup de jeux supportent aujourd'hui les environnements multi-utilisateurs. Les utilisateurs peuvent se battre via Internet ou les réseaux locaux ou alors ils peuvent rejoindre un des serveurs de jeux déjà existants sur l'Internet. Les utilisateurs peuvent également accueillir leurs propres serveurs de jeu et permettre à leurs amis, famille ou même a des inconnus de partager l'excitation de jouer ensemble.

Il y a beaucoup de jeux qui n'exigent aucune configuration de WinRoute. Avant d'essayer de configurer WinRoute pour un jeu spécifique, nous vous recommandons d'essayer de jouer d'abord. À la différence des serveurs Proxy, l'architecture de WinRoute supporte beaucoup de jeux directement "Naturellement."

Certains jeux exigent qu'un port spécifique soit configuré dans WinRoute pour qu'ils puissent marcher. Les ports sont utilisés pour l'identification du joueur auprès du serveur de jeu (en général).

Si le jeu a un port spécifique qui lui est associé, il n'y a pas de problème pour WinRoute! Vous devez juste configurer un Port Mapping dans WinRoute pour rediriger les paquets entrant sur votre réseau vers l'ordinateur du joueur derrière le firewall.

Les ports utilisés sont différents dans chaque jeu. Référez-vous à la documentation accompagnant chaque jeu ou appelez le support technique de l'éditeur du jeu pour plus d'information. Ce manuel contient juste quelques exemples de configurations pour les jeux les plus populaires.

Aasheron's call

Asheron's call est un jeu populaire sur Microsoft Gaming Zone. Afin de jouer à ce jeu à partir d'un l'ordinateur situé derrière GameRouter vous devez configurer le Port Mapping suivant:

1. Aller dans le menu Configuration->Avancée->Port Mapping
2. Exécuter les configurations suivantes:

Nom:	S1	S2	S3	S4	S5
Numero de Port:	2300-2400	9000-9013	6667	28800 - 29000	
IP de destination:	IP du PC avec le jeux	IP du PC avec le jeux	IP du PC avec le jeux	IP du PC avec le jeux	IP du P avec jeux
Protocole:	TCP/UDP	UDP	TCP	TCP	

Battle.net (Blizzard)

Le Port Mapping doit être configurer pour que vous puissez jouer a des jeux sur battle.net. Seul un joueur pourra jouer a la fois.

Protocole: TCP/UDP

IP d'écoute: <non spécifiée>

Port d'écoute: 6112

IP de destination: adresse IP de l'ordinateur du joueur (Par exemple 192.168.1.6)

Port de destination: 6112

Half-Life

Half-Life

Protocole: TCP/UDP

IP d'écoute: <non spécifiée>

Port d'écoute: 27015

IP de destination: adresse IP de l'ordinateur du joueur (Par exemple 192.168.1.6)

Port de destination: 27015

MSN Gaming zone

La configuration suivante a été testée avec MechWarior3 sur **MSN Gaming Zone**. Seul une machine peut accéder à MSN en même temps.

1. Allez au menu *Configuration->Port Mapping*
2. Ajouter un nouveau Port Mapping

Protocole: TCP

IP d’écoute: <non spécifiée>

Port d’écoute: intervalle 2300 à 2400

IP de destination: l'adresse IP local de la machine que vous voulez connecter à MSN

Port de destination: intervalle 2300 à 2400

3 Puis un autre Port Mapping

Protocole: UDP

IP d’écoute: <non spécifiée>

Port d’écoute: intervalle 28800 à 28912

IP de destination: l'adresse IP local de la machine que vous voulez connecter à MSN

Destination port: intervalle 28800 à 28912

Quake

Quake 3

clients Quake 2/3

Aucune configuration spéciale n'est nécessaire

Quake 2/3 Server

Pour le serveur Maitre:

Protocole: UDP

IP d’écoute: <non spécifiée>

Port d’écoute: unique 8002

IP de destination: x.x.x.x

Port de destination: 8002

Pour des clients qui se connectent a un serveur Quake3 Arena:

Protocole: UDP

IP d’écoute: <non spécifiée>

Port d’écoute: unique 27960

IP de destination: x.x.x.x

Port de destination: 27960

StarCraft

Jouer à StarCraft

WinRoute Pro intègre un support unique pour tous les joueurs de StarCraft (Blizzard Entertainment). Plusieurs joueurs sur un réseau connecté à l'Internet via WinRoute Pro peuvent s'amuser en jouant contre leurs "ennemis" virtuels sur l'Internet.

Actuellement, le support entièrement automatique fonctionne seulement dans le cas ou tous les joueurs qui rejoignent un jeu sont sur des ordinateurs derrière WinRoute Pro et non pas sur l'ordinateur hôte.

Pour plus de détails visitez le site www.kerio.com.

Mappings additionnels pour des jeux/applis courants

Ports nécessaires pour des applications diverses

Age of Empires II - 2 port mapping nécessaires

Protocole: TCP

IP d'écoute: <non spécifiée>

Port d'écoute: 47624

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination: 47624

Protocole: TCP/UDP

IP d'écoute: <non spécifiée>

Port d'écoute: Intervalle 2300 - 2400

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination: Intervalle 2300 - 2400

Delta Force

Protocole: TCP

IP d'écoute: <non spécifiée>

Port d'écoute: Intervalle 3568 - 3569

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination: Intervalle 3568 - 3569

Dial Pad

Protocole: UDP

IP d'écoute: <non spécifiée>

Port d'écoute: Intervalle 51200 - 51201

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination: Intervalle 51200 - 51201

Gamespy

Registration

Protocole: UDP

IP d'écoute: <non spécifiée>

Port d'écoute: 25635

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination: 25665

Pour les jeux eux mêmes

Protocole: UDP

IP d'écoute: <non spécifiée>

Port d'écoute: Intervalle 25000 - 30000

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination: Intervalle 25000 - 30000

Kali - 3 port mapping nécessaires

Protocole: UDP

IP d'écoute: <non spécifiée>

Port d'écoute: 2213

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination: 2213

Protocole: UDP

IP d'écoute: <non spécifiée>

Port d'écoute: 6666

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination: 6666

Protocole: UDP

IP d'écoute: <non spécifiée>

Port d'écoute: 57

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination: 57

Mplayer

Protocole: TCP/UDP

IP d'écoute: <non spécifiée>

Port d'écoute: 8000 - 9000

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination: 8000 - 9000

Oracle

Protocole: TCP

IP d'écoute: <non spécifiée>

Port d'écoute: 5000

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination: 5000

PCanywhere versions 2.0 - 7.51 - 2 port mapping nécessaires

Protocole: TCP

IP d'écoute: <non spécifiée>

Port d'écoute: 65301

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination: 65301

Protocole: UDP

IP d'écoute: <non spécifiée>

Port d'écoute: 22

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination: 22

Quicktime - 2 port mapping nécessaires

Protocole: TCP

IP d'écoute: <non spécifiée>

Port d'écoute: 554

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination: 554

Protocole: UDP

IP d'écoute: <non spécifiée>

Port d'écoute: Intervalle 6970 - 6999

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination: Intervalle 6970 - 6999

RTSP

Protocole: UDP

IP d'écoute: <non spécifiée>

Port d'écoute: Intervalle 6970 - 7170

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination Intervalle 6970 - 7170

VNC

Protocole: TCP

IP d'écoute: <non spécifiée>

Port d'écoute: 59xx (depending on the display number)

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination 59xx

Protocole: TCP

IP d'écoute: <non spécifiée>

Port d'écoute: 58xx

IP de destination: adresse IP de la machine qui exécute l'application

Port de destination 58xx

D'autres jeux

Regardez sur www.kerio.com régulièrement pour les dernières mises à jour et ajouts à la liste croissante d'applications supportées. WinRoute supporte probablement votre application même si elle n'est pas énumérée, mais jusqu'à ce qu'elle soit documentée sur le site web vous devrez trouver par vous-même le port mapping si nécessaire.

