Série

VPN Booster 32

- VPN Booster 32
- VPN Booster 32g
- VPN Booster 32i
- VPN Booster 32V
- VPN Booster 32Vg

Guide de l'utilisateur

Avertissement

Les informations contenues dans ce manuel sont susceptibles de modification sans préavis.

BeWAN systems ne peut être tenue pour responsable si une non-conformité partielle apparaît entre ce manuel et le produit qu'il décrit, ni des éventuels dommages accidentels directs ou indirects consécutifs à l'utilisation de ceux-ci.

Edition avril 2005.

Marques déposées et copyright :

- BeWAN, VPN Booster et le logo BeWAN systems sont des marques déposées de BeWAN systems.
- Microsoft, Windows sont des marques déposées de Microsoft Corporation aux Etats-Unis et/ou dans d'autres pays.
- Macintosh est une marque d'Apple Computer, Inc. déposée aux Etats-Unis et dans d'autres pays.
- i-minitel est une marque déposée par France Télécom.

De même, les noms des produits cités dans ce manuel à des fins d'identification peuvent être des marques commerciales, déposées ou non par leurs propriétaires respectifs.

Table des matières

Partie 1 : Introduction

Félicitations, vous venez d'acquérir un VPN Booster, un routeur performant et ergonomique.

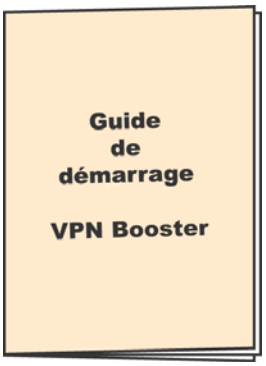
Ce routeur va vous permettre de fédérer en toute sécurité les ordinateurs de votre entreprise en un réseau communiquant grâce notamment à :

- son commutateur Ethernet intégré, qui vous permet de raccorder directement jusqu'à 4 ordinateurs ou plus de 4 ordinateurs via un concentrateur Ethernet externe (non fourni). Le réseau local peut être constitué de différents types d'ordinateurs (PC sous Windows ou Linux, Macintosh, etc.).
- un port WAN, qui vous permet de raccorder un modem xDSL ou un modem câble.
- un port imprimante USB (pour la Série VPN Booster 32 uniquement) qui vous permet de raccorder une imprimante à votre routeur et ainsi de la partager sur le réseau local.
- un port ISDN (VPN Booster 32 i uniquement) qui vous permet de raccorder votre ligne RNIS grâce au câble fourni.
- un point d'accès réseau sans fil (VPN Booster 32 g / 32 Vg) afin de connecter des stations clientes Wireless.

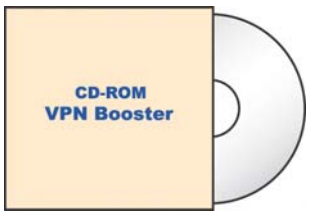
Le VPN Booster gère dynamiquement la connexion à Internet et son partage sur le réseau local. Ce dernier est protégé efficacement grâce aux nombreuses fonctions dont dispose le routeur (firewall complet, VPN, défenses DoS, NAT, gestion de plages horaires, etc.).

Contenu de la boîte du VPN Booster

Dans la boîte du VPN Booster, vous devez trouver, en plus du routeur, les éléments suivants :



Guide de démarrage



CD-ROM Routeurs VPN Booster

Remarque : si vous disposez du VPN Booster 32 g / 32 Vg, vous devez trouver également 2 antennes externes destinées à être vissées à l'arrière du routeur.

Câble d'alimentation électrique

Câble Ethernet droit (bleu)

Câble RNIS (VPN Booster 32 i uniquement)

Adaptateur téléphonique (VPN Booster 32 V / 32 Vg uniquement)

Avant de commencer

Nous considérons dans ce manuel que les conditions suivantes sont réunies :

1. Vos ordinateurs sont équipés de cartes Ethernet.
2. Vous disposez d'un accès xDSL (ADSL, SDSL) et/ou d'un accès Internet par le câble et/ou d'une ligne RNIS (pour le VPN Booster 32 i).
3. Vous avez souscrit un abonnement auprès d'un fournisseur d'accès Internet (FAI) et celui-ci vous a confirmé vos paramètres de connexion (identifiants, mots de passe, serveurs DNS, etc.).

Assistance Technique : Si vous rencontrez des difficultés, l'assistance technique sur le matériel est assurée par le Support Technique de BeWAN systems au **08 92 16 22 92** (Tarif Audiotel 0,34 € TTC/min).

- ✓ du lundi au jeudi, de 9h à 13h et de 14h à 18h.
- ✓ le vendredi, de 9h à 13h et de 14h à 16h30.

Précautions d'utilisation

⚠ Lisez attentivement les instructions de sécurité suivantes avant d'installer ou d'utiliser le VPN Booster. Veillez à respecter rigoureusement les précautions d'emploi.

Emplacement

- Evitez d'utiliser, de placer et de conserver l'appareil dans des endroits exposés à une lumière intense ou à des températures élevées ou près de sources de chaleur.
  Des températures élevées risquent de déformer le boîtier. La température maximum ne peut dépasser 40°C.
- Conservez l'appareil dans un endroit sûr et bien ventilé.
- Evitez d'installer l'appareil dans un endroit humide ou poussiéreux.
  Vous risqueriez entre autres de provoquer un incendie ou une décharge électrique.
- Ne placez pas l'appareil sur un élément non stable.
  Si l'appareil tombe, cela pourrait causer de sérieux dommages.
- L'emplacement de la prise de courant secteur doit être facilement accessible.
  La tension secteur doit correspondre aux indications figurant sur la plaque signalétique de l'adaptateur électrique.
- Conservez l'appareil hors de portée des enfants.

Entretien et maintenance

- Veillez à ne pas ouvrir, désassembler ou modifier une partie de l'appareil.
  Tout désassemblage ou modification pourrait provoquer une forte décharge électrique. Les inspections internes, les modifications et les réparations doivent impérativement être effectuées par des techniciens agréés et qualifiés.
  L'ouverture de l'appareil ou toute modification interne entraînera la perte de la garantie.
- Débranchez le cordon d'alimentation de l'appareil avant de le nettoyer.
- Pour nettoyer l'appareil, n'utilisez pas certains produits chimiques pouvant endommager les matières plastiques. N'utilisez pas de substances contenant de l'alcool, du benzène, du diluant ni d'autres produits inflammables. L'emploi de ces produits pourrait provoquer un incendie.
- Ne mettez pas l'appareil en contact avec de l'eau ou d'autres liquides.
  Aucun liquide ne doit pénétrer à l'intérieur de l'appareil. Si la partie externe de l'appareil entre en contact avec un liquide, essuyez-le à l'aide d'un chiffon doux et absorbant. Si un liquide ou une substance quelconque pénètre à l'intérieur de l'appareil, éteignez-le immédiatement ou débranchez le cordon d'alimentation de la prise électrique. Si vous continuez à l'utiliser, vous risquez de provoquer un incendie ou une décharge électrique.

Alimentation et câbles

- N'utilisez que les accessoires d'alimentation recommandés.
  L'utilisation de sources d'alimentation autres que celles recommandées pour ce matériel pourrait entraîner une surchauffe ou une déformation de l'appareil, et provoquer entre autres un incendie ou une décharge électrique.
- Veillez à ce que les câbles soient dans une position qui évite que quelqu'un puisse trébucher ou marcher dessus.
- Ne tentez pas d'acheminer les câbles dans un passage ou un endroit susceptible de les pincer.
- Veillez à ne pas couper, endommager ou transformer le cordon de l'adaptateur d'alimentation, ni à placer des objets lourds sur ce cordon.
  Vous risqueriez de causer un court-circuit qui pourrait provoquer un incendie ou une décharge électrique.
- Ne touchez pas le cordon d'alimentation si vos mains sont mouillées.
  Vous risqueriez de recevoir une décharge électrique.
- Lorsque vous débranchez le cordon, tenez la partie solide de la prise.
  En tirant sur la partie flexible du cordon, vous pouvez nuire à l'isolation ou dénuder le fil, et créer ainsi un risque d'incendie et de décharge électrique.
- Cessez immédiatement d'utiliser l'appareil si ce dernier se mettait à dégager de la fumée.
  Vous risqueriez sinon de provoquer un incendie ou une décharge électrique. Eteignez aussitôt l'appareil et débranchez le câble d'alimentation de la prise électrique.

Partie 2 : Installation du routeur

Raccordements du routeur

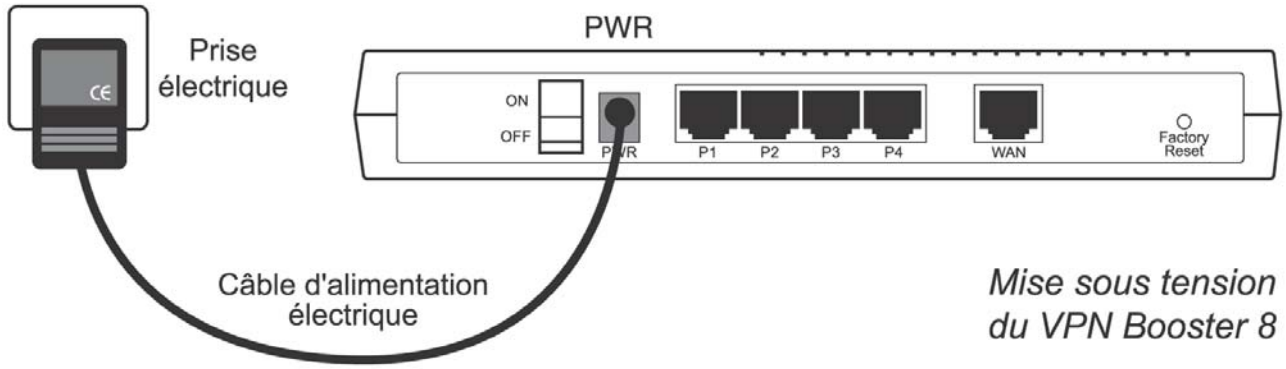
Nous distinguons dans ce chapitre le raccordement du VPN Booster 8 du raccordement de la Série VPN Booster 32.

Raccordements du VPN Booster 8

Raccordement du routeur à l'alimentation électrique

Pour mettre sous tension le VPN Booster 8, procédez comme suit :

1. Munissez-vous du câble d'alimentation électrique fourni dans l'emballage du routeur.
2. Raccordez l'extrémité du câble prévu à cet effet au connecteur **PWR** du routeur.
3. Raccordez l'autre extrémité du câble à une prise électrique compatible avec les spécifications imprimées sur le bloc d'alimentation.

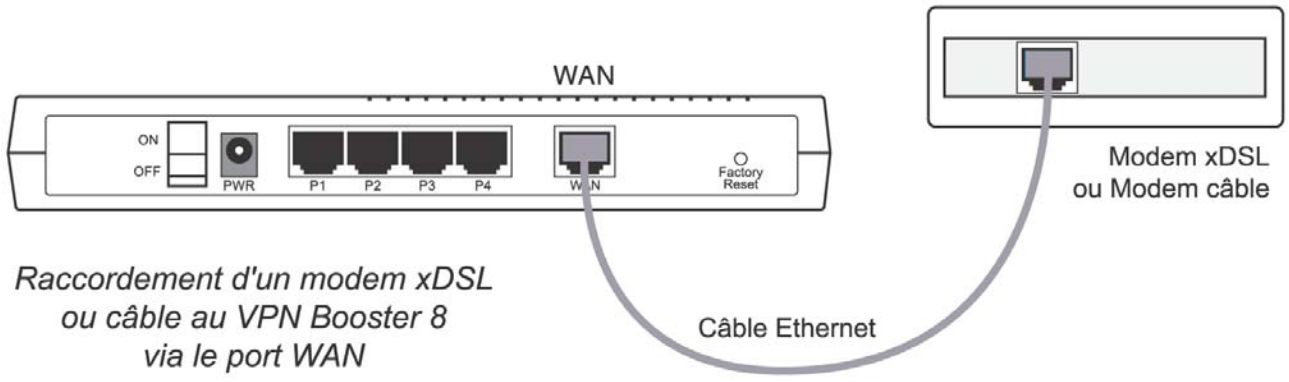


La mise sous tension du routeur suppose également le positionnement de l'interrupteur sur **ON**.

Raccordement du routeur au modem xDSL ou câble

Pour raccorder le VPN Booster 8 au modem xDSL (ADSL, SDSL) ou au modem câble, procédez comme suit :

1. Munissez-vous du câble Ethernet fourni généralement dans l'emballage du modem xDSL ou du modem câble.
2. Raccordez une extrémité de ce câble au port **WAN** du routeur.
3. Raccordez l'autre extrémité du câble au modem xDSL ou au modem câble (modems de type Ethernet).



Raccordement Ethernet

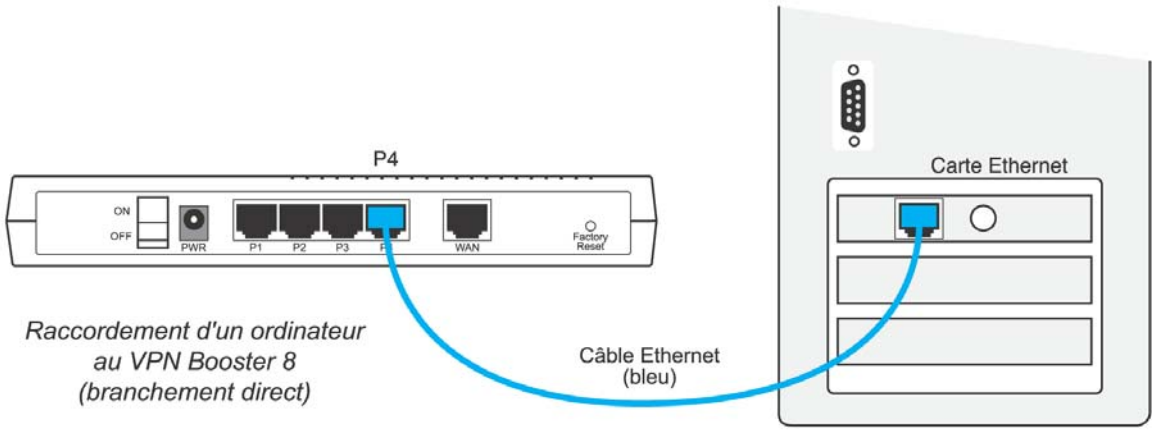
Le raccordement des ordinateurs du réseau local au routeur peut s'effectuer directement grâce au commutateur Ethernet intégré dans le routeur. Il peut également s'effectuer indirectement en utilisant un concentrateur Ethernet externe. Les deux types de raccordement peuvent être utilisés simultanément.

Raccordement direct

Pour raccorder directement un ordinateur au VPN Booster 8, procédez comme suit :

1. Munissez-vous du câble Ethernet bleu fourni dans l'emballage du routeur.
2. Raccordez une extrémité de ce câble à l'un des ports **P1** à **P4** du routeur.
3. Raccordez l'autre extrémité du câble au connecteur RJ45 de la carte Ethernet de l'ordinateur.

Vous pouvez ainsi raccorder directement jusqu'à 4 ordinateurs (câbles supplémentaires non fournis). Au-delà du quatrième ordinateur, vous devez utiliser un concentrateur Ethernet externe (voir section ci-dessous).

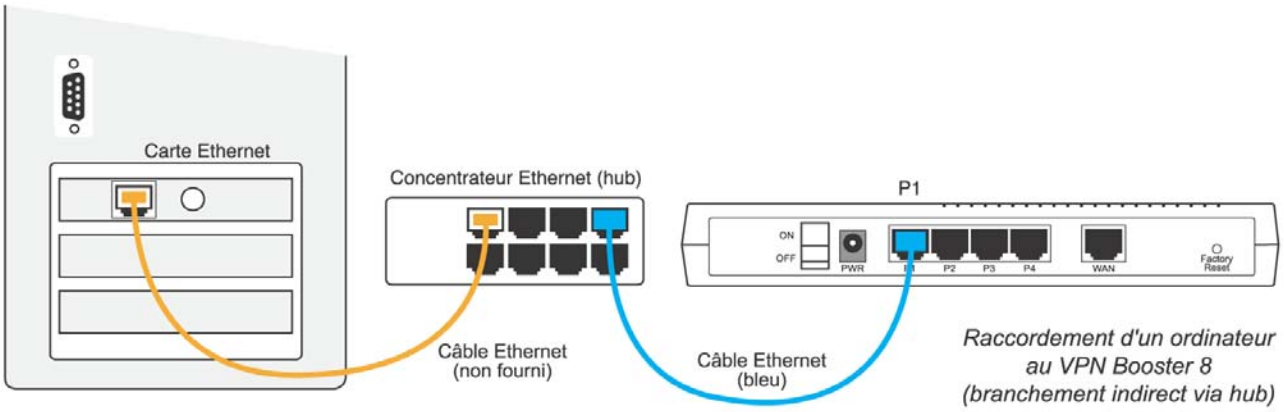


Raccordement indirect via concentrateur externe

Pour raccorder indirectement un ordinateur au VPN Booster 8 via un concentrateur Ethernet externe (non fourni), procédez comme suit :

1. Munissez-vous du câble Ethernet bleu fourni dans l'emballage du routeur.
2. Raccordez une extrémité de ce câble à l'un des ports **P1** à **P4** du routeur.
3. Raccordez l'autre extrémité à l'un des ports Ethernet du concentrateur Ethernet externe.

   Attention : grâce au système d'auto-détection du câblage, vous n'avez pas besoin d'utiliser de câble croisé.
4. Raccordez ensuite l'ordinateur au concentrateur Ethernet externe (câble supplémentaire non fourni).



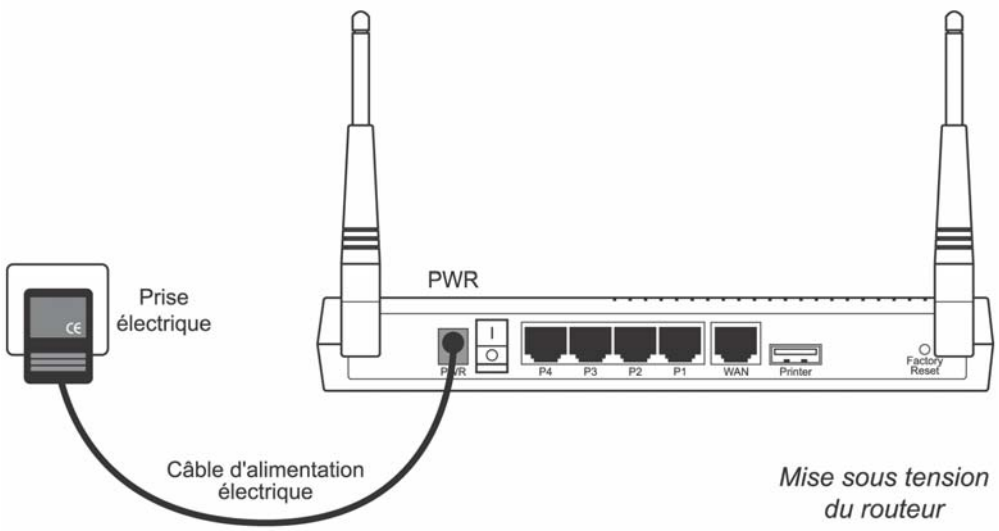
Vous pouvez bien entendu raccorder plusieurs ordinateurs et autres équipements au concentrateur Ethernet externe.

Raccordements des VPN Booster 32, 32 g et 32 i

Raccordement du routeur à l'alimentation électrique

Pour mettre sous tension le VPN Booster 32 / 32 g / 32 i, procédez comme suit :

1. Munissez-vous du câble d'alimentation électrique fourni dans l'emballage du routeur.
2. Raccordez l'extrémité du câble prévu à cet effet au connecteur **PWR** du routeur.
3. Raccordez l'autre extrémité du câble à une prise électrique compatible avec les spécifications imprimées sur le bloc d'alimentation.

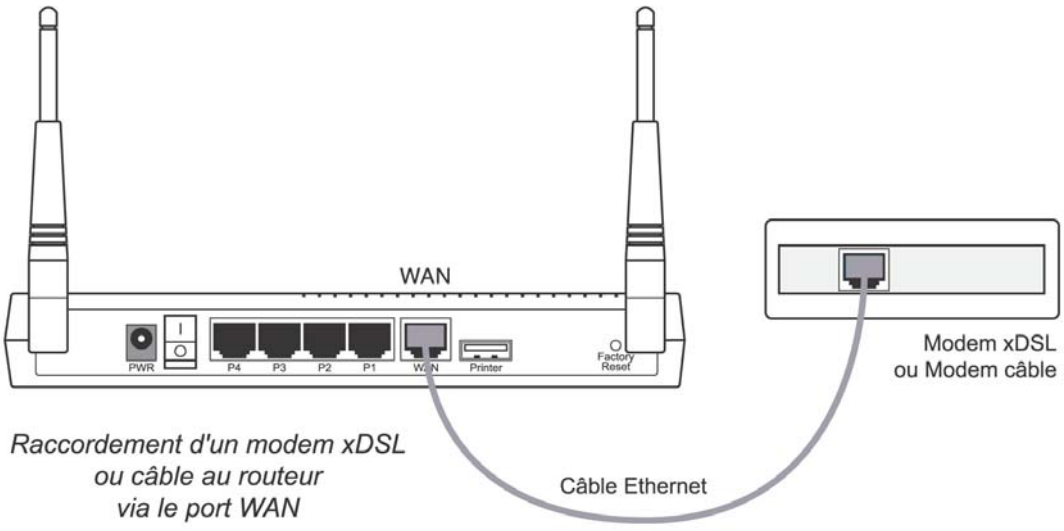


La mise sous tension du routeur suppose également le positionnement de l'interrupteur sur **ON**.

Raccordement du routeur au modem xDSL ou câble

Pour raccorder le VPN Booster 32 / 32 g / 32 i au modem xDSL (ADSL, SDSL) ou au modem câble, procédez comme suit :

1. Munissez-vous du câble Ethernet fourni généralement dans l'emballage du modem xDSL ou du modem câble.
2. Raccordez une extrémité de ce câble au port **WAN** du routeur.
3. Raccordez l'autre extrémité du câble au modem xDSL ou au modem câble (modems de type Ethernet).



Raccordement Ethernet

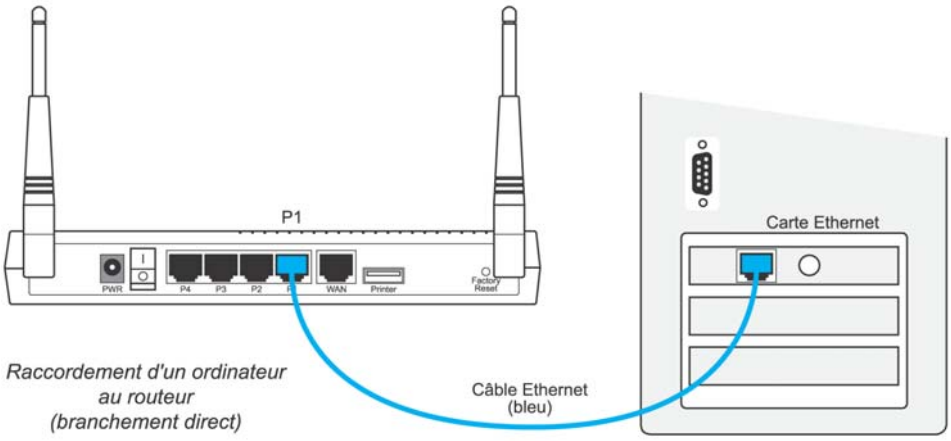
Le raccordement des ordinateurs du réseau local au routeur peut s'effectuer directement grâce au commutateur Ethernet intégré dans le routeur. Il peut également s'effectuer indirectement en utilisant un concentrateur Ethernet externe. Les deux types de raccordement peuvent être utilisés simultanément.

Raccordement direct

Pour raccorder directement un ordinateur au VPN Booster 32 / 32 g / 32 i, procédez comme suit :

1. Munissez-vous du câble Ethernet bleu fourni dans l'emballage du routeur.
2. Raccordez une extrémité de ce câble à l'un des ports **P1** à **P4** du routeur.
3. Raccordez l'autre extrémité du câble au connecteur RJ45 de la carte Ethernet de l'ordinateur.

Vous pouvez ainsi raccorder directement jusqu'à 4 ordinateurs (câbles supplémentaires non fournis). Au-delà du quatrième ordinateur, vous devez utiliser un concentrateur Ethernet externe (voir section ci-dessous).

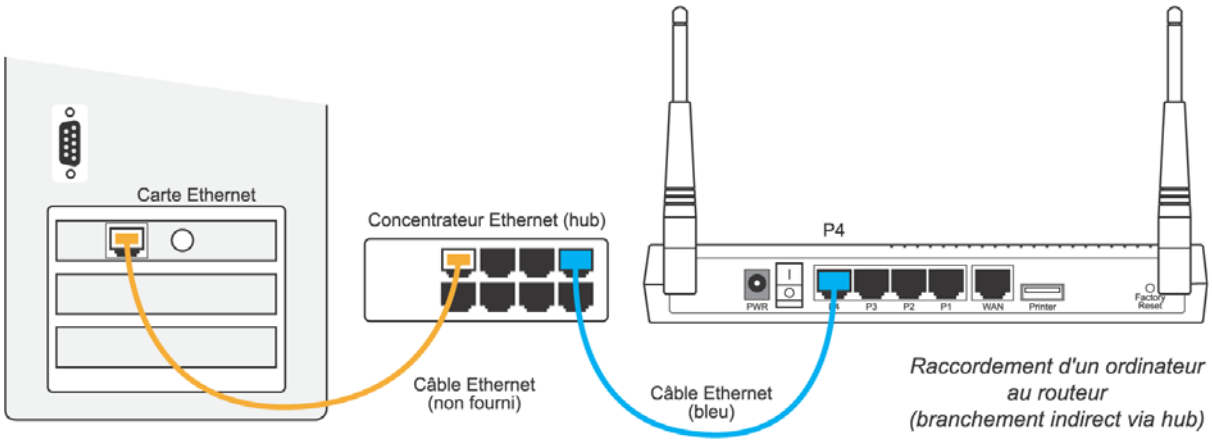


Raccordement indirect via concentrateur externe

Pour raccorder indirectement un ordinateur au VPN Booster 32 / 32 g / 32 i via un concentrateur Ethernet externe (non fourni), procédez comme suit :

1. Munissez-vous du câble Ethernet bleu fourni dans l'emballage du routeur.
2. Raccordez une extrémité de ce câble à l'un des ports **P1** à **P4** du routeur.
3. Raccordez l'autre extrémité à l'un des ports Ethernet du concentrateur Ethernet externe.

   Attention : grâce au système d'auto-détection du câblage, vous n'avez pas besoin d'utiliser de câble croisé.
4. Raccordez ensuite l'ordinateur au concentrateur Ethernet externe (câble supplémentaire non fourni).



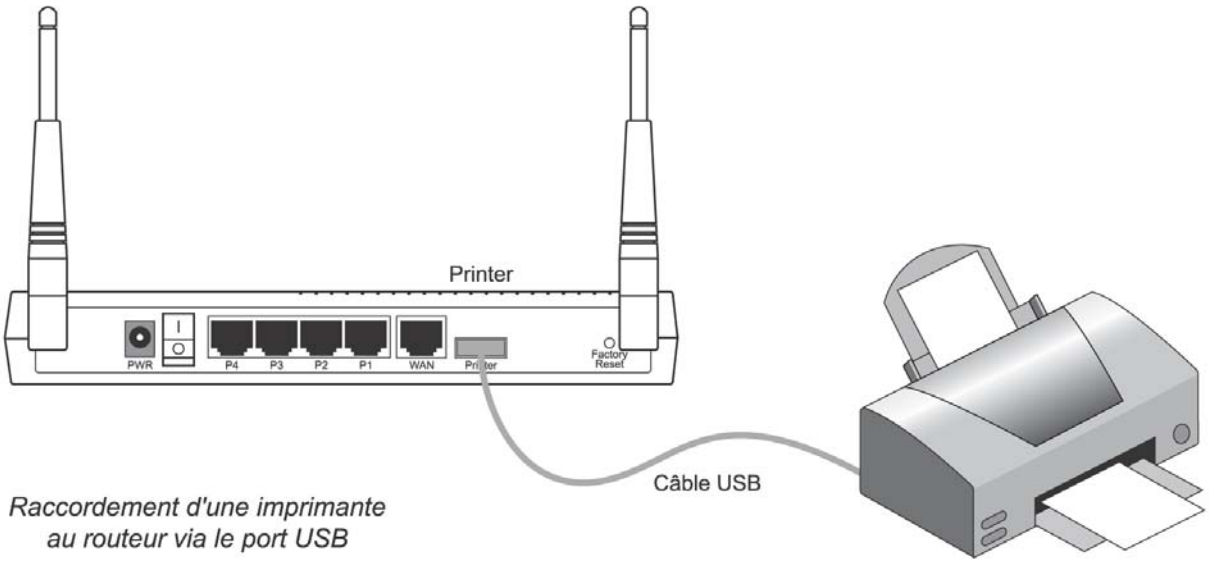
Vous pouvez bien entendu raccorder plusieurs ordinateurs et autres équipements au concentrateur Ethernet externe.

Raccordement d'une imprimante USB au routeur

Grâce au port USB situé à l'arrière du boîtier, vous pouvez raccorder une imprimante USB à votre routeur et ainsi la partager sur le réseau local.

Attention : l'imprimante doit être compatible avec la norme USB 1.1

1. Munissez-vous du câble USB fourni avec votre imprimante USB.
2. Raccordez l'extrémité du câble prévue à cet effet sur le port **Printer** du routeur.
3. Raccordez l'autre extrémité du câble sur votre imprimante.



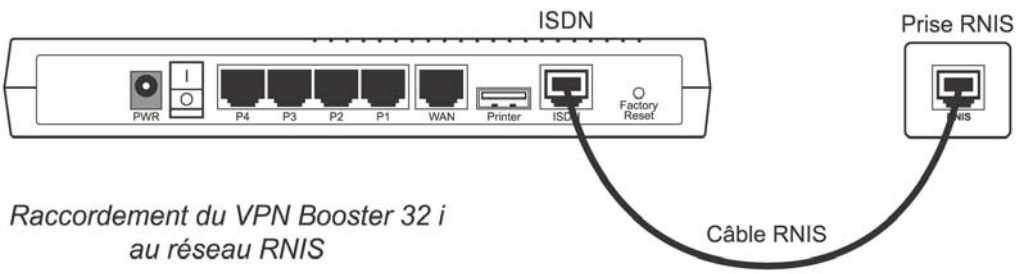
Raccordement d'une imprimante au routeur via le port USB

Remarque : une fois le raccordement effectué, vous devez configurer les ordinateurs qui composent votre réseau. Reportez-vous au chapitre « Partage de l'imprimante USB (Série VPN Booster 32) » page 169.

Raccordement du routeur au réseau RNIS (VPN Booster 32 i)

Pour raccorder le VPN Booster 32 i au réseau RNIS, procédez comme suit :

1. Munissez-vous du câble RNIS noir fourni dans l'emballage du routeur.
2. Raccordez une extrémité de ce câble au port **ISDN** du routeur.
3. Raccordez l'autre extrémité du câble à la prise RNIS dont vous disposez.



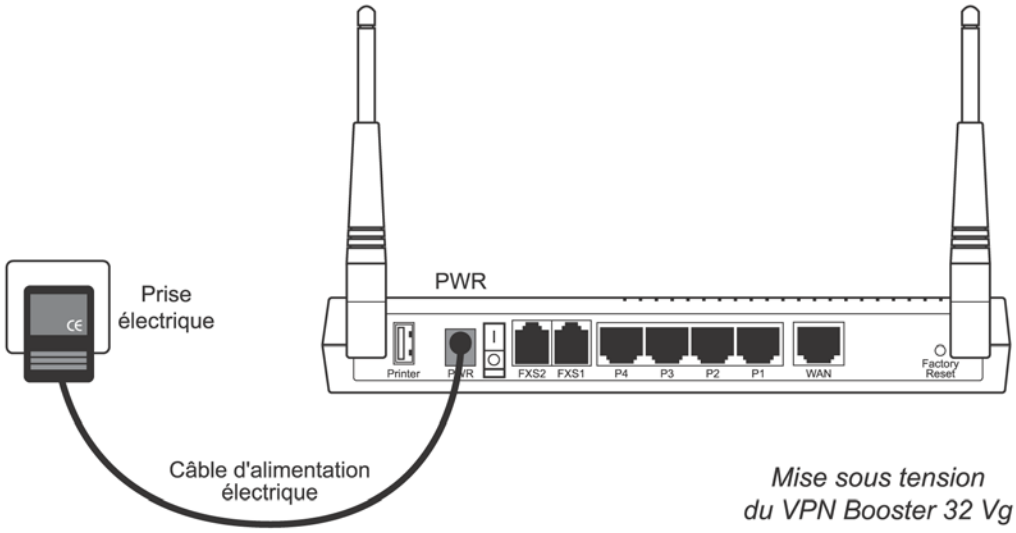
Raccordement du VPN Booster 32 i au réseau RNIS

Raccordements des VPN Booster 32 V et 32 Vg

Raccordement du routeur à l'alimentation électrique

Pour mettre sous tension le VPN Booster 32 V / 32 Vg, procédez comme suit :

1. Munissez-vous du câble d'alimentation électrique fourni dans l'emballage du routeur.
2. Raccordez l'extrémité du câble prévu à cet effet au connecteur **PWR** du routeur.
3. Raccordez l'autre extrémité du câble à une prise électrique compatible avec les spécifications imprimées sur le bloc d'alimentation.



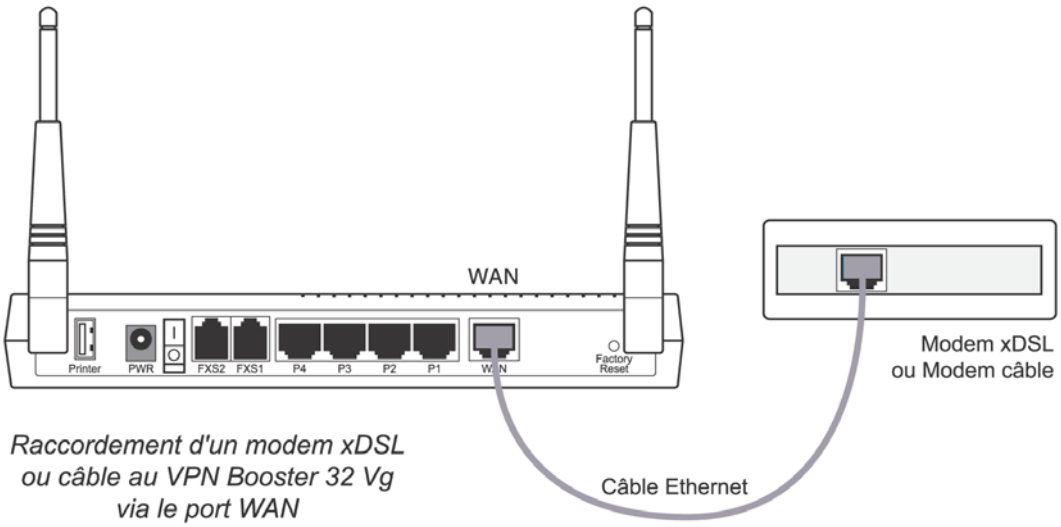
Mise sous tension du VPN Booster 32 Vg

La mise sous tension du routeur suppose également le positionnement de l'interrupteur sur **ON**.

Raccordement du routeur au modem xDSL ou câble

Pour raccorder le VPN Booster 32 V / 32 Vg au modem xDSL (ADSL, SDSL) ou au modem câble, procédez comme suit :

1. Munissez-vous du câble Ethernet fourni généralement dans l'emballage du modem xDSL ou du modem câble.
2. Raccordez une extrémité de ce câble au port **WAN** du routeur.
3. Raccordez l'autre extrémité du câble au modem xDSL ou au modem câble (modems de type Ethernet).



