www.sandbox-team.be

Comprendre les réseaux

1 INTRODUCTION

L'une des forces de la Dreambox, c'est sa capacité à se connecter à un réseau informatique, ce qui la transforme en bien plus qu'un simple récepteur satellite. Ceci étant, cela sort du cadre traditionnel d'usage d'un récepteur satellite, et nécessite des connaissances du monde de l'informatique, que tout le monde ne possède pas.

L'objet de ce document est de vous expliquer, aussi clairement que possible, comment fonctionne un réseau tel que celui que vous allez mettre en œuvre, ceci afin de vous permettre de bien choisir tant le matériel que les solutions à utiliser, pour tirer partie de tout le potentiel de votre Dreambox, ceci sans remettre en cause la sécurité de vos machines.

Ce document se veut pédagogique, et sort un peu du contexte purement audio-visuel, mais cela est nécessaire, car c'est bien d'informatique dont nous parlons maintenant. Nous allons donc principalement parler de notions qui s'appliquent avant tout aux ordinateurs puisque, au fond, la Dreambox en est un !

Comme souvent dans ce type de document, quelques libertés sont prises avec la réalité, et les puristes y trouveront peut être à redire, aussi je leur demande d'excuser par avance les aménagements qui seront faits dans ce qui suit…

2 QU'EST-CE QU'UN RESEAU ?

Vous savez probablement à quoi cela sert : à faire communiquer des ordinateurs entre eux. Mais qu'est-ce que cela regroupe en fait ?

Pour bien comprendre ce qu'est un réseau, nous allons prendre un modèle que vous connaissez bien, et que vous pratiquez au quotidien : celui des transports routiers !

L'objectif d'un réseau est de permettre à des utilisateurs du réseau (vous), de communiquer. Le réseau routier répond bien à cet objectif : il vous permet, grâce aux déplacements qu'il autorise, de joindre toute personne que vous souhaitez rencontrer pour échanger de l'information. L'analogie est donc bonne…

Pour permettre cela, le réseau met à votre disposition différents éléments, que vous utilisez instinctivement chaque jour. Nous allons voir que le réseau informatique, fondamentalement, fait très exactement la même chose, et utilise les mêmes concepts…

2.1 Niveau physique : la route

2.1.1 Ethernet : le bitume

Le premier élément mis à votre disposition par le réseau, c'est ce que l'on va appeler le niveau physique : il s'agit d'éléments matériels dont le but va être de supporter l'ensemble des autres éléments.

Au niveau routier, il s'agit de … la route bien sur, le bitume, l'asphalte. Ce support physique vous permet de vous déplacer d'un point à un autre, dans des conditions bien déterminées, et avec toutes les garanties que vous en demandez.

Dans le monde de l'informatique, ce niveau physique existe également : il s'agit des câbles et des cartes que vous aller utiliser pour brancher vos appareils entre-eux, sachant qu'un type de câble particulier est…l'absence de câble, c'est à dire la transmission sans fil (WIFI).

Tout comme il existe différents types de routes (de l'autoroute au chemin bicinal…), il existe différents supports physiques pour les réseaux informatiques.

De nos jours, on ne trouve pratiquement plus que quelques types de support car, normalisation oblige, le marché a fait ses choix.

Dans le domaine des réseaux filaires, on utilise majoritairement le réseau ETHERNET. Ce type de réseau physique se décline en différentes variantes, dépendant de la vitesse maximale théorique que peut assurer le réseau, de 10 à 100 voir 1000 Mega-Bits / seconde.

Dans le monde du sans fil, on utilise majoritairement la déclinaison de l'Ethernet sous sa forme d'onde, à savoir le WIFI. Il s'agit d'un mode de transport totalement compatible avec l'Ethernet, et cela a son importance, nous allons voir pourquoi par la suite.

Concrètement, un réseau Ethernet est constitué de nos jour des éléments que vous connaissez : des câbles fins contenant 8 fils, équipés de petites prises en plastique

rectangulaires à la norme « RJ45 », servant à relier les différents équipements que vous possédez, au travers de cartes réseau installées dans vos ordinateurs.

2.1.2 Hubs et switchs : les carrefours

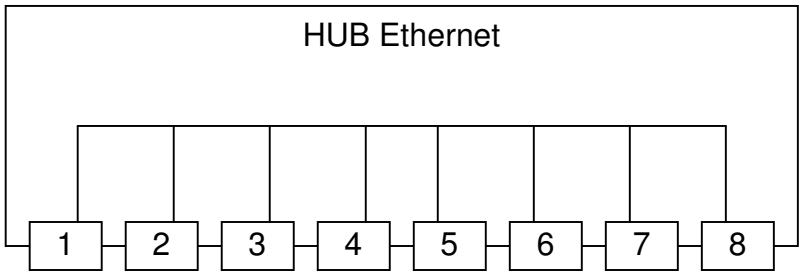
Si vous ne disposiez que d'une seule route, vous ne pourriez relier que deux extrémités, deux points géographiques. Fort heureusement, il existe de nombreuses routes, et elles sont interconnectées entre-elles par des carrefours.

De la même manière, pour relier plusieurs équipements entre-eux, vous avez besoin de plus d'un câble, et d'accessoires permettant de relier ces câbles entre eux : ce sont les hubs et les switchs.

De quoi s'agit-il ?

Ces appareils sont en fait de simples prises multiples. Leur rôle est de relier entre eux les différents câbles, et de faire en sorte que les données puissent librement passer d'un câble à l'autre. Ce sont les carrefours de nos routes.

Les hubs sont des carrefours anciens, qu'on ne trouve plus beaucoup. De conception simple, ils se contentent de mettre en liaison tous les câbles, sans apporter aucune règle relative à la gestion du carrefour. Les bouchons et collisions sont monnaie courante dans ces carrefours (ne riez pas, c'est exactement cela qu'il se passe !) et, de ce fait, les performances d'un hub sont médiocres, ceci d'autant plus que le nombre de connexions à relier entres-elles est élevé.

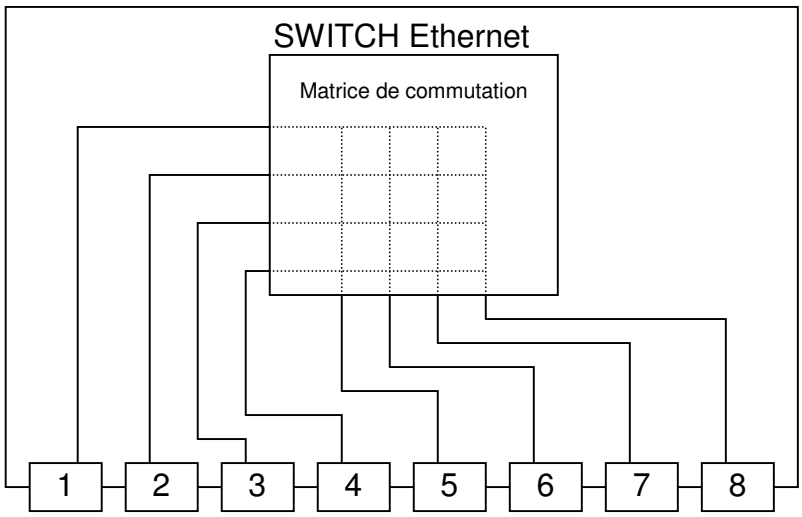


Principe d'un HUB Ethernet

Hub Ethernet 8 ports 3COM OfficeConnect

A l'inverse, les switchs correspondent plus à des carrefours « intelligents ». Ils isolent les différents câbles les uns des autres, et font en sorte que chaque câble puisse être utilisé de façon optimale, en fonction des équipements qu'il dessert, tout en réglementant le passage des données d'un câble à l'autre. Les performances d'un switch sont très nettement supérieures à celles d'un hub, et constantes quel que soit le nombre de connexions.

Les prix ayant fondu comme neige au soleil, on ne trouve pratiquement plus de hub aujourd'hui, rien que des switchs, et c'est tant mieux.



Principe d'un switch Ethernet

Le FS105 de Netgear, un switch Ethernet 5 ports 100 Mbits

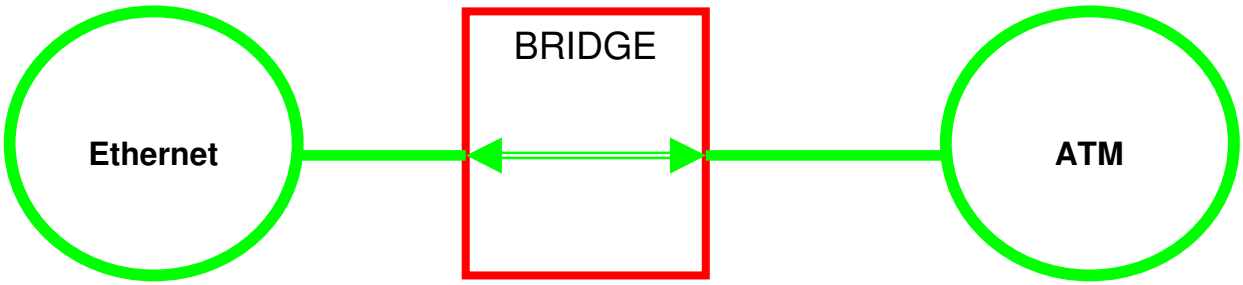
2.1.3 Bridges : les ponts

Nous disposons de routes (nos câbles) et de carrefours pour interconnecter nos routes (les switchs). Cela est déjà très bien, mais il arrive parfois que nous ayons besoin de nous déplacer autrement que sur la route, par exemple pour franchir un obstacle. Pour cela, nous avons besoin de ponts.