Aide vous Vous-même!

Si vos qualifications ont atteint un certain niveau, vous trouverez des solutions pour les autres jeux vous-même. Affichez l'audit de debugage (menue Vues) et dans configurez le pour voir les paquets TCP et UDP (faire un clique droit dans la fenêtre de l'audit de debugage).

Après avoir configuré l'audit lancez le jeu puis rapportez-vous à l'audit pour avoir des informations sur les paquets. Recherchez les paquets venant de l'interface Internet (affichée "from le_nom_de_votre_interface_internet") et regardez leur port de destination. Pour plus d'informations sur la façon de lire les audits référez-vous au chapitre audit de ce manuel.

Solutions DNS

Le relayeur DNS intégré à WinRoute vous permet de rediriger des requêtes DNS vers un serveur DNS pour la résolution de nom de domaine. Il est capable de résoudre les requêtes DNS locales (qui utilisent le nom de l'ordinateur local). Cependant les requêtes DNS telles que *www.quelquechose.com* doivent être résolues par un serveur DNS. Le **relayeur DNS** de WinRoute **redirigera** les requêtes DNS vers le **serveur DNS**.

Serveur DNS sur le PC de WinRoute

Avoir un véritable serveur DNS sur un PC WinRoute ne pose aucune difficulté. Toutes les requêtes DNS faites à votre serveur DNS recevront en réponse l'adresse IP Internet associée à ce domaine. Ce type d'adresse IP doit être associé à l'interface réseau qui relie WinRoute à l'Internet. Les serveurs WWW écoutent aussi bien les interfaces publiques que les privées.

Si le PC local envoie une requête DNS pour résoudre www.mondomaine.com, il obtient une adresse IP public associée à ce domaine et se connecte au serveur web avec une adresse IP (qui est attribuée à l'interface Internet).

Assurez vous que le Port Mapping pour des requêtes DNS soit bien configuré même si vous exécutez le serveur DNS sur le PC de WinRoute! Mapper le protocole UDP et le port 53 sur l'adresse IP de l'interface Internet.

Serveur DNS derrière WinRoute

Vous pouvez exécuter un véritable serveur DNS sur n'importe quel PC dans votre réseau local. Pour cela vous devrez configurer un Port Mapping:

Protocole: UDP

IP d'écoute: <non spécifiée> ou l'adresse IP associée au serveur DNS (mappé en tant que deuxième adresse IP)

Port d'écoute: 53

IP de destination: l'adresse IP privé du PC qui exécute le serveur DNS

Port de destination: 53

Serveur DNS et WWW derrière NAT

Si vous exécutez votre propre serveur DNS et WWW sur le même réseau privé vous pourriez vous poser les questions suivantes:

Comment est-ce que je gère les requêtes DNS pour www.mondomaine.com venant de mon réseau local, comment seront-elle résolues à l'adresse IP privée du serveur web tandis que les requêtes DNS venant d'Internet obtiendront une adresse IP Internet (public) associée à www.mondomaine.com ?

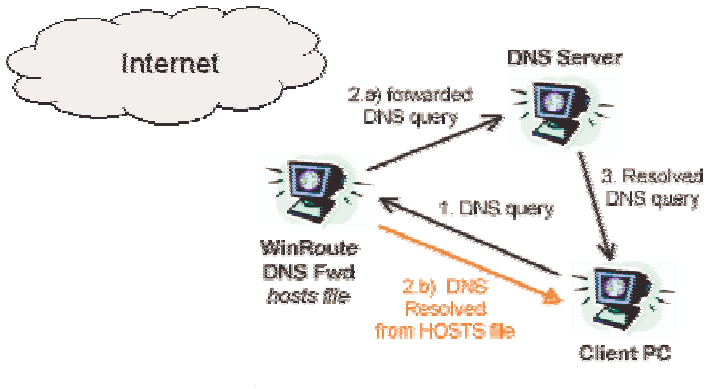
La solution est très simple et vous utiliserez le relayeur DNS intégré à WinRoute pour résoudre le problème. Sur tous les PC clients vous configurerez comme serveur DNS le relayeur DNS de WinRoute. Sur le PC avec WinRoute vous devrez appliquer les configurations suivantes:

- Mettez en marche le relayeur DNS de WinRoute
- Éditez le fichier HOSTS:

  Dans le fichier HOSTS ajoutez un enregistrement décrivant que www.mondomaine.com est une adresse IP privée (celle où votre serveur web fonctionne - par exemple 10.10.10.8). Le fichier HOSTS ce trouve dans la racine de votre répertoire windows (où windows est installé – c:\Windows ou c:\win98 etc.). Vous pouvez également accéder au fichier HOSTS depuis la boite de dialogue "Relayeur DNS" en cliquant sur le bouton "Editer le fichier HOSTS ".

Comment ça marche ?

Toutes les requêtes DNS envoyées par les ordinateurs client de votre réseau local seront d'abord résolues par le relayeur DNS de WinRoute. Toutes les requêtes seront d'abord recherchées dans les enregistrements du fichier HOSTS. Si une requête trouve un enregistrement correspondant elle sera gérée comme l'indique l'enregistrement (une adresse IP privée IP dans notre scénario).



S' il n'y a aucun enregistrement correspondant à la requête dans le fichier HOSTS la requête sera ensuite recherchée dans les enregistrements du cache DNS de WinRoute (qui est intégrée dans le relayeur DNS de WinRoute). Si le cache DNS ne contient pas l'enregistrement correspondant, la requête sera redirigée vers le serveur DNS spécifié.

Toutes les requêtes DNS venant de l'Internet seront redirigées, en fonction de la configurations des Port Mapping, directement au serveur DNS et résolues selon ses enregistrements.

Attention ! Dans un tel scénario vous ne pouvez pas avoir un serveur DNS sur le même ordinateur que WinRoute. Parce que les deux services – le relayeur DNS de WinRoute et le serveur DNS écouteraient le même port - UDP 53. Ceci générerait une erreur !

Problèmes DNS

Exécuter un serveur Web (ou FTP etc...) et un serveur DNS sur le même réseau privé derrière WinRoute NAT

Vous pourriez vouloir exécuter un serveur web avec comme domaine www.mondomaine.com derrière NAT et utiliser votre serveur DNS, fonctionnant sur le même réseau, pour la résolution de nom.

Exécuter un serveur Web (ou FTP etc...) sur le PC de WinRoute.

Si vous exécutez un serveur web sur le PC de WinRoute vous n'aurez aucun problème avec des requêtes locales. Toutes les requêtes DNS pour www.quelquechose.com arrivant à votre serveur DNS recevront en réponse l'adresse IP Internet associée à ce domaine. Ce type d'adresse IP doit être associée à l'interface réseau qui relie WinRoute à l'Internet. Les serveurs WWW écoutent aussi bien les interfaces publiques que les privées

Si le PC local envoie une requête DNS pour la résolution de www.quelquechose.com il obtient une adresse IP public associée à ce domaine. En conséquence il se connecte le serveur web a l'adresse IP (qui est attribué à l'interface Internet comme décrit ci-dessus).