Raccordement d'un modem xDSL ou câble au VPN Booster 32 Vg via le port WAN

Raccordement Ethernet

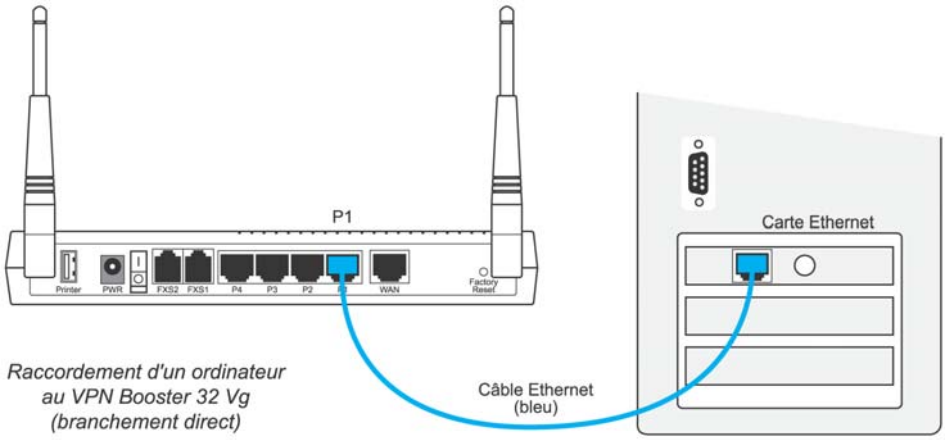
Le raccordement des ordinateurs du réseau local au routeur peut s'effectuer directement grâce au commutateur Ethernet intégré dans le routeur. Il peut également s'effectuer indirectement en utilisant un concentrateur Ethernet externe. Les deux types de raccordement peuvent être utilisés simultanément.

Raccordement direct

Pour raccorder directement un ordinateur au VPN Booster 32 V / 32 Vg, procédez comme suit :

1. Munissez-vous du câble Ethernet bleu fourni dans l'emballage du routeur.
2. Raccordez une extrémité de ce câble à l'un des ports **P1** à **P4** du routeur.
3. Raccordez l'autre extrémité du câble au connecteur RJ45 de la carte Ethernet de l'ordinateur.

Vous pouvez ainsi raccorder directement jusqu'à 4 ordinateurs (câbles supplémentaires non fournis). Au-delà du quatrième ordinateur, vous devez utiliser un concentrateur Ethernet externe (voir section ci-dessous).

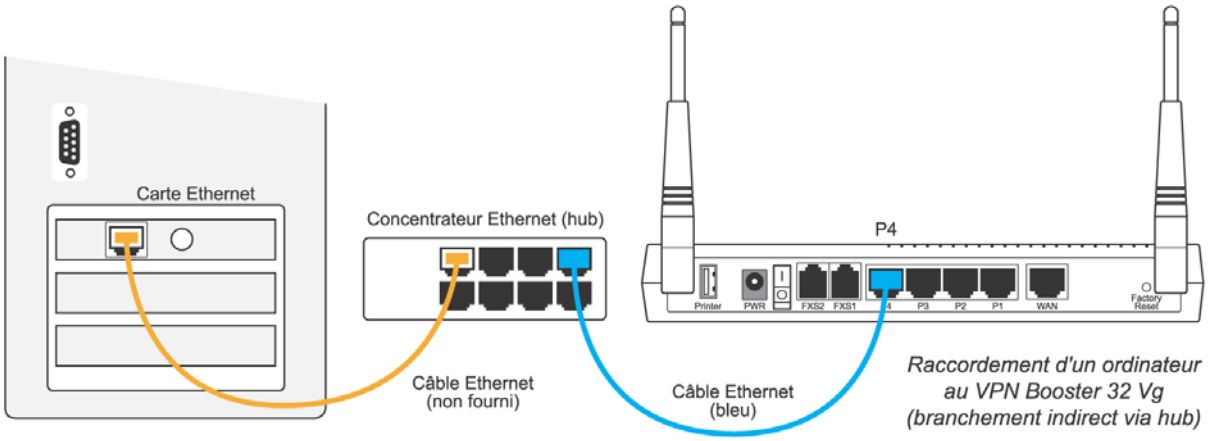


Raccordement indirect via concentrateur externe

Pour raccorder indirectement un ordinateur au VPN Booster 32 V / 32 Vg via un concentrateur Ethernet externe (non fourni), procédez comme suit :

1. Munissez-vous du câble Ethernet bleu fourni dans l'emballage du routeur.
2. Raccordez une extrémité de ce câble à l'un des ports **P1** à **P4** du routeur.
3. Raccordez l'autre extrémité à l'un des ports Ethernet du concentrateur Ethernet externe.

   Attention : grâce au système d'auto-détection du câblage, vous n'avez pas besoin d'utiliser de câble croisé.
4. Raccordez ensuite l'ordinateur au concentrateur Ethernet externe (câble supplémentaire non fourni).



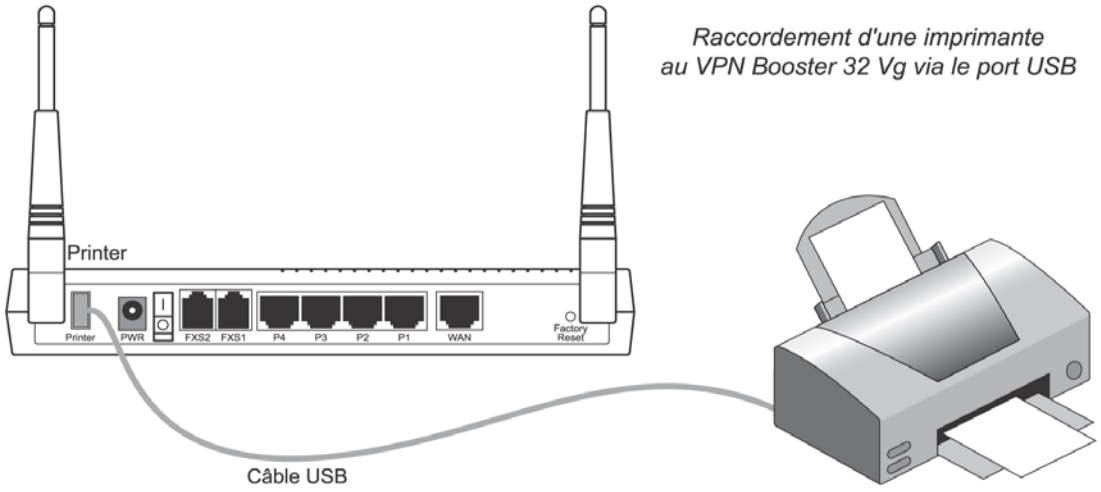
Vous pouvez bien entendu raccorder plusieurs ordinateurs et autres équipements au concentrateur Ethernet externe.

Raccordement d'une imprimante USB au routeur

Grâce au port USB situé à l'arrière du boîtier, vous pouvez raccorder une imprimante USB à votre routeur et ainsi la partager sur le réseau local.

Attention : l'imprimante doit être compatible avec la norme USB 1.1

1. Munissez-vous du câble USB fourni avec votre imprimante USB.
2. Raccordez l'extrémité du câble prévue à cet effet sur le port **Printer** du routeur.
3. Raccordez l'autre extrémité du câble sur votre imprimante.

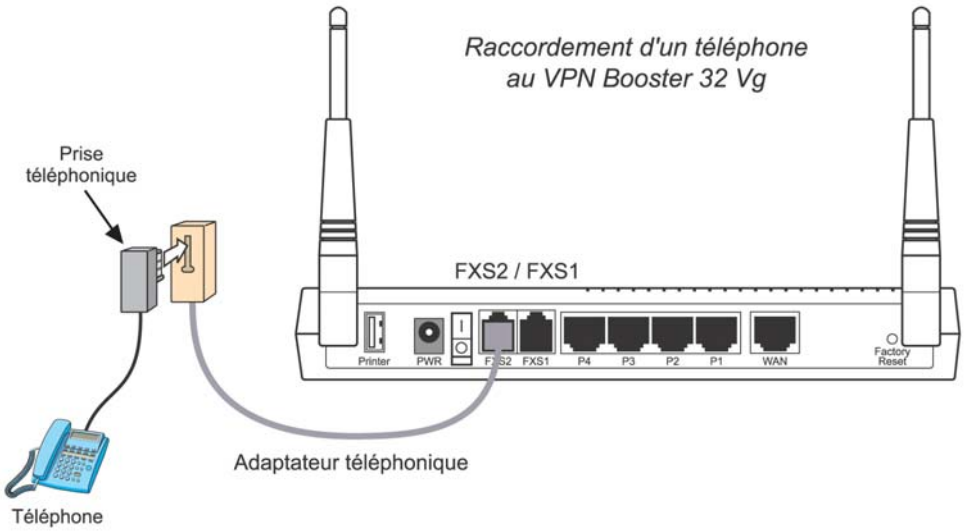


Remarque : une fois le raccordement effectué, vous devez configurer les ordinateurs qui composent votre réseau. Reportez-vous au chapitre « Partage de l'imprimante USB (Série VPN Booster 32) » page 169.

Raccordement de téléphones au routeur

Grâce aux ports FXS1 et FXS2 situés à l'arrière du VPN Booster 32 V / 32 Vg, vous pouvez raccorder les téléphones à votre routeur afin de profiter de la téléphonie sur Internet (VoIP).

1. Munissez-vous de l'adaptateur téléphonique fourni dans l'emballage du routeur.
2. Raccordez l'extrémité du câble sur le port **FXS1** ou **FXS2** du routeur.
3. Munissez-vous ensuite de votre téléphone.
4. Insérez votre prise téléphonique dans la fiche de l'adaptateur prévue à cet effet.



Voyants lumineux et connecteurs du routeur

Voyants lumineux et connecteurs du VPN Booster 8

Voyants lumineux

Situés sur l'avant du VPN Booster 8, les voyants lumineux renseignent sur l'état du routeur et des connexions. Le tableau ci-dessous indique la signification des différents voyants.

Intitulé du voyant		Fonction	Connecteur
ACT		Allumé à la mise sous tension Clignote lorsque le routeur est alimenté et lorsqu'il est actif. Clignote également lors de la mise à jour	PWR
Témoins du débit (3 leds)		Varient selon le taux d'occupation de la bande passante	
WAN		Allumé lorsque le routeur est connecté à un modem xDSL ou à un modem câble	WAN
Online		Allumé lorsque la connexion Internet est établie	
LAN	P1 à P4	Vert, lorsque la communication est établie à 100 Mbps Orange, lorsque la communication est établie à 10 Mbps 1 - Allumé lorsqu'un ordinateur est connecté et qu'aucun paquet n'est émis ou reçu 2 - Clignote lorsque des paquets sont émis ou reçus du commutateur Ethernet ou des ordinateurs connectés	P1 à P4
VPN		Allumé lorsqu'une connexion VPN est établie	

*Remarque : si le voyant **ACT** et le voyant situé à côté clignotent simultanément, cela signifie que le serveur TFTP est démarré. Votre routeur est prêt à recevoir une nouvelle mise à jour.*

Connecteurs

Tous les connecteurs du VPN Booster 8 sont regroupés sur sa face arrière. Reportez-vous aux schémas de raccordement dans la section « Raccordements du VPN Booster 8 » page 12.

Bouton Factory Reset

Si vous désirez remettre votre routeur en configuration d'usine, procédez comme suit :

1. Lorsque votre routeur est sous tension, appuyez et maintenez une pression sur le bouton **Factory Reset** pendant plus de 5 secondes.
2. Une fois que le voyant **ACT** commence à clignoter rapidement, relâchez le bouton. Le routeur redémarrera alors avec les paramètres d'usine.

Pour effectuer une mise à jour sans utiliser le configurateur Web ou Telnet de votre routeur, procédez comme suit :

1. Débranchez l'alimentation votre routeur.
2. Appuyez et maintenez une pression sur le bouton **Factory Reset** tout en rebranchant l'alimentation.
3. Le voyant **ACT** clignote rapidement signifiant que le serveur TFTP est démarré et que votre routeur est prêt à recevoir une nouvelle mise à jour. Relâchez le bouton.
4. Lancez l'Assistant de mise à jour et mettez à jour votre routeur (reportez-vous au chapitre « Mise à jour du routeur » page 197).

Voyants lumineux et connecteurs de la Série VPN Booster 32

Voyants lumineux

Voyants lumineux des VPN Booster 32, 32 g et 32 i

Situés sur l'avant du VPN Booster 32 / 32 g / 32 i, les voyants lumineux renseignent sur l'état du routeur et des connexions. Le tableau ci-dessous indique la signification des différents voyants.

	Intitulé du voyant		Fonction	Connecteur
	ACT		Allumé à la mise sous tension Clignote lorsque le routeur est alimenté et lorsqu'il est actif. Clignote également lors de la mise à jour	PWR
VPN Booster 32	DMZ		Allumé lorsque l'hôte DMZ est activé	
	QoS		Allumé lorsque le contrôle QoS est activé	
VPN Booster 32 g	QoS		Allumé lorsque le contrôle QoS est activé	
	WLAN		Allumé lorsqu'une connexion Wireless est établie	
VPN Booster 32 i	ISDN		Allumé lorsqu'il y a du trafic sur la ligne RNIS	ISDN
	QoS		Allumé lorsque le contrôle QoS est activé	
	Attack		Allumé si les défenses DoS ont été activées et si une tentative d'intrusion (ou une requête interprétée comme telle) a été détectée par le routeur	
	VPN		Allumé lorsqu'une connexion VPN est établie	
	Printer		Allumé lorsqu'une imprimante est branchée sur le port USB du routeur	Printer
	WAN		Allumé lorsque le routeur est connecté à un modem xDSL ou à un modem câble	WAN
	LAN	P1 à P4	Vert, lorsque la communication est établie à 100 Mbps Orange, lorsque la communication est établie à 10 Mbps 1 - Allumé lorsqu'un ordinateur est connecté et qu'aucun paquet n'est émis ou reçu 2 - Clignote lorsque des paquets sont émis ou reçus du commutateur Ethernet ou des ordinateurs connectés	P1 à P4

*Remarque : si le voyant **ACT** et le voyant situé à côté clignotent simultanément, cela signifie que le serveur TFTP est démarré. Votre routeur est prêt à recevoir une nouvelle mise à jour.*

Voyants lumineux des VPN Booster 32 V et 32 Vg

Situés sur l'avant du VPN Booster 32 V / 32 Vg, les voyants lumineux renseignent sur l'état du routeur et des connexions. Le tableau ci-dessous indique la signification des différents voyants.

	Intitulé du voyant		Fonction	Connecteur
	ACT		Allumé à la mise sous tension Clignote lorsque le routeur est alimenté et lorsqu'il est actif. Clignote également lors de la mise à jour	PWR
	QoS		Allumé lorsque le contrôle QoS est activé	
	Phone	FXS1 / FXS2	Clignote lors de la détection de sonnerie Allumé lors de la prise de ligne	FXS1 / FXS2
VPN Booster 32 V	VPN		Allumé lorsqu'une connexion VPN est établie	
VPN Booster 32 Vg	WLAN		Allumé lorsqu'une connexion Wireless est établie	
	Printer		Allumé lorsqu'une imprimante est branchée sur le port USB du routeur	Printer
	WAN		Allumé lorsque le routeur est connecté à un modem xDSL ou à un modem câble	WAN
	LAN	P1 à P4	Vert, lorsque la communication est établie à 100 Mbps Orange, lorsque la communication est établie à 10 Mbps 1 - Allumé lorsqu'un ordinateur est connecté et qu'aucun paquet n'est émis ou reçu 2 - Clignote lorsque des paquets sont émis ou reçus du commutateur Ethernet ou des ordinateurs connectés	P1 à P4

*Remarque : si le voyant **ACT** et le voyant situé à côté clignotent simultanément, cela signifie que le serveur TFTP est démarré. Votre routeur est prêt à recevoir une nouvelle mise à jour.*

Connecteurs

Tous les connecteurs du VPN Booster 32 sont regroupés sur sa face arrière. Selon le modèle dont vous diposez, reportez-vous aux schémas de raccordement dans les sections « Raccordements des VPN Booster 32, 32 g et 32 i » page 14 ou « Raccordements des VPN Booster 32 V et 32 Vg » page 17.

Bouton Factory Reset

Si vous désirez remettre votre routeur en configuration d'usine, procédez comme suit :

1. Lorsque votre routeur est sous tension, appuyez et maintenez une pression sur le bouton **Factory Reset** pendant plus de 5 secondes.
2. Une fois que le voyant **ACT** commence à clignoter rapidement, relâchez le bouton. Le routeur redémarrera alors avec les paramètres d'usine.

Pour effectuer une mise à jour sans utiliser le configurateur Web ou Telnet de votre routeur, procédez comme suit :

1. Débranchez l'alimentation votre routeur.
2. Appuyez et maintenez une pression sur le bouton **Factory Reset** tout en rebranchant l'alimentation.
3. Le voyant **ACT** clignote rapidement signifiant que le serveur TFTP est démarré et que votre routeur est prêt à recevoir une nouvelle mise à jour. Relâchez le bouton.
4. Lancez l'Assistant de mise à jour et mettez à jour votre routeur (reportez-vous au chapitre « Mise à jour du routeur » page 197).

Equipement informatique existant au sein de l'entreprise

Vous pouvez vous trouver dans différents cas de figure au moment d'installer le VPN Booster.

Votre réseau local n'est pas encore installé

Les ordinateurs de l'entreprise que vous souhaitez raccorder au routeur disposent chacun d'une carte Ethernet mais le réseau n'a pas encore été installé.

Vous devez configurer les cartes Ethernet équipant les ordinateurs.

Vous pouvez choisir entre deux modes d'adressage IP pour votre réseau :

- **Adresses IP dynamiques** : les adresses IP sont assignées dynamiquement aux ordinateurs par le serveur DHCP du VPN Booster. Ce mode d'adressage présente l'avantage d'être simple à mettre en œuvre. Il convient dans le cadre de l'accès à Internet et de la connexion de postes distants.

  Si vous êtes dans ce cas, nous vous conseillons de conserver la configuration IP par défaut du VPN Booster (adresse IP : **192.168.1.1**, masque de sous-réseau : **255.255.255.0**, serveur DHCP activé).

  – Pour raccorder les ordinateurs au VPN Booster, en fonction du modèle de routeur dont vous disposez, reportez-vous au chapitre « Raccordements du routeur » page 12, puis suivez les instructions.

  – Pour configurer les ordinateurs, reportez-vous au chapitre « Configuration des ordinateurs » page 26.

  – Pour configurer le routeur, vous pouvez utiliser l'Assistant de démarrage (voir « Installation et utilisation de l'Assistant de démarrage » page 59) ou vous reporter directement au chapitre « Accès à l'administration HTML du routeur » page 66.

- **Adresses IP fixes** : chaque ordinateur possède une adresse IP fixe, paramétrée par l'administrateur. Ce mode d'adressage nécessite une bonne connaissance de l'architecture du réseau local et des adresses IP. Il permet une administration plus avancée du réseau. L'adressage fixe est recommandé dans le cadre de l'interconnexion de réseaux.

  Si vous êtes dans ce cas, nous vous conseillons de conserver l'adresse IP par défaut du VPN Booster (adresse IP = **192.168.1.1**, masque de sous-réseau **255.255.255.0**). Vous devrez désactiver le serveur DHCP du routeur.

  – Pour raccorder les ordinateurs au VPN Booster, en fonction du modèle de routeur dont vous disposez, reportez-vous au chapitre « Raccordements du routeur » page 12, puis suivez les instructions.

  – Pour configurer les ordinateurs, reportez-vous au chapitre « Configuration des ordinateurs » page 26. Attribuez une adresse IP fixe différente à chaque ordinateur (ex. : **192.168.1.2**, **192.168.1.3**, **192.168.1.4**…).

  – Pour configurer le routeur, vous pouvez utiliser l'Assistant de démarrage (voir « Installation et utilisation de l'Assistant de démarrage » page 59) ou vous reporter directement au chapitre « Accès à l'administration HTML du routeur » page 66.

Votre réseau local est déjà installé mais il n'utilise pas le protocole TCP/IP

Votre réseau local est installé mais fonctionne dans un autre protocole que TCP/IP, par exemple NetBEUI ou IPX/SPX.

Vous devez ajouter le protocole TCP/IP sur les ordinateurs du réseau.

Vous pouvez choisir un mode d'adressage IP fixe ou dynamique, en fonction du cadre d'utilisation du routeur (voir la section précédente « Votre réseau local n'est pas encore installé »).

Votre réseau local est déjà installé et utilise le protocole TCP/IP

Si votre réseau local est déjà installé et qu'il utilise le protocole TCP/IP, vous devrez tenir compte du type d'administration qui a été mis en place. Vous vous trouvez dans l'une des deux situations suivantes :

- **Adressage IP dynamique** : les adresses IP sont assignées dynamiquement aux ordinateurs du réseau par un serveur DHCP (Windows NT, autre routeur…). Si vous souhaitez conserver l'architecture réseau existante lors de l'installation du VPN Booster, vous devez :
  - désactiver le serveur DHCP du VPN Booster ;
  - attribuer au VPN Booster une adresse IP appartenant au plan d'adressage du serveur DHCP en place ;

    *Important : si l'adresse IP par défaut du routeur (**192.168.1.1**) n'est pas compatible avec votre réseau, vous devez impérativement la modifier grâce à l'Assistant de démarrage (voir « Installation et utilisation de l'Assistant de démarrage » page 59).*
  - réserver l'adresse IP du VPN Booster sur le serveur DHCP ;
  - compléter la configuration des ordinateurs du réseau local devant utiliser le VPN Booster (passerelle TCP/IP, serveur DNS…).
- **Adressage IP fixe** : une adresse IP fixe a été paramétrée pour chaque ordinateur ou équipement du réseau. Si vous souhaitez conserver l'architecture réseau existante lors de l'installation du VPN Booster, vous devez :
  - désactiver le serveur DHCP du VPN Booster ;
  - attribuer au VPN Booster une adresse IP unique appartenant au plan d'adressage IP du réseau ;

    *Important : si l'adresse IP par défaut du routeur (**192.168.1.1**) n'est pas compatible avec votre réseau, vous devez impérativement la modifier grâce à l'Assistant de démarrage (voir « Installation et utilisation de l'Assistant de démarrage » page 59).*
  - compléter la configuration des ordinateurs du réseau local devant utiliser le VPN Booster (passerelle TCP/IP, serveur DNS…).

Configuration des ordinateurs

Ce chapitre vous concerne si votre réseau local n'est pas encore installé, si votre réseau local n'utilise pas le protocole TCP/IP ou tout simplement si vous souhaitez vérifier la configuration de vos ordinateurs.

Nous documentons ici la configuration des ordinateurs fonctionnant sous les systèmes d'exploitation suivants : Windows 95/98/Me, Windows NT 4.0, Windows 2000, Windows XP, Mac OS 9 et Mac OS X.

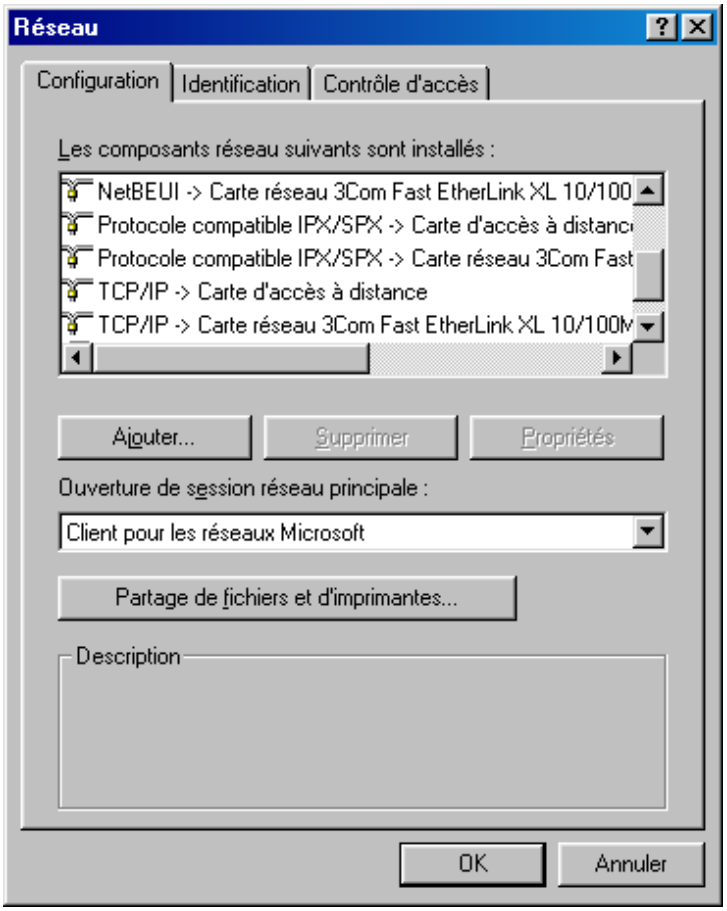
Remarque : nous considérons ici que les cartes Ethernet sont déjà installées dans les ordinateurs. Pour toute question relative à leur installation ou à leur fonctionnement, veuillez vous reporter à la documentation fournie par le constructeur de celles-ci.

PC sous Windows 95/98/Me

Vérification des protocoles

Le VPN Booster utilise le protocole réseau TCP/IP, il faut donc que celui-ci soit installé sur votre PC. Nous vous conseillons aussi d'installer le protocole NetBEUI pour une meilleure gestion du réseau Microsoft. Procédez comme suit :

1. Cliquez sur **Démarrer**, pointez sur **Paramètres**, puis cliquez sur **Panneau de configuration**. Effectuez ensuite un double-clic sur l'icône **Réseau**.



2. Dans la liste **Les composants réseau suivants sont installés** de l'onglet **Configuration**, vérifiez si les éléments suivants sont présents :

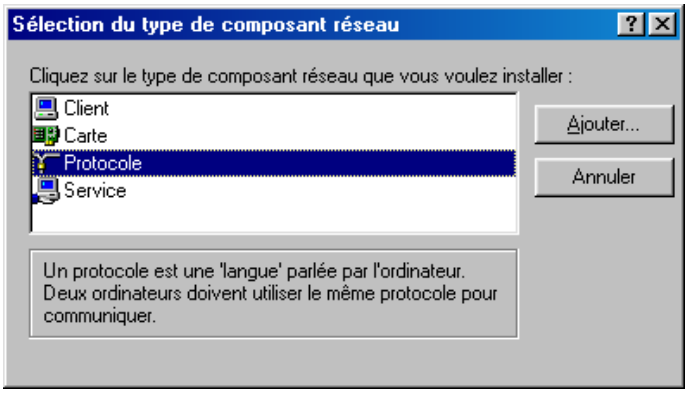
   – **NetBEUI -> *nom de votre carte réseau***

   – **TCP/IP-> *nom de votre carte réseau***

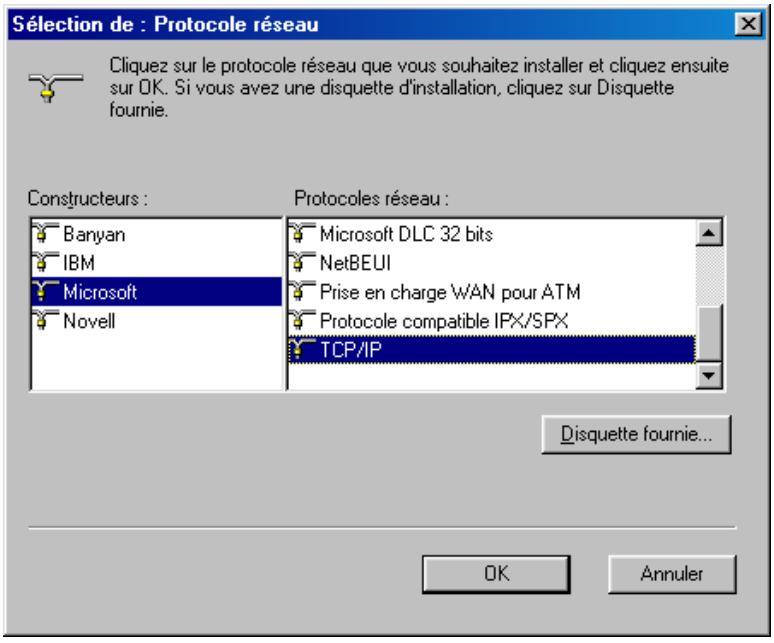
   Si ces composants sont tous les deux présents, passez directement à la section « Paramétrage du PC » page 28. Dans le cas contraire procédez à l'installation des protocoles manquants.

Installation du protocole TCP/IP

1. Dans l'onglet **Configuration** de la fenêtre **Réseau**, cliquez sur **Ajouter…**.
2. Dans la fenêtre **Sélection du type de composant réseau**, sélectionnez **Protocole**, puis cliquez sur **Ajouter…**.



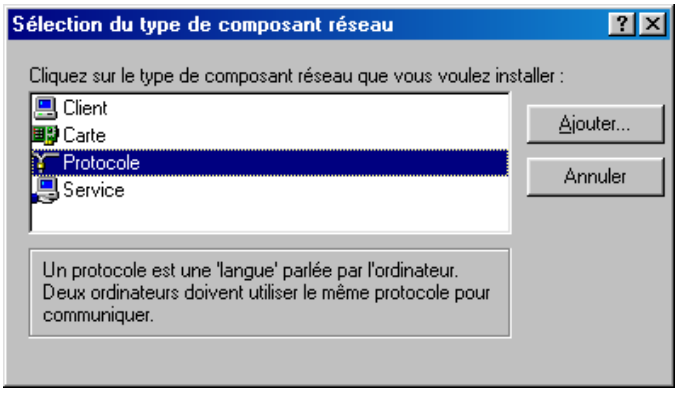
3. Dans la liste **Constructeurs**, sélectionnez **Microsoft** et **TCP/IP** dans la liste **Protocoles réseau**.



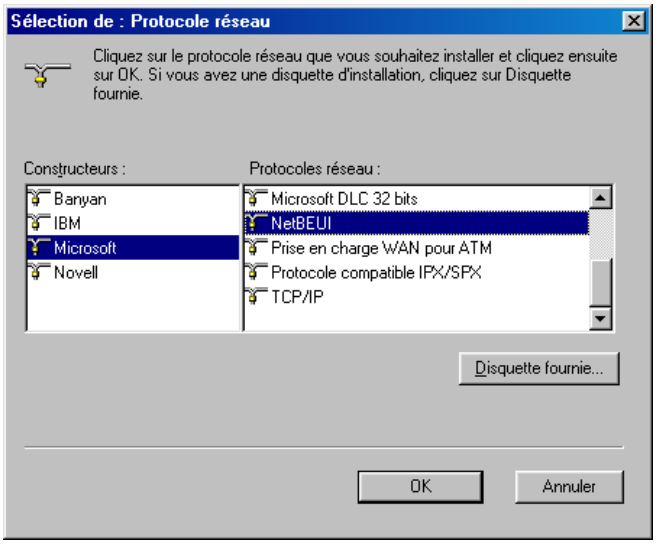
4. Cliquez ensuite sur **OK** dans chacune des fenêtres et suivez les instructions à l'écran afin de valider les modifications.

Installation du protocole NetBEUI

1. Dans l'onglet **Configuration** de la fenêtre **Réseau**, cliquez sur **Ajouter…**.
2. Dans la fenêtre **Sélection du type de composant réseau**, sélectionnez **Protocole**, puis cliquez sur **Ajouter…**.



3. Dans la liste **Constructeurs**, sélectionnez **Microsoft** et **NetBEUI** dans la liste **Protocoles réseau**.



4. Cliquez ensuite sur **OK** dans chacune des fenêtres et suivez les instructions à l'écran afin de valider les modifications.

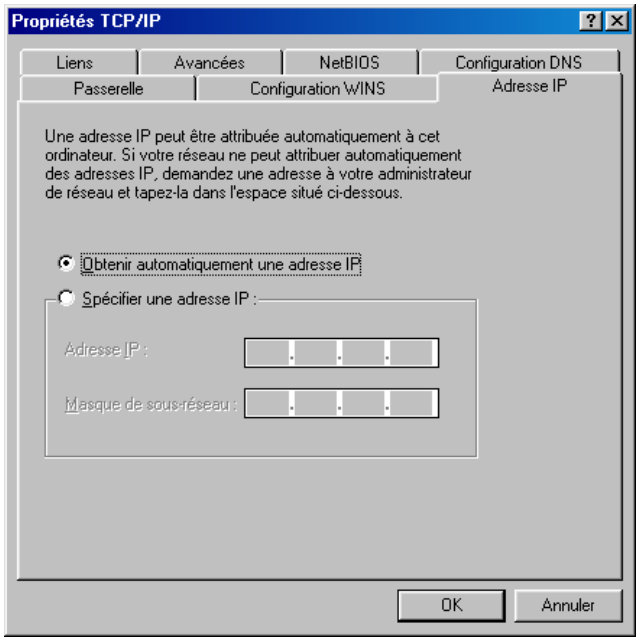
Paramétrage du PC

Nous avons vu dans le chapitre « Equipement informatique existant au sein de l'entreprise » page 24, que votre réseau local TCP/IP pouvait fonctionner avec des adresses IP dynamiques ou fixes. En fonction de votre choix, reportez-vous à la section correspondante.

Adresse IP dynamique

Vous avez choisi d'utiliser le serveur DHCP du VPN Booster afin que celui-ci alloue dynamiquement des adresses IP aux ordinateurs du réseau local, procédez comme suit :

1. Cliquez sur **Démarrer**, pointez sur **Paramètres**, puis cliquez sur **Panneau de configuration**. Effectuez ensuite un double-clic sur l'icône **Réseau**.
2. Dans le groupe **Les composants réseau suivants sont installés**, sélectionnez **TCP/IP -> *nom de votre carte réseau***, puis cliquez sur **Propriétés**.
3. Dans l'onglet **Adresse IP** de la fenêtre **Propriétés TCP/IP**, sélectionnez l'option **Obtenir automatiquement une adresse IP**.



Vous devez ensuite procéder à la configuration de la passerelle. Continuez le paramétrage à l'étape **2** de la section « Passerelle » page 30.

Adresse IP fixe

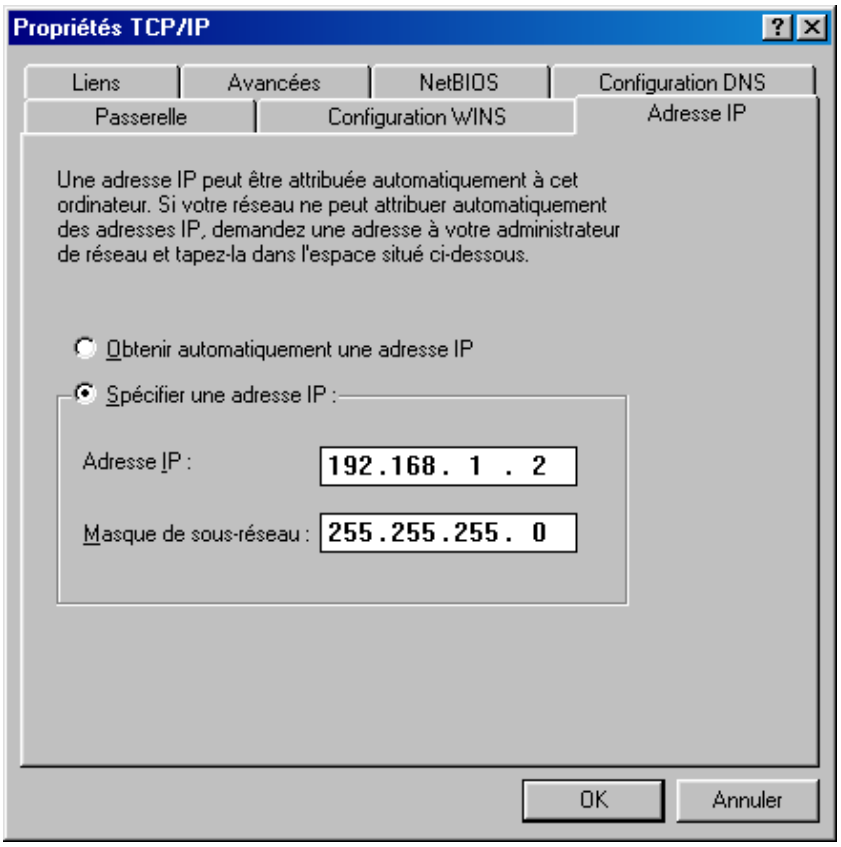
Vous avez choisi d'attribuer des adresses IP fixes aux ordinateurs du réseau local. Procédez comme suit :

1. Cliquez sur **Démarrer**, pointez sur **Paramètres**, puis cliquez sur **Panneau de configuration**. Effectuez ensuite un double-clic sur l'icône **Réseau**.
2. Dans le groupe **Les composants réseau suivants sont installés**, sélectionnez **TCP/IP -> *nom de votre carte réseau***, puis cliquez sur **Propriétés**.
3. Dans l'onglet **Adresse IP** de la fenêtre **Propriétés TCP/IP**, sélectionnez l'option **Spécifier une adresse IP**.
4. Dans la rubrique **Adresse IP**, entrez l'adresse IP que vous avez décidé d'attribuer au PC.

   Important :

   - *L'adresse IP du PC doit impérativement être comprise dans la même plage d'adressage que celle du VPN Booster.*
   - *L'adresse IP du PC doit être unique, c'est-à-dire différente de celle des autres équipements présents sur le réseau local (ordinateurs, VPN Booster …).*
   - *L'adresse IP du PC doit appartenir à une plage réservée aux réseaux privés. En effet votre réseau local ne doit pas utiliser des adresses réservées à Internet. Cela provoquerait des problèmes dans le cadre de la connexion de votre réseau à Internet.*

   En cas de doute sur ces points, vous devez prendre conseil auprès d'un spécialiste réseaux.
5. Dans la rubrique **Masque de sous-réseau**, entrez la valeur du masque de sous-réseau par défaut du VPN Booster, soit « 255.255.255.0 ».