Cette situation existe également dans le monde de l'informatique, car différents moyens de transports existent pour l'interconnexion des ordinateurs. Si nous voulons par exemple relier un ensemble d'ordinateurs utilisant un réseau sans fil WIFI à un autre ensemble d'ordinateurs utilisant un réseau filaire Ethernet, nous utilisons un bridge.

Le rôle du bridge est de permettre la communication directe, et transparente, entre deux supports physiques différents. On utilise donc un bridge pour relier entre-eux des réseaux physiques hétérogènes, comme par exemple un réseau Ethernet et un réseau ATM ou encore Token Ring, ces derniers étant d'autres types de réseaux physiques, tout comme le WIFI.

Ceux d'entre-vous qui possèdent une FreeBox utilisent sans le savoir un bridge. En effet, dans sa configuration par défaut, la FreeBox est un bridge Ethernet vers ATM : elle transporte les données qu'elle reçoit sur sa connexion Ethernet vers le réseau ADSL de Free, qui fonctionne en ATM. Le modem SAGEM Fast 908 peut également faire la même chose, tout comme le modem Speed Touch Home d'ALCATEL.



Principe du Bridge (ou pont)

Le modem SAGEM F@st 908 peut être configuré en BRIDGE Ethernet ⇔ADSL (ATM)

2.1.4 Mise en oeuvre

Nous connaissons désormais les principaux éléments nécessaires à la réalisation physique d'un réseau :

- Nous savons qu'il existe différents moyens de transport des données, impliquant des matériels différents : cartes et câbles.

- Nous savons que, au sein d'un réseau filaire, nous avons besoin d'équipements pour relier entre-eux les ordinateurs : les switchs.

- Enfin, nous savons que si nous voulons exploiter plusieurs modes de transport pour constituer un même réseau, il nous faut des bridges pour réaliser les interconnexions entre ces différentes technologies, par exemple Ethernet ⇔ WIFI ou encore Ethernet ⇔ ADSL, voir même WIFI ⇔ ADSL.

Nous pouvons donc construire et mettre en service notre réseau local.

Le plus simple des réseaux est constitué de deux cartes Ethernet reliées par un câble. Dans cette configuration, on utilise un câble particulier dit « croisé ». Contrairement aux câbles usuels, ou câbles « droits », les deux extrémités d'un câble croisé ne sont pas branchées de la même façon, ce qui permet de brancher directement deux ordinateurs. Les câbles droits sont utilisés dès qu'au moins un élément intermédiaire est présent dans l'installation (hub, switch…)

Si nous branchons un câble croisé, nous établissons ce que l'on appelle le « niveau physique » du réseau. Cela se traduit par l'allumage des LEDs de signalisation, présentes généralement au niveau de chaque connecteur RJ45, sur les cartes Ethernet. Si le voyant s'allume, le réseau Ethernet est opérationnel. Dans le cas contraire, il faut vérifier les câbles et/ou les cartes.

Si le réseau est destiné à un peu plus que le branchement direct de deux ordinateurs, on utilisera nécessairement un switch, sachant qu'on ne trouve plus guère de hubs de nos jours, et qu'un bon switch 4 ou 8 ports coûte désormais moins de 40 € !

Dans cette seconde installation, on utilisera exclusivement des câbles droits, mais il est courant de trouver des switchs qui s'accommodent de câbles croisés (dans les gammes d'appareils pour particuliers seulement !).

2.1.5 Un mot sur les câbles et les vitesses

La norme Ethernet a évolué, depuis sa première déclinaison limitée à quelques 2 mégabits, pour arriver au gigabits en vogue actuellement. Pour des raisons liées aux techniques de transmission des signaux utilisées, la nature des câbles utilisés doit être adaptée à la vitesse de transmission envisagée, ainsi qu'à la distance à parcourir.
Les câbles sont classés par « catégorie », chaque niveau permettant d'atteindre un débit théorique maximum, sur une distance donnée.

Pour faire simple, disons qu'il ne faut pas prendre de câble de catégorie inférieure à 5. La catégorie 5 est nécessaire pour assurer un transport à 100 mégabits, très courant de nos jours.

Pour atteindre le gigabit, il est préférable d'opter pour des câbles de catégorie 6, même si d'autres catégories intermédiaires entre 5 et 6 sont envisageable (5e par exemple).

Un autre point important dans l'obtention d'un réseau Ethernet performant est le « mode duplex » mis en œuvre, ainsi que la vitesse négociée. Explications !

Lorsque vous branchez différents appareils sur un même réseau, il n'est pas possible d'utiliser n'importe quel mode de transport : si les appareils ont des caractéristiques différentes, il faut trouver un dénominateur commun, que chacun saura comprendre, afin que le réseau fonctionne.

Ce processus s'appèle la négociation. Elle est normalement réalisée automatiquement par la carte Ethernet lorsque vous la connectez au réseau, et va constituer à adapter le fonctionnement de la carte aux performances acceptables par les autres cartes du réseau.

Ainsi, si au moins un appareil connecté au réseau ne supporte QUE le 10 mégabits, alors tous les autres appareils vont se limiter à cette vitesse, et donc diminuer les performances globales du réseau.

Cette règle ne s'applique plus si l'on utilise un switch, en lieu et place d'un hub : le switch isole chaque appareil du réseau, et négocie directement avec l'appareil une connexion optimale. Il se charge ensuite de véhiculer les données en provenance d'un appareil, vers un autre, en adaptant la vitesse de transmission. C'est là le grand avantage du switch par rapport au hub : la vitesse maximale du réseau est caractérisée seulement par les capacités du switch, quels que soient les appareils qui lui sont reliés.

Un autre paramètre inclus dans la négociation est la capacité d'émission réception simultanée de la carte (full duplex) ou pas (half duplex). Il semble évident que, en mode full duplex, les performances sont significativement meilleures.

Enfin, on notera que ce processus normalement automatique peut ne pas être parfait, du fait de problèmes de compatibilité. Dans ce cas, il est nécessaire de « forcer » les caractéristiques à utiliser, en configurant manuellement chaque appareil.

2.2 Niveau réseau : les panneaux

Nous disposons maintenant d'une infrastructure réseau physique opérationnelle. C'est un bon début, mais ce n'est pas suffisant pour que nos ordinateurs communiquent. En effet, nous avons les routes, mais il nous faut plus pour pouvoir les utiliser (pour monter en voiture et partir…). Si nous nous lancions ainsi sur le réseau, nous nous perdrions immédiatement : nous n'avons pas de carte, pas de panneaux de signalisation bref, rien qui nous permette de nous guider, de trouver LA BONNE route. Nous avons donc besoin d'éléments nous permettant de nous guider.

2.2.1 Notion d'adresse IP

Lorsque nous envisageons de partir en voiture, nous disposons implicitement de deux informations indispensables : notre point de départ et notre point d'arrivée. Le point de départ est bien sur notre propre maison, que l'on peut assimiler à notre ordinateur dans notre modèle.
Nous savons également ou se trouve la maison de destination, car nous en possédons normalement l'adresse.

Dans le monde informatique, nous avons besoin des mêmes informations : adresse de départ et adresse d'arrivée.

En effet, pour que l'on puisse trouver un chemin sur un réseau, il faut bien pouvoir identifier de façon unique chaque ordinateur présent sur ce réseau. Pour cela, on donne à chaque machine connectée une adresse unique, composée de 4 nombres : c'est l'adresse IP, où IP signifie Internet Protocol. (Note : il existe d'autres normes qu'IP mais, de nos jours, on utilise pratiquement que ce protocole au niveau des particuliers).

Les adresses IP (version 4, les plus courantes) sont constituées de 4 nombres allant de 0 à 254, que l'on note en les séparant par des points, par exemple : 192.168.0.1
Certaines combinaisons de nombres ont des significations particulières, nous en parlerons plus loin.

Ainsi, dans votre réseau local, qui connecte entre-elles vos différentes machines, vous devez attribuer à chaque machine une adresse unique, afin qu'elles puissent s'identifier sans ambiguïté.

Comment savoir quelle adresse donner ?

Et bien vous devez en « demander » à un organisme international qui les réserve à votre usage, et vous garantie que personne d'autre ne les utilisera ! Enfin seulement si vous voulez que vos machines soient toutes directement reliées à Internet ! Dans le cas général, nous allons voir que vous n'avez pas besoin de faire cette démarche (Ouf !!!)

2.2.2 Adresse publique / adresse privée

Le problème des adresses n'est pas nouveau, il est présent dans les préoccupations des informaticiens depuis le début d'Internet. En effet, les combinaisons de nombres disponibles ne sont pas illimitées et, pour tout dire, la majorité des combinaisons est déjà réservée. Il est donc très difficile d'obtenir des adresses IP (V4) disponibles.

Ceci étant, ce n'est pas un problème car, dans la pratique, vous n'avez pas besoin de telles adresses. En effet, ce que vous cherchez à faire, c'est à relier chez vous deux ou plusieurs ordinateurs entre-eux, sans plus.

Comme ce besoin est très courant, la norme IP intègre la notion d'adresses privées. Il s'agit de certaines combinaisons d'adresses qui sont interdites sur un réseau, interdites signifiant ici que, si des données utilisant de telles adresses sont repérées sur le réseau, elles seront immédiatement éliminées par celui-ci.

Ces adresses sont donc prévues pour être utilisées librement par tout utilisateur, dans un contexte privé, interne, mais ne permettent pas d'accéder à un réseau publique comme Internet.
Ainsi, vous pouvez utiliser toute adresse dont les deux premiers chiffres sont 192.168, ou encore 172.16 à 172.31. Il est également possible de choisir toute adresse commençant par 10 (premier nombre).