Exécuter un serveur Web (ou FTP etc...) sur un PC derrière WinRoute

Vous pourriez vouloir exécuter votre serveur web sur un PC derrière WinRoute (avec une adresse IP privée par exemple 10.10.10.8). Le serveur web www.mondomaine.com est physiquement situé à une adresse IP privée 10.10.10.8 mais votre requête DNS sera résolue avec une adresse IP publique (par exemple 206.86.181.25) qui est associée à ce domaine.

Puis votre navigateur web ou votre client ftp se connectera à l'adresse publique, où il n'y a aucun serveur en fonctionnement car le serveur web est à l'intérieur de votre réseau.

Solution

Pour résoudre cette question vous devez utiliser le **relayeur DNS**, intégré à WinRoute, comme serveur de DNS pour vos ordinateurs.

Dans le fichier **HOSTS** vous ajouterez une autre entrée où vous indiquerez que **www.mondomaine.com** est à l'adresse IP **interne** appropriée (classe privée). Vous laisserez le relayeur DNS regarder dans le fichiers HOSTS avant qu'il ne redirige une requête DNS au serveur.

Alors chaque fois que les utilisateurs feront une requête sur **www.mydomain.com** elle sera bien résolue avec l'adresse IP locale appropriée.

Serveurs WWW, FTP, DNS et Telnet derrière WinRoute

WinRoute vous permet d'avoir des ordinateurs qui exécutent des services importants (serveurs) et qu'ils soient accessibles du monde extérieur. Les services (serveurs) doivent fonctionner sur un port spécifique ou sur un intervalle de ports et vous devez mapper ces ports pour permettre aux utilisateurs externes d'atteindre vos services.

Exécuter un serveur WWW derrière NAT

Pour exécuter un serveur Web derrière NAT

1. Allez au menu *Configuration ->Avancée ->Port Mapping*
2. Ajouter un nouveau Port mapping:

   Protocole: TCP

   IP d'écoute: <non spécifiée> ou l'adresse IP associée au domaine. Ce type adresse IP doit être associée à l'interface

Port d'écoute: 80

IP de destination: entrez l'adresse IP du serveur WEB (par exemple 192.168.1.10)

Port de destination: 80

Les utilisateurs accédant à ce service y accéderont soit en utilisant le nom de domaine soit avec l'adresse IP public de votre réseau. Dès que les paquets arriveront à WinRoute ils seront automatiquement rediriger vers l'ordinateur qui a la bonne adresse IP interne.

Exécuter un serveur DNS derrière NAT

Le relayeur DNS intègre à WinRoute vous permet rediriger des requêtes DNS vers un serveur DNS pour la résolution des noms de domaine. Il est capable de résoudre des requêtes DNS locales (qui utilisent le nom de l'ordinateur local). Cependant les requêtes DNS telles que www.quelquechose.com doivent être résolues par un serveur DNS. Le **relayeur DNS** de WinRoute **redirigera** les requêtes DNS vers un **serveur DNS**.

Exécuter un serveur DNS derrière NAT (WinRoute)

Afin d'avoir un serveur DNS derrière NAT/WinRoute vous devez ajouter le Port Mapping décrit ci-dessous. Les serveurs DNS communiquent entre eux avec le protocole **UDP** sur le **port 53**. Si vous n'ajoutez pas cette configuration votre serveur DNS ne sera pas fonctionnel. Vous devez appliquer cette configuration. Quand vous exécutez un serveur DNS sur le même ordinateur que WinRoute, le module d'inspection de WinRoute applique le NAT **AVANT** que les paquets n'atteignent n'importe quelle application, y compris le serveur DNS.

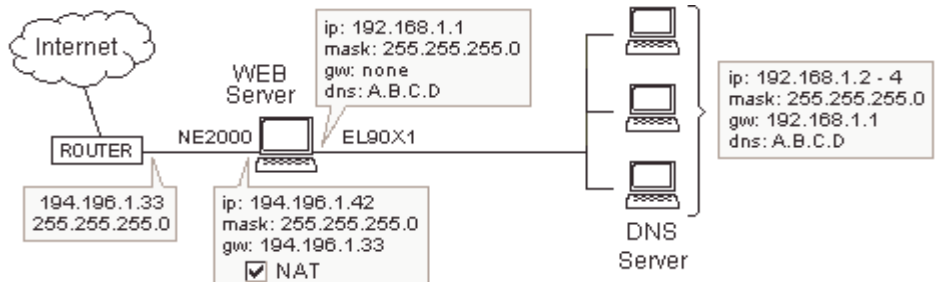
Protocole: UDP

IP d'écoute: <non spécifiée> ou l'adresse IP publique du serveur DNS que vous voulez fais fonctionner

IP de destination: 53

Port de destination: adresse IP publique ou privée du PC de WinRoute

Port de destination: 53



Note! Ce n'est **pas possible** d'exécuter un serveur DNS standard sur le même ordinateur que le relayeur DNS de WinRoute. Les deux services utilisent le port 53 du protocole UDP. L'exécution de ces deux services DNS sur le même PC poserait un problème fatal au routage IP. Cependant vous pouvez éteindre le relayeur DNS de WinRoute si vous voulez exécuter un serveur DNS sur le PC de WinRoute.

Exécuter un serveur FTP derrière NAT

Pour exécuter un serveur FTP derrière NAT

1. Allez au menu Configuration ->Avancéée->Port Mapping
2. Ajouter un nouveau **Port mapping**:

   Protocole: TCP

   IP d'écoute: <non spécifiée> ou l'adresse IP associée au domaine. Une telle adresse IP doit être associée à l'interface

   Port d'écoute: 21

   IP de destination: entrez l'adresse d'IP du serveur FTP (par exemple 192.168.1.10)

   Port de destination: 21

Exécuter d'un serveur FTP avec un port non standard:

Régler le port mapping pour qu'il corresponde au port employé par le serveur FTP.

Exécuter un serveur Mail derrière NAT

Afin d'exécuter un serveur Mail derrière WinRoute il est recommandé de créer deux Port Mapping - un pour le protocole SMTP (qui fonctionne sur le port 25) et un pour le protocole POP3 (qui fonctionne sur le port 110). Ceci permettra à d'autres serveurs SMTP d'atteindre votre serveur SMTP et vous pourrez également rapatrier vos emails en POP3 depuis l'Internet.

Il est nécessaire de configurer le Port Mapping même si le serveur de Mail est sur l'ordinateur de WinRoute. C'est à cause de la position du module d'inspection de WinRoute qui travaille en dessous de la pile TCP ainsi des paquets sont changés/refusés avant qu'ils n'atteignent le système d'exploitation.

protocole SMTP:

Protocole: TCP

IP d'écoute:

Port d'écoute: 25

IP de destination: entrez l'adresse IP du serveur SMTP (par exemple 192.168.1.10)

Port de destination: 25

protocole POP3:

Protocole: TCP

IP d'écoute:

Port d'écoute: 110

IP de destination: entrez l'adresse IP du serveur POP3 (par exemple 192.168.1.10)

Port de destination: 110

Exécuter un serveur Telnet derrière NAT

Telnet est largement répandu par beaucoup de compagnies pour accéder aux données à distance. Particulièrement pour les serveurs AS400 qui utilisent ce protocole.

Pour exécuter un serveur Telnet derrière WinRoute il est nécessaire de configurer un Port Mapping pour le protocole TCP sur le port 23. Aucune configuration n'est exigée pour qu'un client Telnet accède à un serveur Telnet sur l'Internet.