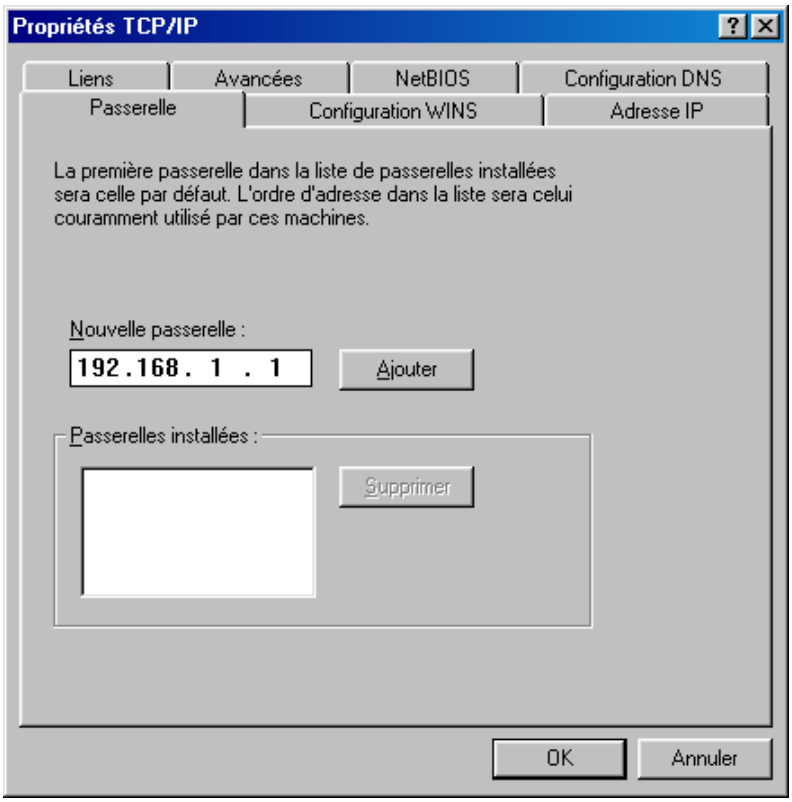
Dans l'exemple ci-dessus, l'adresse IP et le masque de sous-réseau alloués au PC sont compatibles avec les paramètres IP par défaut du VPN Booster.

Vous devez ensuite procéder à la configuration de la passerelle. Continuez le paramétrage à l'étape **2** de la section « Passerelle ».

Passerelle

Quel que soit le mode d'adressage IP choisi (fixe ou dynamique), vous devez indiquer l'adresse IP du VPN Booster. Procédez comme suit :

1. Cliquez sur **Démarrer**, pointez sur **Paramètres**, puis cliquez sur **Panneau de configuration**. Effectuez ensuite un double-clic sur l'icône **Réseau**.
2. Cliquez sur l'onglet **Passerelle**.



3. Dans la rubrique **Nouvelle passerelle**, entrez l'adresse IP attribuée au VPN Booster, puis cliquez sur **Ajouter**.

   Rappel : par défaut, l'adresse IP du VPN Booster est « 192.168.1.1 ».

Vous devez ensuite procéder à la configuration DNS. Continuez le paramétrage à l'étape **2** de la section « DNS ».

DNS

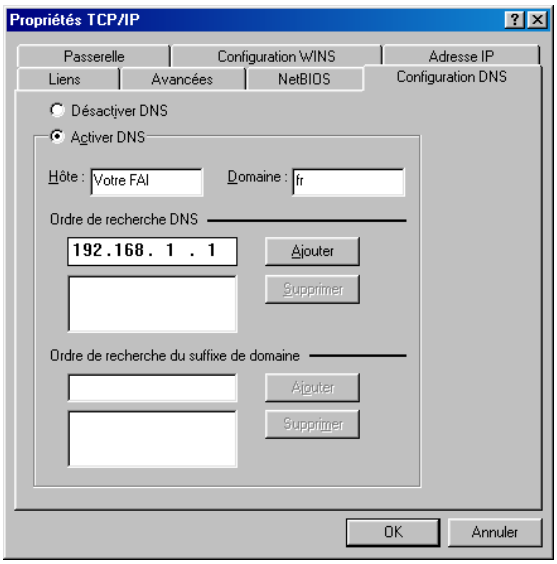
Les serveurs DNS permettent la résolution des noms symboliques sur Internet. Pour effectuer la configuration DNS de votre PC, procédez comme suit :

1. Cliquez sur **Démarrer**, pointez sur **Paramètres**, puis cliquez sur **Panneau de configuration**. Effectuez ensuite un double-clic sur l'icône **Réseau**.
2. Cliquez sur l'onglet **Configuration DNS**.
3. Cochez la case **Activer DNS**.
4. Dans les rubriques **Hôte** et **Domaine**, indiquez respectivement le nom de votre FAI et le suffixe de domaine (exemple : « fr » dans la rubrique **domaine**).
5. Dans la zone **Ordre de recherche DNS**, saisissez de préférence l'adresse IP du routeur. De cette façon, vous utilisez la fonction Proxy DNS du routeur qui permet d'optimiser la navigation.

   Remarque concernant le VPN Booster 32 i : ce paramétrage est notamment nécessaire si vous utilisez deux FAI distincts pour la connexion RNIS et pour la connexion xDSL. La fonction Proxy DNS vous permet de ne pas modifier l'adresse du serveur DNS dans les propriétés TCP/IP à chaque fois que vous changez de mode de connexion.

   Sinon, vous pouvez également saisir l'adresse de serveur DNS indiquée par votre FAI (pour cela, reportez-vous à la documentation fournie par celui-ci lors de la souscription de l'abonnement).

Remarque : le cas échéant, vous pouvez indiquer plusieurs adresses de serveurs DNS. Celle qui apparaît en tête de liste sera utilisée en priorité.



Cliquez ensuite sur **Ajouter**.

6. Cliquez ensuite sur **OK** dans chacune des fenêtres et suivez les instructions à l'écran afin de valider les modifications.

Vérification de la configuration

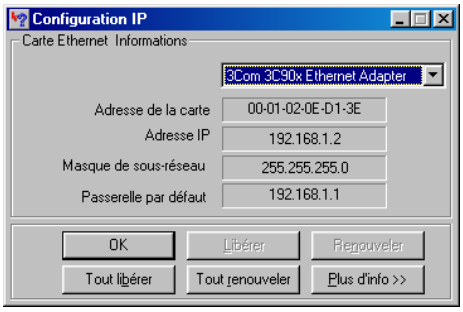
Les utilitaires *Winipcfg* et *Ping*, livrés avec Windows 95/98/Me, vous permettent de vérifier que la configuration réseau du PC est correcte et qu'il peut dialoguer avec le VPN Booster.

Avant d'exécuter ces utilitaires, assurez-vous que le VPN Booster est sous tension et que les câbles Ethernet sont correctement branchés (selon le modèle de routeur dont vous disposez, reportez-vous aux parties « Raccordement du routeur à l'alimentation électrique » et « Raccordement Ethernet » dans le chapitre « Raccordements du routeur » page 12, puis suivez les instructions).

Winipcfg

L'utilitaire *Winipcfg* permet de vérifier que votre configuration a bien été prise en compte. Procédez comme suit :

1. Cliquez sur **Démarrer**, puis sur **Exécuter…**.
2. Tapez « Winipcfg », puis cliquez sur **OK**.



3. Dans la liste déroulante, sélectionnez votre carte Ethernet.

   Vous devez retrouver les valeurs de configuration réseau du PC :

   – **Adresse de la carte** : adresse physique (MAC) de la carte ;
   – **Adresse IP** : adresse IP de la carte. Cette adresse peut varier à chaque démarrage du PC si vous avez opté pour une adresse IP dynamique allouée par le serveur DHCP du VPN Booster ;
   – **Masque de sous-réseau** : masque de sous-réseau de la carte ;
   – **Passerelle par défaut** : adresse IP du VPN Booster.

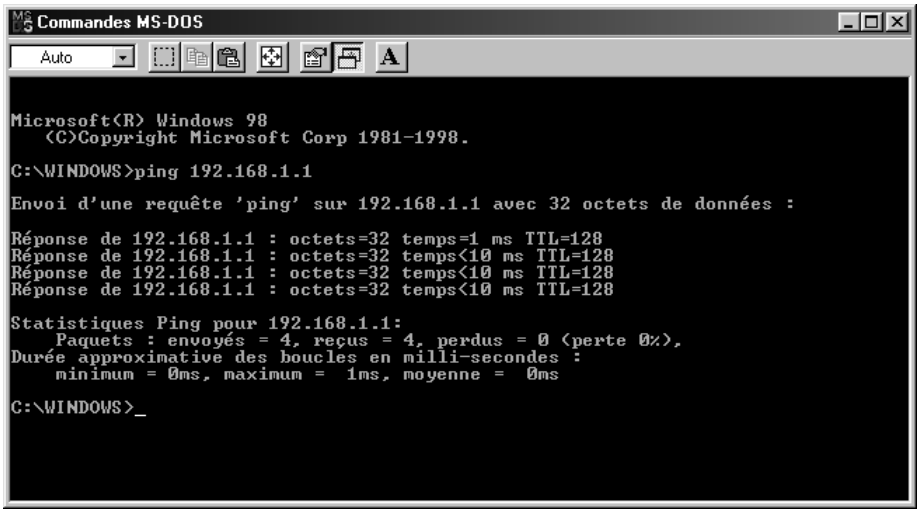
Ping

L'utilitaire Ping permet de tester le dialogue entre le PC et le VPN Booster à travers le protocole TCP/IP. Procédez comme suit :

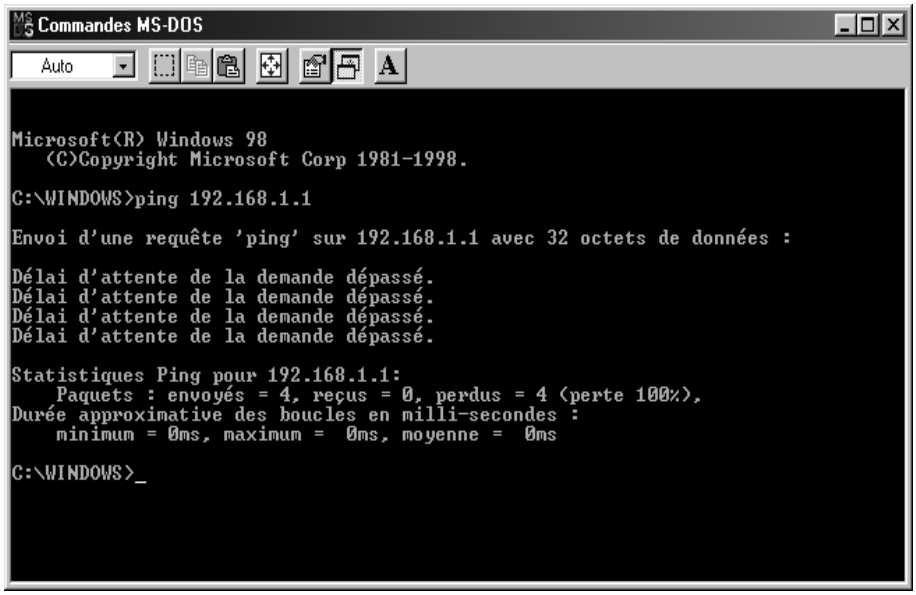
1. Cliquez sur **Démarrer**, pointez sur **Programmes**, puis cliquez sur **Commandes MS-DOS**.
2. Dans la boîte de dialogue de commandes MS-DOS, tapez « ping » suivi de l'adresse IP du VPN Booster, puis appuyez sur la touche **ENTRÉE**.

   Remarque : si vous n'avez pas changé les paramètres IP par défaut du VPN Booster, vous devez donc taper « ping 192.168.1.1 ».

   Dans l'exemple ci-dessous, le dialogue entre le PC et le VPN Booster s'est correctement établi. Si vous obtenez un écran similaire, c'est que votre configuration est opérationnelle.



Dans l'exemple ci-dessous, le PC n'a pu dialoguer avec le VPN Booster. Si vous obtenez un écran similaire, c'est que votre configuration n'est pas opérationnelle. Vérifiez les adresses IP et la connexion des câbles.

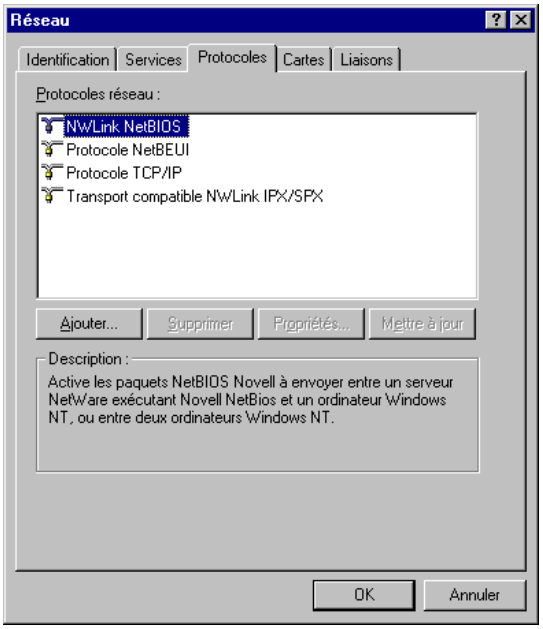


PC sous Windows NT

Vérification des protocoles

Le VPN Booster utilise le protocole réseau TCP/IP, il faut donc que celui-ci soit installé sur votre PC. Nous vous conseillons aussi d'installer le protocole NetBEUI pour une meilleure gestion du réseau Microsoft.

1. Cliquez sur **Démarrer**, pointez sur **Paramètres**, puis cliquez sur **Panneau de configuration**. Effectuez ensuite un double-clic sur l'icône **Réseau**.
2. Cliquez sur l'onglet **Protocoles**.

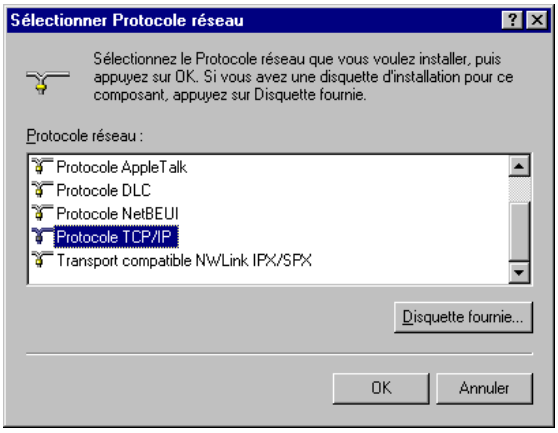


3. Dans la liste **Protocoles réseau**, vérifiez si les éléments suivants sont présents :
   - **Protocole NetBEUI**
   - **Protocole TCP/IP**

   Si ces composants sont tous les deux présents, passez directement à la section « Paramétrage du PC » page 34. Dans le cas contraire, procédez à l'installation des protocoles manquants.

Installation du protocole TCP/IP

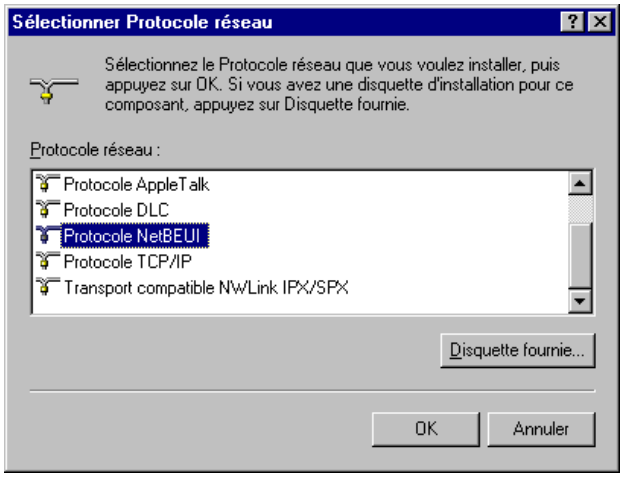
1. Dans l'onglet **Protocoles** de la fenêtre **Réseau**, cliquez sur **Ajouter…**.
2. Dans la liste **Protocole réseau**, sélectionnez **Protocole TCP/IP**.



3. Cliquez ensuite sur **OK** dans chacune des fenêtres et suivez les instructions à l'écran afin de valider les modifications.

Installation du protocole NetBEUI

1. Dans l'onglet **Protocoles** de la fenêtre **Réseau**, cliquez sur **Ajouter…**.
2. Dans la liste **Protocole réseau**, sélectionnez **Protocole NetBEUI**.



3. Cliquez ensuite sur **OK** dans chacune des fenêtres et suivez les instructions à l'écran afin de valider les modifications.

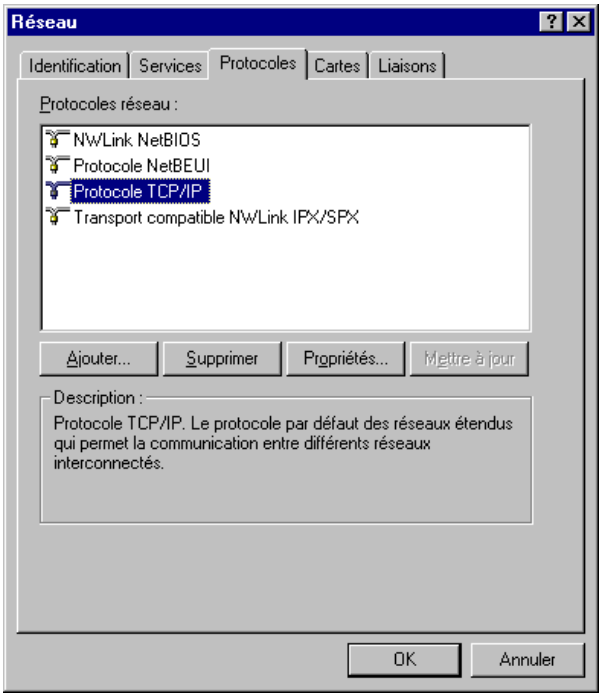
Paramétrage du PC

Nous avons vu dans l'introduction que votre réseau local TCP/IP pouvait fonctionner avec des adresses IP dynamiques ou fixes. En fonction de votre choix, reportez-vous à la section correspondante.

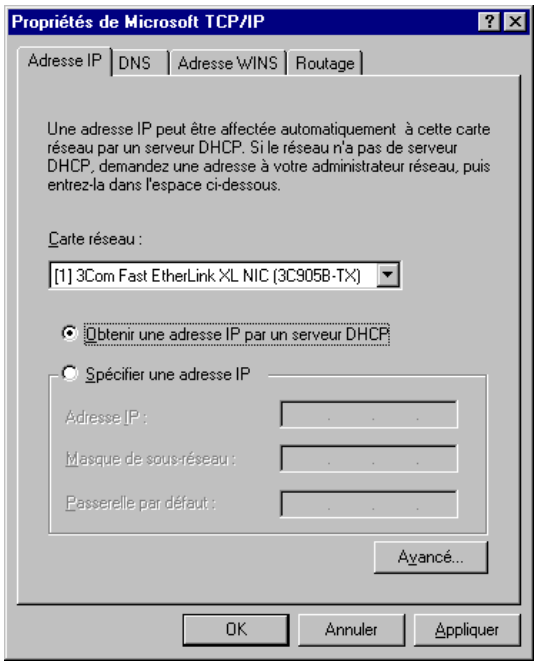
Adresse IP dynamique

Vous avez choisi d'utiliser le serveur DHCP du VPN Booster afin que celui-ci alloue dynamiquement des adresses IP aux ordinateurs du réseau local, procédez comme suit :

1. Cliquez sur **Démarrer**, pointez sur **Paramètres**, puis cliquez sur **Panneau de configuration**. Effectuez ensuite un double-clic sur l'icône **Réseau**.
2. Cliquez sur l'onglet **Protocoles**.
3. Sélectionnez **Protocole TCP/IP**, puis cliquez sur **Propriétés**.



4. La fenêtre **Propriétés de Microsoft TCP/IP** s'ouvre sur l'onglet **Adresse IP**.

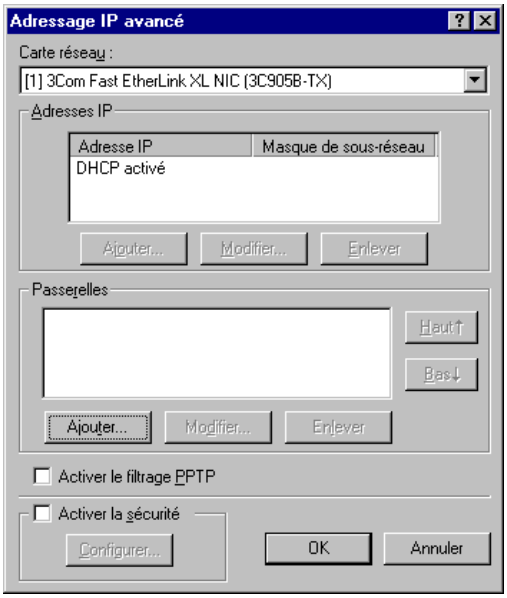


Dans la rubrique **Carte réseau**, sélectionnez votre carte réseau.

5. Sélectionnez l'option **Obtenir une adresse IP par un serveur DHCP**.

   Cliquez sur **Avancé…**.

6. Dans la zone **Passerelles**, cliquez sur **Ajouter…**.



7. Dans la rubrique **Adresse de passerelle**, indiquez l'adresse IP du routeur, puis cliquez sur **Ajouter**.

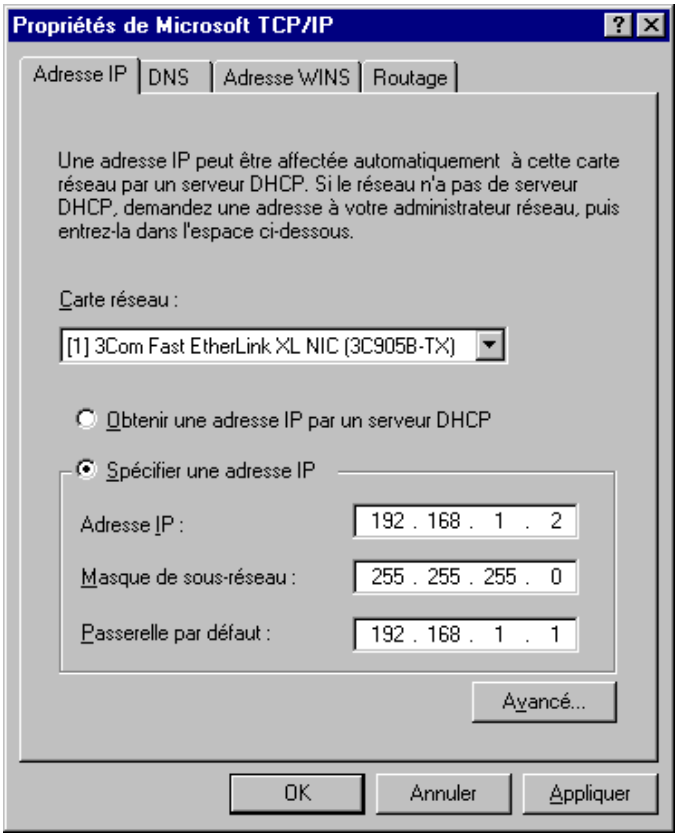
   Rappel : par défaut, l'adresse IP du VPN Booster est « 192.168.1.1 ».

8. Cliquez sur **OK**. Le paramétrage de l'adresse IP de votre PC est terminé. Vous devez maintenant procéder à la configuration DNS. Reportez-vous pour cela à la section « DNS » page 37.

Adresse IP fixe

Vous avez choisi d'attribuer des adresses IP fixes aux ordinateurs du réseau local. Procédez comme suit :

1. Cliquez sur **Démarrer**, pointez sur **Paramètres**, puis cliquez sur **Panneau de configuration**. Effectuez ensuite un double-clic sur l'icône **Réseau**.
2. Cliquez sur l'onglet **Protocoles**.
3. Sélectionnez **Protocole TCP/IP**, puis cliquez sur **Propriétés**. La fenêtre **Propriétés de Microsoft TCP/IP** s'ouvre sur l'onglet **Adresse IP**.
4. Dans la rubrique **Carte réseau**, sélectionnez votre carte réseau.
5. Sélectionnez **Spécifier une adresse IP**.



6. Dans la rubrique **Adresse IP**, entrez l'adresse IP que vous avez décidé d'attribuer au PC.

   Important :

   - *L'adresse IP du PC doit impérativement être comprise dans la même plage d'adressage que celle du VPN Booster.*
   - *L'adresse IP du PC doit être unique, c'est-à-dire différente de celle des autres équipements présents sur le réseau local (ordinateurs, VPN Booster …).*
   - *L'adresse IP du PC doit appartenir à une plage réservée aux réseaux privés. En effet, votre réseau local ne doit pas utiliser des adresses réservées à Internet. Cela provoquerait des problèmes dans le cadre de la connexion de votre réseau à Internet.*

   En cas de doute sur ces points, vous devez prendre conseil auprès d'un spécialiste réseaux.
7. Dans la rubrique **Masque de sous-réseau**, entrez la valeur du masque de sous-réseau par défaut du VPN Booster, soit « 255.255.255.0 ».
8. Dans la rubrique **Passerelle par défaut**, entrez l'adresse IP attribuée au VPN Booster, puis cliquez sur **Ajouter**.

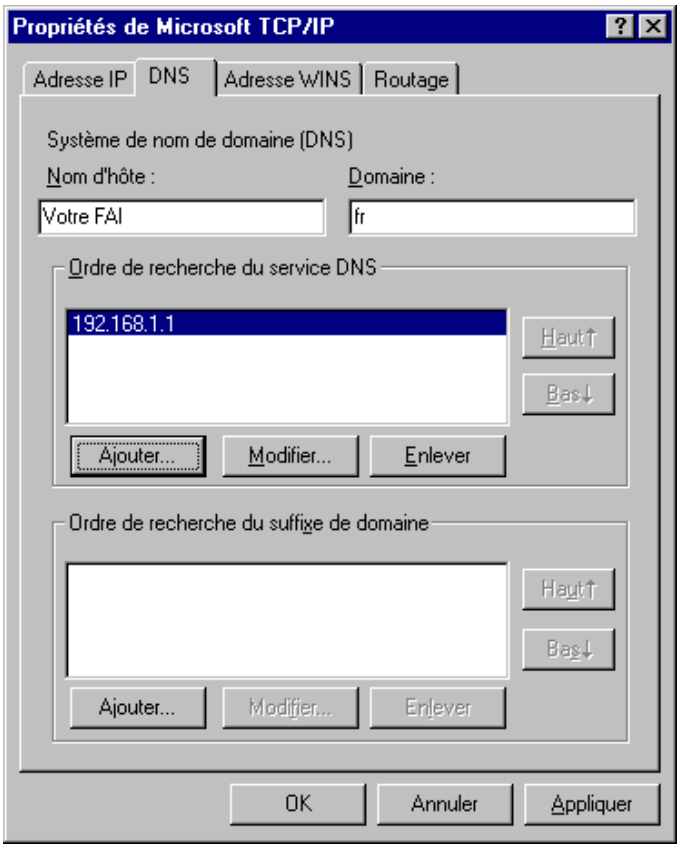
   Rappel : par défaut, l'adresse IP du VPN Booster est « 192.168.1.1 ».

Vous devez ensuite procéder à la configuration DNS (voir ci-après).

DNS

Les serveurs DNS permettent la résolution des noms symboliques sur Internet. Pour effectuer la configuration DNS de votre PC, procédez comme suit :

1. Dans la fenêtre **Propriétés de Microsoft TCP/IP**, cliquez sur l'onglet **DNS**.
2. Dans les rubriques **Nom d'hôte** et **Domaine**, indiquez respectivement le nom de votre FAI et son suffixe de domaine (exemple : « fr » dans la rubrique **Domaine**).

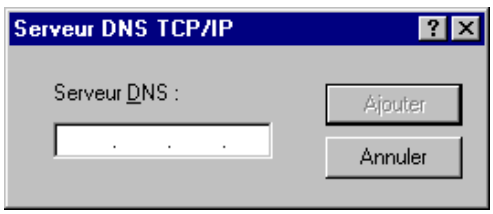


3. Dans la zone **Ordre de recherche du service DNS**, cliquez sur **Ajouter…**.
4. Saisissez de préférence l'adresse IP du routeur. De cette façon, vous utilisez la fonction Proxy DNS du routeur qui permet d'optimiser la navigation.

   Remarque concernant le VPN Booster 32 i : ce paramétrage est notamment nécessaire si vous utilisez deux FAI distincts pour la connexion RNIS et pour la connexion xDSL. La fonction Proxy DNS vous permet de ne pas modifier l'adresse du serveur DNS dans les propriétés TCP/IP à chaque fois que vous changez de mode de connexion.

   Sinon, vous pouvez également saisir l'adresse de serveur DNS indiquée par votre FAI (pour cela, reportez-vous à la documentation fournie par celui-ci lors de la souscription de l'abonnement).

   Remarque : vous pouvez ajouter successivement plusieurs adresses de serveurs DNS. Dans ce cas, c'est celle qui apparaît en tête de liste qui sera utilisée en priorité.



   Cliquez ensuite sur **Ajouter**.

5. Cliquez ensuite sur **OK** dans chacune des fenêtres et suivez les instructions à l'écran afin de valider les modifications.

Vérification de la configuration

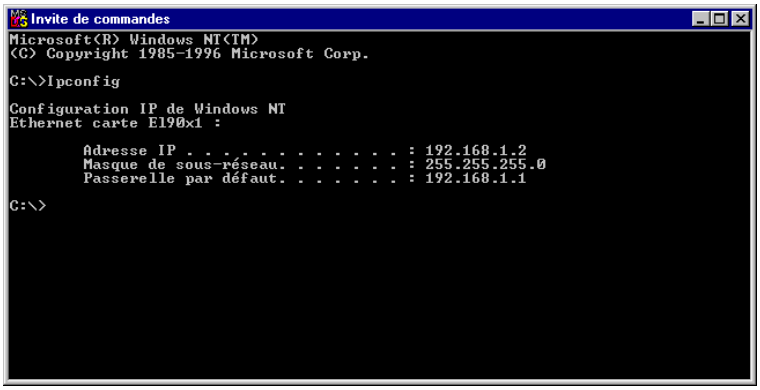
Les utilitaires *Ipconfig* et *Ping*, livrés avec Windows NT, vous permettent de vérifier que la configuration réseau du PC est correcte et qu'il peut dialoguer avec le VPN Booster.

Avant d'exécuter ces utilitaires, assurez-vous que le VPN Booster est sous tension et que les câbles Ethernet sont correctement branchés (selon le modèle de routeur dont vous disposez, reportez-vous aux parties « Raccordement du routeur à l'alimentation électrique » et « Raccordement Ethernet » dans le chapitre « Raccordements du routeur » page 12, puis suivez les instructions).

Ipconfig

L'utilitaire Ipconfig permet de vérifier que votre configuration a bien été prise en compte. Procédez comme suit :

1. Cliquez sur **Démarrer**, pointez sur **Programmes**, puis cliquez sur **Invite de commande**.
2. Dans la fenêtre **Invite de commandes**, tapez « Ipconfig », puis appuyez sur la touche **ENTRÉE**.



La fenêtre affiche les principales caractéristiques de la configuration IP de votre PC, à savoir :

- le modèle de carte Ethernet installé ;
- l'adresse IP de la carte. Cette adresse peut varier à chaque démarrage du PC si vous avez opté pour une adresse IP dynamique allouée par le serveur DHCP du VPN Booster ;
- le masque de sous-réseau utilisé ;
- la passerelle par défaut (adresse IP du VPN Booster).

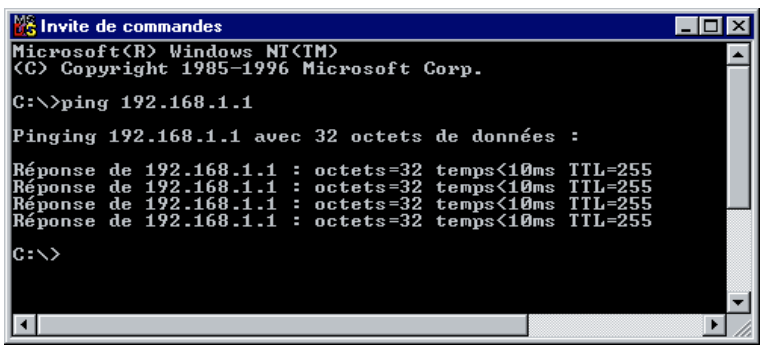
Ping

L'utilitaire Ping permet de tester le dialogue entre le PC et le VPN Booster à travers le protocole TCP/IP. Procédez comme suit :

1. Cliquez sur **Démarrer**, pointez sur **Programmes**, puis cliquez sur **Invite de commandes**.
2. Dans la fenêtre **Invite de commandes**, tapez « ping » suivi de l'adresse IP du VPN Booster, puis appuyez sur la touche **ENTRÉE**.

   Remarque : si vous n'avez pas changé les paramètres IP par défaut du VPN Booster, vous devez donc taper « ping 192.168.1.1 ».

   Dans l'exemple ci-dessous, le dialogue entre le PC et le VPN Booster s'est correctement établi. Si vous obtenez un écran similaire, c'est que votre configuration est opérationnelle.



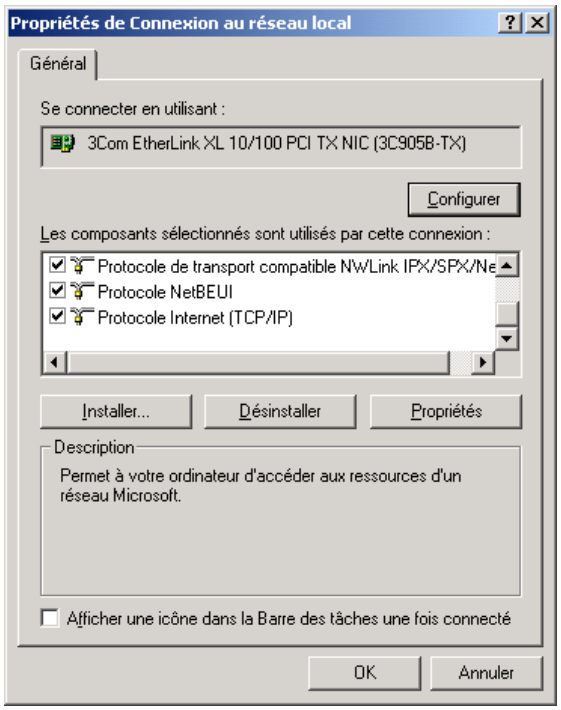
Dans l'exemple ci-dessous, le PC n'a pu dialoguer avec le VPN Booster. Si vous obtenez un écran similaire, c'est que votre configuration n'est pas opérationnelle. Vérifiez les adresses IP et la connexion des câbles.

PC sous Windows 2000

Vérification des protocoles

Le VPN Booster utilise le protocole réseau TCP/IP. Celui-ci est installé par défaut dans Windows 2000. Nous vous conseillons aussi d'installer le protocole NetBEUI pour une meilleure gestion du réseau Microsoft.

1. Cliquez sur **Démarrer**, pointez sur **Paramètres**, puis cliquez sur **Panneau de configuration**. Effectuez ensuite un double-clic sur l'icône **Connexions réseau et accès à distance**.
2. Avec le bouton droit de la souris, cliquez sur **Connexion au réseau local** et sélectionnez **Propriétés** dans le menu.