Le choix de telle ou telle séquence de nombres dépend de vos besoins en nombre d'adresses. Comme on peut considérer que vous aurez rarement besoin de plus de 65000 adresses, la

plupart des équipements réseau sont pré-configurés pour utiliser la plage d'adresse 192.168.x .y, ou vous pouvez choisir librement les valeurs de X et Y (entre 0 et 254, sauf pour Y qui doit être supérieur ou égal à 1).

Prenons un exemple : vous voulez relier deux machines par un câble croisé.

Vous donnez à la première machine l'adresse 192.168.0.1.
Vous donnez à la seconde machine l'adresse 192.168.0.2.

Par la suite, vous utiliserez ces adresses numériques pour indiquer à un outil réseau quelconque, comme un logiciel de transfert de fichier (FTP) quelle est la machine que vous souhaitez joindre.

2.2.3 Notion de masque de sous-réseau

Les adresses IP sont utilisées conjointement à une seconde notion que l'on appèle le masque de sous-réseau.

En effet, si vous souhaitez composer plusieurs réseaux, indépendant les uns des autres, mais que vous puissiez relier entre-eux de façon contrôlée, vous avez besoin de pouvoir définir le périmètre qui constitue chacun des sous-réseaux.

Pour cela, vous utilisez le masque. Celui-ci est constitué de façon identique à une adresse IP mais, pour faire simple, disons qu'il n'utilise que les nombres 255 et 0.

Pour bien comprendre, prenons quelques exemples :

Imaginons que nous utilisions le masque suivant : 255.255.0.0. Qu'est-ce que cela signifie ?

Que toutes les adresses de la forme a.b.x.y pour lesquelles a et b sont identiques font partie du même sous-réseau. Avec un tel masque, toutes les adresses de la forme 192.168.x.y constituent un seul et unique réseau, tout comme les adresses de la forme 172.18.x.y, ou encore de la forme 10.1.x.y.
Ceci étant, si nous branchons sur un même câble des machines qui portent pour certaines, des adresses de la forme 192.168, et d'autres portant des adresses de la forme 172.18, ces deux groupes de machines ne pourront pas communiquer entre-elles !

En effet : si une machine possède l'adresse 192.168.0.1 et un masque de 255.255.0.0, le fait de tenter d'accéder à une machine dont l'adresse est 172.18.0.5 correspond, pour notre machine, à l'action de « sortir » du réseau local privé, ce qu'elle ne sait pas faire toute seule. Pour cela, elle a besoin d'une passerelle…

2.2.4 Notion de passerelle (gateway)

Nous avons constitué notre réseau privé, en utilisant des adresses adéquates. Dès que nous souhaitons communiquer avec l'extérieur de notre réseau, nous devons cependant nous conformer aux règles des réseaux IPs, notamment celles relatives aux adresses privées, dont la circulation est interdite sur un réseau publique.

Pour pouvoir communiquer avec l'extérieur, nous avons donc besoin d'un intermédiaire, d'un équipement qui se charge de la communication et adapte les données pour les rendre conformes. C'est le rôle de la passerelle.

La passerelle est un équipement réseau possédant sa propre adresse IP, celle que vous réglez dans le champ « Gateway » de vos ordinateurs. Lorsqu'une machine souhaite sortir du réseau local, elle envoie les données à la passerelle, en lui précisant l'adresse à atteindre. La passerelle utilise alors différentes techniques pour transmettre les données aux destinataire, comme par exemple la translation d'adresse, que nous verrons par la suite.

2.2.5 Notion de routage

Maintenant que nos machines disposent d'adresses, que nous savons comment passer d'un réseau vers l'extérieur de ce réseau (via une passerelle), nous devons trouver un moyen d'établir un itinéraire depuis notre point de départ jusqu'à notre point d'arrivée.

Ce processus s'appelle le routage. Effectué par les équipements nommés « routeurs », il consiste à identifier les différents tronçons de route à emprunter successivement pour, connaissant un point de départ, atteindre un point d'arrivée.

Les routeurs d'un réseau sont des équipements complexes, qui dialoguent entre eux, et se communiquent en permanence l'état du réseau : routes valides, routes invalides, routes engorgées, etc. Partant de ces informations, chaque routeur est en mesure de déterminer, à tout instant, une route valide permettant de joindre le destinataire.

Le résultat produit, la route identifiée, peut être visualisée depuis votre ordinateur en utilisant la commande « traceroute » ou « tracert » (sous Windows). Cette commande, qui reçoit en paramètre l'adresse IP du destinataire, vous affiche la liste des différentes routes empruntées pour le joindre, ainsi que les temps de transfert requis pour communiquer avec le destinataire.

2.2.6 Notion de serveur de noms : le DNS

Nous disposons désormais de tout ce dont nous avons besoin pour établir notre réseau. Il reste cependant que retenir des adresses sous forme de suites de nombres n'est pas très facile pour un humain. Nous retenons plus facilement les noms. Vous n'avez d'ailleurs probablement jamais utilisé d'adresse sous forme numérique, mais plus probablement ce que l'on appelle des noms symboliques, comme « www.linux.org ».

En fait, vous utilisez bien en permanence des adresses numériques, mais ces dernières sont masquées derrière des noms symboliques, compréhensibles et facilement mémorisables. Lorsque vous demandez à accéder au site web ww.sandbox-team.be, vous demandez à votre ordinateur de traduire ce nom symbolique en une adresse IP.

Pour faire cela, votre ordinateur s'appuie sur un serveur de nom ou DNS (Domain Name Serveur, serveur de nom de domaines).

Votre ordinateur connaît l'adresse IP d'un ou plusieurs serveurs de noms, car vous les lui avez communiqué en même temps que son adresse IP, son masque de sous-réseau et sa passerelle.

Dès lors, lorsque vous demandez une « résolution de nom », votre ordinateur va interroger un serveur de nom, en lui fournissant le nom symbolique que vous cherchez à joindre. Le DNS va répondre en fournissant une adresse numérique que votre ordinateur pourra ensuite directement utiliser pour communiquer avec la machine cible.

Il faut bien comprendre que ce fonctionnement n'est qu'un confort (souvent indispensable, mais cela reste un confort) et que le réseau peut très bien fonctionner sans DNS, sous réserve de ne pas utiliser de noms symboliques.

2.2.7 Notion de translation d'adresse

Comme nous l'avons vu précédemment, lorsque nous avons découvert les passerelles, il est fréquent de devoir adapter les données en provenance d'un réseau privé pour les faire circuler sur un réseau publique, par exemple Internet.

La solution à ce problème s'appèle la translation d'adresse.

Elle suppose de disposer d'au moins une adresse publique, donc valide sur un réseau comme Internet. Cette adresse est généralement celle que vous attribue votre fournisseur d'accès à Internet qui, lui, en dispose de nombreuses qu'il met à votre disposition, à raison d'une adresse par abonné.

La passerelle va alors utiliser cette adresse, en modifiant les données que vous lui envoyez pour y remplacer vos adresses privées par cette adresse publique. Ce faisant, elle rend « valide » les données et peut les transmettre sur le réseau.

Lorsque l'ordinateur destinataire reçoit les données, il pense dialoguer avec la passerelle, et c'est à elle qu'il va répondre, en utilisant son adresse publique comme adresse de réponse. Les données de réponses arrivant à la passerelle, cette dernière va les modifier à nouveau et ré-introduire votre adresse privée en lieu et place de son adresse publique, avant de vous les envoyer, bouclant ainsi la boucle.

Pour faire ce travail, la passerelle mémorise à chaque instant quels sont les flux de données qui sont établis entre vos différentes machines « internes », et les machines à l'extérieur de votre réseau privé. Elle maintient donc ce que l'on appelle une table de translation.

Ce fonctionnement présente de nombreux avantages :

- Il permet de partager une seule adresse publique pour un nombre important de machines présentes dans un réseau privé.
- Il masque la structure interne de votre réseau privé, car seule la passerelle est visible sur le réseau publique (elle seule dispose d'une adresse publique).
- En faisant passer tout le trafic à destination du réseau publique par un point central, il permet la mise en œuvre de contrôles de sécurité à ce point, via par exemple la mise en œuvre de firewalls, que nous verrons plus loin.

En contre-partie, cette technique rend impossible l'établissement directe d'un lien en provenance d'une machine extérieure, et à destination des machines de votre réseau privé : ces machines ne sont pas visibles depuis l'extérieur !

En fait, seul le trafic SORTANT depuis votre réseau vers le réseau publique est rendu possible. Dans la majorité des cas, c'est un atout, car c'est une sécurité supplémentaire mise en œuvre implicitement. Il arrive cependant que cela pose problème à certaines techniques de communication telles que le transport de la voix ou de l'image.

Dans de tels cas, il est possible d'exposer des parties de votre réseau interne via ce que l'on appèle la translation de ports. Nous aborderons ce point plus tard, quand nous parlerons de l'accès à la Dreambox depuis Internet.

2.2.8 Configuration automatique : le DHCP

Terminons notre voyage au cœur de techniques réseau en évoquant le système DHCP, ou Dynamic Host Configuration Protocol.

Comme vous l'avez vu auparavant, la mise en œuvre d'un réseau IP suppose de régler sur CHAQUE machine du réseau au moins 4 paramètres :

- Une adresse IP différente pour chaque machine
- Un masque identique pour chaque machine du réseau
- Une adresse de passerelle, pour sortir du réseau
- Une adresse de serveur de noms, pour manipuler des noms symboliques.