Protocole: TCP

IP d’écoute: <non spécifiée> IP du serveur Telnet

Port d’écoute: 23

IP de destination: entrez l'adresse d'IP du serveur Telnet (par exemple 192.168.1.10)

Port de destination: 23

Problèmes FTP lors de l'utilisation de ports non-standards

WinRoute reserve le port 21 pour les communications utilisant le protocole FTP. Dans quelques circonstances, généralement pour des raisons de sécurité, un serveur FTP peut être configuré pour utiliser un port différent. Quelques complications mineures apparaissent dans les scénarios de ce type. Les deux chapitres suivants expliquent les problèmes et les solutions connus aux problèmes résultant de l'allocation d'un port non standard aux serveurs FTP à l'intérieur et en dehors d'un réseau WinRoute.

Accéder à un serveur FTP qui utilise des ports non-standards

Si vous êtes derrière WinRoute et que vous essayez d'accéder à un serveur FTP avec un numéro de port différent de 21, vous ne recevrez pas la liste de répertoire. Pour que cela fonctionne vous devez faire ce qui suit:

1. Aller sur la machine de WinRoute
2. Arrêter le moteur de WinRoute
3. Aller dans le menu Démarrer->Exécuter sur le bureau
4. Taper regedit pour accéder à l'éditeur de base de registre;
5. Trouvez HKEY_LOCAL_MACHINE\SOFTWARE\Kerio\WinRoute\Module\0
6. Modifier la valeur de SpecPARAMS de sorte à ce qu'elle soit égale au numéro de port du serveur de FTP auquel vous voulez accéder
7. Rallumer le moteur de WinRoute.

Ceci devrait permettre à n'importe qui derrière WinRoute d'accéder à un serveur FTP sur l'Internet qui utilise un port non standard.

Note! Vous pouvez indiquer plusieurs ports en séparant chaque valeur par un espace.

Serveur FTP derrière WinRoute utilisant un port non-standard

Dans quelques circonstances (par exemple un client de l'entreprise situer derrière un firewall) un utilisateur peut être limité à un accès FTP en mode **passif** uniquement. Si un serveur FTP derrière WinRoute utilise un port non standard, aucun accès en mode **passif** ne peut être établi. C'est parce que WinRoute attribue (par défaut) le port 21 au FTP, ainsi si l'utilisateur souhaite utiliser un port différent, WinRoute doit être réglé. La procédure suivante corrige ce problème et permettra l'accès en mode **passif**.

1. Aller sur la machine de WinRoute
2. Arrêter le moteur de WinRoute
3. Aller dans le menu Démarrer->Exécuter sur le bureau
4. Taper regedit pour accéder à l'éditeur de base de registre;
5. Trouver HKEY_LOCAL_MACHINE\SOFTWARE\Kerio\WinRoute\Mport. Vous verrez alors les sous répertoires qui comprennent les informations correspondant aux ports mappés. S'il n'y a aucun sous répertoire, c'est qu'il n'y a aucun port mappé.
6. Trouver le répertoire qui contient le Port Mapping utiliser par le serveur FTP
7. Modifier la clef "*flags*" à '1'
8. Modifier la clef "*NatApp*" à 'FTP'
9. Rallumer le moteur de WinRoute.

Ces configurations "indiquent" à WinRoute que les paquets arrivant sur le port que vous avez défini seront du protocole FTP et donc WinRoute utilisera d'autres fonctions pour faire traverser ce protocole complexe.

Réseaux spéciaux

Réseaux Token Ring

Connecter des réseaux Token Ring

Le Token Ring est un type de réseau très spécifique. En conséquence, nous supposerons que seul les professionnels du réseau utilisent le Token Ring et nous n'entrerons pas dans une explication détaillée ici.

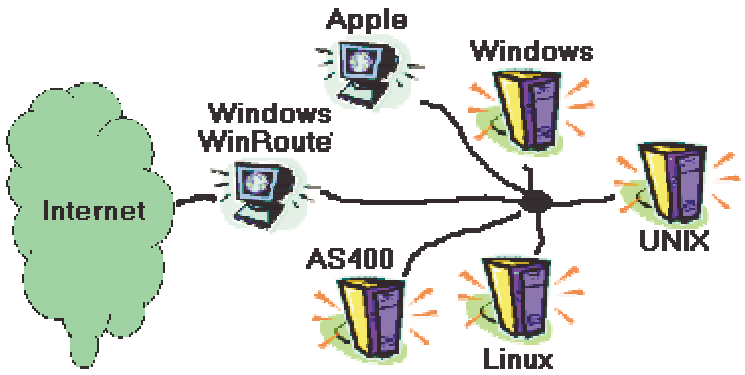
- Tous les ordinateurs du Token Ring ont besoin d'une MTU (maximum transmission unit) réglé à 1500
- Sur l'ordinateur de WinRoute aller dans le menu Configuration->Avancée->Options diverses et sélectionner "Support for Token Ring networks"
- Suivez d'autres instructions de configuration spécifiques pour chaque type de connexion Internet

Environnement au système d'exploitation multiple (Linux, AS400, Apple)

Interconnections d'environnements hétérogène (systèmes d'exploitation multiples; Linux, Unix, AS400, Apple)

WinRoute convient pour la connections de différents types de systèmes d'exploitation à l'Internet. WinRoute agit comme un routeur logiciel. En fait, il supporte n'importe quel environnement TCP/IP standard.

NOTE: Un système d'exploitation basé sur Windows doit accueillir l'application WinRoute. Par conséquent, au moins un ordinateur basé sur Windows 95/98/NT est exigé sur un réseau WinRoute. Le serveur ne peut pas être un système UNIX. Cependant, UNIX peut fonctionner parfaitement en tant que client.



Connecter des réseaux multiples

WinRoute est un routeur logiciel qui vous permet de connecter plusieurs réseaux à l'Internet via l'intermédiaire d'une connexion unique partagée (et d’une adresse IP). Normalement il est difficile de connecter et de configurer la connexion de tels environnements. WinRoute permet de connecter ces réseaux avec facilité.

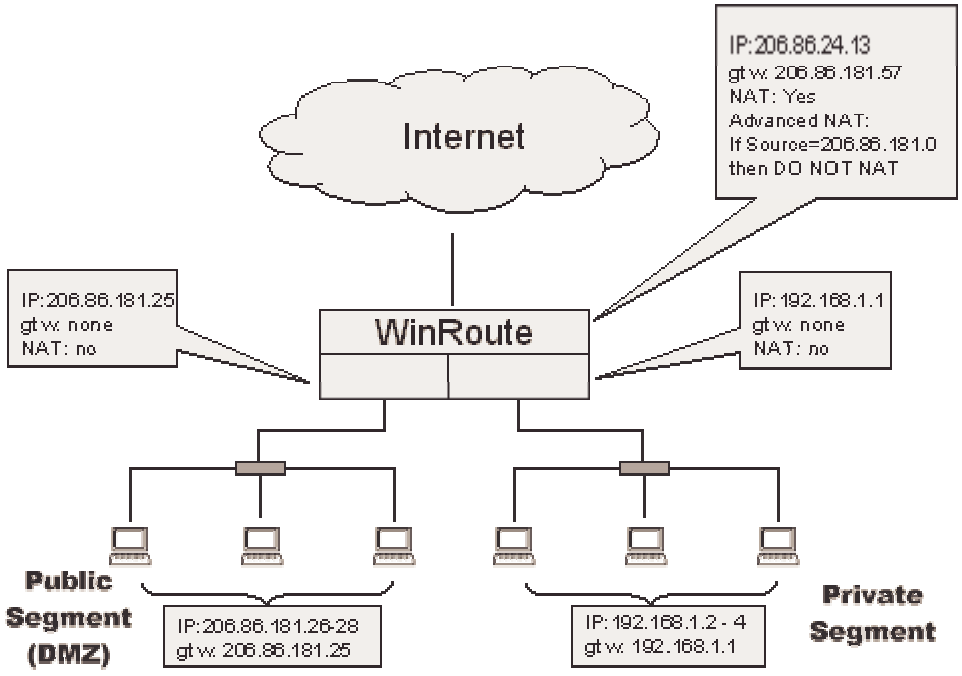
Ces réseaux peuvent être interconnectés par l'intermédiaire de l'Ethernet, du TokenRing, du frame relay, de Microsoft's PPTP ou même d'une ligne dial-up RAS. Cela signifie que les compagnies, avec plusieurs succursales, peuvent bénéficier de leur WAN privé sécurisée et se connecté à l'Internet via une connexion unique avec un coût minimum.