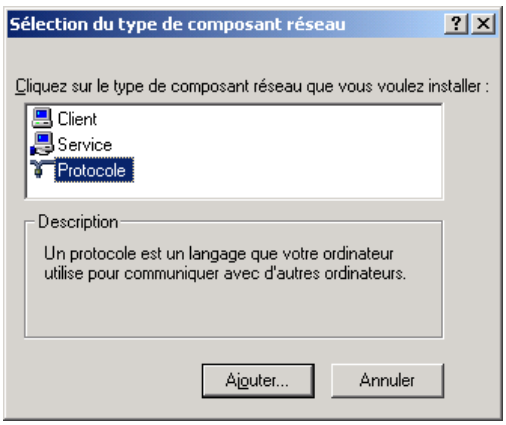


3. Dans la liste **Les composants sélectionnés sont utilisés par cette connexion**, vérifiez si les éléments suivants sont présents :
   - **Protocole NetBEUI**
   - **Protocole Internet (TCP/IP)**

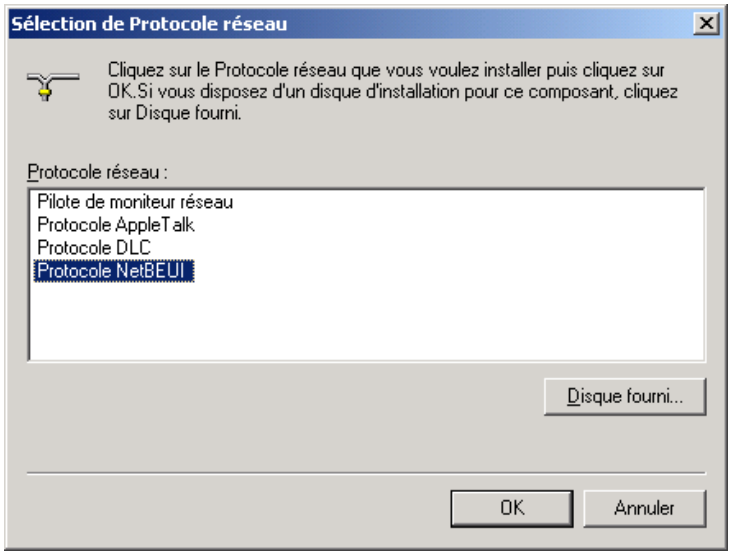
   Si ces composants sont tous les deux présents, passez directement à la section « Paramétrage du PC » page 41. Si le protocole NetBEUI est manquant, procédez à son installation.

Installation du protocole NetBEUI

1. Cliquez sur **Installer…**. Dans la fenêtre **Sélection du type de composant réseau**, sélectionnez **Protocole**, puis cliquez sur **Ajouter…**.



2. Sélectionnez la ligne **Protocole NetBEUI**, puis cliquez sur **OK**.



3. Cliquez ensuite sur **OK** et suivez les instructions à l'écran afin de valider les modifications.

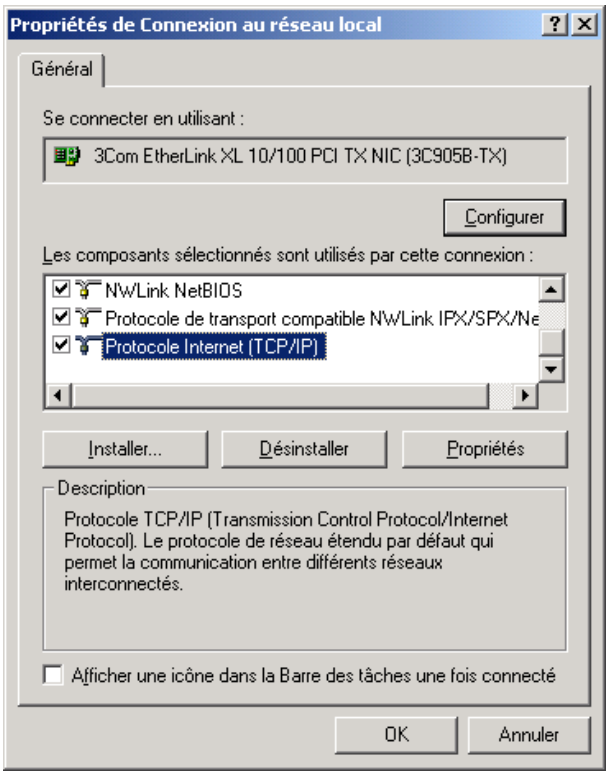
Paramétrage du PC

Nous avons vu dans l'introduction que votre réseau local TCP/IP pouvait fonctionner avec des adresses IP dynamiques ou fixes. En fonction de votre choix, reportez-vous à la section correspondante.

Adresse IP dynamique

Vous avez choisi d'utiliser le serveur DHCP du VPN Booster afin que celui-ci alloue dynamiquement des adresses IP aux ordinateurs du réseau local, procédez comme suit :

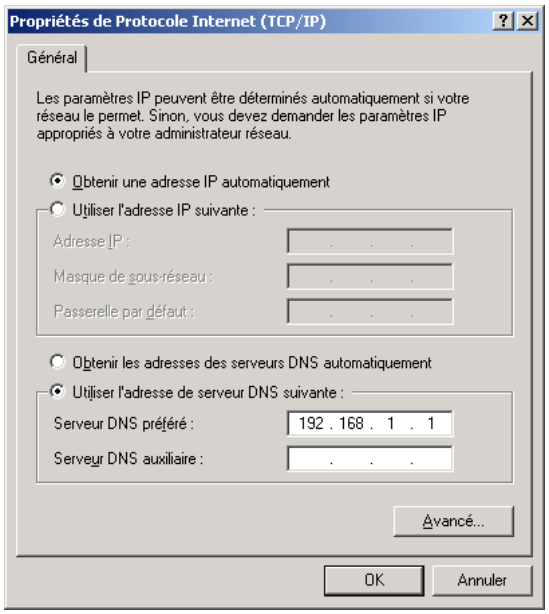
1. Cliquez sur **Démarrer**, pointez sur **Paramètres**, puis cliquez sur **Panneau de configuration**. Effectuez ensuite un double-clic sur l'icône **Connexions réseau et accès à distance**.
2. Avec le bouton droit de la souris, cliquez sur **Connexion au réseau local** et sélectionnez **Propriétés** dans le menu.
3. Sélectionnez l'élément **Protocole Internet (TCP/IP)**, puis cliquez sur **Propriétés**.



4. Sélectionnez l'option **Obtenir une adresse IP automatiquement**.
5. Sélectionnez l'option **Utiliser l'adresse de serveur DNS suivante**.

   Saisissez de préférence l'adresse IP du routeur. De cette façon, vous utilisez la fonction Proxy DNS du routeur qui vous permet d'optimiser la navigation.

   Remarque concernant le VPN Booster 32 i : ce paramétrage est notamment nécessaire si vous utilisez deux FAI distincts pour la connexion RNIS et pour la connexion xDSL. La fonction Proxy DNS vous permet de ne pas modifier l'adresse du serveur DNS dans les propriétés TCP/IP à chaque fois que vous changez de mode de connexion.



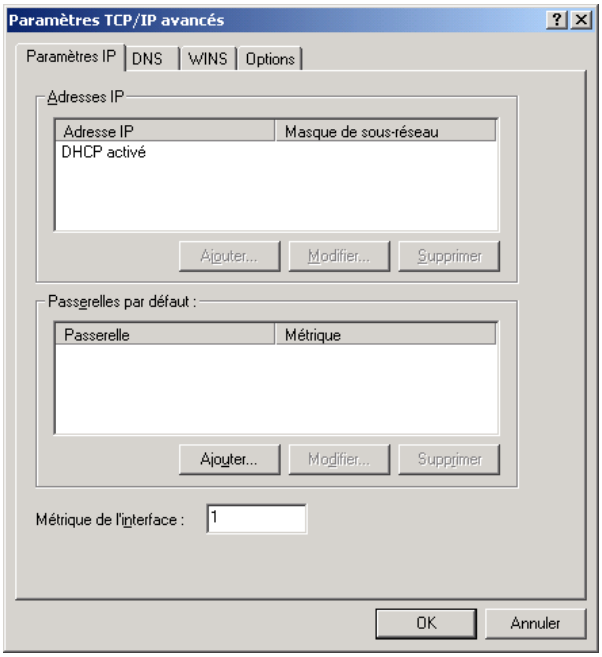
   Sinon, vous pouvez également saisir l'adresse de serveur DNS indiquée par votre FAI (pour cela, reportez-vous à la documentation fournie par celui-ci lors de la souscription de l'abonnement).

   Le cas échéant, vous pouvez ajouter une adresse de serveur DNS secondaire dans la rubrique **Serveur DNS auxiliaire**.

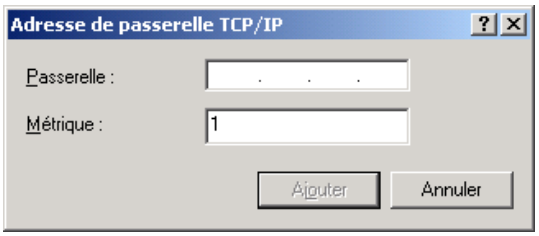
   Rappel : les serveurs DNS permettent la résolution des noms symboliques sur Internet.

   Cliquez sur **Avancé…**.

6. Dans la zone **Passerelles par défaut**, cliquez sur **Ajouter…**.



7. Dans la rubrique **Passerelle**, indiquez l'adresse IP du routeur, puis cliquez sur **Ajouter**.



Rappel : par défaut, l'adresse IP du VPN Booster est « 192.168.1.1 ».

8. Cliquez ensuite sur **OK** dans chacune des fenêtres et suivez les instructions à l'écran afin de valider les modifications.

Adresse IP fixe

Vous avez choisi d'attribuer des adresses IP fixes aux ordinateurs du réseau local. Procédez comme suit :

1. Cliquez sur **Démarrer**, pointez sur **Paramètres**, puis cliquez sur **Panneau de configuration**. Effectuez ensuite un double-clic sur l'icône **Connexions réseau et accès à distance**.
2. Avec le bouton droit de la souris, cliquez sur **Connexion au réseau local** et sélectionnez **Propriétés** dans le menu.
3. Sélectionnez l'élément **Protocole Internet (TCP/IP)**, puis cliquez sur **Propriétés**.
4. Sélectionnez **Utiliser l'adresse IP suivante**.
5. Dans la rubrique **Adresse IP**, entrez l'adresse IP que vous avez décidé d'attribuer au PC.

   Important :

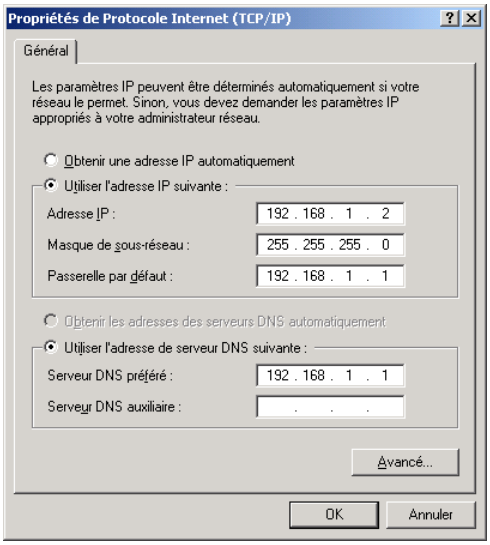
   - *L'adresse IP du PC doit impérativement être comprise dans la même plage d'adressage que celle du VPN Booster.*
   - *L'adresse IP du PC doit être unique, c'est-à-dire différente de celle des autres équipements présents sur le réseau local (ordinateurs, VPN Booster …).*
   - *L'adresse IP du PC doit appartenir à une plage réservée aux réseaux privés. En effet, votre réseau local ne doit pas utiliser des adresses réservées à Internet. Cela provoquerait des problèmes dans le cadre de la connexion de votre réseau à Internet.*

   En cas de doute sur ces points, vous devez prendre conseil auprès d'un spécialiste réseaux.
6. Dans la rubrique **Masque de sous-réseau**, entrez la valeur du masque de sous-réseau par défaut du VPN Booster, soit « 255.255.255.0 ».
7. Dans la rubrique **Passerelle par défaut**, entrez l'adresse IP attribuée au VPN Booster, puis cliquez sur **Ajouter**.

   Rappel : par défaut, l'adresse IP du VPN Booster est « 192.168.1.1 ».
8. Sélectionnez l'option **Utiliser l'adresse de serveur DNS suivante**.

   Saisissez de préférence l'adresse IP du routeur. De cette façon, vous utilisez la fonction Proxy DNS du routeur qui permet d'optimiser la navigation.

   Remarque concernant le VPN Booster 32 i : ce paramétrage est notamment nécessaire si vous utilisez deux FAI distincts pour la connexion RNIS et pour la connexion xDSL. La fonction Proxy DNS vous permet de ne pas modifier l'adresse du serveur DNS dans les propriétés TCP/IP à chaque fois que vous changez de mode de connexion.



Sinon, vous pouvez également saisir l'adresse de serveur DNS indiquée par votre FAI (pour cela, reportez-vous à la documentation fournie par celui-ci lors de la souscription de l'abonnement).

Le cas échéant, vous pouvez ajouter une adresse de serveurs DNS secondaire dans la rubrique **Serveur DNS auxiliaire**.

Rappel : les serveurs DNS permettent la résolution des noms symboliques sur Internet.

9. Cliquez sur **OK** afin de valider les modifications.

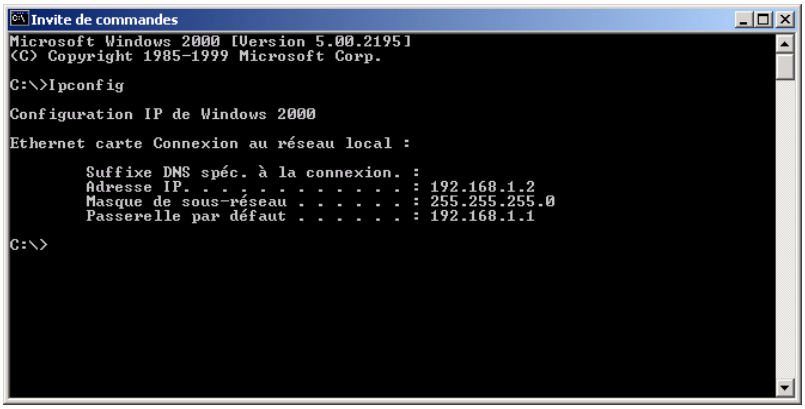
Vérification de la configuration

Les utilitaires *Ipconfig* et *Ping*, livrés avec Windows 2000, vous permettent de vérifier que la configuration réseau du PC est correcte et qu'il peut dialoguer avec le VPN Booster.

Avant d'exécuter ces utilitaires, assurez-vous que le VPN Booster est sous tension et que les câbles Ethernet sont correctement branchés (selon le modèle de routeur dont vous disposez, reportez-vous aux parties « Raccordement Ethernet » et « Raccordement du routeur à l'alimentation électrique » dans le chapitre « Raccordements du routeur » page 12, puis suivez les instructions).

Ipconfig

1. Cliquez sur **Démarrer**, pointez sur **Programmes**, **Accessoires**, puis cliquez sur **Invite de commandes**.
2. Dans la fenêtre **Invite de commandes**, tapez « Ipconfig », puis appuyez sur la touche **ENTRÉE**.



La fenêtre affiche les principales caractéristiques de la configuration IP de votre PC, à savoir :

- l'adresse IP de la carte. Cette adresse peur varier à chaque démarrage du PC si vous avez opté pour une adresse IP dynamique allouée par le serveur DHCP du VPN Booster ;
- le masque de sous-réseau utilisé ;
- la passerelle par défaut (adresse IP du VPN Booster).

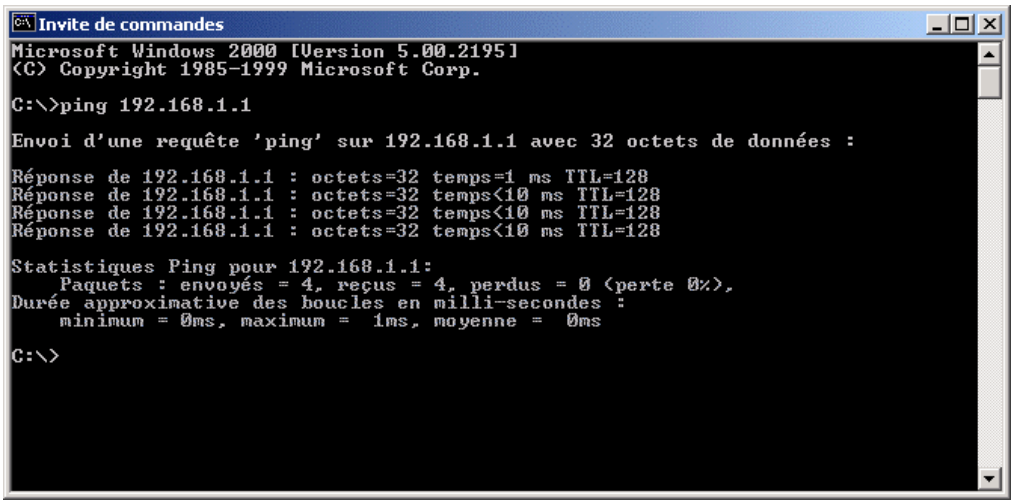
Ping

L'utilitaire Ping permet de tester le dialogue entre le PC et le VPN Booster à travers le protocole TCP/IP. Procédez comme suit :

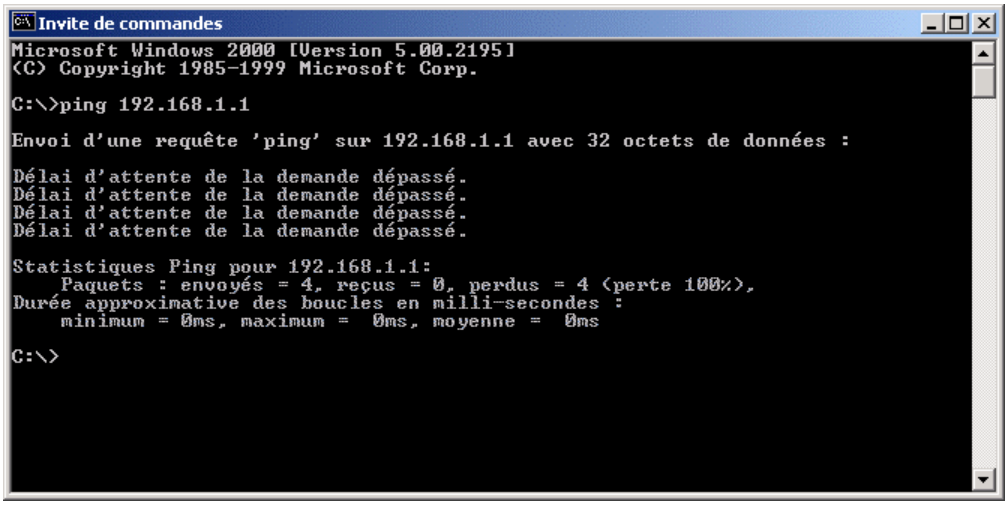
1. Cliquez sur **Démarrer**, pointez sur **Programmes**, **Accessoires**, puis cliquez sur **Invite de commandes**.
2. Dans la fenêtre **Invite de commandes**, tapez « ping » suivi de l'adresse IP du VPN Booster, puis appuyez sur la touche **ENTRÉE**.

   Remarque : si vous n'avez pas changé les paramètres IP par défaut du VPN Booster, vous devez donc taper « ping 192.168.1.1 ».

   Dans l'exemple ci-dessous, le dialogue entre le PC et le VPN Booster s'est correctement établi. Si vous obtenez un écran similaire, c'est que votre configuration est opérationnelle.



Dans l'exemple ci-dessous, le PC n'a pu dialoguer avec le VPN Booster. Si vous obtenez un écran similaire, c'est que votre configuration n'est pas opérationnelle. Vérifiez les adresses IP et la connexion des câbles.

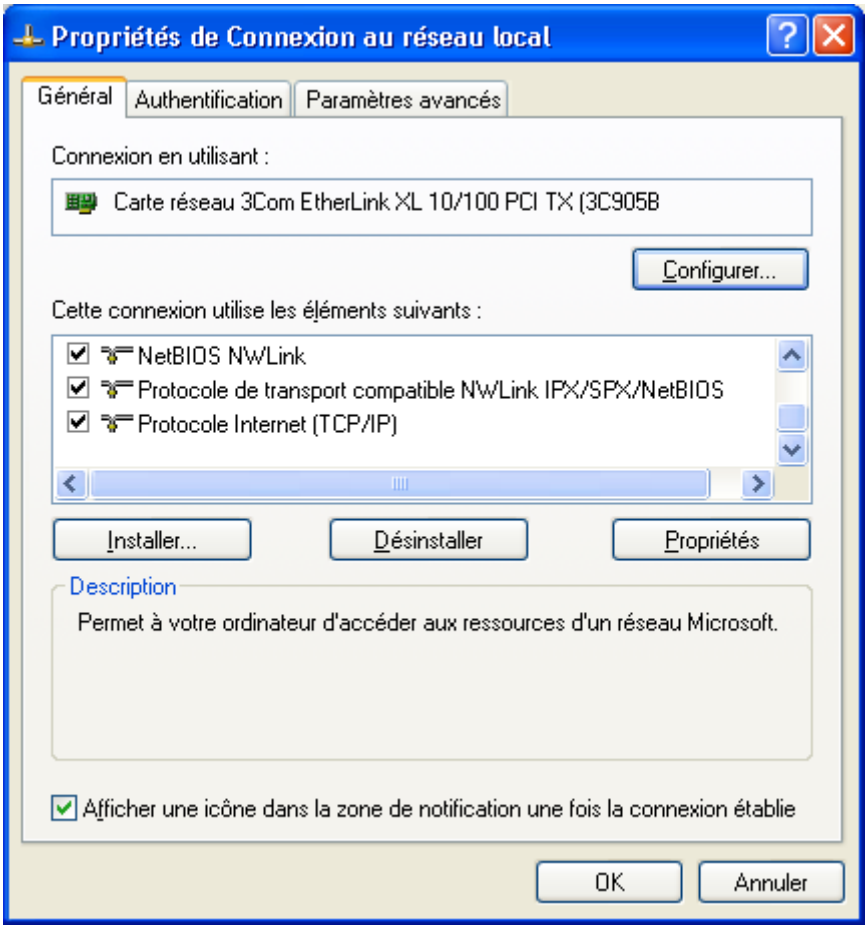


PC sous Windows XP

Vérification des protocoles

Le VPN Booster utilise le protocole réseau TCP/IP. Celui-ci est installé par défaut dans Windows XP.

1. Cliquez sur **démarrer**, puis sur **Panneau de configuration**.
2. Cliquez sur **Connexions réseau et Internet**, puis sur **Connexions réseau**.
3. Avec le bouton droit de la souris, cliquez sur **Connexion au réseau local**, puis sélectionnez **Propriétés** dans le menu.



4. Dans la liste **Cette connexion utilise les éléments suivants**, l'élément suivant est présent :
   - **Protocole Internet (TCP/IP)**

Paramétrage du PC

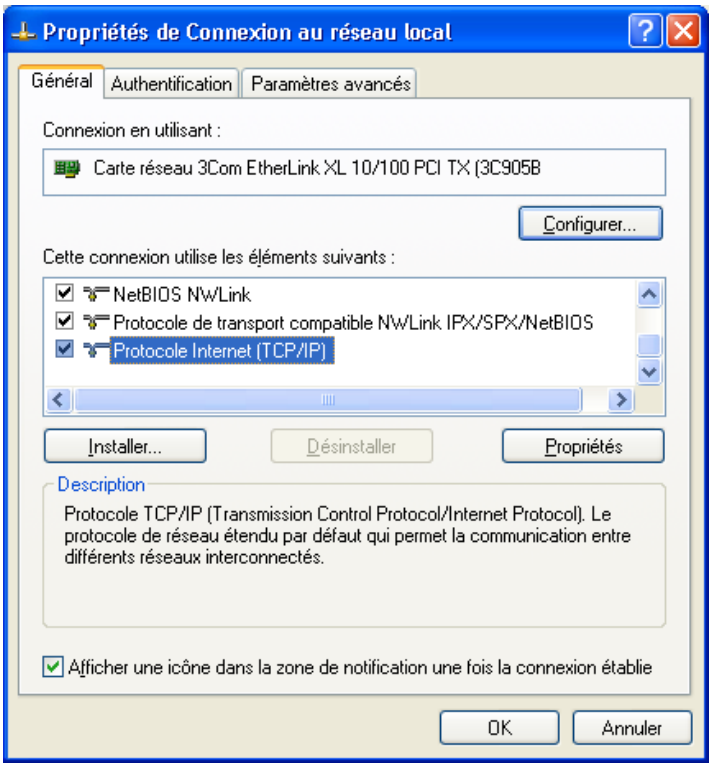
Nous avons vu dans l'introduction que votre réseau local TCP/IP pouvait fonctionner avec des adresses IP dynamiques ou fixes. En fonction de votre choix, reportez-vous à la section correspondante.

Adresse IP dynamique

Vous avez choisi d'utiliser le serveur DHCP du VPN Booster afin que celui-ci alloue dynamiquement des adresses IP aux ordinateurs du réseau local, procédez comme suit :

1. Cliquez sur **démarrer**, puis sur **Panneau de configuration**.
2. Cliquez sur **Connexions réseau et Internet**, puis sur **Connexions réseau**.
3. Avec le bouton droit de la souris, cliquez sur **Connexion au réseau local**, puis sélectionnez **Propriétés** dans le menu.

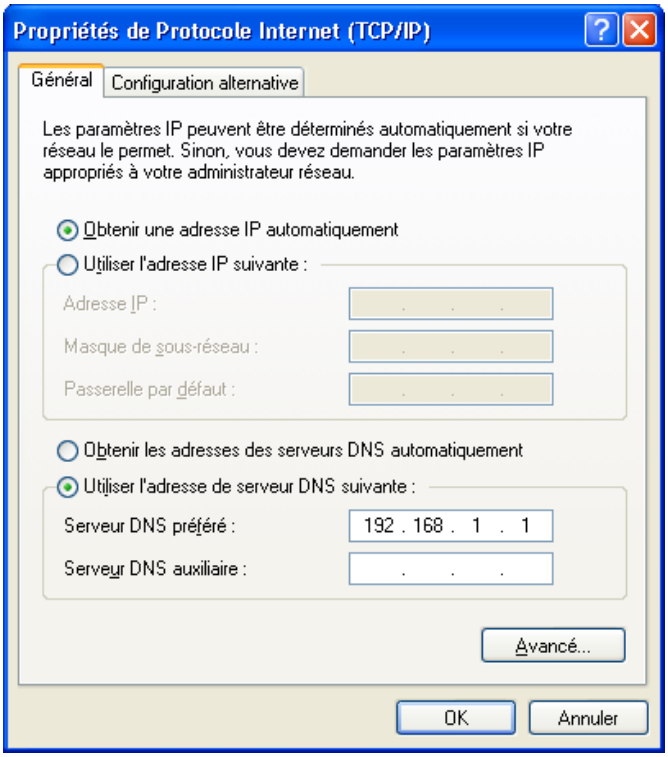
4. Sélectionnez l'élément **Protocole Internet (TCP/IP)**, puis cliquez sur **Propriétés**.



5. Sélectionnez l'option **Obtenir une adresse IP automatiquement**.
6. Sélectionnez l'option **Utiliser l'adresse de serveur DNS suivante**.

   Saisissez de préférence l'adresse IP du routeur. De cette façon, vous utilisez la fonction Proxy DNS du routeur qui vous permet d'optimiser la navigation.

   Remarque concernant le VPN Booster 32 i : ce paramétrage est notamment nécessaire si vous utilisez deux FAI distincts pour la connexion RNIS et pour la connexion xDSL. La fonction Proxy DNS vous permet de ne pas modifier l'adresse du serveur DNS dans les propriétés TCP/IP à chaque fois que vous changez de mode de connexion.



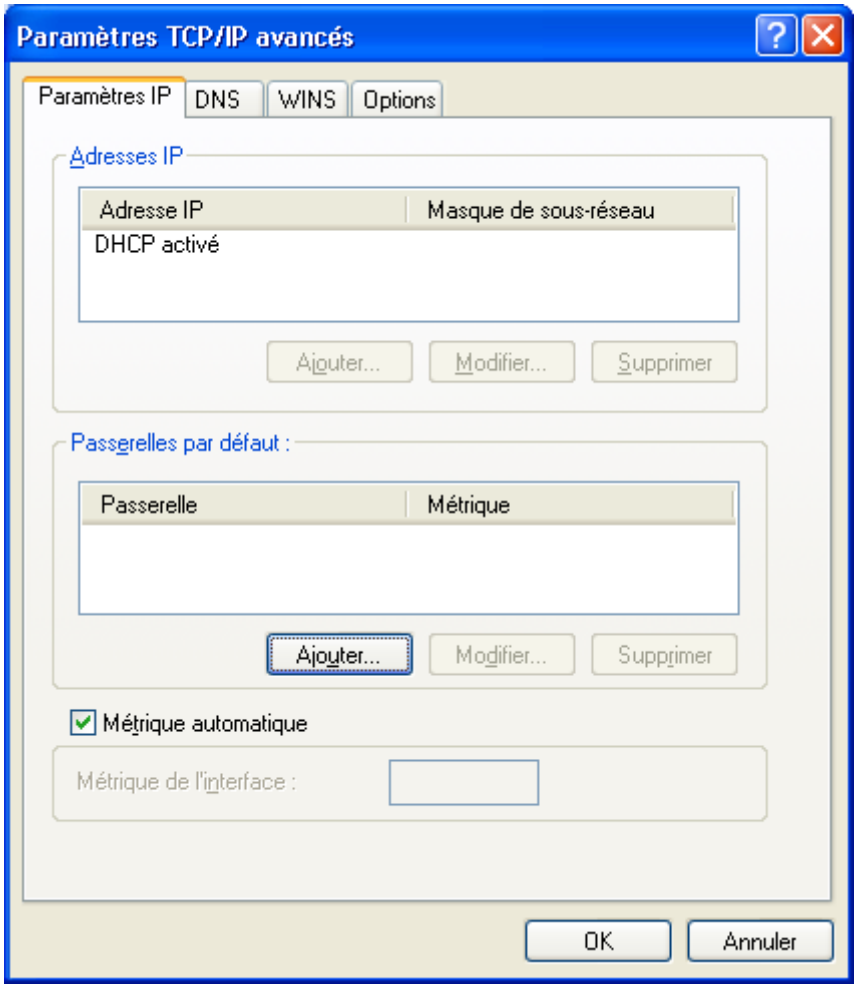
Sinon, vous pouvez également saisir l'adresse de serveur DNS indiquée par votre FAI (pour cela, reportez-vous à la documentation fournie par celui-ci lors de la souscription de l'abonnement).

Le cas échéant, vous pouvez ajouter une adresse de serveur DNS secondaire dans la rubrique **Serveur DNS auxiliaire**.

Rappel : les serveurs DNS permettent la résolution des noms symboliques sur Internet.

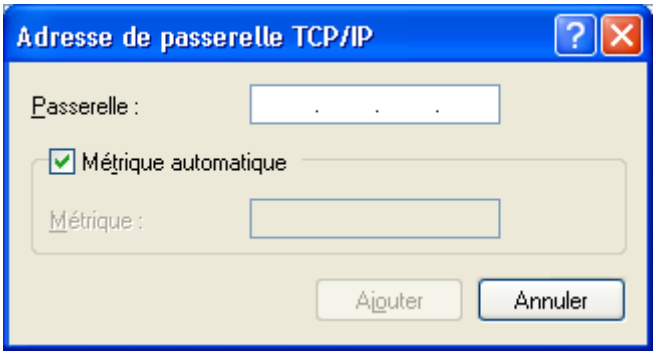
Cliquez sur **Avancé…**.

7. Dans la zone **Passerelles par défaut**, cliquez sur **Ajouter…**.



8. Dans la rubrique **Passerelle**, indiquez l'adresse IP du routeur, puis cliquez sur **Ajouter**.

   Rappel : par défaut, l'adresse IP du VPN Booster est « 192.168.1.1 ».

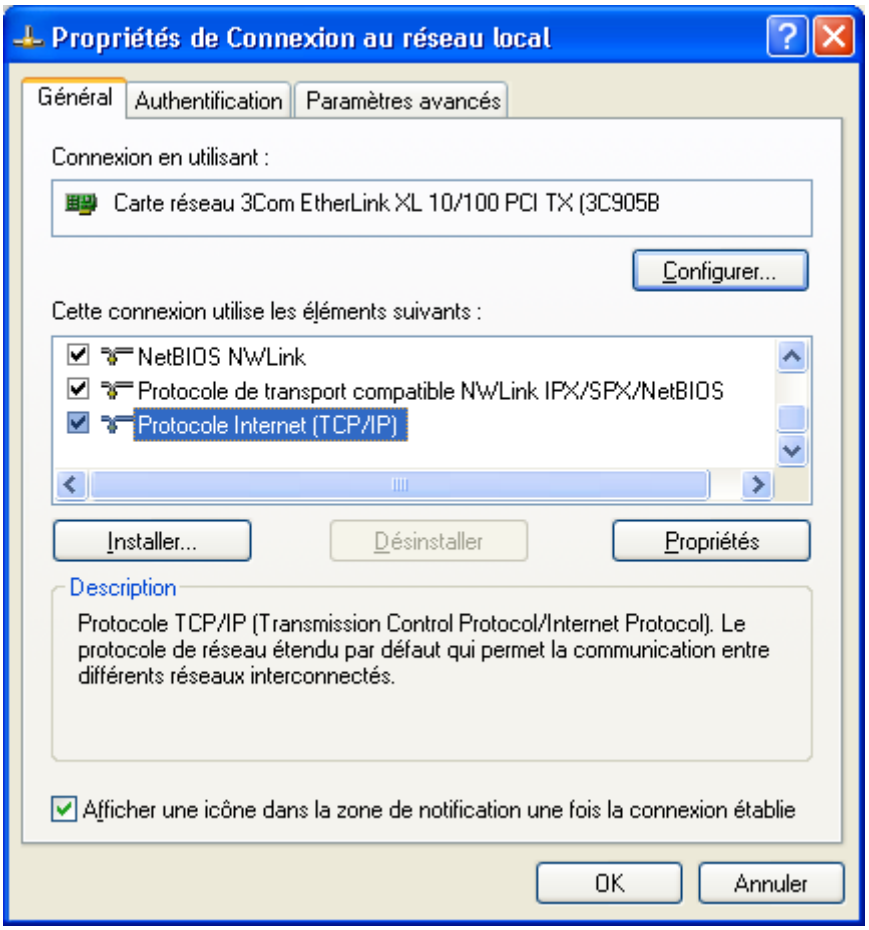


9. Cliquez ensuite sur **OK** dans chacune des fenêtres et suivez les instructions à l'écran afin de valider les modifications.

Adresse IP fixe

Vous avez choisi d'attribuer des adresses IP fixes aux ordinateurs du réseau local. Procédez comme suit :

1. Cliquez sur **démarrer**, puis sur **Panneau de configuration**.
2. Cliquez sur **Connexions réseau et Internet**, puis sur **Connexions réseau**.
3. Avec le bouton droit de la souris, cliquez sur **Connexion au réseau local**, puis sélectionnez **Propriétés** dans le menu.
4. Sélectionnez l'élément **Protocole Internet (TCP/IP)**, puis cliquez sur **Propriétés**.



5. Sélectionnez **Utiliser l'adresse IP suivante**.
6. Dans la rubrique **Adresse IP**, entrez l'adresse IP que vous avez décidé d'attribuer au PC.

   Important :

   - *L'adresse IP du PC doit impérativement être comprise dans la même plage d'adressage que celle du VPN Booster.*
   - *L'adresse IP du PC doit être unique, c'est-à-dire différente de celle des autres équipements présents sur le réseau local (ordinateurs, VPN Booster …).*
   - *L'adresse IP du PC doit appartenir à une plage réservée aux réseaux privés. En effet, votre réseau local ne doit pas utiliser des adresses réservées à Internet. Cela provoquerait des problèmes dans le cadre de la connexion de votre réseau à Internet.*

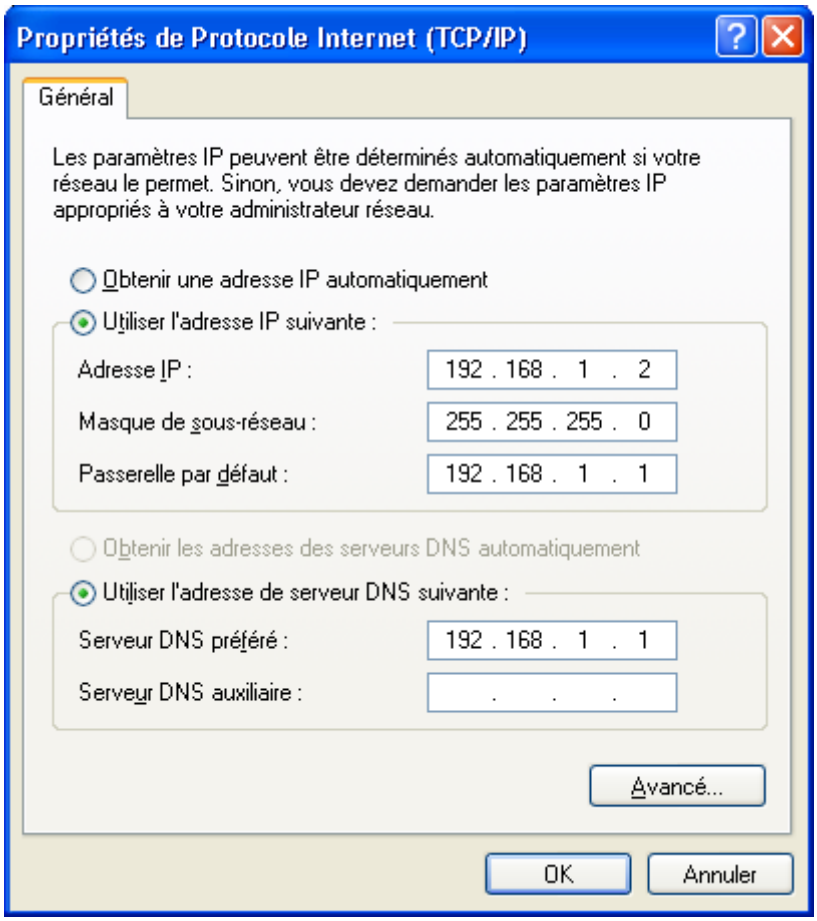
   En cas de doute sur ces points, vous devez prendre conseil auprès d'un spécialiste réseaux.
7. Dans la rubrique **Masque de sous-réseau,** entrez la valeur du masque de sous-réseau par défaut du VPN Booster, soit « 255.255.255.0 ».
8. Dans la rubrique **Passerelle par défaut**, entrez l'adresse IP attribuée au VPN Booster.