La mise en place de ces réglages et leur maintenance, quand le réseau évolue, peut vite devenir compliquée quand le réseau devient grand. Pour ces raisons, mais aussi pour simplifier l'accès au réseau pour les particulier, l'utilisation du DHCP peut être envisager.

DHCP est un système automatique de configuration des paramètres réseau. Il suppose la présence sur le réseau d'un serveur DHCP, qui met a disposition ses services de configuration automatique. Tous les routeurs d'accès ADSL possèdent cette fonction en interne.

Avec un tel système en place, il suffit de brancher une nouvelle machine sur le réseau pour qu'elle soit immédiatement configurée avec les paramètres nécessaires au bon fonctionnement du réseau. En contre-partie, il est clair que les paramètres de chaque machine peuvent changer en fonction, par exemple, de l'ordre d'allumage des machines !

3 MISE EN ŒUVRE

Maintenant que nous savons tout (ou presque) sur les réseaux locaux, nous allons prendre un cas réaliste, et voir comment nous pouvons réaliser un réseau adapté.

Nous sommes nombreux à disposer d'une connexion ADSL, ainsi que d'un ou plusieurs ordinateurs personnels. A partir de deux ordinateurs, le partage de la connexion Internet devient intéressant. Notez d'ailleurs que le second ordinateur peut très bien être une … Dreambox !

3.1 Matériel nécessaire

Nous voulons donner un maximum d'autonomie à chaque machine présente sur le réseau. Si tel n'était pas le cas, nous pourrions envisager d'utiliser le partage de connexion Internet de Windows, mais cela implique que la machine qui possède le modem soit allumée en permanence, ce que nous voulons éviter.

Nous optons donc pour l'utilisation d'un point d'accès Internet autonome.

De nombreux fournisseurs d'accès Internet imposent l'usage d'un équipement propre, afin de pouvoir disposer de toutes les fonctionnalités (télévision, téléphonie…), aussi il est important que nos équipements ne remettent pas en cause l'usage de ces appareils. Dans notre cas d'étude, nous prendrons pour hypothèse que nous possédons un abonnement chez Free, et possédons une Freebox.

Quels sont les équipements dont nous avons besoin ?

Il nous faut des cartes réseau Ethernet pour chaque ordinateur. Aujourd'hui, tous les ordinateurs intègrent cela en standard, mais si tel n'est pas le cas, vous pouvez trouver ces cartes pour seulement quelques euros.

En plus des cartes, il nous faut des câbles. Il s'agit uniquement de câbles droits, puisque nous allons utiliser des équipements dans le réseau. Si vous avez acheté un kit de deux cartes Ethernet fournies avec un câble, il s'agit d'un câble croisé, que vous ne pouvez donc pas utiliser.

Bien, jusque là, rien de compliqué. Par contre, le choix du point d'accès Internet n'est pas simple. Quoi prendre ?

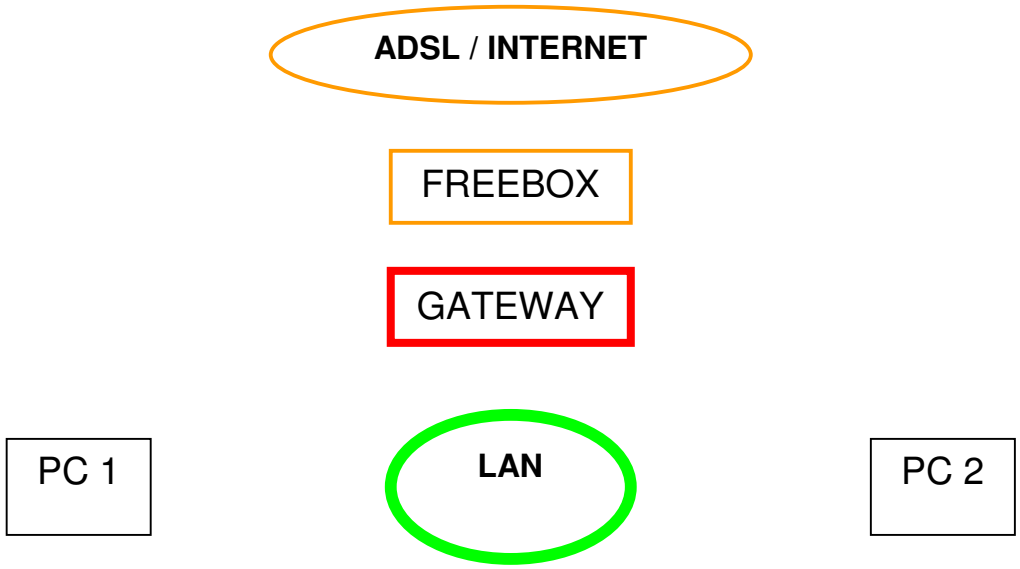
On trouve des matériels qui intègrent tout ce dont nous avons besoin pour seulement quelques dizaines d'euros, mais il faut bien comprendre ce que l'on achète.

En fait, nous avons besoin de plusieurs appareils : un switch, pour interconnecter nos appareils, une passerelle, pour faire le lien avec le réseau public (Internet) et un pont pour nous relier à Internet via notre connexion ADSL. Ajoutons à cela un firewall pour nous protéger efficacement, et nous serons bien équipés !

Heureusement pour nous, nous n'avons pas à acheter tous ces appareils les uns après les autres. Tout d'abord, nous en possédons déjà un : le pont.

En effet, la Freebox, par défaut, est un bridge Ethernet ⇔ ADSL. Nous disposons donc déjà de cet équipement.

Par ailleurs les fabricants, conscients des problèmes posés par la multiplication des équipements, proposent des appareils tout-en-un, pour seulement quelques Euros. Ainsi, nous pouvons trouver en un seul appareil un ensemble passerelle + firewall + switch. On appelle souvent ces appareils « Routeurs d'accès Internet ». Ils comportent tout ce qui est nécessaire pour mettre en œuvre un petit réseau local, connecté à Internet.
Nous prendrons dans notre exemple le RP 614 de Netgear, mais d'autres appareils équivalents sont disponibles chez d'autres marques telles que Lynksis.

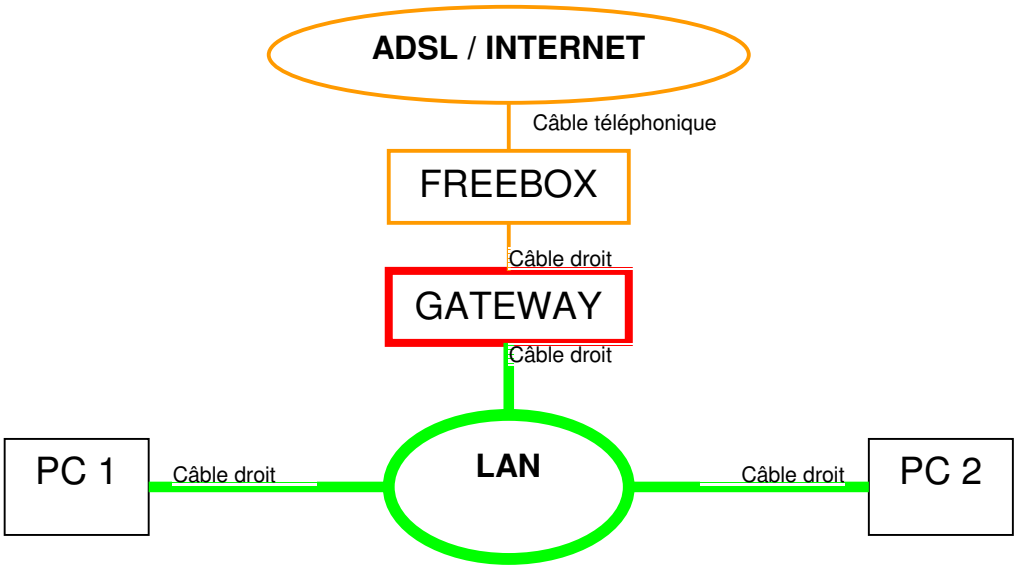


Les éléments à mettre en oeuvre

3.2 Connexion des appareils

La connexion de tous ces équipements est très simple :

- Un câble droit relie le PC 1 au routeur d'accès.
- Un câble droit relie le PC 2 au routeur d'accès.
- Un câble droit relie la Freebox au port WAN du routeur (port Internet).
- Enfin, la Freebox est reliée au réseau téléphonique / ADSL.



Les éléments reliés entre-eux

3.3 Réglages

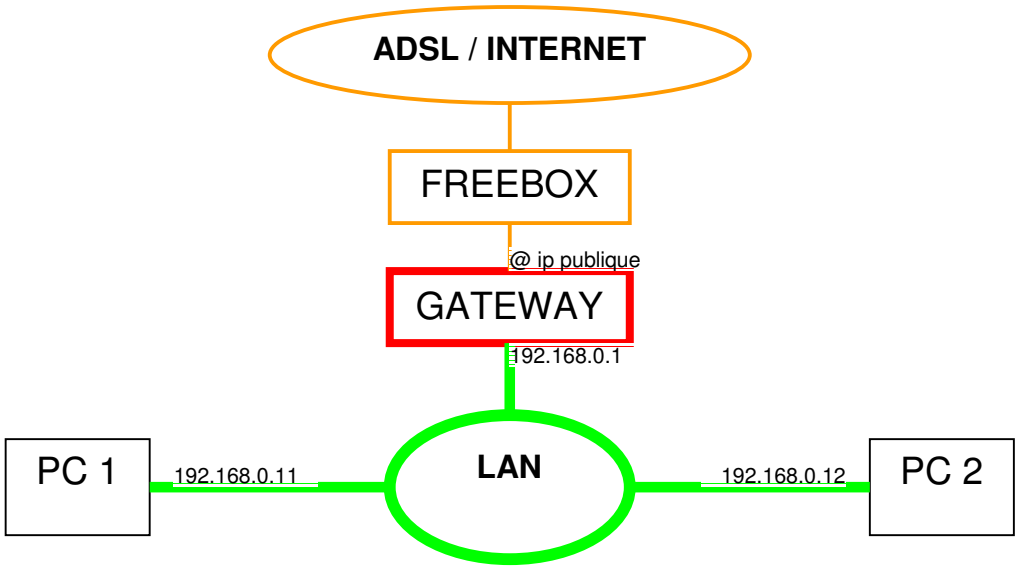
Il nous faut maintenant configurer tous nos appareils.