Connecter des segments Publics et Privés (DMZ)

Un segment privé se compose d'ordinateurs qui utilisent des adresses Internet de type privé. De telles adresses sont réservées aux réseaux privés et ne peuvent pas être utilisées sur l'Internet. C'est pourquoi vous avez besoin de WinRoute pour traduire ces adresses privées en adresses publiques qui vous permettent de vous connecter à l'Internet. Les ordinateurs avec une adresse privée ne sont pas directement accessibles de l'extérieur (Internet).

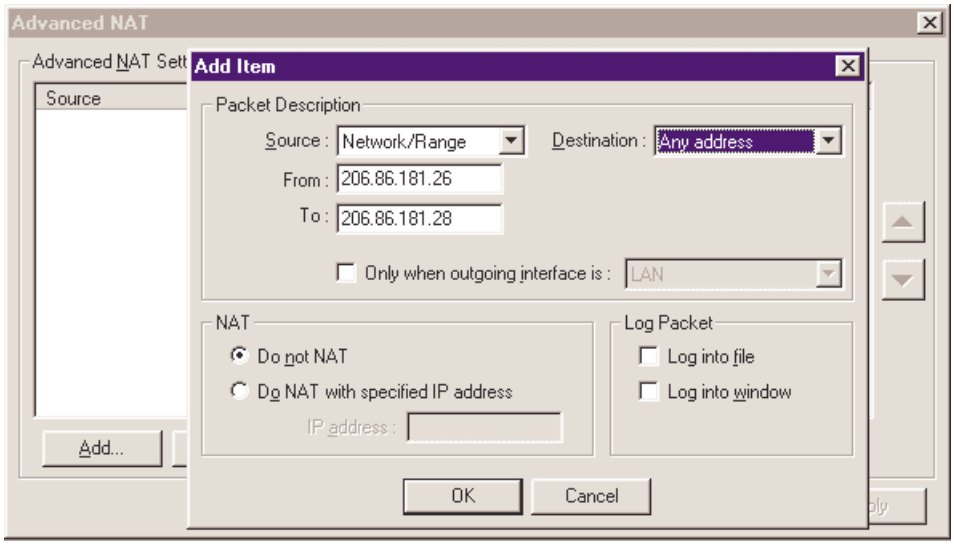
Un segment public se compose d'ordinateurs où chaque ordinateur a une adresse IP public. Ces systèmes, si vos règles de sécurité le permettent, peuvent être directement accessibles depuis l'Internet

Chaque segment doit avoir sa propre interface réseau sur l'ordinateur de WinRoute. Ainsi le moteur de WinRoute permettra à vos segments privés et publics de partager une connexion Internet unique.



Configurations de WinRoute

Il est nécessaire d'ajouter des configurations NAT avancées, ainsi WinRoute n'appliquera pas le NAT pour des paquets allant vers le segment public. Pour faire ceci aller dans le menu Configuration=>Avancée=>NAT.



Configurations de réseaux publics et privés

Ces réseaux seront configurés comme décrit dans d'autres parties de ce manuel. Pour les segments publics la seule différence est que vous utiliserez des adresses IP public sur le segment. De manière simple respectez les règles suivantes:

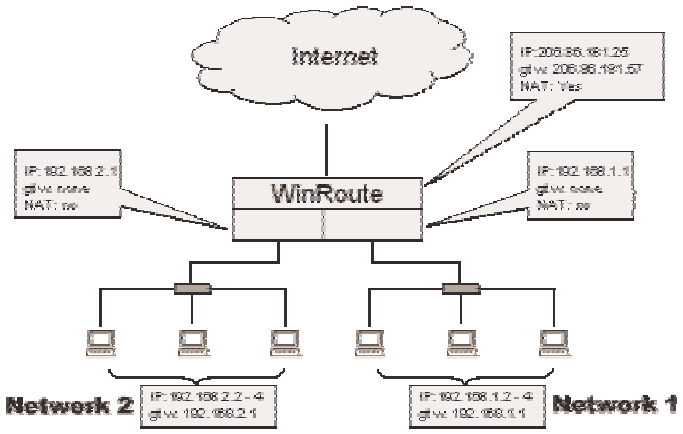
- AUCUNE passerelle par défaut sur les interfaces de WinRoute
- L'adresse IP de ces interfaces sera utilisée comme passerelle par défaut pour le reste de leur réseau.
- AUCUN NAT sur les interfaces de WinRoute

… regardez ***CheckList*** pour davantage d'explications

Partager la connexion pour deux réseaux avec 1 adresse IP

Au cas où vous auriez deux réseaux connectés à l'Internet par l'intermédiaire d'un ordinateur exécutant WinRoute, il n'y a aucune configuration spécifique. Fondamentalement il y a plusieurs segments menant à l'ordinateur de WinRoute, chacun à une interface réseau séparé. Dans notre exemple il y a trois interfaces réseau dans l'ordinateur de WinRoute:

- L'interface Internet
- L'interface du réseau 1
- L'interface du réseau 2



Les seules configurations que l'on doit garder à l'esprit sont:

Interface d'Internet

Le NAT est activé
L'adresse IP est réglée comme l'a indiqué votre ISP
La passerelle est réglée comme l'a indiqué votre ISP

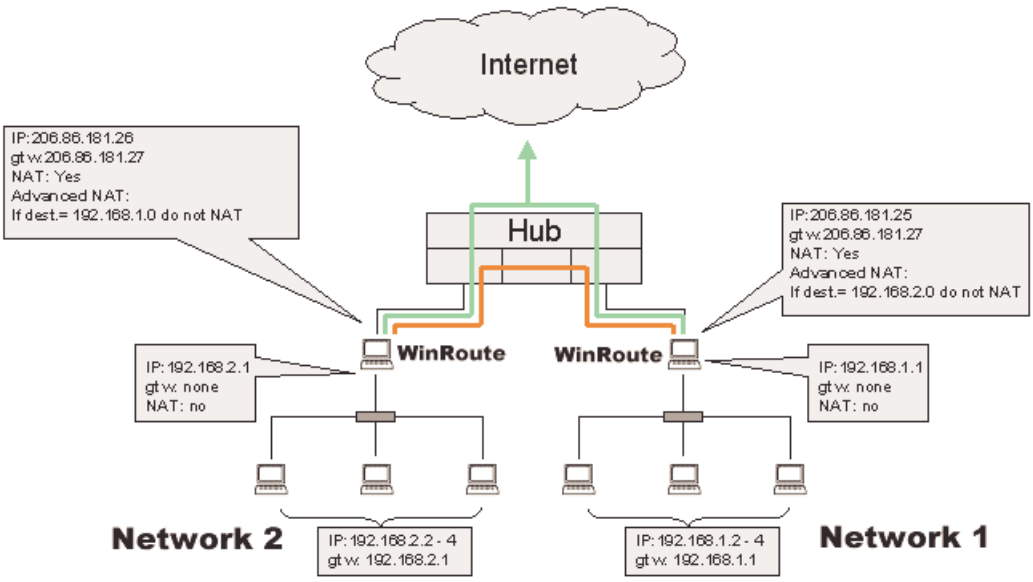
Interfaces internes

Le NAT est désactivé
Il n'y a AUCUNE passerelle par défaut configurée sur les deux interfaces
L'adresse IP est de type interne (par exemple 192.168.1.1)

Les autres options sont identiques à celles décrites dans d'autres chapitres de ce manuel. Le trafic entrant de chaque sous-réseau est routé vers l'autre sous-réseau ou vers l'Internet et réciproquement.