   Rappel : par défaut, l'adresse IP du VPN Booster est « 192.168.1.1 ».

9. Sélectionnez l'option **Utiliser l'adresse de serveur DNS suivante**.

   Saisissez de préférence l'adresse IP du routeur. De cette façon, vous utilisez la fonction Proxy DNS du routeur qui vous permet d'optimiser la navigation.

   Remarque concernant le VPN Booster 32 i : ce paramétrage est notamment nécessaire si vous utilisez deux FAI distincts pour la connexion RNIS et pour la connexion xDSL. La fonction Proxy DNS vous permet de ne pas modifier l'adresse du serveur DNS dans les propriétés TCP/IP à chaque fois que vous changez de mode de connexion.



   Sinon, vous pouvez également saisir l'adresse de serveur DNS indiquée par votre FAI (pour cela, reportez-vous à la documentation fournie par celui-ci lors de la souscription de l'abonnement).

   Le cas échéant, vous pouvez ajouter une adresse de serveurs DNS secondaire dans la rubrique **Serveur DNS auxiliaire**.

   Rappel : les serveurs DNS permettent la résolution des noms symboliques sur Internet.

10. Cliquez sur **OK** afin de valider les modifications.

Vérification de la configuration

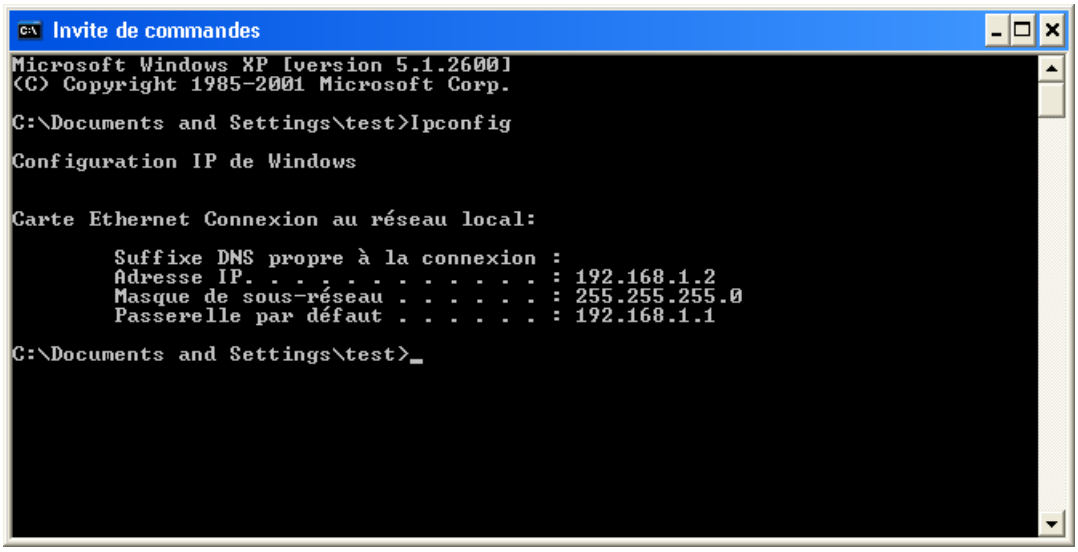
Les utilitaires *Ipconfig* et *Ping*, livrés avec Windows XP, vous permettent de vérifier que la configuration réseau du PC est correcte et qu'il peut dialoguer avec le VPN Booster.

Avant d'exécuter ces utilitaires, assurez-vous que le VPN Booster est sous tension et que les câbles Ethernet sont correctement branchés (selon le modèle de routeur dont vous disposez, reportez-vous aux parties « Raccordement Ethernet » et « Raccordement du routeur à l'alimentation électrique » dans le chapitre « Raccordements du routeur » page 12, puis suivez les instructions).

Ipconfig

L'utilitaire *Ipconfig* permet de vérifier que votre configuration a bien été prise en compte. Procédez comme suit :

1. Cliquez sur **démarrer**, **Tous les programmes**, pointez sur **Accessoires**, puis cliquez sur **Invite de commandes**.
2. Dans la fenêtre **Invite de commandes**, tapez « Ipconfig », puis appuyez sur la touche **ENTRÉE**.



La fenêtre affiche les principales caractéristiques de la configuration IP de votre PC, à savoir :

- l'adresse IP de la carte. Cette adresse peur varier à chaque démarrage du PC si vous avez opté pour une adresse IP dynamique allouée par le serveur DHCP du VPN Booster ;
- le masque de sous-réseau utilisé ;
- la passerelle par défaut (adresse IP du VPN Booster).

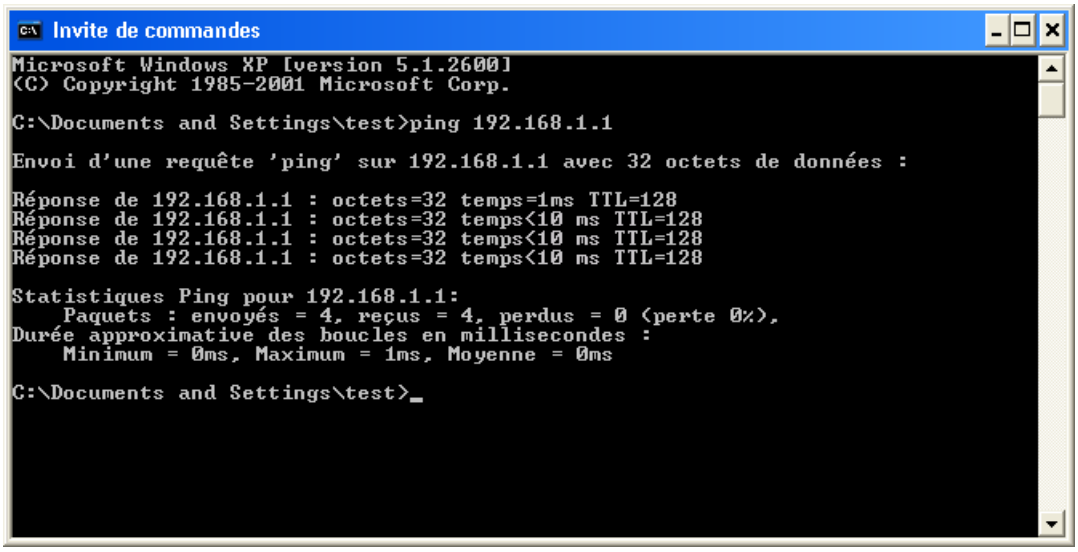
Ping

L'utilitaire Ping permet de tester le dialogue entre le PC et le VPN Booster à travers le protocole TCP/IP. Procédez comme suit :

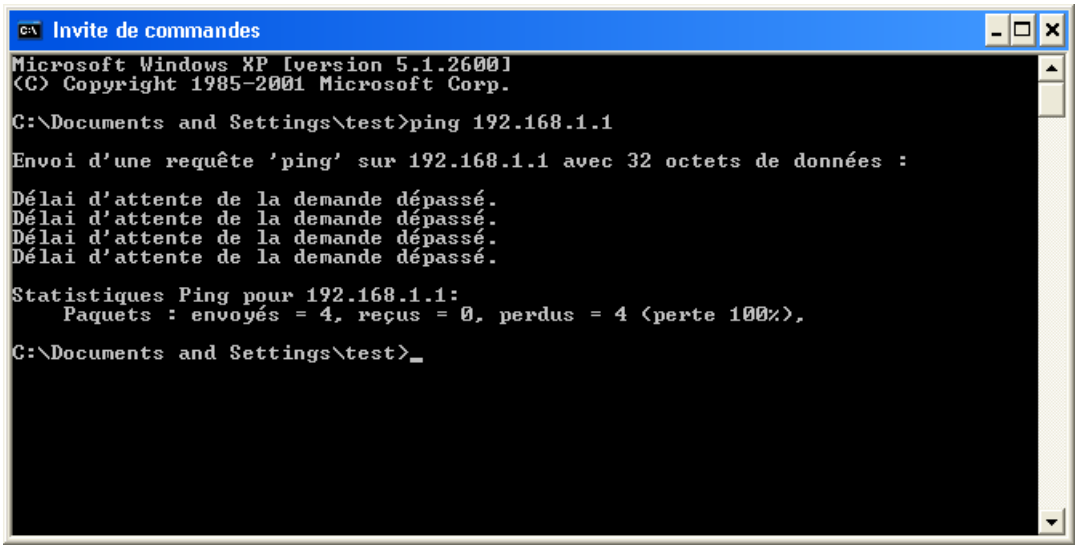
1. Cliquez sur **démarrer**, **Tous les programmes**, pointez sur **Accessoires**, puis cliquez sur **Invite de commandes**.
2. Dans la fenêtre **Invite de commandes**, tapez « ping » suivi de l'adresse IP du VPN Booster, puis appuyez sur la touche **ENTRÉE**.

   Remarque : si vous n'avez pas changé les paramètres IP par défaut du VPN Booster, vous devez donc taper « ping 192.168.1.1 ».

Dans l'exemple ci-dessous, le dialogue entre le PC et le VPN Booster s'est correctement établi. Si vous obtenez un écran similaire, c'est que votre configuration est opérationnelle.



Dans l'exemple ci-dessous, le PC n'a pu dialoguer avec le VPN Booster. Si vous obtenez un écran similaire, c'est que votre configuration n'est pas opérationnelle. Vérifiez les adresses IP et la connexion des câbles.



Macintosh (Mac OS 9)

Vérification des protocoles

Le VPN Booster utilise le protocole réseau TCP/IP, il faut donc que celui-ci soit installé sur votre Macintosh. Le protocole TCP/IP est inclus par défaut dans les versions récentes de Mac OS, notamment les versions Mac OS 8.0 et supérieures.

Remarque : nous ne documentons pas ici la configuration de Macintosh utilisant un système d'exploitation antérieur à Mac OS 9. Si vous êtes dans ce cas, veuillez vous reporter à la documentation fournie par le constructeur ou faites-vous assister par un spécialiste.

Paramétrage du Macintosh

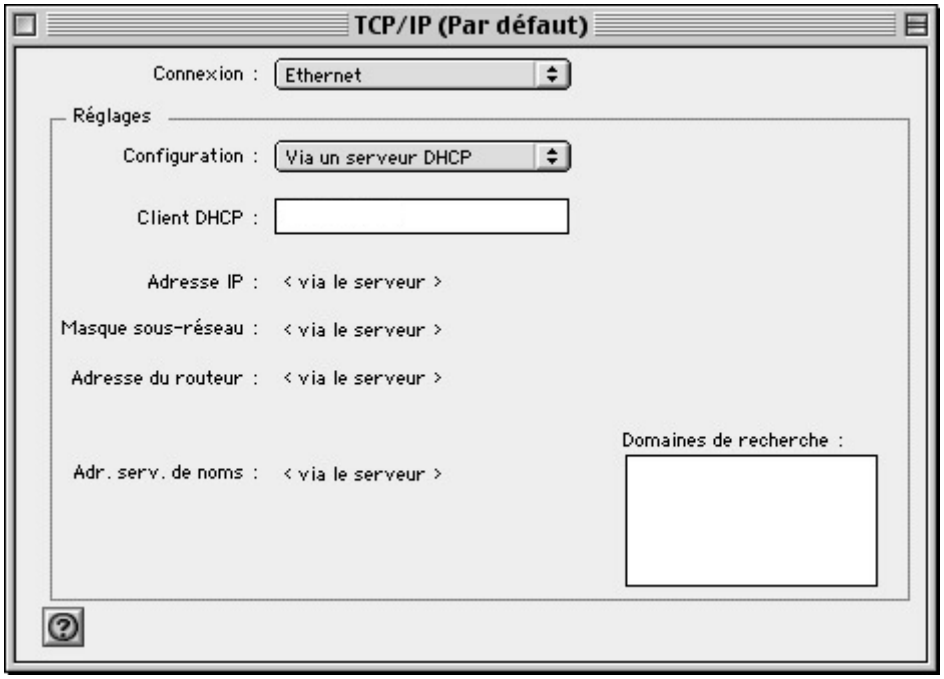
Nous avons vu dans le chapitre « Equipement informatique existant au sein de l'entreprise » page 24, que votre réseau local TCP/IP pouvait fonctionner avec des adresses IP dynamiques ou fixes. En fonction de votre choix, reportez-vous à la section correspondante.

Adresse IP dynamique

Vous avez choisi d'utiliser le serveur DHCP du VPN Booster afin que celui-ci alloue dynamiquement des adresses IP aux ordinateurs du réseau local, procédez comme suit :

1. Choisissez menu **Pomme > Tableau de bord > TCP/IP**.
2. Dans le menu **Connexion**, sélectionnez **Ethernet**.
3. Dans le menu **Configuration**, sélectionnez **Via un serveur DHCP**.
4. Dans la rubrique **Client DHCP**, spécifiez un nom attribué au VPN Booster.

   Rappel : par défaut, l'adresse IP du VPN Booster est « 192.168.1.1 ».



5. Dans la barre des menus, choisissez **Fichier,** puis **Quitter**.
6. Dans la fenêtre de confirmation des modifications, cliquez sur **Enregistrer**.
7. Redémarrez le Macintosh.

Adresse IP fixe

Vous avez choisi d'attribuer des adresses IP fixes aux ordinateurs du réseau local. Procédez comme suit :

1. Choisissez menu **Pomme > Tableau de bord > TCP/IP**.
2. Dans le menu **Connexion,** sélectionnez **Ethernet**.
3. Dans le menu **Configuration,** sélectionnez **Manuellement**.
4. Dans la rubrique **Adresse IP**, spécifiez l'adresse IP que vous avez décidé d'attribuer à votre Macintosh.

   Important :

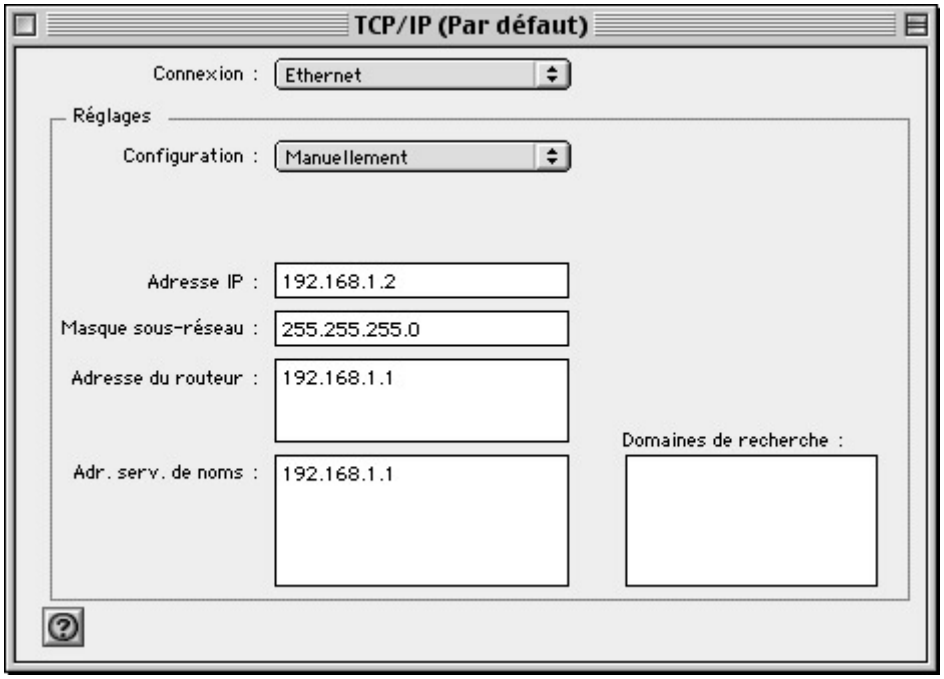
   - *L'adresse IP du Macintosh doit impérativement être comprise dans la même plage d'adressage que celle du VPN Booster.*
   - *L'adresse IP du Macintosh doit être unique, c'est-à-dire différente de celle des autres équipements présents sur le réseau local (ordinateurs, VPN Booster …).*
   - *L'adresse IP du Macintosh doit appartenir à une plage réservée aux réseaux privés. En effet, votre réseau local ne doit pas utiliser des adresses réservées à Internet. Cela provoquerait des problèmes dans le cadre de la connexion de votre réseau à Internet.*

   En cas de doute sur ces points, vous devez prendre conseil auprès d'un spécialiste réseaux.
5. Dans la rubrique **Masque sous-réseau**, spécifiez la valeur du masque de sous-réseau par défaut du VPN Booster, soit « 255.255.255.0 ».
6. Dans la rubrique **Adresse du routeur**, spécifiez l'adresse IP attribuée au VPN Booster.

   Rappel : par défaut, l'adresse IP du VPN Booster est « 192.168.1.1 ».
7. Dans la rubrique **Adr. serv. de noms**, saisissez de préférence l'adresse IP du routeur. De cette façon, vous utilisez la fonction Proxy DNS du routeur qui permet d'optimiser la navigation.

   Remarque concernant le VPN Booster 32 i : ce paramétrage est notamment nécessaire si vous utilisez deux FAI distincts pour la connexion RNIS et pour la connexion xDSL. La fonction Proxy DNS vous permet de ne pas modifier l'adresse du serveur DNS dans les propriétés TCP/IP à chaque fois que vous changez de mode de connexion.

   Sinon, vous pouvez également saisir l'adresse de serveur DNS indiquée par votre FAI (pour cela, reportez-vous à la documentation fournie par celui-ci lors de la souscription de l'abonnement).



8. Dans la fenêtre de confirmation des modifications, cliquez sur **Enregistrer**.
9. Redémarrez le Macintosh.

Macintosh (Mac OS X)

Paramétrage du Macintosh

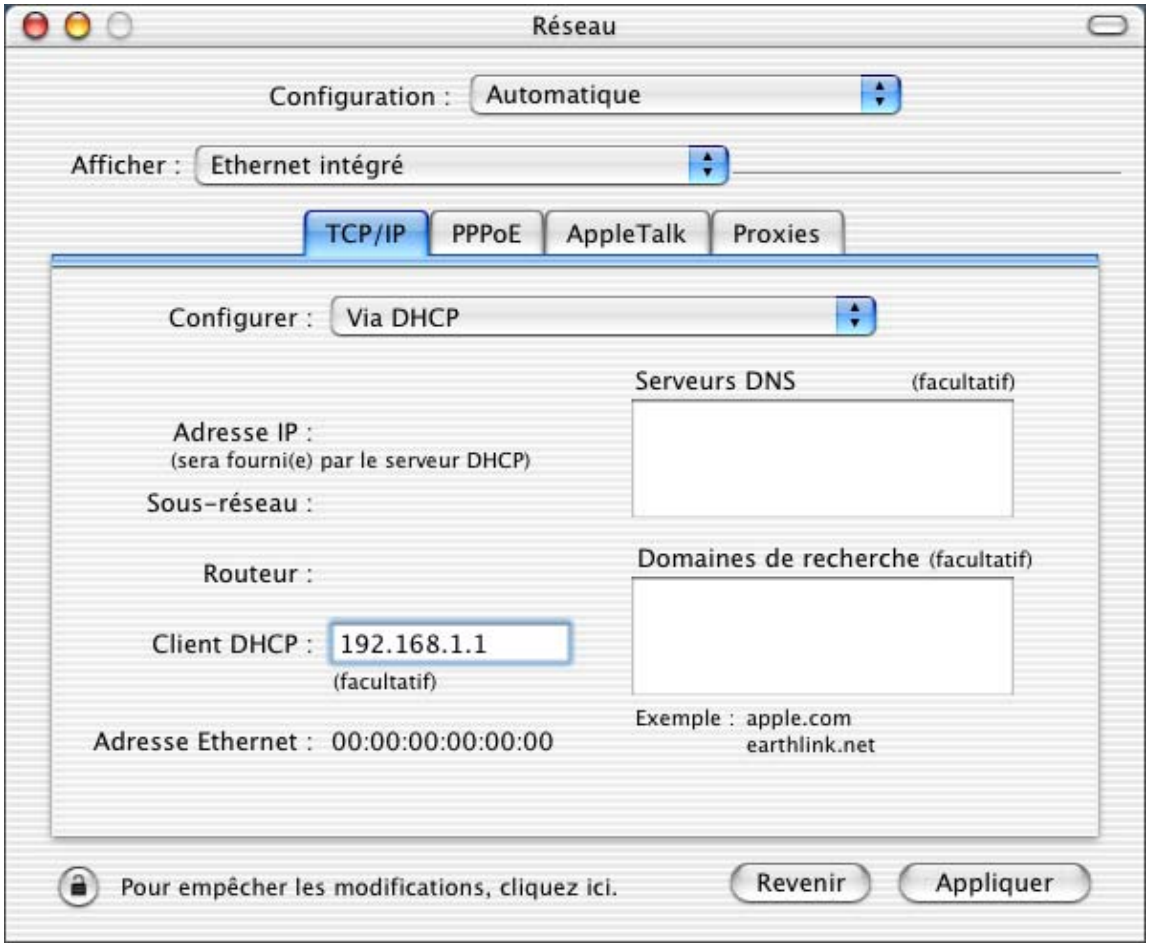
Nous avons vu dans le chapitre « Equipement informatique existant au sein de l'entreprise » page 24, que votre réseau local TCP/IP pouvait fonctionner avec des adresses IP dynamiques ou fixes. En fonction de votre choix, reportez-vous à la section correspondante.

Adresse IP dynamique

Vous avez choisi d'utiliser le serveur DHCP du VPN Booster afin que celui-ci alloue dynamiquement des adresses IP aux ordinateurs du réseau local, procédez comme suit :

1. Effectuez un double-clic sur l'icône de votre disque dur, sur **Applications**, puis sur **Préférences Système**.
2. Cliquez ensuite sur **Réseau**.
3. Dans le menu **Afficher**, sélectionnez **Ethernet intégré**.
4. Dans le menu **Configurer** de l'onglet **TCP/IP**, sélectionnez **Via DHCP**.
5. Dans la rubrique **Client DHCP**, spécifiez un nom attribué au VPN Booster.

   Rappel : par défaut, l'adresse IP du VPN Booster est « 192.168.1.1 ».



6. Cliquez sur le bouton **Appliquer** pour sauvegarder vos modifications.
7. Dans le menu **Préférences Système**, cliquez sur **Quitter Préférences Système**.

Adresse IP fixe

Vous avez choisi d'attribuer des adresses IP fixes aux ordinateurs du réseau local. Procédez comme suit :

1. Effectuez un double-clic sur l'icône de votre disque dur, sur **Applications**, puis sur **Préférences Système**.
2. Cliquez ensuite sur **Réseau**.
3. Dans le menu **Afficher**, sélectionnez **Ethernet intégré**.
4. Dans le menu **Configurer** de l'onglet **TCP/IP**, sélectionnez **Manuellement**.
5. Dans la rubrique **Adresse IP**, spécifiez l'adresse IP que vous avez décidé d'attribuer à votre Macintosh.

   Important :

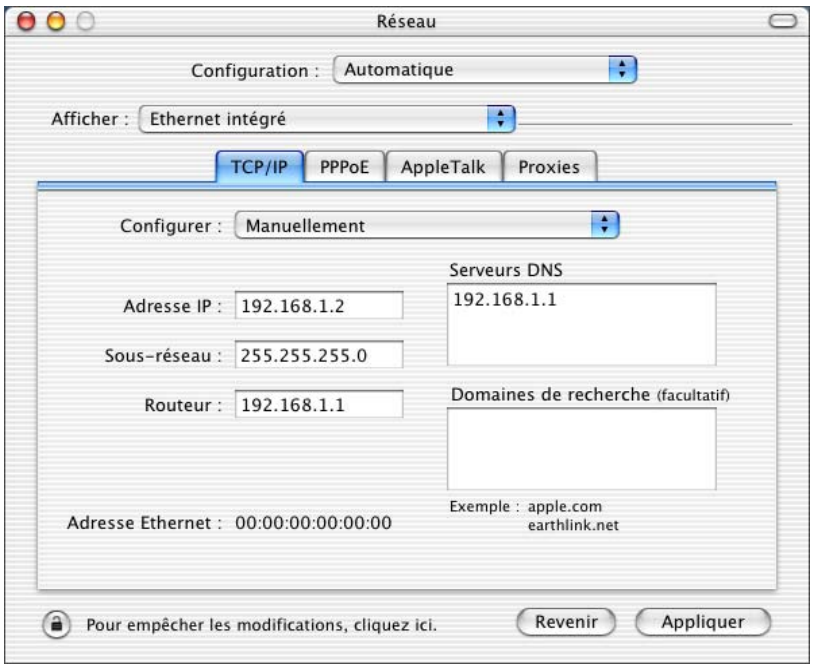
   - *L'adresse IP du Macintosh doit impérativement être comprise dans la même plage d'adressage que celle du VPN Booster.*
   - *L'adresse IP du Macintosh doit être unique, c'est-à-dire différente de celle des autres équipements présents sur le réseau local (ordinateurs, VPN Booster …).*
   - *L'adresse IP du Macintosh doit appartenir à une plage réservée aux réseaux privés. En effet, votre réseau local ne doit pas utiliser des adresses réservées à Internet. Cela provoquerait des problèmes dans le cadre de la connexion de votre réseau à Internet.*

   En cas de doute sur ces points, vous devez prendre conseil auprès d'un spécialiste réseaux.
6. Dans la rubrique **Sous-réseau,** spécifiez la valeur du masque de sous-réseau par défaut du VPN Booster, soit « 255.255.255.0 ».
7. Dans la rubrique **Routeur**, spécifiez l'adresse IP attribuée au VPN Booster.

   Rappel : par défaut, l'adresse IP du VPN Booster est « 192.168.1.1 ».
8. Dans la rubrique **Serveurs DNS**, saisissez de préférence l'adresse IP du routeur. De cette façon, vous utilisez la fonction Proxy DNS du routeur qui permet d'optimiser la navigation.

   Remarque concernant le VPN Booster 32 i : ce paramétrage est notamment nécessaire si vous utilisez deux FAI distincts pour la connexion RNIS et pour la connexion xDSL. La fonction Proxy DNS vous permet de ne pas modifier l'adresse du serveur DNS dans les propriétés TCP/IP à chaque fois que vous changez de mode de connexion.

   Sinon, vous pouvez également saisir l'adresse de serveur DNS indiquée par votre FAI (pour cela, reportez-vous à la documentation fournie par celui-ci lors de la souscription de l'abonnement).



9. Cliquez sur le bouton **Appliquer** pour sauvegarder vos modifications.
10. Dans le menu **Préférences Système**, cliquez sur **Quitter Préférences Système**.

Configuration des logiciels de navigation

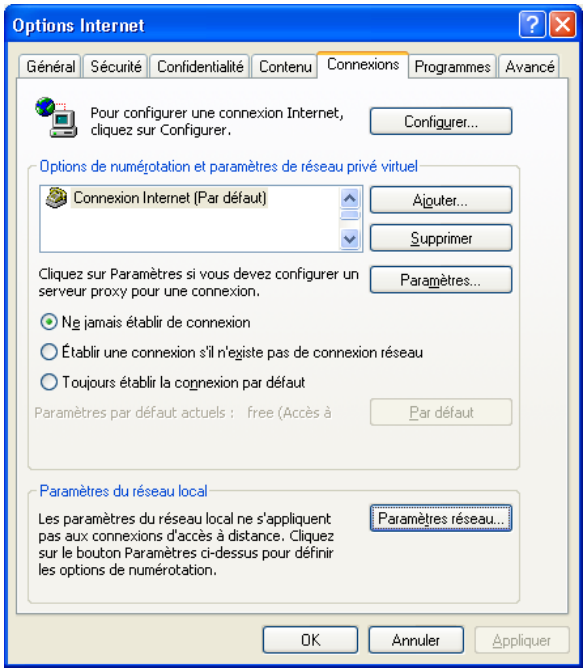
Nous indiquons dans ce chapitre comment les logiciels de navigation installés sur les ordinateurs du réseau local doivent être configurés pour pouvoir utiliser le VPN Booster.

Nous avons pris l'exemple des logiciels les plus couramment utilisés, à savoir Microsoft® Internet Explorer et Mozilla. Si vous disposez d'un autre logiciel de navigation, vous devez vous référer à sa documentation pour toute information sur son mode de configuration.

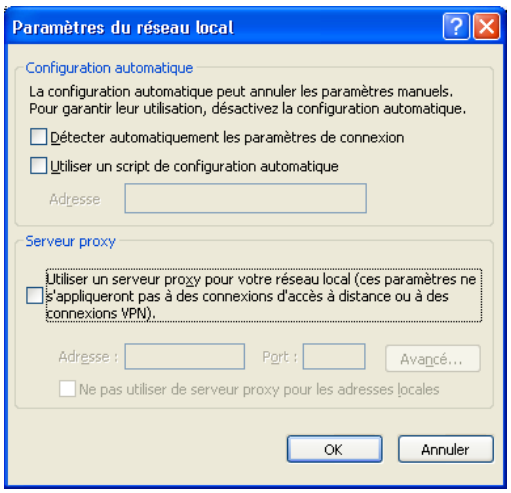
Microsoft® Internet Explorer

Pour un ordinateur disposant de Microsoft® Internet Explorer, procédez comme suit :

1. Lancez le logiciel **Internet Explorer**.
2. Dans le menu **Outils**, sélectionnez **Options Internet…**.
3. Cliquez sur l'onglet **Connexions**.



4. Dans la zone **Options de numérotation et paramètres de réseau privé virtuel**, si une connexion Internet est déjà configurée, sélectionnez **Ne jamais établir de connexion**.
5. Cliquez sur le bouton **Paramètres réseau…** et vérifiez ensuite qu'aucune case n'est cochée dans la fenêtre **Paramètres du réseau local**.

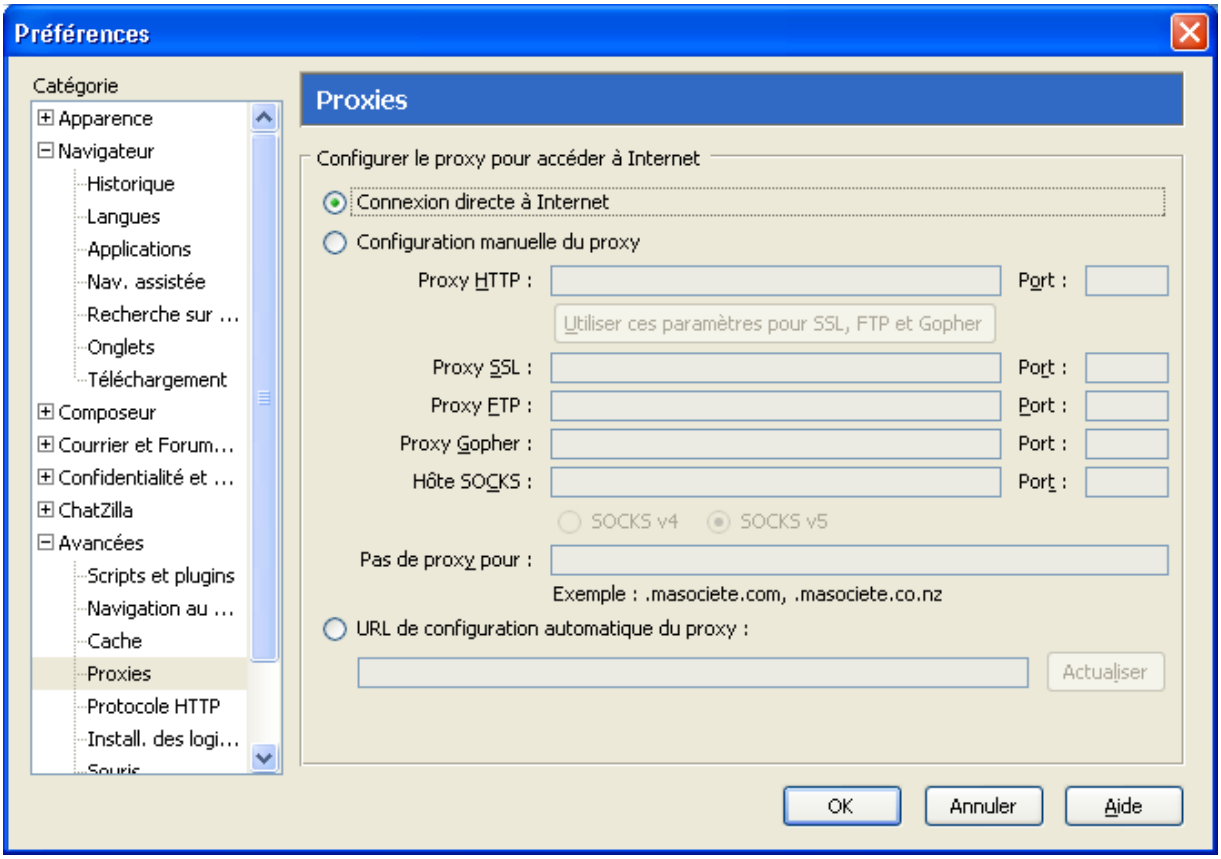


6. Refermez toutes les fenêtres en cliquant sur **OK**.

Mozilla

Pour un ordinateur disposant de Mozilla, procédez comme suit :

1. Lancez le logiciel **Mozilla**.
2. Dans le menu **Edition**, sélectionnez **Préférences…**.
3. Dans la liste **Catégorie**, développez la catégorie **Avancées** et sélectionnez **Proxies**.
4. Sélectionnez **Connexion directe à Internet**.



5. Cliquez sur **OK** afin de valider votre configuration.

Installation et utilisation de l'Assistant de démarrage

L'Assistant de démarrage permet de configurer l'adresse IP du VPN Booster, puis de lancer son configurateur HTML ou démarrer une session Telnet afin de compléter le paramétrage.

Remarque : l'utilisation de l'Assistant de démarrage n'est pas nécessaire si l'adresse IP par défaut du VPN Booster est compatible avec le plan d'adressage de votre réseau. Vous pouvez dans ce cas paramétrer directement le VPN Booster en mode HTML (voir « Accès à l'administration HTML du routeur » page 66) ou Telnet (voir « Commandes Telnet » page 183).

Configuration requise

Pour utiliser l'Assistant de démarrage du VPN Booster, vous devez disposer d'un ordinateur dans la configuration suivante :

- systèmes d'exploitation :
  - PC : Windows 95, 98, Me, NT 4.0, 2000 ou XP,
  - Macintosh : Mac OS 9 à Mac OS X.
- un lecteur de CD-ROM,
- une carte réseau Ethernet et le protocole TCP/IP correctement installés (voir « Configuration des ordinateurs » page 26).

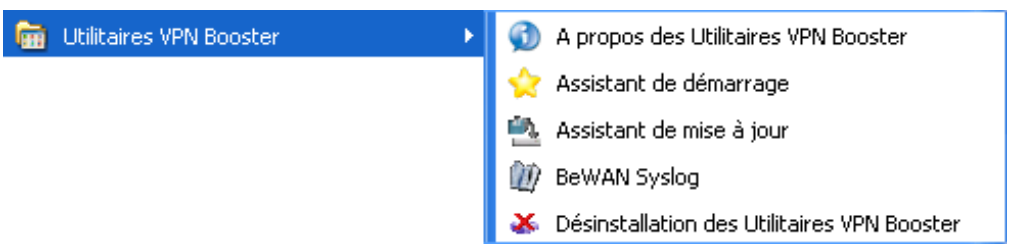
Configuration pour PC

Votre ordinateur doit être correctement raccordé au VPN Booster, soit directement, soit via un concentrateur Ethernet (selon le modèle de routeur dont vous disposez, reportez-vous à la partie « Raccordement Ethernet » du chapitre « Raccordements du routeur » page 12).