Si nous optons pour la configuration automatique, nous n'avons rien à faire : le RP 614 possède en interne un serveur DHCP pré-configuré, et il se charge donc de piloter la configuration des PCs, également configurés par défaut en DHCP (sous Windows).
Tout au plus devons nous indiquer au RP 614 comment il se connecte à Internet via la Freebox : connexion sans identification, en client DHCP. Notez que ce dernier réglage reste valide même si nous optons pour une configuration manuelle des autres paramètres.

Si nous optons pour la configuration manuelle, nous adoptons les réglages suivants :

- Pour toutes les machines, le masque sera 255.255.255.0
- L'adresse IP du RP 614 (c'est lui la passerelle) est par défaut 192.168.0.1, qui convient parfaitement.
- Nous configurons donc cette adresse comme valeur de « passerelle » sur les deux PCs.
- Nous configurons également cette adresse comme valeur de « DNS » sur les deux PCs, car le RP 614 joue pour nous le rôle de DNS (il fait relais…)
- Nous réglons l'adresse 192.168.0.11 pour le PC 1.
- Nous réglons l'adresse 192.168.0.12 pour le PC 2.

Une fois ces réglages mis en oeuvre, notre réseau est totalement opérationnel. Nous pouvons atteindre les différentes machines présentes sur Internet grâce à leur nom symbolique. En interne, nous pouvons atteindre nos machines en les désignant grâce à leur adresse IP.



Le réseau final configuré

Dans cette configuration, les différentes machines qui constituent le réseau privé n'ont pas de raison d'embarquer des éléments de protection tels que des firewalls logiciels. Ces derniers peuvent d'ailleurs poser des problèmes lors de l'utilisation de certaines fonctions entre deux ordinateurs du réseau interne. Il est donc souvent préférable de les supprimer.

3.4 Vérification du bon fonctionnement

Afin de nous assurer que tout va bien, ou pour trouver la cause d'un dysfonctionnement, nous disposons de différents outils (en ligne de commande) permettant de faire « fonctionner » le réseau. Voyons rapidement comment les utiliser…

Supposons que vous ayez branché votre Dreambox sur votre réseau local, mais que vous n'arriviez pas à télécharger des plugins par exemple. Vous avez affecté l'adresse IP 192.168.0.10 à la Dreambox. Un PC est également présent sur le réseau, à l'adresse 192.168.0.2.

Depuis une invite de commande DOS, vous exécutez les commandes suivantes :

```
ping 192.168.0.10
```

Vous devez obtenir en réponse une suite de lignes indiquant qu'une réponse en provenance de l'adresse demandée a été reçue, ainsi que le temps de réponse. Si tel n'est pas le cas, c'est soit que vous avez mal réglé l'adresse IP de la Dreambox, soit que le niveau physique (câbles…) ne fonctionne pas. Vérifiez tout cela…

Si cela fonctionne, alors vous pouvez vous connecter à la Dreambox depuis votre PC :

```
telnet 192.168.0.10
```

Après avoir saisi le login (root) et le mot de passe (dreambox ou sandbox sur POD), vous pouvez taper les commandes suivantes :

Ping 192.168.0.1

Tout comme cela vous indiquait que la Dreambox « répondait » au PC ci-avant, cette fois ci, cela vous indique que la passerelle répond à la Dreambox. Cela doit fonctionner. Vérifiez également que vous avez bien configuré l'adresse de la passerelle…

Si tout est OK, vous pouvez faire le test suivant :

```
ping www.yahoo.fr
```

Cette fois-ci, vous allez solliciter toute la chaine de transmission IP.

Si vous obtenez une réponse « Unknown host name » ou approchante, c'est que la résolution de nom via le DNS ne marche pas. Si votre routeur Internet fais relais (c'est notre cas), vérifiez que vous avez bien configuré son adresse (192.168.0.1) dans les paramètres de la dreambox. Si votre routeur ne fait pas relais, vous devez configurer l'adresse IP du DNS de votre fournisseur d'accès Internet. Votre routeur peut vous donner cette information mais, dans ce

cas, il est probablement plus simple de vous placer en DHCP pour obtenir automatiquement les réglages appropriés.

Si la commande fonctionne, c'est à dire si vous obtenez des réponses du site Yahoo, votre liaison est normale. Il est alors probable que ce soit le site de téléchargement que cherches à atteindre la Dreambox qui ne soit plus opérationnel.

Pour vérifier cela, utilisez les commandes suivantes :

```
cd /tmp
wget http://www.microsoft.com/index.htm
```

Cela doit télécharger une page html depuis le site de Microsoft. Si le téléchargement fonctionne, c'est que tout est correctement configuré : votre Dreambox accède bien à Internet.

4 LA SÉCURITÉ DE VOTRE RÉSEAU

4.1 Prendre conscience des risques

Dès que l'on connecte entre-elles plusieurs machines, il convient de mesurer quels sont les risques potentiels encourus, au regard de l'importance de chaque machine. Cette considération n'est pas à faire à la légère : par défaut, les ordinateurs sont des systèmes très ouverts, on pourrait même dire des passoires, et le risque de perte d'informations est toujours présent. La connexion à un réseau local augmente de façon significative les risques encourus, mais ce n'est rien comparé aux risques liés à une connexion à Internet.

La toile est en effet en permanence utilisée pour véhiculer toutes sortes d'attaques, lancées par des individus sans scrupules. En dehors des « simples » virus, on trouve par exemple aussi toutes les tentatives d'intrusion pour l'hébergement de sites pirates, et plus encore…

Donc le risque existe, mais s'il existe, il est aussi maîtrisable, pour peu que l'on s'en préoccupe. Il n'est pas nécessaire d'être ingénieur en sécurité des systèmes pour être capable de protéger simplement mais efficacement son installation : beaucoup de bon sens et une petite dose de technique suffisent à créer une base solide.

4.2 Maîtriser les risques

Si nous reprenons notre analogie du réseau routier, nous pouvons comparer notre ordinateur (ou plus globalement notre réseau local) comme notre maison : elle est connectée au réseau publique, et comme elle est connue (elle a une adresse), elle est potentiellement vulnérable.

Pourtant, bien que le risque d'agression sur notre maison existe, nous arrivons à dormir la nuit. Alors réfléchissons simplement à cette question : pourquoi ?

La réponse est simple : parce que nous avons mis application deux concepts, nous permettant d'assurer un niveau de sécurité pour notre maison compatible avec nos attentes.

Lesquels ?

- Le bon sens avec des habitudes, des usages adaptés au risque,
- La technique, avec des outils de protection également adaptés.

Ces deux concepts répondent à deux formes de risques distincts, mais complémentaires :

- Le risque d'intrusion par un inconnu malveillant,
- Le risque de dérive de comportementale de toute personne qui serait entrée.

Explications :

Si l'on vous demande comment vous protégez votre maison, vous allez répondre des choses comme : j'ai une alarme, j'ai des serrures haute sécurité, des portes blindées, etc.

Ces éléments techniques visent à vous protéger d'un risque, bien réel : celui de l'intrusion. Vous mettez en œuvre des moyens techniques qui permettent de garantir (tout est relatif) que, sans votre accord, personne ne pourra pénétrer chez vous.

Sont-ce là les seuls moyens que vous mettez en œuvre pour vous protéger ? Oui ?

En fait je suis sur que non. Inconsciemment, vous appliquez également des règles de conduites, qui vous dictent ce qu'il convient de faire en cas de tentative d'intrusion, ou de dérive comportementale d'une personne présente chez vous.

En effet, si quelqu'un sonne à votre porte, vous n'ouvrez pas tout de suite, vous cherchez d'abord à identifier le visiteur. Si vous avez un doute, vous ne le laissez pas entrer. Si vous l'avez identifié, et qu'il est de confiance tout va bien, mais dans le cas contraire, le fait que vous ouvriez la porte ne signifie pas que vous le laissiez entrer, ce n'est qu'une étape. Finalement, même si vous laissez entrer une personne, elle est implicitement surveillée : vous vous assurez en permanence qu'elle respecte des règles de bonne conduite adaptée. Si tel n'est pas le cas, vous demandez à la personne de sortir !

Vous utilisez donc bien deux concepts pour votre sécurité : des bonnes habitudes, et des moyens techniques. Et bien en matière de sécurité informatique, il en va exactement de même, nous allons voir comment…

4.2.1 Les bonnes habitudes

Partant du fait que vous êtes conscient des risques liés à votre connexion à Internet, la première chose à faire c'est … d'adopter dès les début les bonnes habitudes, de vous forcer à être prudent.

En effet, dans le monde de l'informatique, on a tendance à toujours rechercher l'outil qui va faire le travail à notre place. Aussi, dès que l'on parle de sécurité informatique, on pense firewall, anti-virus etc.