Partager la connexion pour deux réseaux avec 2 adresse IP

Vous pouvez vouloir partager un accès Internet entre deux réseaux alors que chaque réseau est derrière une adresse IP publique différente. En même temps vous voudriez pouvoir accéder aux ordinateurs des deux réseaux privés.



Il est TRÈS important lorsque vous appliquez le scénario de routage suivant:

- Ne PAS NATer les paquets allant vers l'autre réseau.
- NATer tous les paquets allant à l'Internet

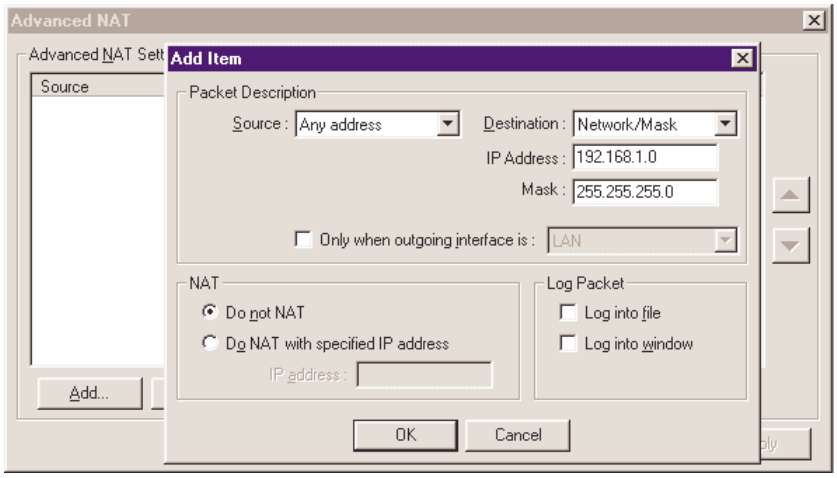
Dans d'autres termes WinRoute appliquera le NAT ou pas en en fonction de la destination des paquets IP qui passent par lui. Les paquets allant vers le réseau distant ne seront pas NATés tandis que les paquets allant vers l'Internet seront entièrement NATé.

Routeur ou hub?

En se basant sur vos besoins vous devez décider si vous voulez avoir un routeur entre vos réseaux ou si un hub suffit. Dans notre scénario un hub fournit assez de fonctionnalité pour permettre à deux réseaux de partager une connexion Internet (à grande vitesse).

Pour configurer WinRoute pour ne NATer ou pas en se basant sur la destination du paquet:

1. Aller au menu Configuration->Avancée->NAT.
2. Écrire les critères de destination - habituellement le sous-réseau ou l'intervalle des adresses IP
3. Choisissez l'option "Ne pas faire de NAT"



Conseil: Dans la configuration avancée du NAT vous trouverez une autre option permettant de ne pas appliquer le NAT en se basant sur l'adresse IP de la source. Cette option pourrait être utile quand vous connaissez les postes de travail qui n'auront pas besoin d'accéder à l'Internet. Puis plutôt que de régler des règles de firewall vous pouvez trouver une autre solution dans les configurations avancées du NAT.

Si vous n'appliquer pas le NAT à certains paquets, la source gardera son adresse IP interne, elle n'obtiendra jamais de réponses en retour. En d'autres termes, un tel utilisateur pourra essayer de se connecter à l'Internet très longtemps sans aucune chance d'accéder à l'Internet un jour.

Remote Access Server (dial-in et acces à l'internet)

Solution d'accès à distance au serveur

Parfois il peut être nécessaire d'accéder à votre réseau d'entreprise depuis le monde extérieur par l'intermédiaire du téléphone et utiliser cet accès à internet. WinRoute fournit cette fonctionnalité sur WindowsNT avec les services RAS installés et configurés.

Il y a des règles spécifiques qui doivent être respectées:

- Votre réseau d'entreprise a un sous-réseau (par exemple 192.168.1.0)
- Le serveur DHCP de WindowsNT donne aux utilisateurs venant par le RAS des adresses IP d'un sous-réseau différent (par exemple. 192.168.2.0)
- Le NAT sera activé seulement sur l'interface menant à l'Internet

Dans d'autres termes, la carte réseau (NIC) menant à votre réseau local doit avoir une adresse IP d'un des sous-réseau (par exemple 192.168.1.1) tandis que l'utilisateur se connectant à votre serveur par l'intermédiaire du RAS doit obtenir une adresse IP d'un réseau différent (par exemple 192.168.2.1). WinRoute agit en tant que routeur - il peut router des paquets entre deux, ou plus, interfaces réseaux différentes - pas sur la même.

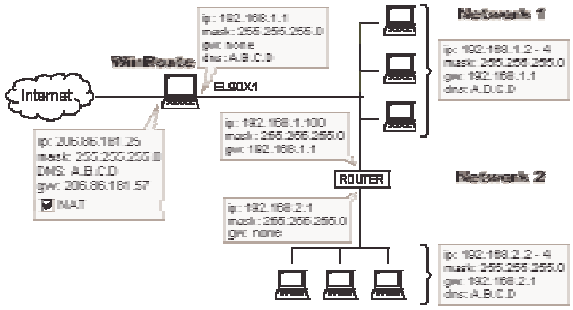
Ce type de d'installation reproduit ce qui se passe chez un petit ISP. WinRoute ne limite pas le nombre d'utilisateurs simultanés pouvant accéder à votre NT serveur. Tant que votre serveur NT donne aux utilisateurs distants des adresses IP de sous-réseaux différents (différentes de celles du réseau principal), seul le nombre d'interfaces RAS installées limite le nombre d'utilisateurs.

Connecter des segments en cascade via 1 adresse IP

Le type d'installation réseau, où tous les réseaux qui doivent être connectés ne sont pas directement reliés à l'ordinateur de WinRoute, bien qu'étant connectés par un routeur, s'appelle segments en cascade.

Figure 1: Connecting cascaded segments to the Internet

Le routeur entre les deux réseaux peut être n'importe quel routeur matériel, un ordinateur WindowsNT ou n'importe quel ordinateur Windows 95/98 avec WinRoute. WinRoute agira en tant que routeur avec ou sans le NAT.



En général il est nécessaire de "dire" à l'ordinateur de WinRoute où seront envoyés les paquets entrants pour les autres réseaux ; alors que pour les paquets sortants il doit y avoir des liens semblables sur le routeur (en divisant les deux réseaux) pour indiquer où les paquets sortant du deuxième réseau seront envoyés. Ceci peut être fait par l'ajout des nouvelles routes - une sur l'ordinateur de WinRoute (pour les paquets entrants) et une sur le routeur (pour les paquets sortants).