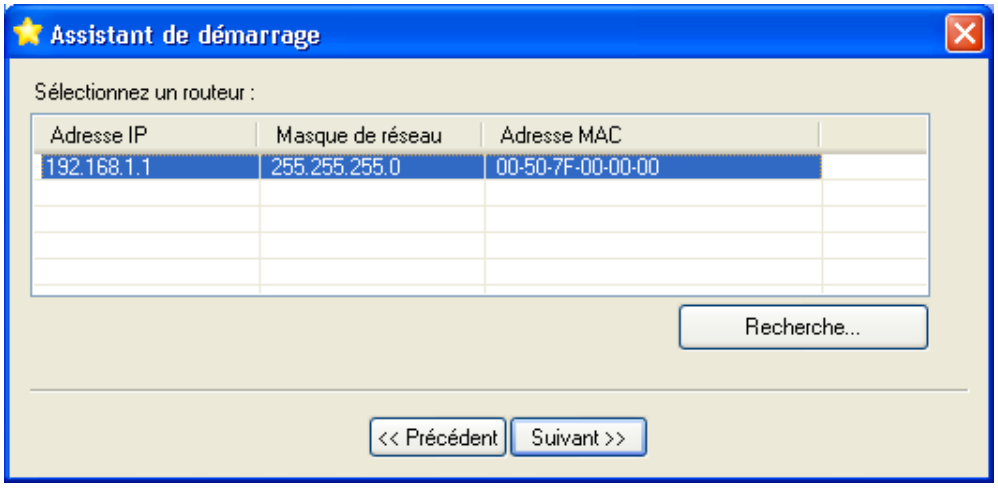
Le VPN Booster doit être raccordé à une prise électrique (selon le modèle de routeur dont vous disposez, voir la partie « Raccordement du routeur à l'alimentation électrique » dans le chapitre « Raccordements du routeur » page 12).

Procédez comme suit :

1. Insérez le CD-ROM Routeurs VPN Booster dans le lecteur du PC. Si la configuration du PC l'autorise, le programme d'installation est lancé automatiquement. Si le lancement n'est pas automatique, exécutez le programme **autorun.exe** qui se trouve à la racine du CD-ROM.
2. Cliquez sur **Débuter l'installation**, le modèle VPN Booster dont vous disposez, **Utilitaires**, puis sur **Utilitaires VPN Booster**.
3. Une fois dans le programme d'installation des Utilitaires, il vous suffit de suivre les instructions de l'Assistant et de cliquer plusieurs fois sur **Suivant**.
4. Dans la fenêtre intitulée **Confirmation**, cliquez sur **Démarrer**.
5. Une fenêtre vous indique ensuite que les Utilitaires VPN Booster ont bien été installés. Cliquez sur **Quitter**.
6. Pour lancer l'Assistant de démarrage, cliquez sur **démarrer**, pointez sur **Tous les programmes**, **Utilitaires VPN Booster**, puis sur **Assistant de démarrage**.

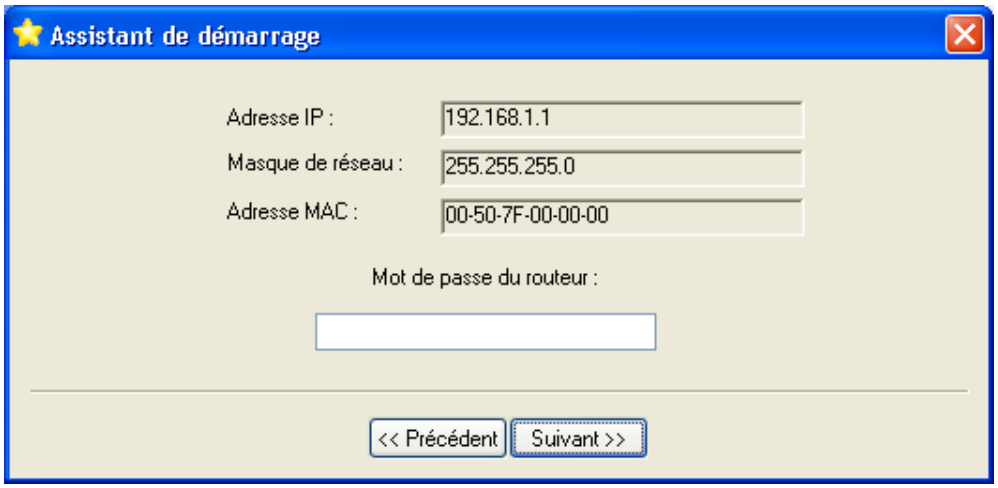


7. L'Assistant de démarrage apparaît. La première fenêtre donne la liste de tous les routeurs présents sur votre réseau. Ils sont répertoriés avec leurs différents identifiants (adresse IP, masque de réseau, adresse MAC). Sélectionnez le routeur à configurer, puis cliquez sur **Suivant>>**.

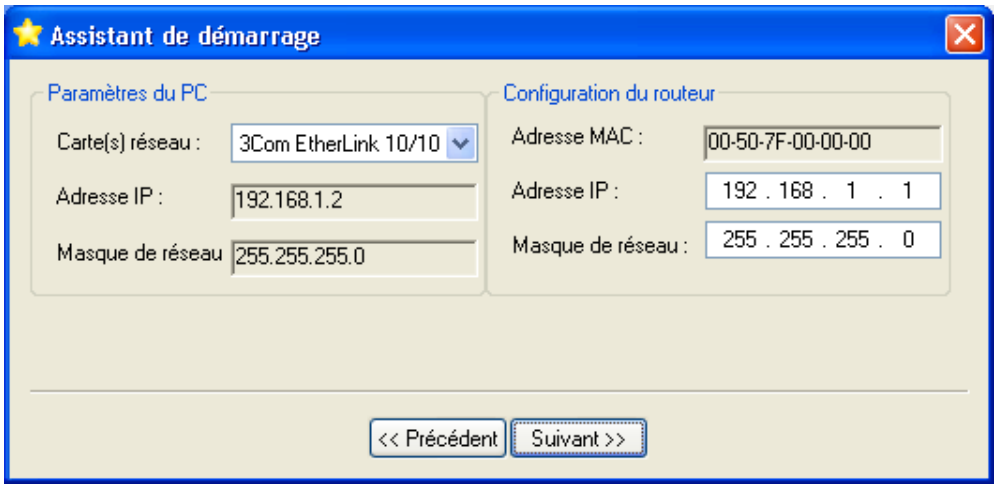


Remarque : si l'Assistant de démarrage ne trouve pas le VPN Booster sur le réseau, vérifiez les raccordements du câble Ethernet et la configuration du PC (carte réseau et protocole TCP/IP).

8. La fenêtre d'accueil de l'Assistant de démarrage est montrée ci-dessous. Dans la rubrique **Mot de passe du routeur**, entrez le mot de passe du VPN Booster, puis cliquez sur **Suivant>>**. Par défaut, le mot de passe est **bewan**.



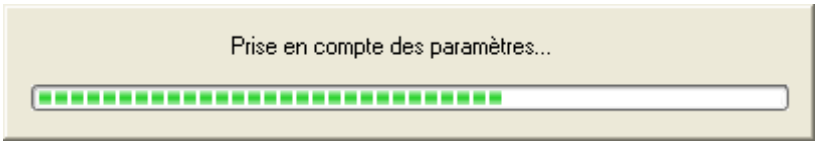
9. Après l'acceptation de votre authentification, l'Assistant de démarrage affiche la fenêtre ci-dessous. Celle-ci rappelle la configuration TCP/IP du PC et permet de configurer l'adresse IP du routeur.

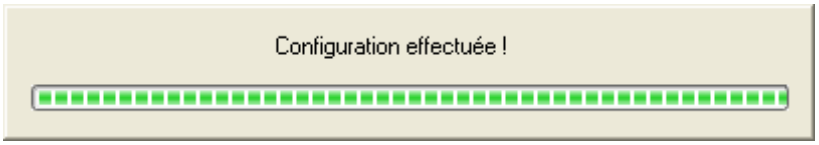


Nous vous conseillons de conserver la configuration TCP/IP par défaut du routeur sauf si celle-ci est incompatible avec votre réseau existant (voir « Equipement informatique existant au sein de l'entreprise » page 24). Dans ce dernier cas, vous devez modifier l'adresse IP du routeur et le masque de réseau afin de les rendre compatibles avec votre plan d'adressage.

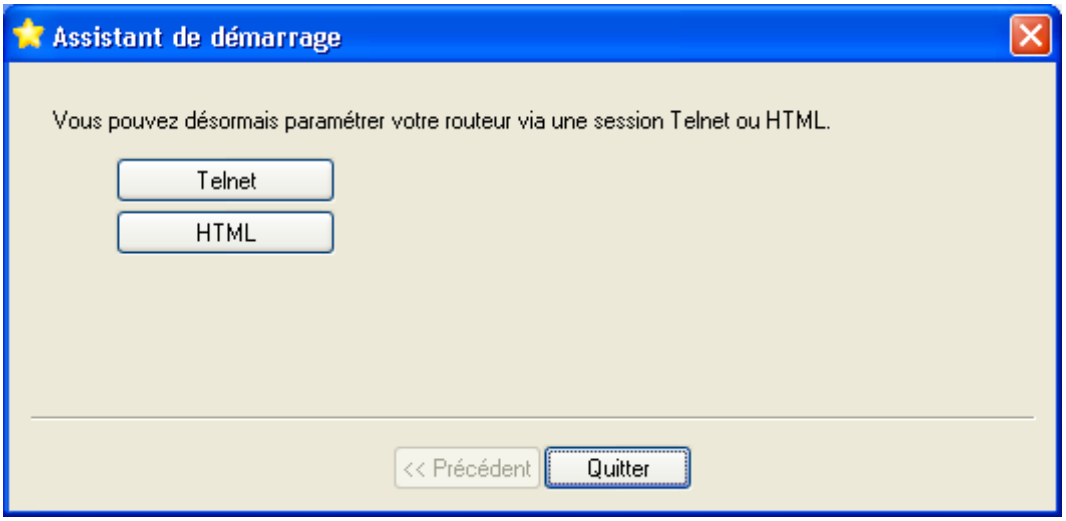
Cliquez sur **Suivant>>**.

10. La configuration choisie est enregistrée et le redémarrage du routeur peut commencer (écrans ci-dessous).





11. Une fois le redémarrage du routeur terminé, sélectionnez le mode par lequel vous allez le configurer : Telnet ou HTML.



- Le *mode HTML* permet de configurer le VPN Booster de façon très conviviale, à partir du navigateur Web installé sur le PC. Il permet de définir l'ensemble des paramètres de fonctionnement du routeur.

  Si vous souhaitez paramétrer le VPN Booster en mode HTML, cliquez sur le bouton **HTML**. Le navigateur Web par défaut du PC est alors automatiquement lancé et la connexion avec le VPN Booster est établie. Poursuivez la lecture de ce manuel au chapitre « Accès à l'administration HTML du routeur » page 66.

- Le *mode Telnet* permet également de configurer le VPN Booster, mais il requiert une expérience certaine de ce mode de configuration.

  Si vous souhaitez paramétrer le VPN Booster en mode Telnet, cliquez sur le bouton **Telnet**. Le logiciel Telnet du PC est alors automatiquement lancé et la connexion avec le VPN Booster est établie. Pour toute information concernant le mode Telnet, reportez-vous au chapitre « Commandes Telnet » page 183.

  Attention : la configuration de certains paramètres n'est pas possible en session Telnet. Ce mode est davantage réservé au dépannage ou au paramétrage avancé.

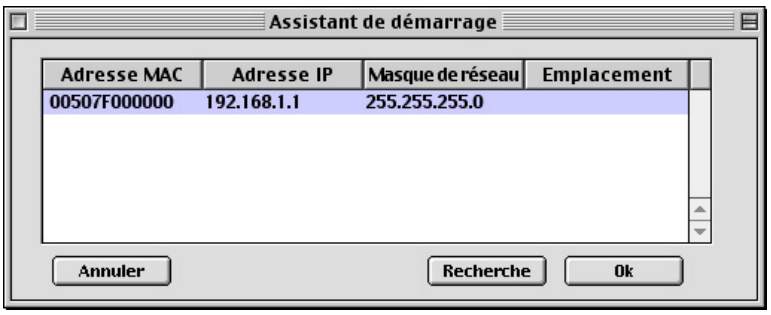
Configuration pour Mac OS 9

Votre ordinateur doit être correctement raccordé au VPN Booster, soit directement, soit via un concentrateur Ethernet (selon le modèle de routeur dont vous disposez, reportez-vous à la partie « Raccordement Ethernet » du chapitre « Raccordements du routeur » page 12).

Le VPN Booster doit être raccordé à une prise électrique (selon le modèle de routeur dont vous disposez, voir la partie « Raccordement du routeur à l'alimentation électrique » dans le chapitre « Raccordements du routeur » page 12).

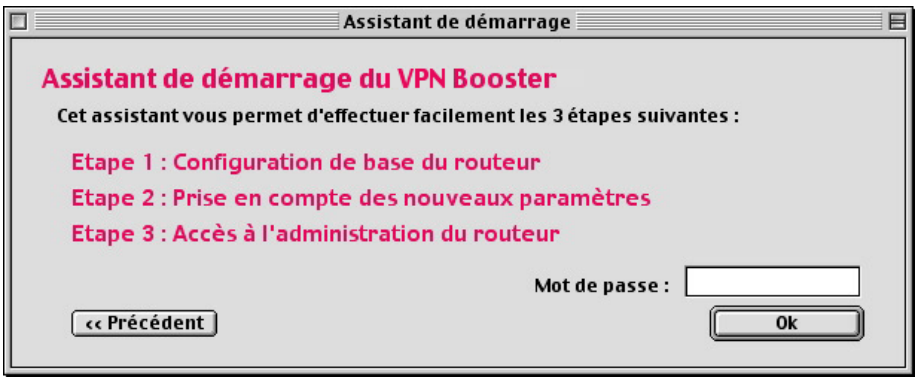
Procédez comme suit :

1. Insérez le CD-ROM Routeurs VPN Booster dans le lecteur de votre Macintosh.
2. Effectuez un double-clic sur l'icône du CD-ROM.
3. Effectuez un double-clic sur le dossier correspondant au modèle VPN Booster dont vous disposez, **Utilitaires**, **Mac OS Classic**, puis sur **Utilitaires VPN Booster** afin de lancer le programme d'installation des utilitaires.
4. Une fenêtre apparaît. Cliquez sur **Continuer**.
5. Sélectionnez **Installation Standard**, puis cliquez sur **Installer**. Les Utilitaires VPN Booster s'installent ensuite automatiquement dans des dossiers spécifiques de votre système.
6. A la fin, un message doit vous indiquer que l'installation a réussi. Cliquez sur **OK**.
7. Lancez ensuite l'Assistant de démarrage. Pour cela, cliquez sur le menu **Pomme**, pointez sur **Tableaux de bord**, **Utilitaires VPN Booster**, puis cliquez sur **Assistant de démarrage**.
8. La première fenêtre donne la liste de tous les routeurs présents sur votre réseau. Ils sont répertoriés avec leurs différents identifiants (adresse MAC, adresse IP, masque de réseau, emplacement). Sélectionnez le routeur à configurer, puis cliquez sur **Ok**.

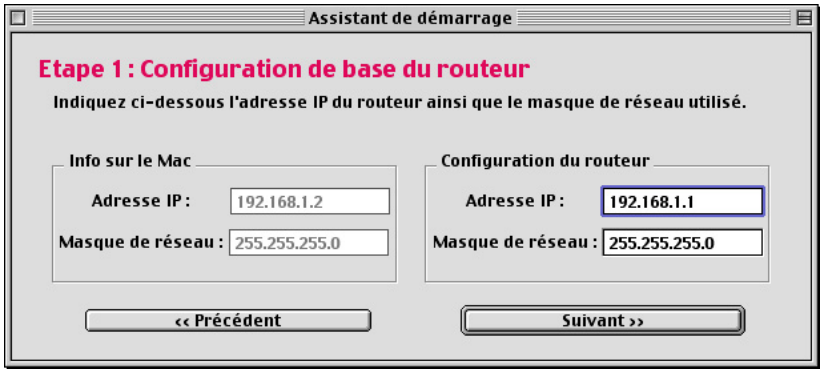


Remarque : si l'Assistant de démarrage ne trouve pas le VPN Booster sur le réseau, vérifiez les raccordements du câble Ethernet et la configuration du Mac (carte réseau et protocole TCP/IP).

9. La fenêtre d'accueil de l'Assistant de démarrage est montrée ci-dessous. Dans la rubrique **Mot de passe**, entrez le mot de passe du VPN Booster, puis cliquez sur **Ok**. Par défaut, le mot de passe est **bewan**.

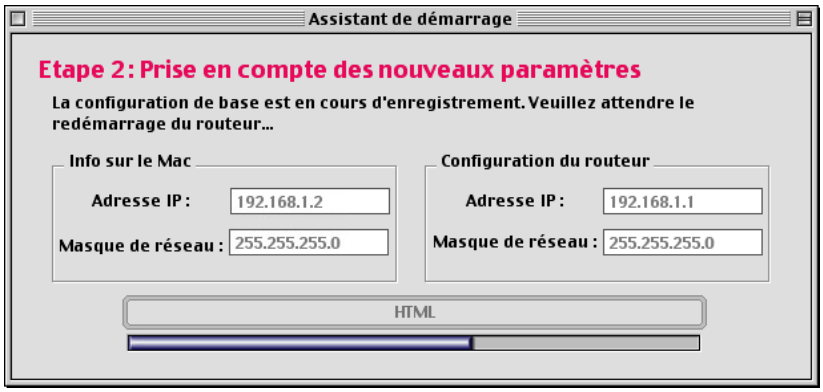


10. Après l'acceptation de votre authentification, l'Assistant de démarrage affiche la fenêtre ci-dessous. Celle-ci rappelle la configuration TCP/IP du Mac et permet de configurer l'adresse IP du routeur.

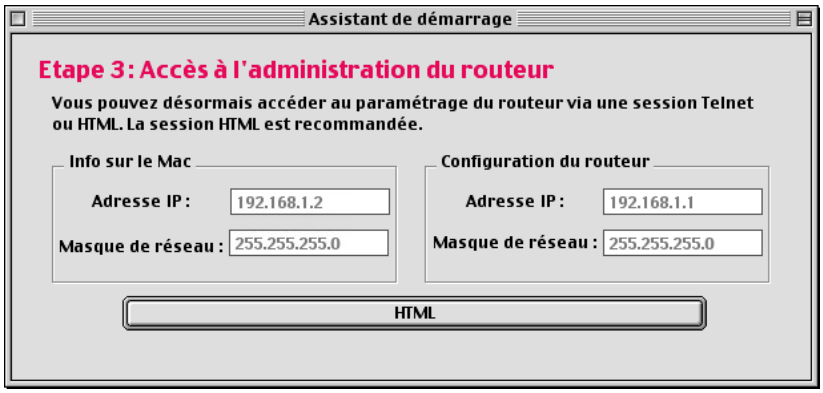


Nous vous conseillons de conserver la configuration TCP/IP par défaut du routeur sauf si celle-ci est incompatible avec votre réseau existant (voir « Equipement informatique existant au sein de l'entreprise » page 24). Dans ce dernier cas, vous devez modifier l'adresse IP du routeur et le masque de réseau afin de les rendre compatibles avec votre plan d'adressage. Cliquez sur **Suivant>>**.

11. La configuration choisie est enregistrée et le redémarrage du routeur peut commencer (écran ci-dessous).



12. Une fois le redémarrage du routeur terminé, cliquez sur **HTML** pour accéder à la configuration du routeur.



Le mode HTML permet de configurer le VPN Booster de façon très conviviale, à partir du navigateur Web installé sur le Macintosh. Il permet de définir l'ensemble des paramètres de fonctionnement du routeur.

Le navigateur Web par défaut du Macintosh est alors automatiquement lancé et la connexion avec le VPN Booster est établie. Poursuivez la lecture de ce manuel au chapitre « Accès à l'administration HTML du routeur » page 66.

Remarque : la configuration du routeur via une session Telnet est également possible sur Mac OS 9. Un logiciel Telnet est fourni sur le CD-ROM du VPN Booster. Ensuite, reportez-vous au chapitre « Commandes Telnet » page 183 pour poursuivre la configuration du routeur.

Attention : la configuration de certains paramètres n'est pas possible en session Telnet. Ce mode est davantage réservé au dépannage ou au paramétrage avancé.

Configuration pour Mac OS X

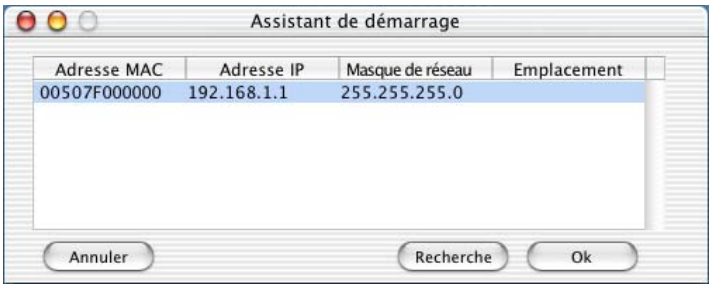
Votre ordinateur doit être correctement raccordé au VPN Booster, soit directement, soit via un concentrateur Ethernet (selon le modèle de routeur dont vous disposez, reportez-vous à la partie « Raccordement Ethernet » du chapitre « Raccordements du routeur » page 12).

Le VPN Booster doit être raccordé à une prise électrique (selon le modèle de routeur dont vous disposez, voir la partie « Raccordement du routeur à l'alimentation électrique » dans le chapitre « Raccordements du routeur » page 12).

Procédez comme suit :

1. Insérez le CD-ROM Routeurs VPN Booster dans le lecteur de votre Macintosh.
2. Effectuez un double-clic sur l'icône du CD-ROM.
3. Effectuez un double-clic sur le dossier correspondant au modèle VPN Booster dont vous disposez, **Utilitaires**, **Mac OS X**, puis sur **Utilitaires VPN Booster.dmg**.
4. Un disque virtuel **Utilitaires VPN Booster** est créé sur le bureau de votre Macintosh. Effectuez un double clic sur ce disque.

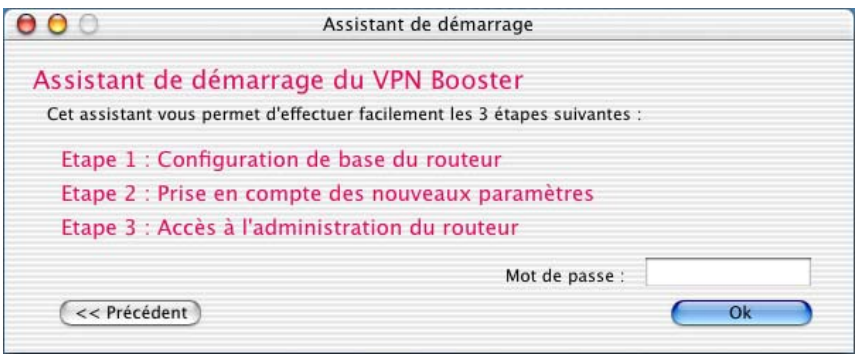
5. Une fenêtre s'ouvre. Lancez ensuite l'Assistant de démarrage.
6. La première fenêtre donne la liste de tous les routeurs présents sur votre réseau. Ils sont répertoriés avec leurs différents identifiants (adresse MAC, adresse IP, masque de réseau, emplacement). Sélectionnez le routeur à configurer, puis cliquez sur **Ok**.



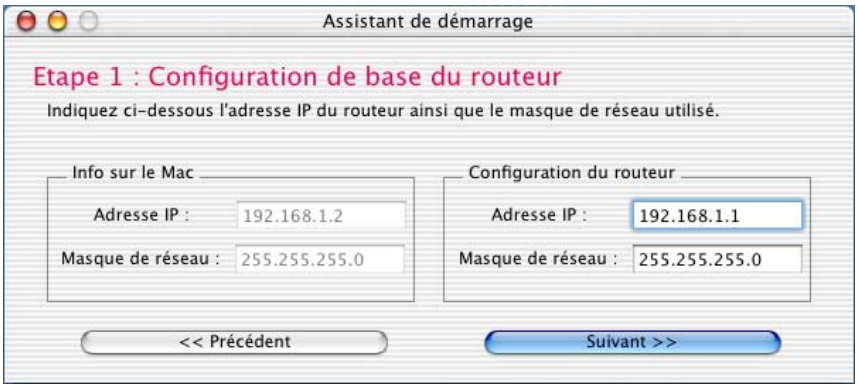
Remarques :

- *Si l'Assistant de démarrage ne trouve pas le VPN Booster sur le réseau, vérifiez les raccordements du câble Ethernet et la configuration du Macintosh (carte réseau et protocole TCP/IP).*
- *Si vous rencontrez toujours des difficultés pour détecter votre routeur, veuillez alors au préalable attribuer à votre Macintosh une adresse IP compatible avec le plan d'adressage du routeur (reportez-vous au chapitre « Configuration des ordinateurs », section « Macintosh (Mac OS X) » page 55). Lancez ensuite votre navigateur Internet et tapez l'adresse IP de votre routeur pour accéder au configurateur Web.*

7. La fenêtre d'accueil de l'Assistant de démarrage est montrée ci-dessous. Dans la rubrique **Mot de passe**, entrez le mot de passe du VPN Booster, puis cliquez sur **Ok**. Par défaut, le mot de passe est **bewan**.

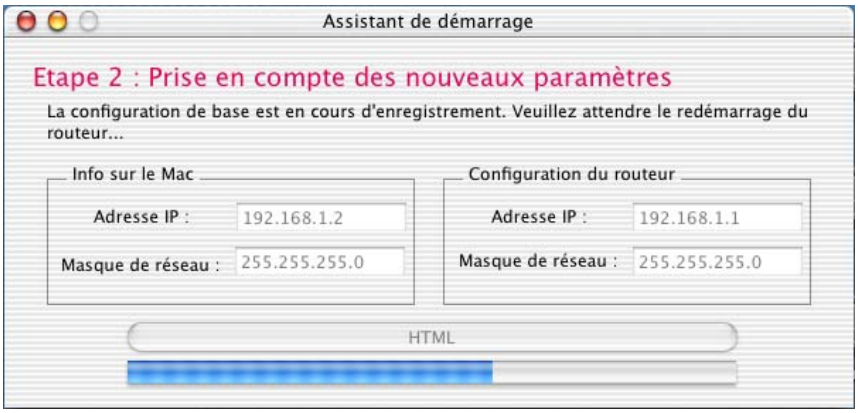


8. Après l'acceptation de votre authentification, l'Assistant de démarrage affiche la fenêtre ci-dessous. Celle-ci rappelle la configuration TCP/IP du Mac et permet de configurer l'adresse IP du routeur.

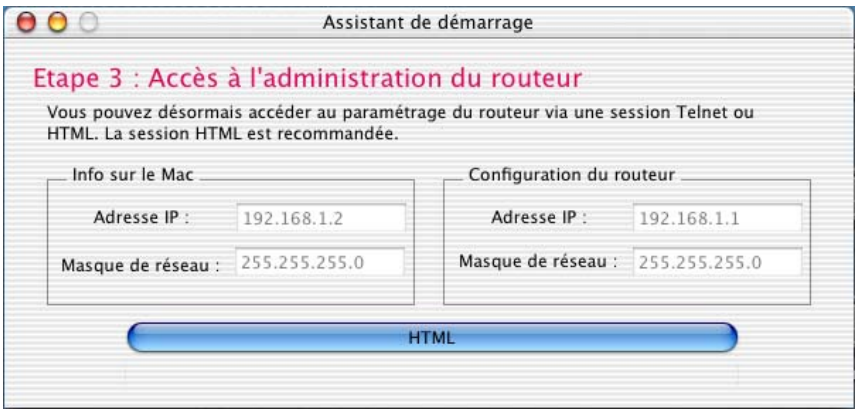


Nous vous conseillons de conserver la configuration TCP/IP par défaut du routeur sauf si celle-ci est incompatible avec votre réseau existant (voir « Equipement informatique existant au sein de l'entreprise » page 24). Dans ce dernier cas, vous devez modifier l'adresse IP du routeur et le masque de réseau afin de les rendre compatibles avec votre plan d'adressage. Cliquez sur **Suivant**>>.

9. La configuration choisie est enregistrée et le redémarrage du routeur peut commencer (écran ci-dessous).



10. Une fois le redémarrage du routeur terminé, cliquez sur **HTML** pour accéder à la configuration du routeur.



Le mode HTML permet de configurer le VPN Booster de façon très conviviale, à partir du navigateur Web installé sur le Macintosh. Il permet de définir l'ensemble des paramètres de fonctionnement du routeur.

Le navigateur Web par défaut du Macintosh est alors automatiquement lancé et la connexion avec le VPN Booster est établie. Poursuivez la lecture de ce manuel au chapitre « Accès à l'administration HTML du routeur » page 66.

Remarque : la configuration du routeur via une session Telnet est également possible sur Mac OS X. Utilisez l'application ***Terminal****. Ensuite, reportez-vous au chapitre « Commandes Telnet » page 183 pour poursuivre la configuration du routeur.*

Attention : la configuration de certains paramètres n'est pas possible en session Telnet. Ce mode est davantage réservé au dépannage ou au paramétrage avancé.

Accès à l'administration HTML du routeur

Le mode HTML permet de configurer le VPN Booster de façon très conviviale, à partir du navigateur Web installé sur votre ordinateur. Votre logiciel de navigation doit être correctement configuré (voir « Configuration des logiciels de navigation » page 57).

Suivant la version de navigateur Web utilisé, les boîtes de dialogue et l'affichage des pages HTML peuvent varier légèrement. Dans nos exemples, nous utilisons le logiciel Microsoft® Internet Explorer 6.0.

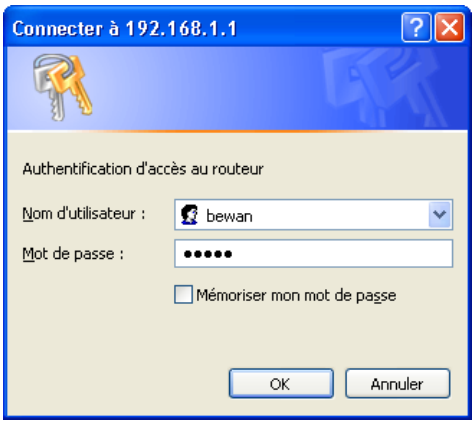
Identification lors de la première configuration

Après avoir choisi le mode de configuration HTML de l'Assistant de démarrage, le logiciel de navigation installé sur votre PC ou sur votre Mac est automatiquement lancé. Une boîte de dialogue apparaît. Elle vous permet de saisir le nom d'utilisateur et le mot de passe nécessaires pour administrer le routeur.

Par défaut, ces paramètres d'identification sont les suivants :

- Nom d'utilisateur : **bewan**
- Mot de passe : **bewan**

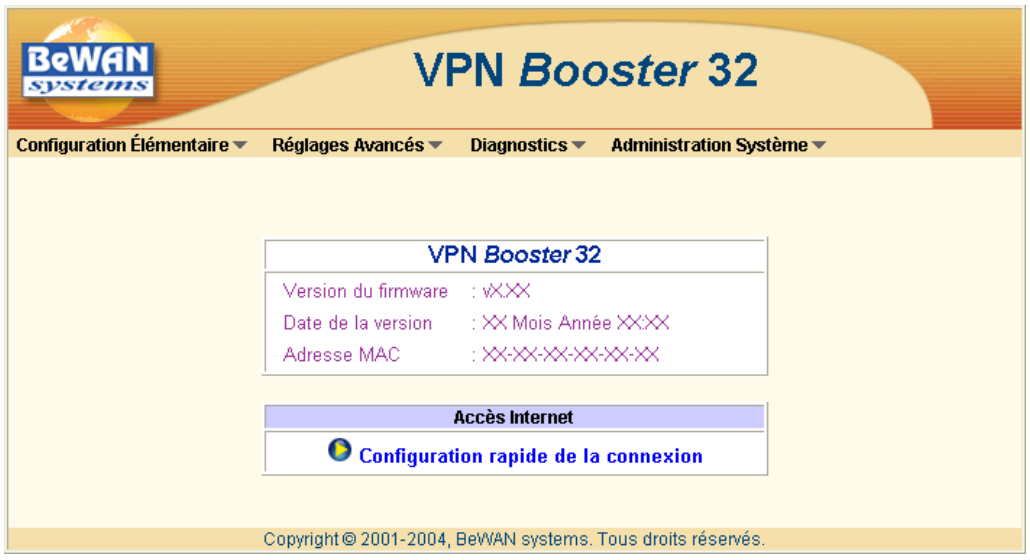
1. Entrez les éléments de votre identification. Cliquez sur **OK**.



   Si vous ne souhaitez pas vous identifier à chaque fois que vous configurez le routeur depuis cet ordinateur, cochez **Mémoriser mon mot de passe**.

   Attention : dans ce cas, toute personne ayant accès à cet ordinateur pourra entrer en mode configuration du VPN Booster. Pour des raisons de sécurité, nous vous conseillons de ne pas cocher cette case.

2. Dès que votre identification a été acceptée, le Menu principal du configurateur HTML du VPN Booster apparaît.



Remarque : avant toute chose, si vous n'avez pas encore modifié le nom et le mot de passe d'administration du routeur, nous vous recommandons vivement de le faire pour des raisons de sécurité. Pour cela, reportez-vous au chapitre suivant « Modification des paramètres administrateur » page 69.

Identification lors des accès suivants

Après votre configuration initiale, pour accéder de nouveau au configurateur HTML du VPN Booster, procédez comme suit :

1. Lancez votre logiciel de navigation.
2. Dans la rubrique **Adresse**, entrez l'adresse IP du VPN Booster.

   Rappel : par défaut, l'adresse IP du VPN Booster est « 192.168.1.1 ».
3. Dès que votre navigateur a établi la connexion avec le routeur, une boîte de dialogue apparaît. Renseignez les rubriques **Nom d'utilisateur** et **Mot de passe**. Cliquez ensuite sur **OK**.

Partie 3 : Configuration du routeur

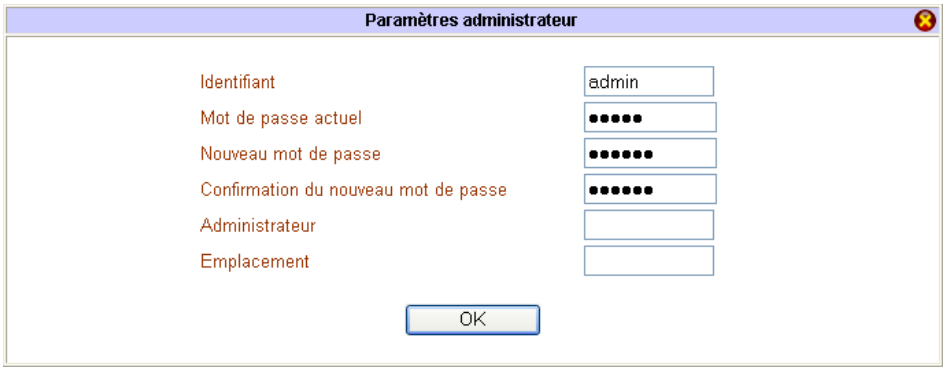
Modification des paramètres administrateur

L'administrateur du réseau peut changer le nom et le mot de passe qui permettent d'accéder à la configuration du routeur. En configuration d'usine, comme nous avons pu le voir auparavant, ces paramètres sont les suivants :

- Nom d'utilisateur : **bewan**
- Mot de passe : **bewan**

Pour modifier ces paramètres, procédez comme suit :

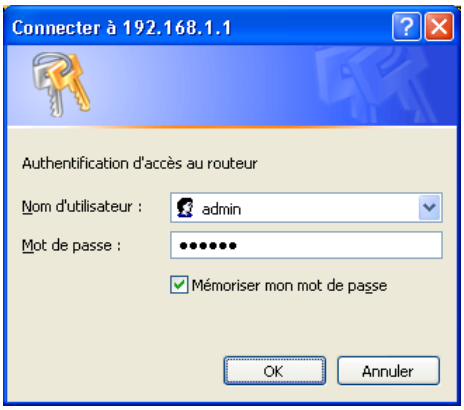
1. Dans le menu **Administration Système**, cliquez sur **Paramètres administrateur**.
2. Dans la rubrique **Identifiant**, remplacez l'ancien nom d'utilisateur par un nouveau nom de votre choix (dans notre exemple : **admin**).



3. Dans la rubrique **Mot de passe actuel**, saisissez le mot de passe qui vous a servi à accéder au configurateur HTML.
4. Dans la rubrique **Nouveau mot de passe**, saisissez un nouveau mot de passe de votre choix. Saisissez ensuite ce mot de passe dans la rubrique **Confirmation du nouveau mot de passe**.