Or ces outils, bien que souvent efficaces, ne pourront jamais parer à des manipulations inconsidérées, à des imprudences de votre part. Ils ne seront là que pour vous assister dans la sécurisation de vos systèmes, mais jamais pour l'assumer à votre place.

Il en va de même que pour votre maison : les outils se chargent principalement de la sécurité physique des portes, mais pas de la surveillance et de l'identification des personnes.

Si l'on considère que vous allez mettre en œuvre tous les outils nécessaires à la sécurisation des portes (nous verrons cela par la suite), il vous reste principalement à gérer la surveillance des personnes qui sonnent à votre porte, et que vous allez laisser entrer.

Dans le monde informatique, une personne c'est un programme. De tous les programmes que votre ordinateur va voir passer, certains seront installés à votre initiative, et ceux-ci sont réputés fiables, donc vous ne vous en préoccuperez pas (suite bureautique, tous les logiciels achetés dans le commerce d'une façon générale).

En plus de ces programmes fiables, votre ordinateur va recevoir, notamment par le biais de la messagerie Internet (les eMails !) des données dont certaines peuvent être des programmes.

Ces derniers constituent les intrus potentiels : ceux qui cherchent à entrer, et qui ont déjà passé la porte ou sont sur le point de le faire !

Les programmes malveillants adoptent en effet la forme la plus courante des données que vous avez l'habitude de laisser entrer, par exemple votre courrier électronique. Dissimulés dans des courriers factices, ils tentent de franchir la barrière de sécurité ultime : votre vigilance. Si vous les laissez entrer, ils se déchaînent et dévastent votre système, votre maison.

Ainsi, la plupart des virus récents, et particulièrement malveillants, sont ce que l'on appel des vers : ils s'infiltrent le plus souvent via un courrier électronique porteur, puis utilisent les données trouvées sur votre système pour se propager (votre carnet d'adresses, vos archives d'eMails) pour, finalement entrer dans une phase de destruction une fois leur travail de propagation fait.

Pour ce protéger de ce type d'intrusion, il n'y a qu'une seule solution : DOUTER DE TOUT CE QUE VOUS RECEVEZ !

Tout eMail notamment, avant d'être ouvert, doit être inspecté méticuleusement afin d'y détecter toute trace de tentative d'intrusion. Un bon anti-virus, constamment maintenu à jours en ce qui concerne sa base de données de virus, est un assistant très efficace dans ce travail, mais il n'est pas infaillible !

En effet, le principe de fonctionnement d'un anti-virus repose sur la reconnaissance de virus connus. Lorsqu'un nouveau virus est lancé sur Internet, il n'est par définition pas connu, et passe donc au travers des protections anti-virus !

Ceci étant, on s'aperçoit rapidement que, si l'on a les bons réflexes, ont est pas sujet à de telles attaques. En effet, les moyens de dissimulation des virus dans les eMails par exemple, sont aujourd'hui très limités. Les virus ne peuvent être véhiculés que sous la forme de pièces jointes, et tant que vous n'ouvrez pas ces pièces jointes, vous ne risquez rien.

En clair, quand vous recevez un courrier, vous pouvez en lire le contenu sans risque, mais vous ne devez JAMAIS ouvrir la moindre pièce jointe sans en avoir auparavant identifié précisément la nature. En cas de doute, la seule option possible est…la corbeille ! On ouvre pas un eMail ou une pièce jointe dont on est pas absolument sur !

A ce sujet, précisons que les images et les sons sont, comme les programmes, des pièces jointes et que, sous le couvert d'un son, on peut trouver des virus.

Ainsi, le célèbre Win32.Nimda, qui a sévi voici quelques années, se propageait principalement par eMail, sous la forme d'une pièce jointe simulant la présence d'un inoffensif son…qui était en fait la souche virale !

Enfin, il convient d'ajouter que le simple fait d'avoir identifié l'expéditeur de l'eMail ne saurait constituer une sécurité suffisante : tous les vers actuels se propagent en utilisant votre carnet d'adresse, et se font passer pour vous ! S'ils le font chez vous, ils le font chez vos connaissances. Quand vous recevez un eMail contenant un fichier exécutable (un programme), en provenance de votre meilleur copain, avant de vouloir quelle bonne blague il vous envoi, ayez le réflexe de vous demander si, par hasard, il n'aurait pas besoin d'un coup de main pour supprimer les virus présents sur sa machine.
Plus subtiles encore, les vers récents utilisent des anciens eMails échangés par vous et vos proches, et conservés en archive, pour simuler des réponses à des sujets de conversation !

Bref, comme vous le voyez, les concepteurs de virus, bozos et autres piratins, sont toujours en avance d'un coup sur les systèmes de protection, et seule votre vigilance peut les empêcher de pénétrer sur votre système…

4.2.2 Le firewall

Après ce chapitre long et insistant sur les bonnes habitudes, voyons maintenant ce que nous pouvons faire pour gérer le problème finalement le plus simple : la sécurisation des portes de notre réseau !

Comme pour votre maison, ce domaine dispose d'outils efficaces, que vous pouvez facilement mettre en œuvre pour apporter le niveau de sécurité convenable. Véritable concentré de porte blindé, associé à des serrures de haute sécurité et à une alarme hightech, le firewall est aujourd'hui un de ces outils…indispensable !

Tout comme vous n'envisagez pas un seul instant de laisser portes et fenêtres ouvertes en permanence, il n'est pas question de laisser tout et n'importe qui venir regarder de trop près à ce qui se passe sur votre réseau local, et plus encore, sur vos machines.

Dans le chapitre consacré à la translation d'adresse (et aux passerelles), nous avons vu que cette technique permet déjà, dans une certaine mesure, de protéger votre système.

En effet, dès lors que vous passez par un système de translation, la réalité de votre réseau local n'est pas visible de l'extérieur : seule la passerelle est visible. Elle est donc également vulnérable et, comme elle est reliée directement à votre réseau local, si elle est attaquée et prise (hackée), alors l'intérieur de votre réseau le sera à son tour.

Une simple translation d'adresse n'est donc pas suffisante pour apporter un niveau de sécurité satisfaisant, mais on considère qu'elle est cependant indispensable.

Si vous protégeons également la passerelle alors, par transitivité, nous protégeons notre réseau local. Ce travail est confié au firewall…

Le firewall, c'est le gardien, le cerbère de la porte et le maître des clefs. Son but est de contrôler toute tentative d'entrée (ou de sortie) de données au travers de la passerelle, et d'autoriser ou d'interdire ces passages de données. Il agit nécessairement sur un point de passage central, isolant un réseau d'un autre, donc sur une passerelle, et les fonctions sont donc techniquement liées l'une à l'autre.

Le firewall travail au niveau réseau IP (pas au niveau Ethernet).

Techniquement, il va analyser la nature de chaque paquet de données arrivant sur le flux Ethernet. S'il ne s'agit pas d'un flux IP, les données seront rejetées (sauf si vous l'autorisez explicitement, mais c'est très rare).

Si les données sont dans un flux IP, le firewall va s'assurer que le service qui est demandé au travers du flux de données est bien autorisé. Si tel n'est pas le cas, les données sont détruites.

Comment est réalisée la vérification ?

Et bien elle s'appuie sur les informations que contiennent les trames IP, à savoir les adresses d'expéditeur et de destinataire (que vous connaissez déjà) ainsi que les ports.

Késako un port ?

Un port, c'est une valeur numérique de 0 à 65535, qui est présente dans toute transmission de données IP. Il y en a toujours deux : un pour l'expéditeur et un pour le destinataire.

Au niveau de l'expéditeur, le port est souvent sans importance (il y a de rares exceptions, comme pour les réponses des services DNS). Il identifie seulement un point d'entrée pour les données de retour à la demande envoyée. Une même adresse peut donc être à l'origine d'environ 65000 demandes simultanées.

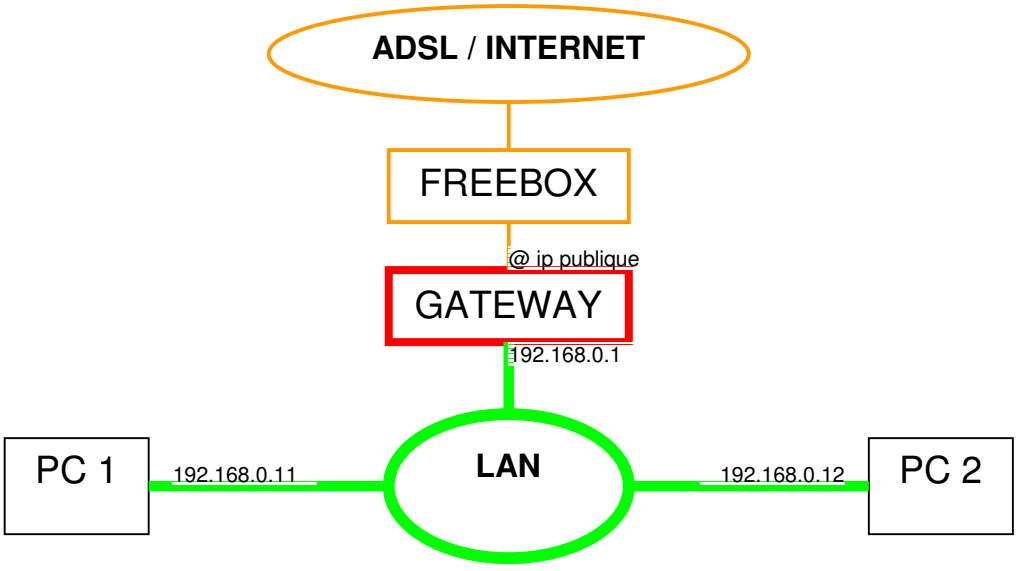
Au niveau du destinataire, en revanche, le port revêt une importance capitale : il identifie sans ambiguïté possible le service recherché. Les ports sont en effet normalisés. Ainsi, le port 23 correspond au service telnet. Le port 80 correspond au service http (service de pages WEB), et le port 443 au service https (service de pages WEB sécurisé, crypté).