- La ROUTE sur l'ordinateur de WinRoute (membre du Reseau1) routera les paquets IP à destination de l'autre réseau (Reseau2) à l'adresse IP du routeur du Reseau1. Ce routeur transportera ces paquets plus loin.
- La ROUTE par DÉFAUT du routeur (qui connecte les deux réseaux) routera tous les paquets venant du Reseau2 à l'adresse IP de l'ordinateur de WinRoute du Reseau1. Alors WinRoute gérera ces paquets avec le NAT et les enverra vers l'Internet

Exemple

Notre exemple comporte deux réseaux 192.168.1.x et 192.168.2.x., l'IP du routeur est 192.168.1.100.

Note! Vous pouvez utiliser comme routeur n'importe quel routeur hardware mais également n'importe quel ordinateur Win95/98 avec WinRoute ou encore WindowsNT.

Configurations du Reseau1 (réseau primaire)

- Vous devez indiquer à l'ordinateur de WinRoute: "tous les paquets allant au réseau 192.168.2.0 doivent passer par le routeur 192.168.1.100":
- 1. Aller à l'invite MS-DOS
- 2. Écrire la commande suivante:

```
Route -p add 192.168.2.0 mask 255.255.255.0
192.168.1.100
```

- Sur le routeur 192.168.1.100, la route par défaut doit mener à l'ordinateur de WinRoute, c-à-d. 192.168.1.1. En d'autres termes, vous devez dire à votre routeur d'envoyer tous les paquets qui vont vers l'Internet au PC de WinRoute.

- Toutes les autres paramètres du réseau sont décrits dans d'autres chapitres (configuration de réseau).

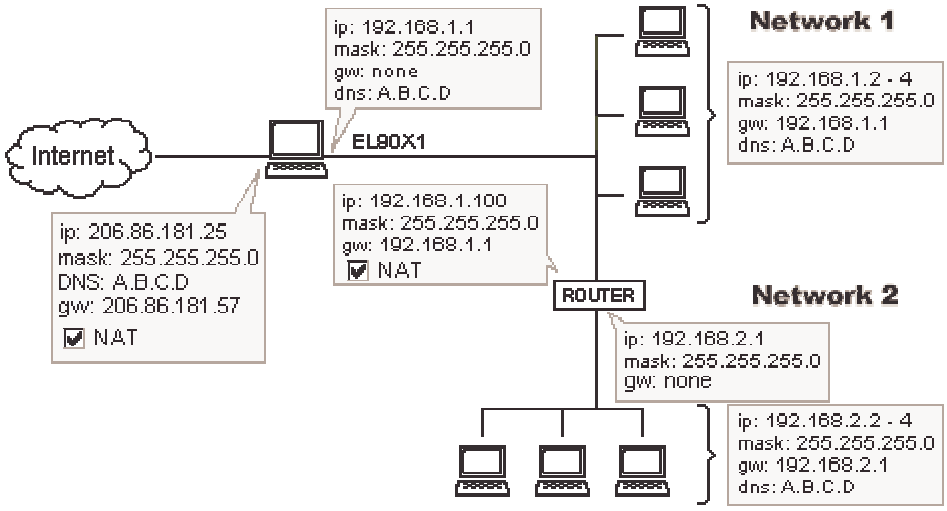
Configurations du Reseau2 (réseau secondaire)

Toutes les options sont standard, comme si le Reseau2 était le seul réseau. La passerelle par défaut de tous les ordinateurs du Reseau2 est l'adresse IP du routeur du Reseau2 (192.168.2.1 dans notre exemple).

NAT entre le Reseau1 et le Reseau2

Figure 2: Connecting cascaded segments to the Internet

Vous pouvez utiliser WinRoute et activer la fonction NAT pour interconnecter les réseaux primaires et secondaires. Le réseau secondaire ressemblera un ordinateur unique ainsi vous bénéficierez d'une administration plus facile et d'une sécurité plus élevée du réseau secondaire. Vous devrez régler correctement les options NAT avancées car vous ne voulez pas modifier le trafic entre ces deux réseaux.



Configurations NAT avancée sur le PC de WinRoute divisant le Reseau1 et le Reseau2

En se basant sur l'adresse IP de destination vous appliquerez ou pas le NAT. Dans notre exemple, si la destination des paquets est sur le réseau 192.168.1.0 alors les paquets ne seront pas NATés. Ceci permettra la transmission de données entre ces deux réseaux comme s'il n'y avait pas de NAT.

Pour la configuration du réseau suivez les règles décrites dans le reste de ce manuel.

Glossaire des termes

A

Adresse IP

Une adresse IP est un nombre de 32 bits, qui identifie un hote (un ordinateur) sur un réseau IP. Une adresse IP unique est assignée à chaque ordinateur sur Internet. Chaque paquet transittant sur Internet contient des informations telles que l'adresse IP de provenance et l'adresse IP de destination du paquet.

Adresse MAC

Une adresse MAC (Media Access Control) est l'adresse physique (matérielle) d'un adaptateur réseau et ne peut donc être changée.

ARP

Le protocole ARP (Address Resolution Protocol) permet d'associer une adresse IP avec une adresse matérielle en faisait une requête sur la machine émettrice. La requête demande l'adresse MAC de la machine distante. WinRoute utilise ARP pour des raisons d'audit et de sécurité.

B

BOOTP

Le protocole BOOTP (Bootstrap Protocol) permet d'assigner des adresses IP à des ordinateurs du réseau local, dynamiquement depuis un serveur DHCP.

C

Cache

Une mémoire cache stocke temporairement des données. WinRoute utilise une mémoire cache pour stocker temporairement les pages web et économiser de la bande passante.

D

DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole qui permet d'organiser et de simplifier l'administration des adresses IP d'un réseau local. Dans de nombreux cas (comme avec WinRoute) un serveur DNS est intégré au serveur DHCP pour de nombreuses simplifications. En spécifiant l'adresse IP d'un adaptateur réseau particulier, habituellement l'interface connectée à Internet, DHCP utilisera les valeurs DNS associées avec cette interface.

DNS

DNS (Domain Name System) est un système de nommage pour les adresses IP. Par exemple, www.kerio.com est un nom de domaine associé à une adresse IP. Un serveur DNS associe un nom à une adresse IP. Ce système est utilisé car il est plus facile de se rappeler d'un nom de domaine que d'une adresse IP numérique.

E

ETRN

ETRN est une commande utilisée par les serveurs SMTP pour récupérer du courrier SMTP.

La commande ETRN est utilisée lorsqu'un serveur SMTP n'est pas en ligne 24h/24 et que les emails envoyés sur ce serveur doivent être stockés temporairement sur un autre serveur SMTP. La commande permet ainsi de récupérer les messages sur le serveur temporaire.

F

FAI

Fournisseur d'Accès à Internet (ISP en anglais). C'est le fournisseur de services qui vous permet de connecter votre ordinateur à Internet.

ex: AOL, Wanadoo, Club Internet, etc.

Firewall

Ou parfeu. C'est un module de filtrage, situé sur une passerelle, qui examine les trafics entrant et sortant pour déterminer si il doit être ou non routé jusqu'à destination. WinRoute fournit un firewall via: sa fonctionalité de Translation d'Adresse (NAT), son filtre de paquets permettant d'appliquer des règles les adresses IP, et sa capacité d'enregistrer certaines informations sur les paquets sortants pour qu'ils puissent être autorisés sur le chemin du retour.

Flags

Les Flags sont des informations étendues faisant partie du paquet. Ces informations sont utilisées par les routeurs. Voici une liste des flags affichés par WinRoute:

SYNC - Synchronize - le paquet d'initialisation d'une connexion TCP

ACK - Acknowledge - le paquet d'accord de connexion

RST - Reset - demande pour re-établir la connexion

URG - Urgent - paquet urgent

PSH - Push - demande la délivrance immédiate du paquet à la couche la plus haute

FIN - Finalize - termine la connexion

FTP

Le protocole FTP (File Transfer Protocol) est un protocole de la couche application utilisé pour transférer, mettre à jour, supprimer, déplacer, renommer ou copier des fichiers à travers Internet.