   Attention :

   - *Choisissez un nom et un mot de passe que vous pourrez mémoriser facilement. Si vous les oubliez, vous ne pourrez plus accéder à votre configuration. Vous serez alors obligé d'effectuer un « reset » en pointant sur le bouton à l'arrière du VPN Booster, perdant ainsi tous les éléments de votre configuration actuelle.*
   - *Lorsque vous saisissez vos identifiants d'administration, il est impératif de tenir compte des majuscules et des minuscules.*
5. Vous pouvez renseigner les rubriques **Administrateur** et **Emplacement** à titre d'information. Sachez que ces rubriques n'ont aucune incidence sur le fonctionnement du VPN Booster.
6. Cliquez sur **OK** pour valider vos nouveaux paramètres d'identification.
7. **Si vous utilisez Microsoft® Internet Explorer**, une boîte de dialogue apparaît. Saisissez le nom d'utilisateur et le mot de passe que vous avez choisis, puis cliquez sur **OK**.



8. Après la saisie de vos paramètres d'identification sur l'un ou l'autre des logiciels de navigation, vous avez de nouveau accès au configurateur Web du VPN Booster.

Configuration des paramètres Wireless (VPN Booster 32 g / 32 Vg)

Le réseau sans fil (WLAN ou Wireless LAN) est principalement employé lorsqu'il s'agit d'interconnecter des utilisateurs nomades (par exemple des portables PC ou Macintosh) entre eux et/ou de les relier à un réseau local filaire de manière simple et rapide. Le réseau sans fil utilise des ondes radio plutôt qu'une infrastructure câblée. Ces ondes en effet ne sont pas affectées par les structures d'un bâtiment et peuvent se réfléchir pour contourner les obstacles. Le WLAN offre un accès sans fil à l'ensemble des ressources et des services du réseau de l'entreprise sur un ou plusieurs bâtiments.

L'accès sans fil au réseau local permet aux utilisateurs de n'importe quel ordinateur portable d'avoir constamment accès aux ressources du réseau tout en se déplaçant librement à l'intérieur d'un site ou d'un bâtiment sans que l'accès réseau soit interrompu. Les postes pourront se déplacer sans problème à l'intérieur d'une cellule autour du point d'accès constitué par les antennes du routeur.

Basé sur le standard IEEE 802.11g (54 Mbps), le VPN Booster 32 g / 32 Vg est également compatible avec des équipements sans fil 802.11b. Le standard 802.11g a été développé pour favoriser et assurer l'interopérabilité des matériels entre eux. Elle présente de nombreux avantages permettant de minimiser les interférences, de maximaliser la bande passante sur les canaux.

Remarque : dès lors, un matériel 802.11g d'un constructeur pourra fonctionner sans problème avec un matériel 802.11g d'un autre fabricant. Cela signifie que vous pouvez acheter des matériels Wireless de fabricants différents et les utiliser pour communiquer avec le VPN Booster 32 g / 32 Vg.

Pour établir une liaison entre le routeur et un équipement de liaison 802.11g (par exemple, un portable), plusieurs conditions sont nécessaires :

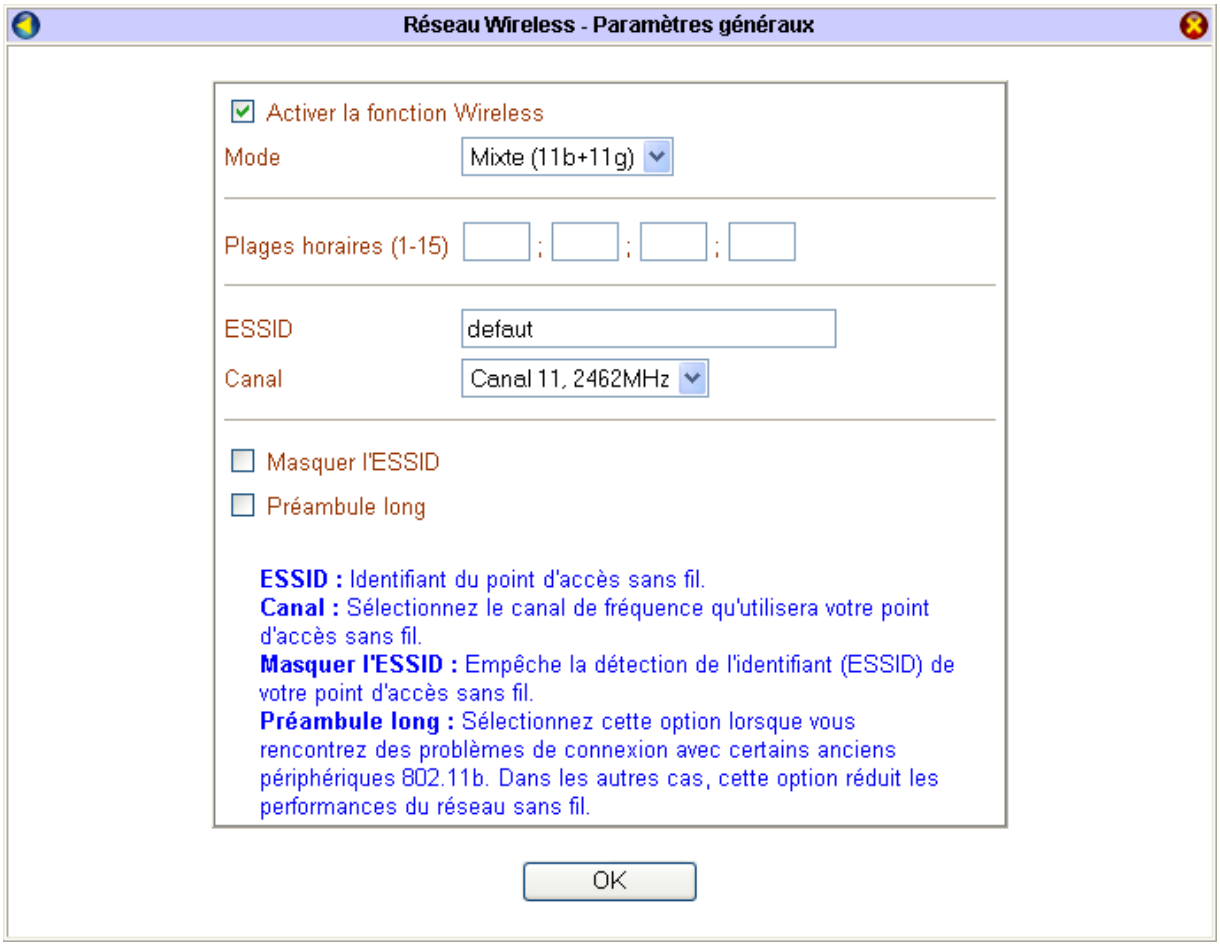
- les antennes fournies avec le routeur doivent être vissées à l'arrière du boîtier. Elle constitue le point d'accès et agit comme un hub sur lequel les utilisateurs sans fil se connectent via les ondes.
- la station Wireless doit posséder un équipement qui fonctionne avec la norme 802.11b ou 802.11g (cartes PCMCIA, cartes PCI, boîtier USB).
- les deux matériels doivent être paramétrés de façon à pouvoir dialoguer (identification du point d'accès, choix du canal, paramètres de sécurité, autorisation d'accès).

Une fois les antennes vissées dans les emplacements prévus à l'arrière du routeur, dans le menu **Configuration Elémentaire**, cliquez sur **Réseau Wireless**.

Dans la partie **Informations du réseau Wireless**, l'adresse MAC du routeur apparaît.

Paramètres généraux

Par défaut, la fonction Wireless est activée.



Mode

Le VPN Booster 32 g / 32 Vg utilise donc la norme IEEE 802.11g mais est également compatible avec la norme 802.11b. Dans la rubrique **Mode**, sélectionnez le mode de fonctionnement du routeur.

- Si vous sélectionnez l'option **11g seulement**, seules les connexions avec des matériels 802.11g peuvent être établies.
- Si vous sélectionnez l'option **11b seulement**, seules les connexions avec des matériels 802.11b peuvent être établies.
- Si vous sélectionnez l'option **Mixte (11b+11g)**, cela signifie que, outre des matériels 802.11g, des matériels 802.11b peuvent également établir la connexion avec le VPN Booster 32 g / 32 Vg.

ESSID

La valeur d'identification du point d'accès, baptisée ESSID, est reportée dans la configuration. Il vous suffit ensuite de rentrer un ESSID autre que celui qui est proposé par défaut, et de communiquer ce nouvel identifiant aux postes clients qui profiteront du partage de connexion. Par défaut, le SSID est **defaut**. Pour une raison de sécurité, nous vous conseillons de changer ce SSID lors de l'installation du VPN Booster 32 g / 32 Vg. Il peut être réglé jusqu'à 31 caractères. Il est sensible à la casse.

La station Wireless choisit le point d'accès auquel elle va s'associer. Lorsqu'elle entre dans la zone d'un point d'accès et est acceptée par ce point d'accès, la station Wireless s'accorde au canal radio auquel le point d'accès est rattaché.

Ces paramètres devront être les mêmes sur tous les postes du réseau pour qu'il fonctionne. Bien sûr il faudra paramétrer les paramètres standards pour qu'un réseau fonctionne, comme le nom de domaine ou le paramétrage TCP/IP par exemple.

Canal

Il faut choisir la fréquence sur laquelle les postes devront communiquer. Le choix du canal dépend du point d'accès.

Ainsi, le canal sélectionné dans la rubrique correspondante sera celui utilisé pour le dialogue entre les stations Wireless et le routeur. Pour que la transmission fonctionne, il faut que les stations Wireless soient paramétrées sur la même fréquence.

Masquer l'ESSID

Cette fonction vous permet de masquer ou non l'ESSID sur le réseau sans fil. Si vous cochez l'option, le VPN Booster 32 g / 32 Vg ne sera pas visible. Pour s'y connecter, il vous faudra alors obligatoirement intégrer ce nom à la configuration sans fil du matériel Wireless distant (exemple : PC portable). Ceci a pour but de renforcer la sécurité.

Remarque : la rapidité de la connexion dépend de la distance entre la station Wireless et le point d'accès, mais aussi du type de bâtiment dans lequel le réseau est installé. Le transfert étant effectué par ondes radio, il profite des avantages et inconvénients de celui-ci. Par exemple si les murs du bâtiment à partir duquel le réseau est installé ont des armatures métalliques, des perturbations risquent de se faire sentir.

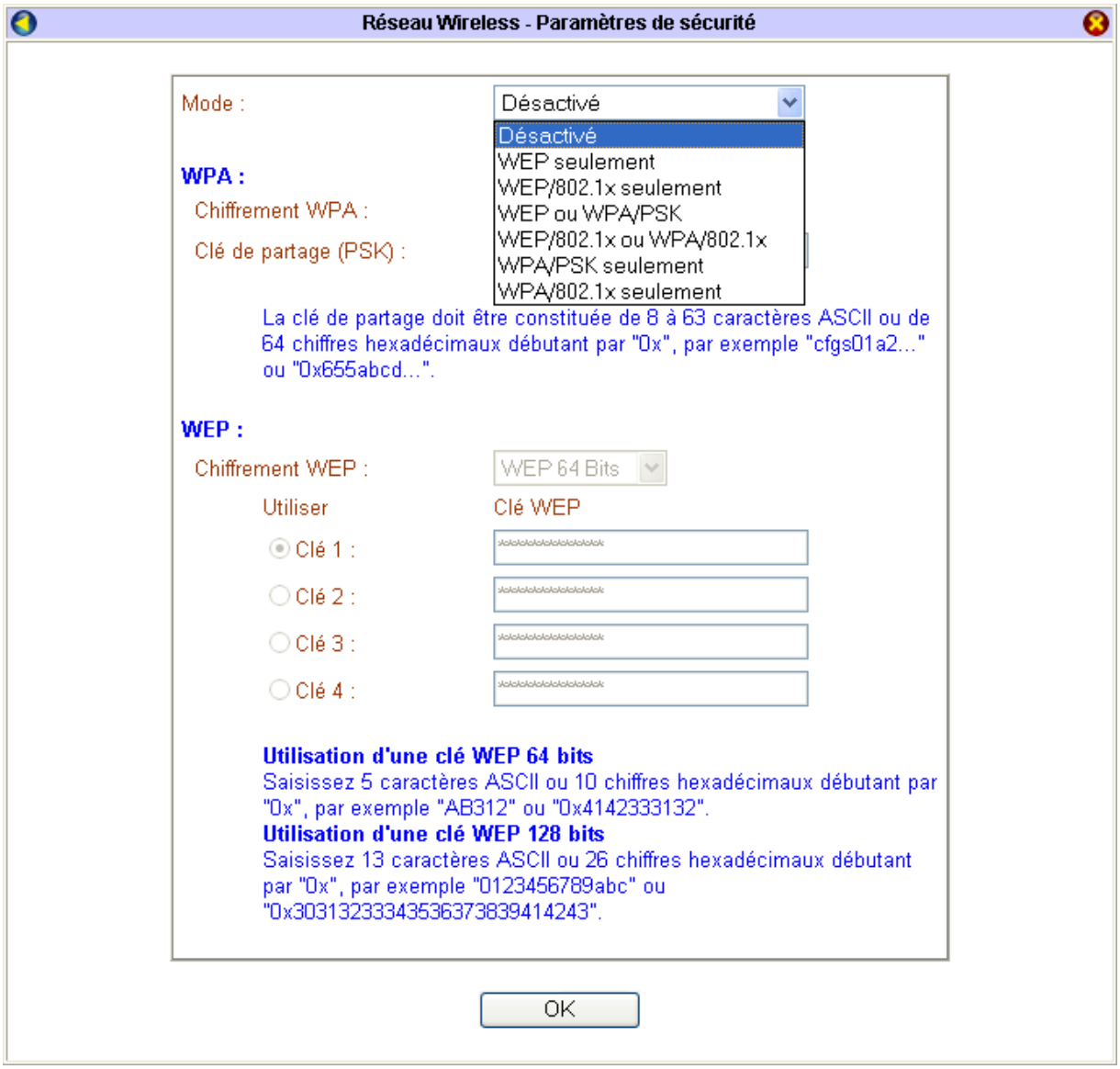
Paramètres de sécurité

Lorsque vous avez déterminé une valeur d'identification et un canal de transmission, l'un des aspects majeurs du réseau sans fil est la sécurité. C'est pourquoi le VPN Booster 32 g / 32 Vg prévoit des mécanismes d'authentification, un mode de cryptage afin de sécuriser les données entre la station et le point d'accès. En effet, sans encryption, n'importe qui dans la zone de couverture du réseau peut intercepter et décoder les trames qui ne lui sont pas destinées. L'objectif est de permettre une confidentialité des données équivalente, voire supérieure, aux réseaux câblés et donc d'accentuer la fiabilité dans la transmission des paquets de données.

Pour paramétrer la sécurité, procédez comme suit :

1. Dans le menu **Configuration Elémentaire**, cliquez sur **Réseau Wireless**, puis sur **Paramètres de sécurité**.
2. Sélectionnez votre mode d'encryption. Le VPN Booster 32 g / 32 Vg propose 6 types de sécurité :

   *Remarque : par défaut, le mode est positionné sur **Désactivé**.*



WEP seulement

Le WEP (***W**ired **E**quivalent **P**rivacy*) est un mécanisme d'authentification des utilisateurs. Vous sécurisez la transmission des données entre le VPN Booster 32 g / 32 Vg et une station cliente ou entre deux Points d'Accès au moyen d'une clé d'encryption. En effet, sans encryption, n'importe qui dans la zone de couverture du réseau peut intercepter et décoder les trames qui ne lui sont pas destinées. Cette clé est suffisante pour une utilisation domestique.

La clé WEP est statique. Pour la modifier, il faut une intervention manuelle.

1. Dans la rubrique **Chiffrement WEP**, sélectionnez le niveau d'encryption (correspondant à la longueur de la clé) : **WEP 64 Bits** ou **WEP 128 Bits**. Nous vous conseillons d'utiliser le niveau d'encryption le plus élevé.

   Si vous sélectionnez l'option **WEP 64 Bits**, vous devez saisir 5 caractères ASCII ou 10 chiffres hexadécimaux.

   Si vous sélectionnez l'option **WEP 128 Bits**, vous devez saisir 13 caractères ASCII ou 26 chiffres hexadécimaux.

2. Indiquez ensuite votre clé WEP.

   Si vous sélectionnez le mode ASCII, choisissez vos caractères entre "a-z", "A-Z" et "0-9". En revanche, si vous sélectionnez le mode Hexadécimal, vos caractères doivent être compris entre "a-f", "A-F" et "0-9" précédés de "0x".

   Exemple du format d'une clé WEP 64 Bits en mode ASCII ou en mode Hexadécimal :

   - *En ASCII : MaCle*
   - *En Hexadécimal : 0x11AA22BB33*

3. Cliquez sur **OK**.

Attention : Le WEP utilise une clé secrète. Pour que la station distante puisse dialoguer avec le routeur, il faut qu'elle utilise la même clé d'encryption. Il existe 4 clés, mais une seule peut être sélectionnée.

L'important, est de noter très soigneusement le résultat obtenu pour pouvoir ensuite configurer vos stations clientes ou un autre Point d'Accès. Activez alors le WEP sur chacun de vos équipements Wireless, puis reportez la clé du VPN Booster 32 g / 32 Vg que vous avez saisie, et la liaison se rétablira entre vos équipements Wireless et le VPN Booster 32 g / 32 Vg (en effet, lorsque vous avez activé l'encryption WEP sur le VPN Booster 32 g / 32 Vg, la liaison s'est logiquement rompue avec les autres équipements composant votre réseau sans fil...).

WPA/PSK seulement

Le WPA (***W**i-Fi **P**rotected **A**ccess*) est un protocole de sécurité destiné à remplacer l'actuel WEP (***W**ired **E**quivalent **P**rivacy*) pour les liaisons Wi-Fi, lequel utilise des clés statiques qu'il faut changer manuellement.

Par défaut, le WPA utilise le protocole de cryptage des données (ou algorithme) TKIP (***T**emporal **K**ey **I**ntegrity **P**rotocol*). Au lieu d'utiliser une clé fixe pour chiffrer les paquets de données, il génère régulièrement de nouvelles clés dynamiques dérivées de la clé principale, permettant ainsi une sécurité accrue.

Remarque : tous les matériels existants peuvent en bénéficier en effectuant une simple mise à jour logicielle.

Pour paramétrer l'encryption WPA, procédez comme suit :

1. Dans la rubrique **Chiffrement WPA**, l'option **TKIP** est sélectionnée par défaut.
2. Dans la rubrique **Clé de partage (PSK)**, saisissez la valeur de votre clé. Cette clé doit comporter 32 caractères.
3. Cliquez sur **OK**.

Remarque : pour la configuration des postes clients en WPA, veuillez vous reportez à la documentation fournie avec votre matériel.

WEP ou WPA/PSK

Si vous sélectionnez cette option, cela signifie que vous pouvez paramétrer un clé WEP ou une encryption WPA simultanément. Les équipements Wireless distants pourront donc utiliser l'une ou l'autre méthode de sécurité. Pour des stations qui ne pourraient utiliser le WPA (par exemple si elles sont sur des systèmes d'exploitation 98 ou Me), elles peuvent toujours se connecter en Wi-Fi via le WEP. Pour le paramétrage des deux options, reportez-vous aux deux sections précédentes.

WEP/802.1x seulement

Pour contrôler efficacement l'accès au réseau sans fil, la fonction d'authentification peut se faire grâce à un serveur d'authentification de type RADIUS.

L'utilisation d'un serveur RADIUS permet de protéger au maximum l'accès par identification des utilisateurs après définition de leur profil. Cette clé permettra à l'utilisateur d'être authentifié par le serveur et de pouvoir accéder au réseau.

1. Après avoir sélectionné **WEP/802.1x seulement**, cliquez sur **OK**.
2. Dans le menu **Réglages Avancés** du routeur, cliquez sur **Client RADIUS**.
3. Cochez **Activer**.
4. Dans la rubrique **Adresse IP du serveur**, indiquez l'adresse IP de votre serveur RADIUS pour faire pointer le routeur vers le serveur.
5. Indiquez le port du serveur RADIUS.

   Remarque : le port de destination 1812 présent par défaut correspond au port standard RADIUS. Si vous le modifiez, veillez bien à en faire de même du côté Serveur.
6. Indiquez le mot de passe secret partagé échangé entre le serveur et le client RADIUS. Demandez-le à votre administrateur RADIUS si vous ne le connaissez pas. Le mot de passe doit être identique sur le serveur RADIUS et le VPN Booster 32 g / 32 Vg.
7. Cliquez sur **OK** pour valider les informations. Le routeur doit ensuite redémarrer.

WPA/802.1x seulement

La configuration est identique l'encryption WEP/802.1x seulement. Reportez-vous à la section précédente.

WEP/802.1x ou WPA/802.1x

Si vous sélectionnez cette option, cela signifie que les équipements Wireless distants pourront utiliser l'une ou l'autre méthode de sécurité pour se connecter au routeur.

Contrôle d'accès

En plus des méthodes de cryptage (reportez-vous à la section précédente **Paramètres de sécurité**), afin d'accroître encore la sécurité, le VPN Booster 32 g / 32 Vg gère une table des adresses MAC qui, sous forme de liste de contrôle, interdira l'accès aux matériels Wireless distants (stations clientes) dont l'adresse MAC ne figure pas dans la liste. Chaque client peut ainsi être inclus ou non à volonté. Seule l'adresse MAC paramétrée et validée peut accéder au réseau.

Attention :

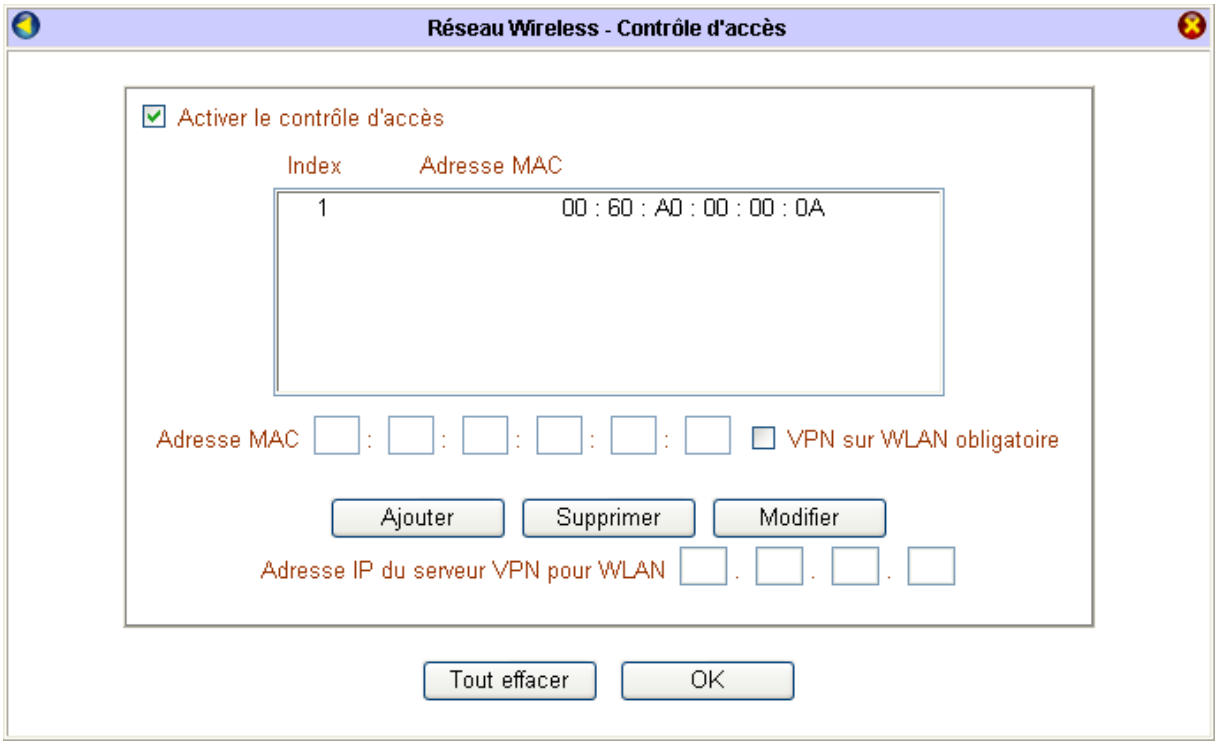
- ***si vous n'avez pas appliqué de mécanisme de cryptage et si le contrôle d'accès n'est pas activé, par défaut, toutes les stations Wireless pourront accéder au réseau.***
- ***si vous avez activé le contrôle d'accès sans spécifier d'adresse MAC, cela revient à bloquer l'accès à toutes les stations Wireless. Aucune station ne pourra dialoguer avec le routeur.***

L'adresse MAC est l'identifiant physique d'une carte. Cette adresse est unique. Bien que cette solution soit lourde à gérer pour peu que l'on dispose de nombreuses cartes d'accès à saisir, elle permet de limiter les risques d'intrusion.

Pour activer le contrôle d'accès au routeur pour ces stations, procédez comme suit :

1. Dans le menu **Configuration Elémentaire**, cliquez sur **Réseau Wireless**, puis sur **Contrôle d'accès**.
2. Cochez **Activer le contrôle d'accès**.
3. Renseignez la rubrique **Adresse MAC**. Vous spécifiez ainsi l'adresse MAC de la station autorisée à accéder au réseau.
4. Cliquez sur le bouton **Ajouter**, puis sur **OK** afin de valider les informations.

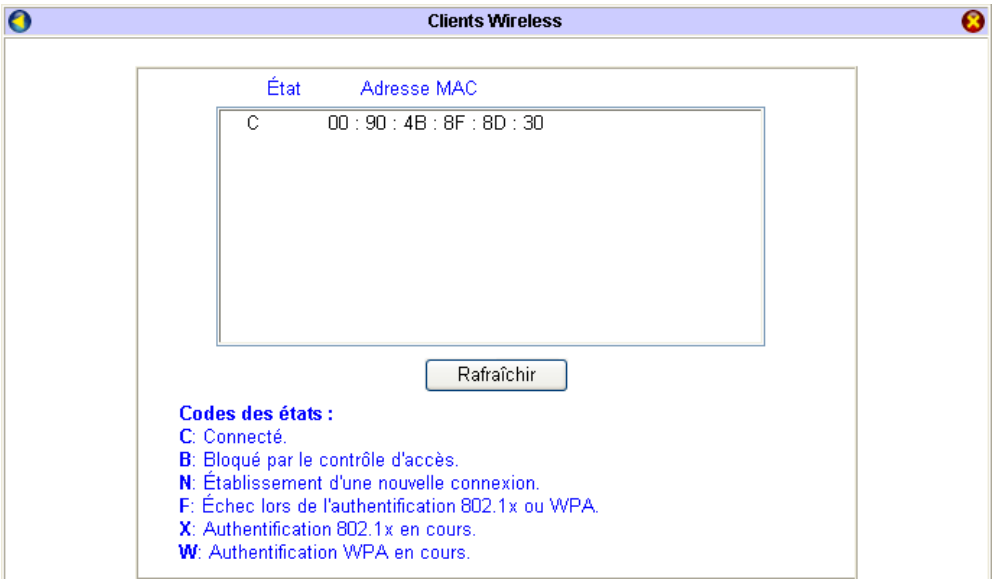
   Remarque : si vous souhaitez ensuite supprimer une adresse MAC, sélectionnez-la dans la liste, puis cliquez sur le bouton ***Supprimer****.*



Clients Wireless

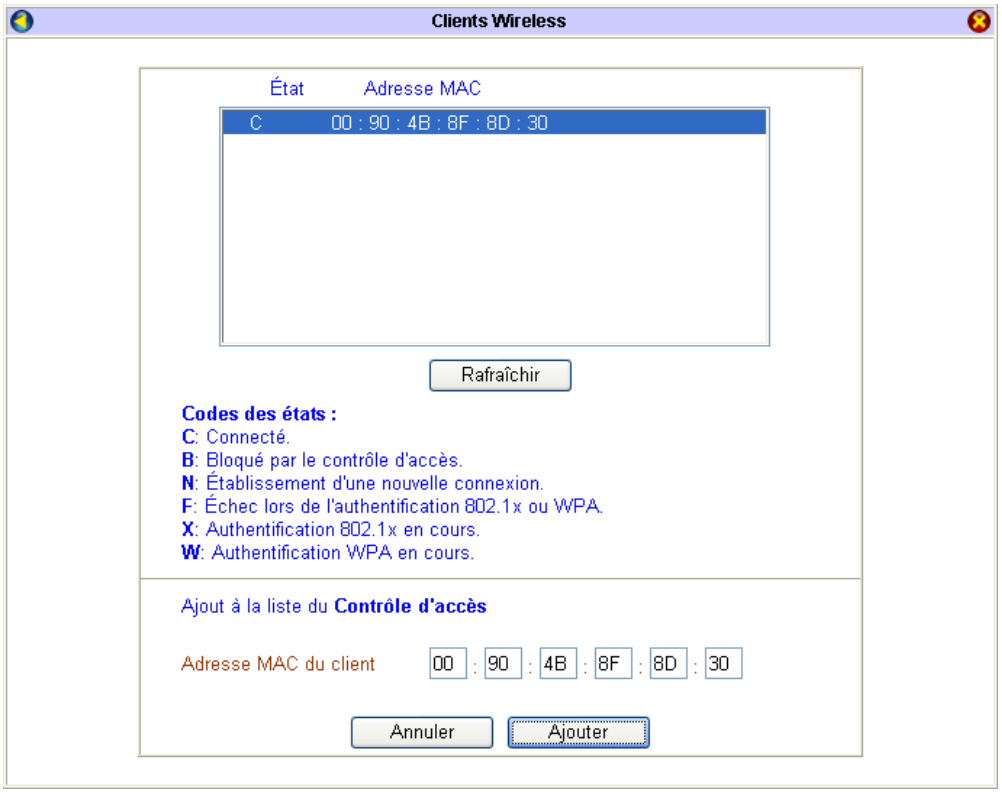
Grâce à une table de contrôle actualisable, le VPN Booster 32 g / 32 Vg vous permet de scanner toutes les stations Wireless proches du routeur. Cette liste vous indique l'état de connexion au routeur et l'adresse MAC de ces clients.

1. Dans le menu **Configuration Elémentaire**, cliquez sur **Réseau Wireless**, puis sur **Clients Wireless**.
2. Dans la table, sont répertoriées toutes les stations Wireless détectées par le routeur.

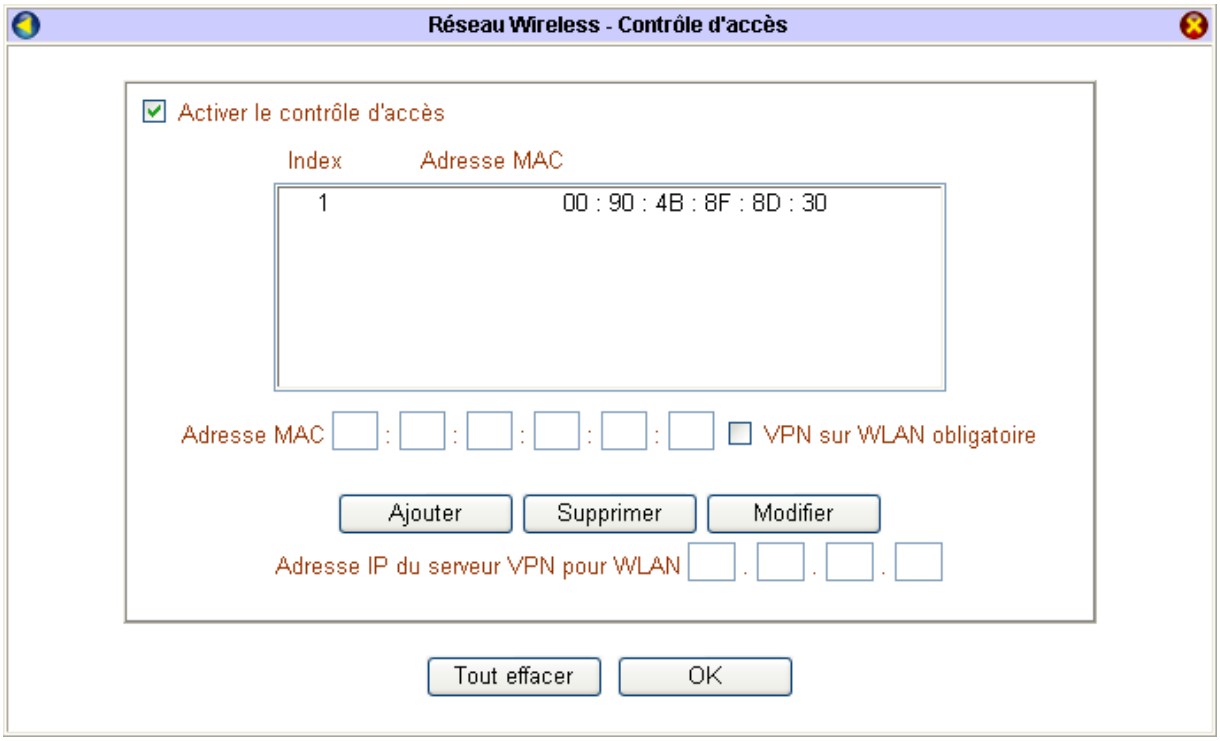


Si vous souhaitez ajouter un client Wireless dans le contrôle d'accès, procédez comme suit :

1. Sélectionnez le client Wireless détecté. L'adresse MAC de la station est alors prise en compte dans la rubrique **Adresse MAC du client**.
2. Cliquez sur le bouton **Ajouter**.



3. L'adresse MAC en question est alors automatiquement prise en compte dans le contrôle d'accès. Cette adresse est alors autorisée à accéder au ressources du réseau via le VPN Booster.



Accès à Internet

Avant de procéder à la configuration de votre connexion, selon le modèle de routeur dont vous disposez, vérifiez que votre raccordement est correctement établi dans le chapitre « Raccordements du routeur » page 12.

Accès à Internet via un modem xDSL ou câble

1. Sur la page d'accueil du configurateur, cliquez sur **Configuration rapide de la connexion**.
2. Dans la rubrique **Connexion haut débit via un périphérique externe**, vous avez le choix entre différents types de connexion. Sélectionnez votre type de connexion en cliquant sur le bouton correspondant (en cas de doute, renseignez-vous auprès de votre opérateur télécom pour connaître la nature de la liaison). En fonction du protocole sélectionné, suivez la procédure décrite ci-après.

Connexion Internet via le protocole PPPoE

1. En face de l'intitulé **Lien PPPoE**, sélectionnez l'option **Activer**.
2. Dans la rubrique **Nom de la connexion**, entrez un nom de connexion. Le choix de ce nom est arbitraire et n'a pas d'incidence sur la connexion.
3. Dans les rubriques **Nom d'utilisateur** et **Mot de passe**, entrez le nom d'utilisateur et le mot de passe de connexion que vous a attribués le FAI.

   Attention : lorsque vous entrez le nom d'utilisateur et le mot de passe, il est impératif de tenir compte des majuscules et des minuscules.
4. Si vous désirez gérer des heures de connexion, dans les rubriques des plages horaires, saisissez les numéros des plages horaires que vous souhaitez assigner à votre connexion xDSL.

   Remarque : au préalable, vous devez avoir paramétré et activé les plages horaires (reportez-vous au chapitre « Gestion des plages horaires » page 141).
5. Si vous disposez du routeur VPN Booster 32 i, c'est-à-dire avec le module RNIS intégré, vous avez une rubrique supplémentaire à paramétrer consacrée au mode de déclenchement du backup RNIS. Sélectionnez votre mode :
   - **Aucun** : lorsque cette option est sélectionnée, le backup RNIS n'est pas activé.
   - **Immédiatement** : si la connexion xDSL est interrompue, le backup RNIS se déclenchera immédiatement.
   - **Au prochain paquet** : si la connexion xDSL est interrompue, le backup RNIS ne sera actif que lorsqu'un nouveau paquet sera émis depuis le réseau local.
6. Dans la rubrique **Authentification PPP** de la **Configuration du protocole PPP**, sélectionnez **PAP ou CHAP** ou **PAP seulement** :

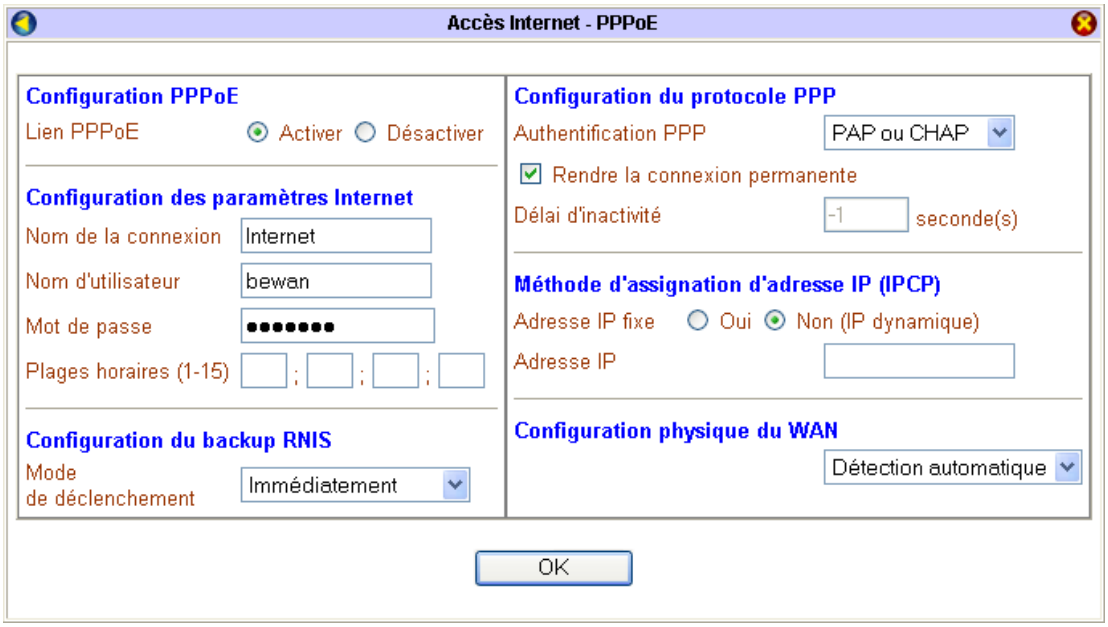
   Remarques :
   - *Si vous sélectionnez **PAP ou CHAP**, l'authentification pourra s'effectuer quel que soit le FAI.*
   - *Les protocoles d'authentification PPP acceptés dépendent du FAI. En cas de doute, contactez votre FAI.*
7. Si vous souhaitez bénéficier d'une connexion permanente, cochez la case correspondante (configuration recommandée). Dans ce cas, après une coupure, le routeur se reconnectera automatiquement.