Ainsi, si vous tentez de demander une page web sur le port 23 d'une machine, vous n'obtiendrez pas de réponse, ou une réponse totalement incohérente : ce service n'est pas le bon.

Un firewall va donc déterminer, en fonction des éléments de configuration que vous lui aurez indiqué, quels sont les transmissions de données qui sont autorisées au travers de la passerelle, pour toutes les combinaisons possibles.
Toute transmission qui n'est pas explicitement autorisée, est implicitement interdite, et aboutie à la destruction des données transmises (leur élimination du réseau).

4.2.3 Configuration d'un firewall

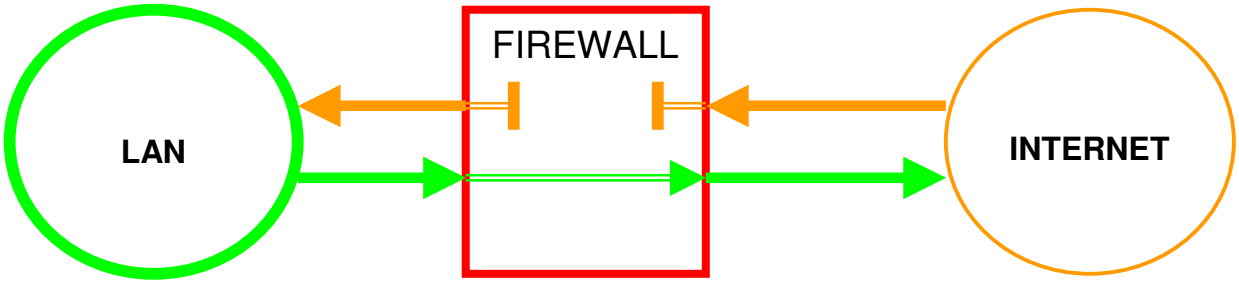
Pour illustrer ce point, reprenons notre exemple de réseau local : nous disposons d'un réseau constitué d'un routeur d'accès Internet connecté à une Freebox. Sur le réseau, sont présentes deux machines PC1 et PC2. Reportez-vous au chapitre correspondant pour avoir le détail de la configuration de ce réseau. Le schéma ci-dessous en reprend la structure.



Le réseau à sécuriser

Nous voulons protéger notre réseau contre les intrusions. Le réseau n'héberge pas de services à destination du publique. Nous ne sommes finalement que des utilisateurs d'Internet. Cela correspond à la majorité des utilisateurs…

Dans ces conditions, nous n'avons besoin d'ouvrir aucune porte d'entrée. Par contre, nous ne voulons pas de limitations sur notre capacité à sortir vers Internet. La configuration de défaut des firewall grand publique correspond à ce type d'usage. On peut la représenter ainsi :



Comme l'illustre ce schéma, tout trafic en provenance du LAN et à destination d'Internet va pouvoir traverser le firewall, tout en étant surveillé de près.
A l'inverse, tout trafic en provenance d'Internet et à destination du LAN va être bloqué par le firewall, et ne peut donc entrer sur le LAN pour attaquer vos machines.

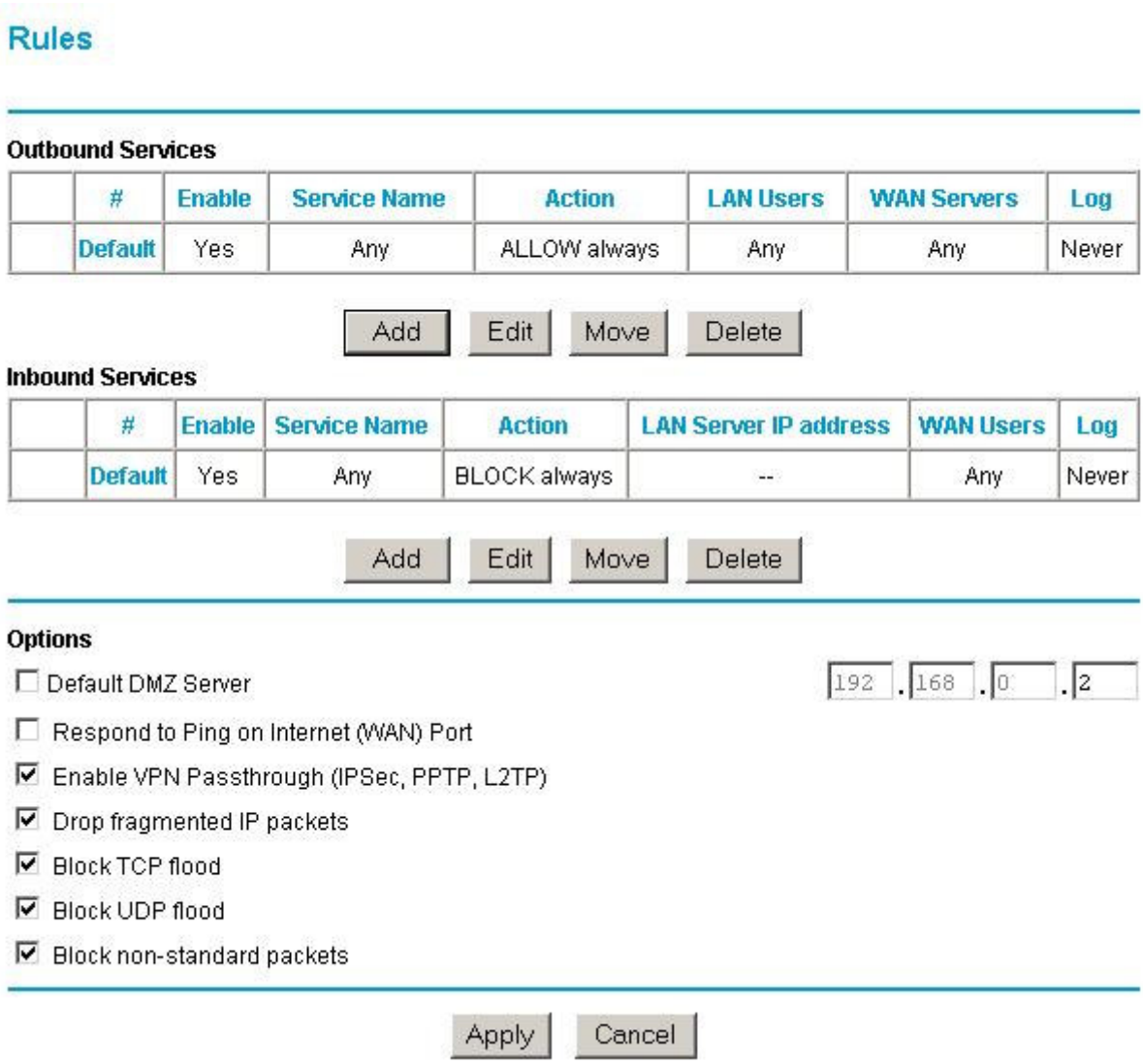
Ce fonctionnement amène deux remarques :

- La passerelle, de ce point de vue, est située à l'intérieur du firewall (dans le carré rouge) et, de ce fait, elle bénéficie du même niveau de protection que le reste du réseau.

- Le trafic en provenance d'Internet n'est pas complètement bloqué : le firewall laisse passer les données qui sont des réponses à des demandes à l'initiatives du LAN. Sans cela, vous ne pourriez jamais récupérer la moindre donnée, et votre liaison Internet n'aurait que peu d'intérêt. Ainsi, vous ne pourriez pas visualiser le contenu d'une page WEB, bien que le serveur vous ai envoyé le contenu. A tout moment, le firewall sait quelles sont les demandes de données qui ont été émises vers des machines extérieures, il sait par qui et vers qui (table de translation), et il autorise des données en retour à le traverser. Dès que la liaison de demande est coupée, la voie de retour est automatiquement fermée. A noter que cette voie de retour n'est utilisable que par le destinataire de la demande, dans le cadre de cette demande et de rien d'autre. La sécurité est donc assurée.

Comment ce type de configuration est-elle mise en œuvre ?

Par défaut, elle l'est sur la plupart des routeurs d'accès Internet, mais aussi sur la protection firewall de WindowsXP. Sur un routeur Netgear, nous pouvons le vérifier au travers de l'interface d'administration WEB. La page « rules » nous indique quelles sont les règles qui régissent les autorisations de transmissions.



Configuration simple d'un firewall Netgear

Cette écran montre que les services sortants (Outbound services) sont autorisés en permanence, pour toute machine du réseau local (LAN) vers toute machine d'Internet (WAN, le réseau distant).

A l'inverse, les services entrants (Inbound services) sont bloqués de façon permanente, quelle que soit le type de service et de machine demandé.

A notez également les quelques options « bonus » présentes sous ces règles fondamentales, que proposent aujourd'hui la majorité des routeurs d'accès (protection contre les attaques de saturation, autorisation de passage pour les tunnels de sécurité VPN, etc).

4.2.4 Accéder à sa Dreambox depuis Internet

Comme vous ne voulez jamais rien rater, vous souhaitez pouvoir accéder à votre Dreambox depuis votre lieu de travail, pour pouvoir programmer des enregistrements par exemple.