I

ICMP

Le protocole ICMP (Internet Control Message Protocol) utilise des datagrames pour rapporter les erreurs de transmission entre les machines et les passerelles.

Interface réseau

L'interface réseau est l'adaptateur qui connecte un ordinateur avec les autres ordinateurs. Une interface réseau peut être une carte Ethernet, un modem, une carte RNIS (ISDN - Numéris), etc. L'ordinateur envoie et reçoit des données en utilisant cette interface réseau.

IPSEC

IPSEC (Internet Protocol Security), en bref, permet la création de réseau privé virtuel (VPN) en utilisant une authentification et un cryptage pour échanger les informations. WinRoute supporte IPSEC.

L

LAN

Un réseau local (LAN - Local Area Network) est un groupe d'ordinateurs interconnectés ayant la capacité de partager des ressources.

M

Masque réseau

Le masque réseau est utilisé pour regrouper des adresses IP ensemble. Il y a un groupe d'adresses IP assigné à chaque segment du réseau. Par exemple, le masque 255.255.255.0 (ou /24) regroupe 254 adresses IP. Si on a, par exemple, un sous-réseau 194.196.16.0 avec un masque de 255.255.255.0, les adresses que l'on peut assigner aux ordinateurs du sous-réseau vont de 194.196.16.1 à 194.196.16.254.

N

NAT

Avec la Translation d'adresse (NAT - Network Address Translator) vous pouvez connecter votre réseau local à Internet en utilisant une seule adresse IP. Les ordinateurs de votre réseau local accèdent à Internet comme s'ils étaient reliés directement à Internet (certaines limitations peuvent cependant se produire).

La connexion du réseau local tout entier en utilisant une seule et unique adresse IP, est rendue possible par le fait que le module NAT remplace l'adresse source contenue dans les paquets, envoyés depuis le réseau local, par l'adresse IP publique de l'ordinateur WinRoute.

La technologie NAT est très différente des technologies utilisées par les différents serveurs proxy ou passerelles basées sur la couche application. Ce type de technologies ne sera jamais capable de supporter autant de protocoles que la technologie NAT.

P

Paquet

Un paquet est une unité de donnée de communication utilisée lors d'envois de données d'un ordinateur à un autre. Chaque paquet contient un certain volume de données. La taille maximum d'un paquet dépend du média de communication. Par exemple, sur un réseau Ethernet, la taille maximum est de 1500 octets. Chaque paquet est composé de deux parties: l'en-tête et les données. L'en-tête contient des informations concernant le paquet. De plus amples informations peuvent être obtenues dans la section Filtrage des paquets.

Passerelle

C'est le (un) point d'entrée d'un réseau depuis un autre. Une passerelle est reponsable de la bonne distribution des paquets entrant et sortant du réseau local. WinRoute doit être installé sur la machine passerelle.

POP3

Le protocole **POP3** est principalement utilisé par les logiciels clients de messagerie pour récupérer les messages contenues dans des boites aux lettres électroniques compatibles POP3. Le serveur de messagerie de WinRoute à cette fonctionalité. Il peut, par exemple, récupérer les messages contenus dans plusieurs boites aux lettres chez votre FAI, et les distribuer localement dans les boites aux lettres des utilisateurs WinRoute.

POP3 est un protocole basé sur le protocole **TCP** et utilisant le **port 110**. Si vous voulez accéder à un serveur de messagerie POP3 situé derrière une machine WinRoute exécutant le module de NAT, vous devez créer un **Port Mapping** pour le protocole TCP sur le port 110 et l'envoyer vers l'adresse **privée** de la machine exécutant le serveur de messagerie.

Port

Un port est un numéro de 16 bits (ce qui permet un intervalle de 1 à 65535) utilisé par le protocole de la couche de transport - les protocoles TCP et UDP. Les ports sont utilisés pour adresser des applications (services) s'exécutant sur un ordinateur.

Un numéro de port peut être vue comme l'adresse d'une application tournant sur une machine.

Port mapping

Un Port mapping (ou Port Address Translation - PAT) est un processus qui analyse les paquets arrivant sur une interface et qui les route selon leur adresse et port de destination. Cela permet de faire passer des informations entrantes vers un ordinateur situé à l'intérieur du réseau privé. On peut définir plusieurs types de Port mapping selon le protocole qui l'on désire faire passer.

PPTP

Le protocole PPTP (Point To Point Tunnelling Protocol) est un protocole de VPN utilisé par les systèmes d'exploitation Microsoft pour crypter les communications entre deux ordinateurs.

Protocole

Défini des règles pour la tranmission de données.

Proxy

Proxy est une autre méthode de partage d'accès Internet. La technologie Proxy opère sur la couche la plus haute (la couche application) des couches réseau. Cela rend cette technologie peut efficace et surtout dépendante d'une application spéciale permettant les transferts via Proxy. De plus, une nouvelle implémentation du Proxy est nécessaire pour chaque nouveau protocole.

R

RAS

Le service d'accès distant (Remote Access Service) permet à un ordinateur d'appeler un autre ordinateur à distance. Pour WinRoute, RAS correspond à une connexion distante.

S

SMTP

Le protocole **SMTP** (Simple Mail Transfer Protocol) est utilisé pour les communications directes entre les serveurs de messagerie (comme le serveur de messagerie de WinRoute et le serveur de messagerie de votre FAI) et pour envoyer des messages depuis votre logiciel client de courrier électronique. SMTP est un protocole unidirectionnel - c'est à dire que votre message peut être envoyé via ce protocole, mais ne peut être récupéré. Vous devez utilisé les protocole POP3 pour cela.

SMTP est un protocole basé sur TCP et travaillant sur le **port 25**. Si vous voulez placer un serveur SMTP derrière une machine WinRoute, vous devez faire un port mapping sur le port TCP 25 et le diriger vers l'adresse privée de votre serveur SMTP à l'intérieur de votre réseau privé.

T

Table de routage

La table de routage et une table de règles utilisées par la pile TCP/IP pour transmettre les paquets sur un réseau IP. Elle permet donc à WinRoute de transmettre correctement les paquets. Pour voir la table de routage depuis une fenêtre MS-DOS, tapez la commande suivante: `route print`.

TCP/IP

TCP/IP est une combinaison de protocoles utilisée pour assurer des communications entre ordinateurs. Tous les protocoles sont basés sur des paquets; c'est à dire que les données sont "découpées" en petites sous-parties et envoyées à travers le réseau. Les protocoles de la famille TCP/IP sont: IP, TCP, UDP, ICMP, et d'autres protocoles basés sur IP.

U

UDP

Le protocole UDP (User Datagram Protocol) est typiquement utilisé pour envoyer des données qui ne nécessitent pas de controle d'erreur de transmission, etc. Par exemple, UDP peut être utilisé pour envoyer des datagrammes servant à transporter les données d'une communication "téléphonique" entre deux personnes (le protocole UDP est utilisé dans la recommendation H.323).

V

VPN

Virtual Private Network ou Réseau Privé Virtuel. Cela permet de partager, de manière sécurisée, des ressources à travers internet. Cela en créant un ou plusieurs tunnels qui assurent une transmission cryptée des données dans les deux sens. WinRoute supporte les VPN basés sur le protocole PPTP.

Index

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V