Comme vous êtes également bien conscient des problèmes de sécurité, et rigoureux, vous ne souhaitez pas faire les choses sans réfléchir, et vous avez également mis en place un firewall.

Quelles sont les modifications à mettre en œuvre pour pouvoir assouvir votre besoin sans prendre trop de risques ?

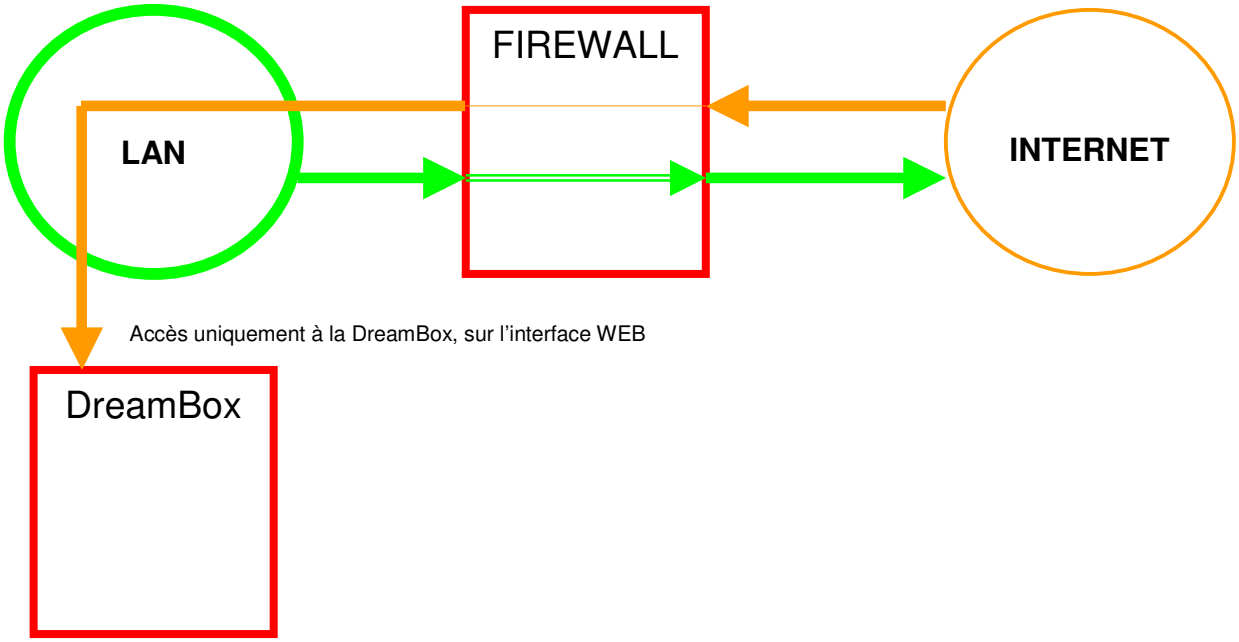
La première étape est toujours la même : avoir du bon sens !

L'accès à votre Dreambox va être « publique », possible par tout un chacun sur Internet, pourquoi seulement vous ? Donc il convient de verrouiller correctement cet accès, et pour cela, le minimum sera d'utiliser des mots de passes efficace.

Lorsque vous vous connectez à votre Dreambox depuis un navigateur, vous devez vous identifier. Le mot de passe de l'utilisateur root est connu de tous, donc il convient de le changer, et d'utiliser un mot de passe qui ne soit pas évident. Du bon sens que diable !

La seconde étape va consister à permettre au trafic, en provenance d'Internet cette fois, à atteindre votre Dreambox. Il n'est cependant pas question d'autoriser tout et n'importe quoi. Nous allons en effet faire une brèche dans la protection firewall, et cette brèche doit être parfaitement contrôlée. Voyons comment faire…

Ce que nous voulons obtenir précisément, c'est cela :



Principe d'exposition d'un service sur Internet

Pour que cela soit possible, nous devons permettre à une machine (la DreamBox) qui ne possède qu'une adresse privée, à être accessible depuis un réseau publique.

Cela n'étant pas possible, nous allons tricher.

En fait, nous allons exposer le service désiré au niveau de la seule machine qui possède une adresse publique, c'est à dire la passerelle, donc également le firewall.

Le firewall va donc recevoir les demandes de pages web en provenance des navigateurs. Que va-t-il en faire ? C'est à nous de le lui dire !

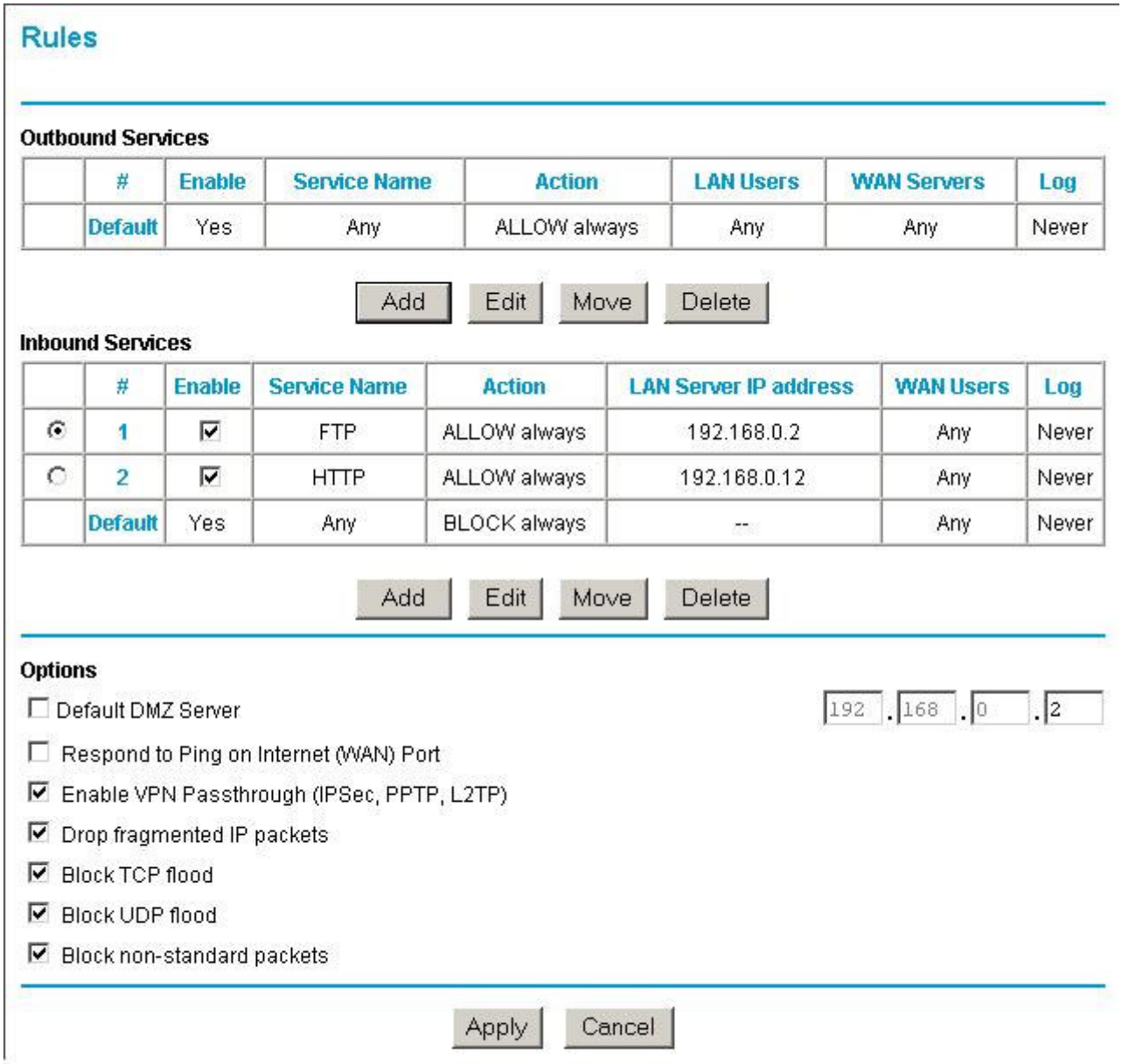
Pour cela, nous allons configurer une règle de translation inversée. C'est une règle qui précise, pour un trafic entrant sur un service donné, QUI dans le réseau privé va traiter réellement ce trafic. Dans notre cas, c'est la DreamBox.

Cette dernière se trouve sur l'adresse privée 192.168.0.12 (par exemple). Le service exposé est http, qui se trouve être le port 80. Nous allons donc configurer une règle spéciale sur notre firewall :

- Pour TOUT trafic ENTRANT sur le PORT 80
- Le LAISSER PASSER uniquement VERS 192.168.0.12

A notre que, suivant la capacité de votre firewall, vous pouvez au passage modifier le port utilisé, afin de « masquer » le port réel qu'utilise votre machine. Ainsi, vous pouvez configurer votre DreamBox pour qu'elle expose le service http sur le port 1080 (par exemple) et indiquer au firewall qu'il doit transformer la demande de service pour qu'elle vise ce port, et pas le port 80 initialement demandé. Les routeurs Netgear ne proposent pas cette technique dite du « Port Mapping ».

Voici, à titre d'exemple, la configuration obtenue sur notre routeur. A noter qu'il y a aussi une règle en place pour l'accès à un serveur FTP, présent sur l'adresse 192.168.0.2.



Configuration d'un routeur Netgear exposant deux services FTP et HTTP