   Sinon, dans la rubrique **Délai d'inactivité**, entrez le nombre de secondes d'inactivité au terme duquel la connexion à Internet sera automatiquement interrompue si aucun ordinateur du réseau local ne l'utilise.

   Remarque : si vous saisissez « 0 », vous pourrez bénéficier d'une connexion permanente. En revanche, après une coupure, le rétablissement de la connexion ne sera pas effectif.
8. Suivant votre abonnement xDSL, votre fournisseur d'accès Internet peut vous fournir une adresse IP fixe ou vous allouer dynamiquement une adresse IP à chaque connexion.
   - Si votre fournisseur d'accès Internet vous a communiqué une adresse IP fixe, sélectionnez **Oui** dans la rubrique **Adresse IP fixe** et saisissez l'adresse IP.

     Remarque : même avec un abonnement avec IP fixe, cette opération n'est pas obligatoire. En effet, lors de votre connexion, en fonction de votre nom et de votre mot de passe, votre adresse IP fixe vous est automatiquement affectée.

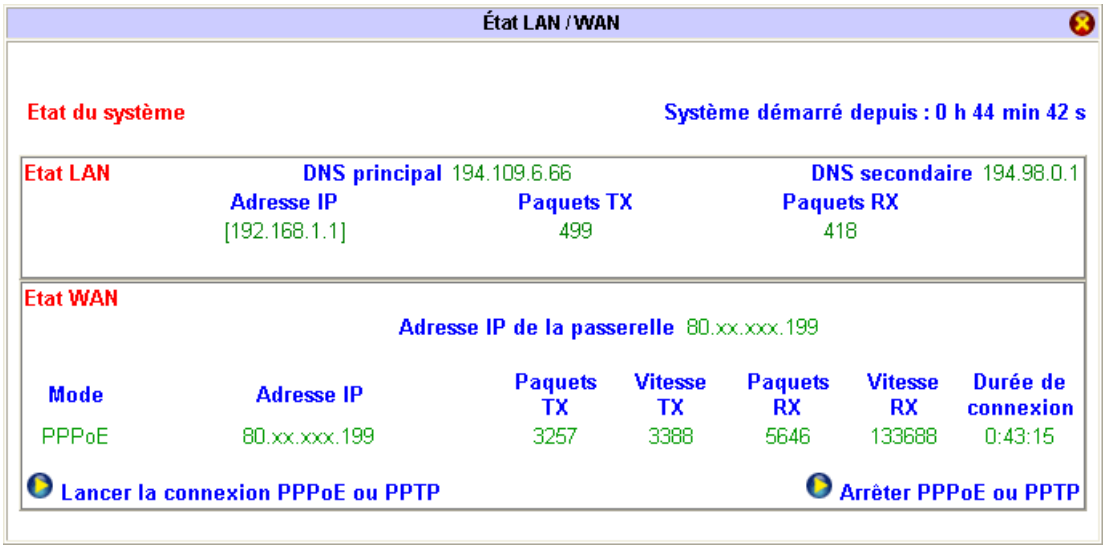
- Si votre fournisseur d'accès Internet ne vous a pas communiqué une adresse IP fixe, sélectionnez **Non** dans la rubrique **Adresse IP fixe**.



9. La configuration de votre accès Internet est terminée. Cliquez sur **OK** pour valider les informations.
10. Si vous désirez tester votre connexion, lancer votre requête Internet et ainsi vérifier l'exactitude des paramètres saisis, dans le menu **Diagnostics**, cliquez sur **Etat LAN / WAN**.
11. La fenêtre **Etat LAN / WAN** apparaît. Dans la partie **Etat WAN**, cliquez sur **Lancer la connexion PPPoE ou PPTP**. Votre mode de connexion doit alors apparaître. Un rafraîchissement a lieu toutes les 5 secondes.

Si ce n'est pas le cas, vérifiez les éléments suivants :

- Assurez-vous de nouveau du bon raccordement de votre routeur au modem xDSL (selon le modèle de routeur dont vous disposez, dans le chapitre « Raccordements du routeur » page 12, reportez-vous à la partie « Raccordement du routeur au modem xDSL ou câble »).
- Si le problème n'est pas résolu, assurez-vous ensuite auprès de votre opérateur que votre ligne ADSL a bien été activée.



Votre connexion est établie. Vous pouvez désormais ouvrir une seconde fenêtre dans votre logiciel afin de naviguer sur Internet.

*Remarque : pour interrompre la connexion, cliquez sur **Arrêter PPPoE ou PPTP**.*

Connexion Internet via le protocole PPTP

1. En face de l'intitulé **Lien PPTP**, sélectionnez l'option **Activer**.
2. Dans la rubrique **Adresse IP du modem ADSL**, entrez "10.0.0.138" (sauf avis contraire de votre opérateur télécom). Cette adresse est celle généralement utilisée.
3. Dans la rubrique **Nom de la connexion**, entrez un nom de connexion. Le choix de ce nom est arbitraire et n'a pas d'incidence sur la connexion.
4. Dans les rubriques **Nom d'utilisateur** et **Mot de passe**, entrez le nom d'utilisateur et le mot de passe de connexion que vous a attribués le FAI.

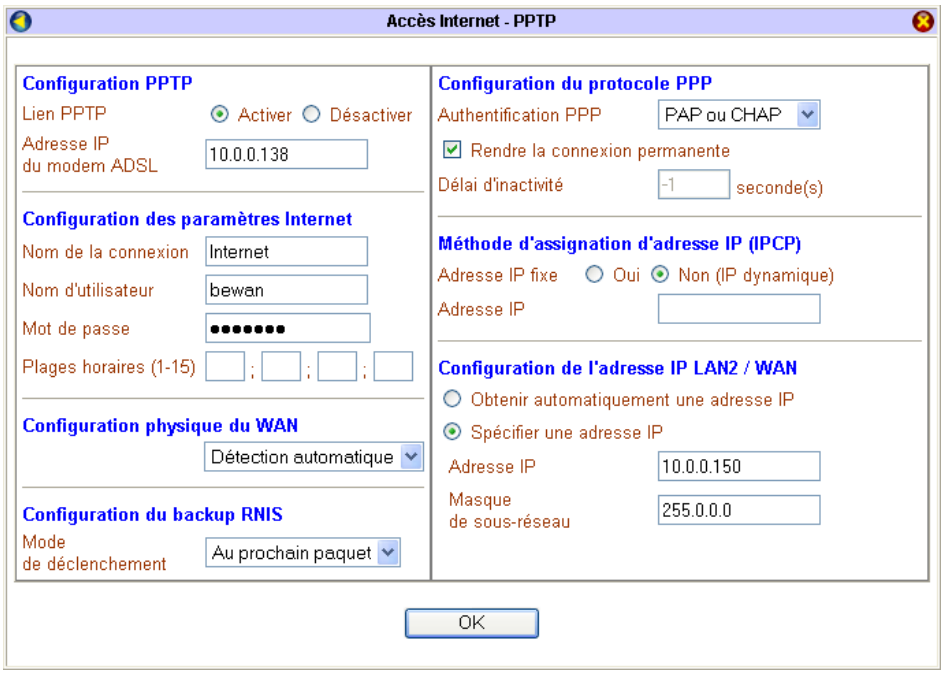
   Attention : lorsque vous entrez le nom d'utilisateur et le mot de passe, il est impératif de tenir compte des majuscules et des minuscules.
5. Si vous désirez gérer des heures de connexion, dans les rubriques des plages horaires, saisissez les numéros des plages horaires que vous souhaitez assigner à votre connexion ADSL.

   Remarque : au préalable, vous devez avoir paramétré et activé les plages horaires (reportez-vous au chapitre « Gestion des plages horaires » page 141).
6. Si vous disposez du routeur VPN Booster 32 i, c'est-à-dire avec le module RNIS intégré, vous avez une rubrique supplémentaire à paramétrer consacrée au mode de déclenchement du backup RNIS. Sélectionnez votre mode :
   - **Aucun** : lorsque cette option est sélectionnée, le backup RNIS n'est pas activé.
   - **Au prochain paquet** : si la connexion ADSL est interrompue, le backup RNIS ne sera actif que lorsqu'un nouveau paquet sera émis depuis le réseau local.
7. Dans la rubrique **Authentification PPP** de la **Configuration du protocole PPP**, sélectionnez **PAP ou CHAP** ou **PAP seulement** :

   Remarques :
   - *Si vous sélectionnez **PAP ou CHAP**, l'authentification pourra s'effectuer quel que soit le FAI.*
   - *Les protocoles d'authentification PPP acceptés dépendent du FAI. En cas de doute, contactez votre FAI.*
8. Si vous souhaitez bénéficier d'une connexion permanente, cochez la case correspondante (configuration recommandée). Dans ce cas, après une coupure, le routeur se reconnectera automatiquement.

   Sinon, dans la rubrique **Délai d'inactivité**, entrez le nombre de secondes d'inactivité au terme duquel la connexion à Internet sera automatiquement interrompue si aucun ordinateur du réseau local ne l'utilise.

   Remarque : si vous saisissez « 0 », vous pourrez bénéficier d'une connexion permanente. En revanche, après une coupure, le rétablissement de la connexion ne sera pas effectif.



9. Suivant votre abonnement ADSL, votre fournisseur d'accès Internet peut vous fournir une adresse IP fixe ou vous allouer automatiquement une adresse IP à chaque connexion.

   - Si votre fournisseur d'accès Internet vous a communiqué une adresse IP fixe, sélectionnez **Oui** dans la rubrique **Adresse IP fixe** et saisissez l'adresse IP.

     Remarque : même avec un abonnement avec IP fixe, cette opération n'est pas obligatoire. En effet, lors de votre connexion, en fonction de votre nom et de votre mot de passe, votre adresse IP fixe vous est automatiquement affectée.

   - Si votre fournisseur d'accès Internet ne vous a pas communiqué une adresse IP fixe, sélectionnez **Non** dans la rubrique **Adresse IP fixe**.

10. Dans la partie **Configuration de l'adresse IP LAN2/WAN**, sélectionnez **Spécifier une adresse IP**.

    Dans les rubriques **Adresse IP** et **Masque de sous-réseau**, veillez à saisir une adresse IP et un masque de sous-réseau compatibles avec le plan d'adressage du modem ADSL.

11. La configuration de votre accès Internet est terminée. Cliquez sur **OK** pour valider les informations.

12. Si vous désirez tester votre connexion, lancer votre requête Internet et ainsi vérifier l'exactitude des paramètres saisis, dans le menu **Diagnostics**, cliquez sur **Etat LAN / WAN**.

13. La fenêtre **Etat LAN / WAN** apparaît. Dans la partie **Etat WAN**, cliquez sur **Lancer la connexion PPPoE ou PPTP**. Votre mode de connexion doit alors apparaître. Un rafraîchissement a lieu toutes les 5 secondes.

Si ce n'est pas le cas, vérifiez les éléments suivants :

- Assurez-vous de nouveau du bon raccordement de votre routeur au modem ADSL (selon le modèle de routeur dont vous disposez, dans le chapitre « Raccordements du routeur » page 12, reportez-vous à la partie « Raccordement du routeur au modem xDSL ou câble »).
- Si le problème n'est pas résolu, assurez-vous ensuite auprès de votre opérateur que votre ligne ADSL a bien été activée.

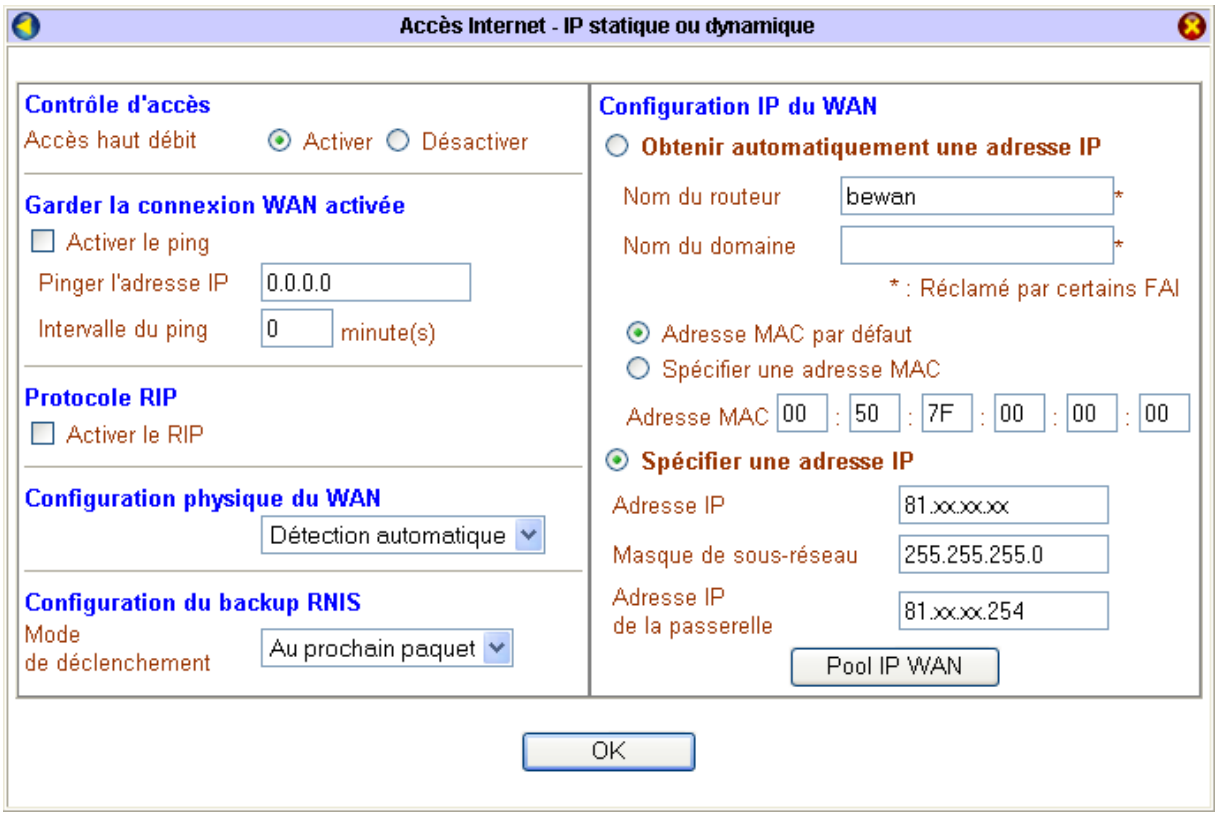
Votre connexion est établie. Vous pouvez désormais ouvrir une seconde fenêtre dans votre logiciel afin de naviguer sur Internet.

*Remarque : pour interrompre la connexion, cliquez sur **Arrêter PPPoE ou PPTP**.*

Connexion Internet en IP statique ou dynamique

Champ d'application : la plupart des utilisateurs du câble ou des réseaux xDSL dégroupés (via un modem Ethernet ou un équipement regroupant l'accès Internet et différents services) sélectionneront ce type de connexion. Renseignez-vous auprès de votre FAI pour connaître la nature de la liaison Internet.

1. En face de l'intitulé **Accès haut débit**, sélectionnez l'option **Activer**.
2. Si vous disposez du routeur VPN Booster 32 i, c'est-à-dire avec le module RNIS intégré, vous avez une rubrique supplémentaire à paramétrer consacrée au mode de déclenchement du backup RNIS. Sélectionnez votre mode :
   - **Aucun** : lorsque cette option est sélectionnée, le backup RNIS n'est pas activé.
   - **Au prochain paquet** : si la connexion xDSL est interrompue, le backup RNIS ne sera actif que lorsqu'un nouveau paquet sera émis depuis le réseau local.
3. Suivant votre abonnement, votre opérateur peut vous allouer automatiquement une adresse IP à chaque connexion ou vous fournir une adresse IP fixe.
   - Si votre opérateur ne vous a pas communiqué une adresse IP fixe, sélectionnez **Obtenir automatiquement une adresse IP**.
   - Si votre opérateur vous a communiqué une adresse IP fixe, sélectionnez **Spécifier une adresse IP**, puis saisissez dans les rubriques correspondantes l'adresse IP ainsi que le masque de sous-réseau indiqués par votre opérateur.

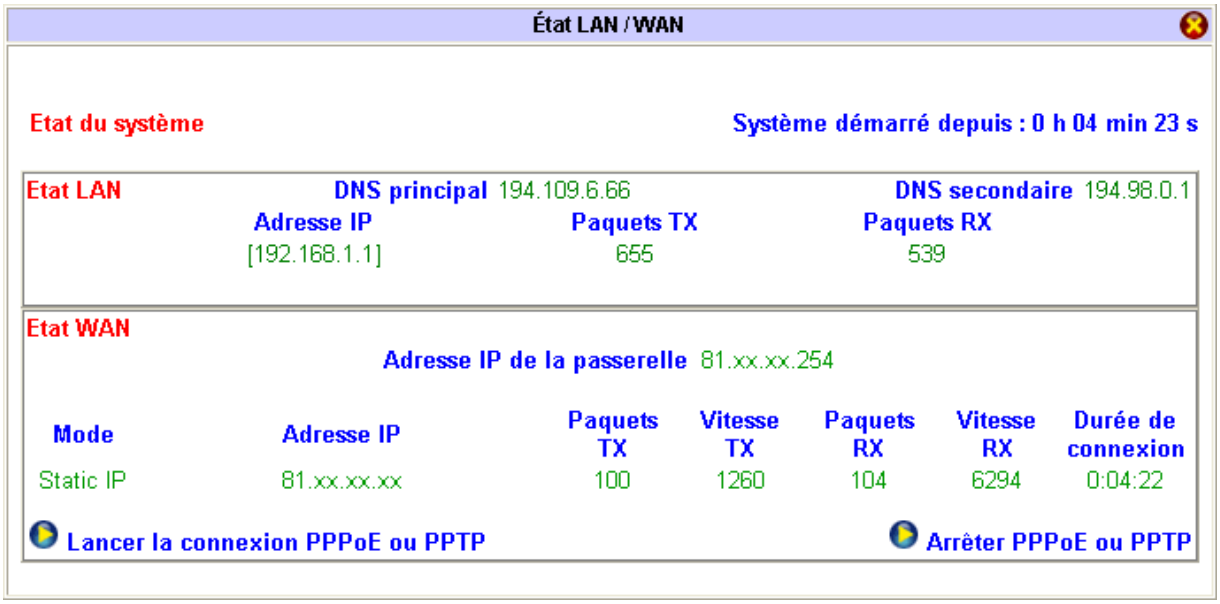


4. La configuration de votre accès Internet est terminée. Cliquez sur **OK** pour valider les informations.
5. Le routeur doit redémarrer pour prendre en compte les nouveaux paramètres. Sélectionnez **Conserver la configuration actuelle**, puis cliquez sur **OK**. Attendez 5 secondes pour que le redémarrage soit terminé.

   Attention : n'éteignez surtout pas le VPN Booster pendant cette phase de redémarrage. Vous risqueriez d'endommager sa mémoire et de le rendre inutilisable (dommage non couvert par la garantie).

   Une nouvelle fenêtre apparaît. Cliquez sur l'adresse http, qui est en fait l'adresse IP de votre routeur, afin de retourner sur le configurateur du VPN Booster.
6. Si vous désirez tester votre connexion, lancer votre requête Internet et ainsi vérifier l'exactitude des paramètres saisis, dans le menu **Diagnostics**, cliquez sur **Etat LAN / WAN**.

7. La fenêtre **Etat LAN / WAN** apparaît. Dans la partie **Etat WAN**, votre mode de connexion doit alors apparaître (**DHCP Client** si votre opérateur vous a fourni dynamiquement une adresse IP ou **Static IP** si vous avez une adresse IP fixe). Un rafraîchissement a lieu toutes les 5 secondes. Pour vérifier que votre connexion est bien établie, sous **Paquets RX** et **Vitesse RX**, les valeurs ne doivent pas être à « 0 ».



Votre connexion est établie. Vous pouvez désormais ouvrir une seconde fenêtre dans votre logiciel afin de naviguer sur Internet.

*Remarque : pour interrompre la connexion, dans la partie **IP statique ou dynamique**, en face de l'intitulé **Accès haut débit**, sélectionnez l'option **Désactiver**. Cliquez ensuite sur **OK** pour valider. Le routeur doit redémarrer pour que les nouveaux paramètres soient pris en compte et pour que votre connexion soit interrompue.*

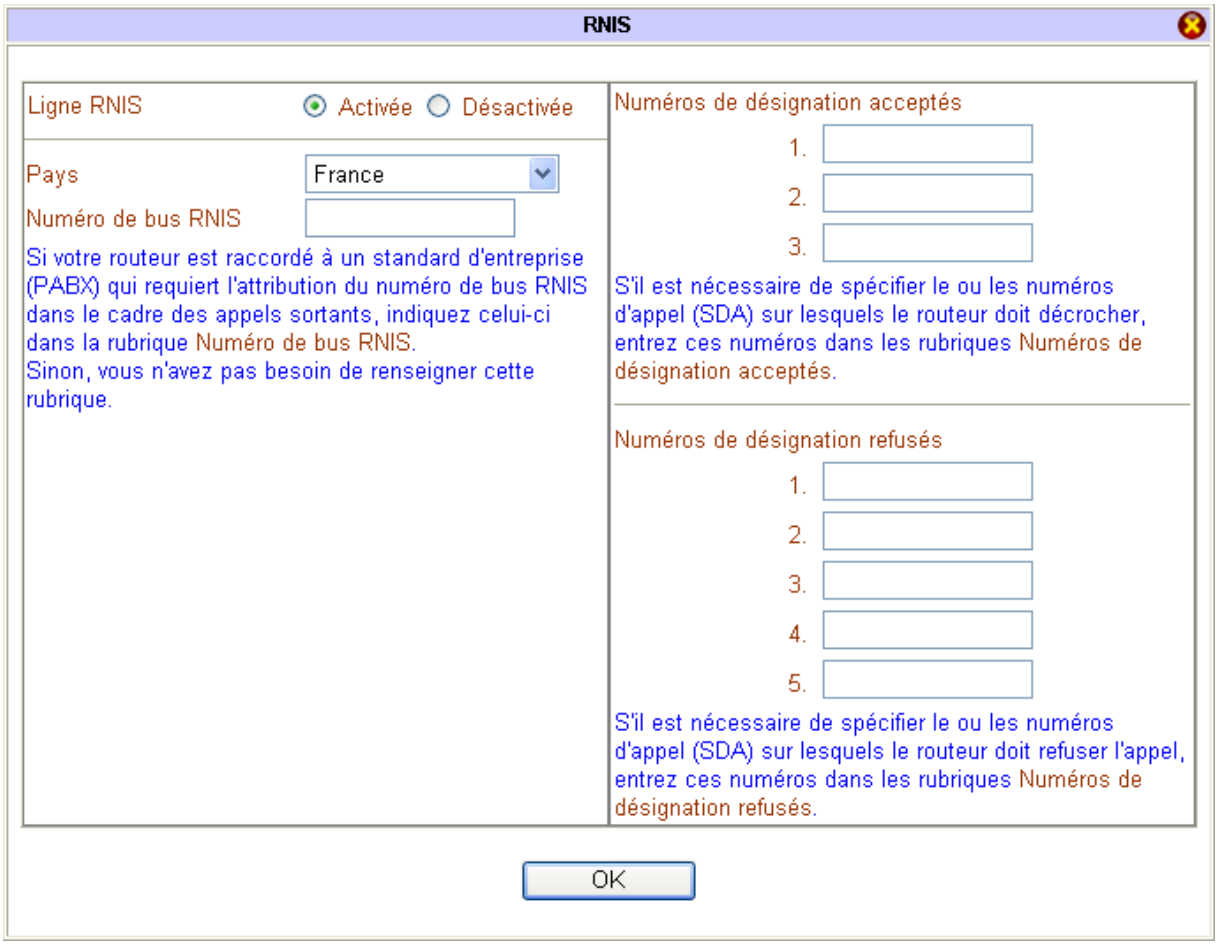
Accès à Internet via le réseau RNIS (VPN Booster 32 i uniquement)

L'accès à Internet via RNIS peut être utilisé comme liaison principale ou comme liaison de secours (backup) si la liaison principale s'effectue via un modem ADSL par exemple (reportez-vous à la section « Accès à Internet via un modem xDSL ou câble » page 79).

Avant de procéder à la configuration de votre connexion, vérifiez au préalable que votre raccordement est correctement effectué comme indiqué dans la partie « Raccordements du routeur au réseau RNIS (VPN Booster 32 i) » page 16.

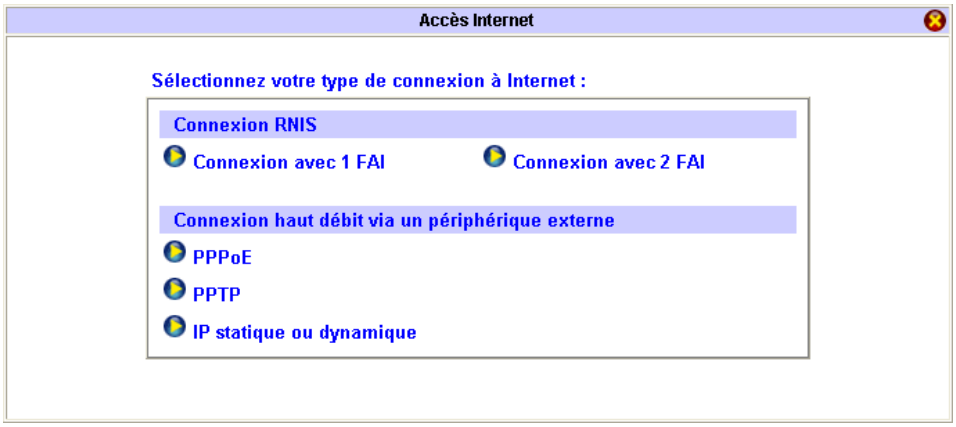
Vérifiez également que la ligne RNIS est bien activée dans le configurateur HTML du routeur. Procédez comme suit :

1. Dans le menu **Configuration Elémentaire**, cliquez sur **RNIS**. L'écran suivant apparaît :



2. La ligne RNIS est activée par défaut. Vérifiez que l'option **Activée** est bien sélectionnée.
3. Dans la rubrique **Pays**, sélectionnez le pays dans lequel est installé le VPN Booster.
4. Dans la rubrique **Numéro de bus RNIS** :
   - Si le VPN Booster est connecté à une ligne directe (accès de base Numéris…), n'entrez rien dans cette rubrique.
   - Si le VPN Booster est relié à un standard d'entreprise (PABX), il peut être nécessaire dans certains cas d'indiquer votre numéro de poste. Attention, le numéro de poste n'est généralement pas un numéro du plan de numérotation national attribué par l'opérateur de télécommunication, mais un numéro de poste à 2, 3 ou 4 chiffres défini par l'installateur du PABX. En cas de doute, renseignez-vous auprès du responsable du PABX.
5. Cliquez sur **OK** pour valider.
6. Sur la page d'accueil du configurateur, cliquez sur **Configuration rapide de la connexion**.

7. Dans la rubrique **Connexion RNIS**, il est possible de configurer l'accès à un ou deux fournisseurs d'accès Internet (FAI). Vous devez disposer des informations fournies par le (les) FAI auprès duquel (desquels) vous avez souscrit votre abonnement. En fonction du type de connexion, suivez la procédure décrite ci-après.



Connexion avec 1 FAI

1. Dans la rubrique **Nom de la connexion** de la partie **Configuration des paramètres Internet**, entrez un nom de connexion. Le choix de ce nom est arbitraire et n'a pas d'incidence sur la connexion.
2. Dans la rubrique **Numéro à composer**, entrez le numéro d'appel du FAI (ne mettez pas d'espace ni de virgule).

   Remarque : si le VPN Booster est relié à un standard d'entreprise, n'oubliez pas, si nécessaire, de préciser le préfixe de sortie de celui-ci (généralement le "0").
3. Dans les rubriques **Nom d'utilisateur** et **Mot de passe**, entrez le nom d'utilisateur et le mot de passe de connexion que vous a attribués le FAI.

   Attention : lorsque vous entrez le nom d'utilisateur et le mot de passe, il est impératif de tenir compte des majuscules et des minuscules.
4. Si vous désirez gérer des heures de connexion, dans les rubriques des plages horaires, saisissez les numéros des plages horaires que vous souhaitez assigner à votre connexion RNIS.

   Remarque : au préalable, vous devez avoir paramétré et activé les plages horaires (reportez-vous au chapitre « Gestion des plages horaires » page 141).
5. Dans la rubrique **Type de connexion** de la **Configuration du protocole PPP / MLPPP**, sélectionnez le type de connexion Internet souhaité :
   - **Connexion désactivée** : lorsque cette option est sélectionnée, la connexion est impossible.
   - **Connexion 64 Kbps** : la connexion s'établira sur un canal B à 64 Kbps.
   - **Connexion 128 Kbps** : la connexion s'établira sur deux canaux B agrégés à 128 Kbps.

     Attention : vérifiez que votre FAI autorise bien la connexion à 128 Kbps. N'oubliez pas que vous payez dans ce cas deux communications téléphoniques.
   - **Connexion BOD** : la connexion s'établira initialement sur un seul canal B, mais le deuxième canal B pourra se connecter et se déconnecter en fonction du besoin en bande passante. Au cours d'une connexion, le débit pourra donc varier entre 64 et 128 Kbps afin d'optimiser le rapport confort/coût de communication.

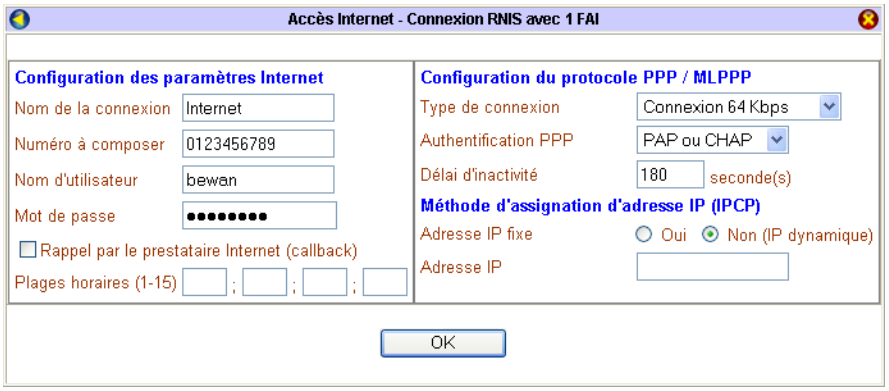
     Attention : vérifiez que votre FAI autorise bien la connexion à 128 Kbps. Vous payez deux communications téléphoniques lorsque la communication utilise deux canaux B.

     *Remarque : si vous souhaitez modifier les paramètres par défaut de la connexion BOD, dans le menu **Réglages Avancés**, cliquez sur **Débit RNIS et options de rappel**.*
6. Dans la rubrique **Authentification PPP**, sélectionnez **PAP ou CHAP** ou **PAP seulement**.

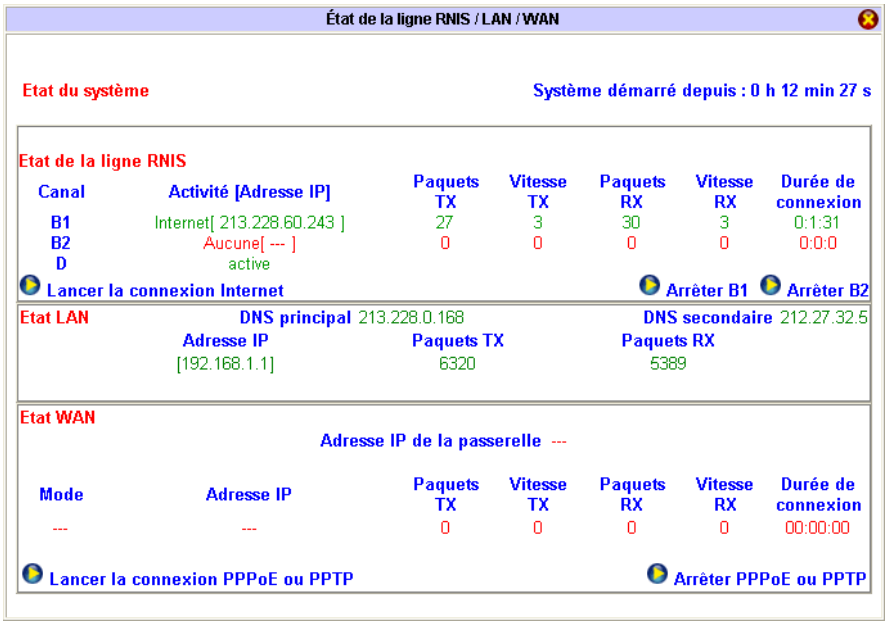
   Remarques :
   - *Si vous sélectionnez **PAP ou CHAP**, l'authentification pourra s'effectuer quel que soit le FAI.*
   - *Les protocoles d'authentification PPP acceptés dépendent du FAI. En cas de doute, contactez votre FAI.*

7. Dans la rubrique **Délai d'inactivité**, entrez le nombre de secondes d'inactivité au terme duquel la connexion à Internet sera automatiquement interrompue si aucun ordinateur du réseau local ne l'utilise.
8. Suivant votre abonnement, votre FAI peut vous fournir une adresse IP fixe ou vous allouer automatiquement une adresse IP à chaque connexion.
   - Si votre FAI vous a communiqué une adresse IP fixe, sélectionnez **Oui** dans la rubrique **Adresse IP fixe** et saisissez l'adresse IP.

     Remarque : même avec un abonnement avec IP fixe, cette opération n'est pas obligatoire. En effet, lors de votre connexion, en fonction de votre nom et de votre mot de passe, votre adresse IP fixe vous est automatiquement affectée.
   - Si votre FAI ne vous a pas communiqué une adresse IP fixe, sélectionnez **Non** dans la rubrique **Adresse IP fixe**.



9. La configuration de votre accès Internet est terminée. Cliquez sur **OK** pour valider les informations.
10. Si vous désirez tester votre connexion, lancer votre requête Internet et ainsi vérifier l'exactitude des paramètres saisis, dans le menu **Diagnostics**, cliquez sur **Etat de la ligne RNIS / LAN / WAN**.
11. La fenêtre **Etat de la ligne RNIS / LAN / WAN** apparaît. Dans la partie **Etat de la ligne RNIS**, cliquez sur **Lancer la connexion Internet**. Un rafraîchissement a lieu toutes les 5 secondes. Sur le canal D, la signalisation RNIS devient active. Le nom de votre connexion doit apparaître sur l'un des deux canaux B si vous êtes connecté à 64 Kbps, sur les deux si vous êtes connecté à 128 Kbps.



Votre connexion RNIS est établie. Vous pouvez désormais ouvrir une seconde fenêtre dans votre logiciel afin de naviguer sur Internet. Si vous désirez ensuite vérifier la durée de votre connexion ou avoir des informations sur les paquets transmis ou reçus, revenez dans la première fenêtre du navigateur sur la page **Etat de la ligne RNIS / LAN / WAN**.

*Remarque : pour interrompre la connexion, cliquez sur **Arrêter B1** et/ou **Arrêter B2**.*

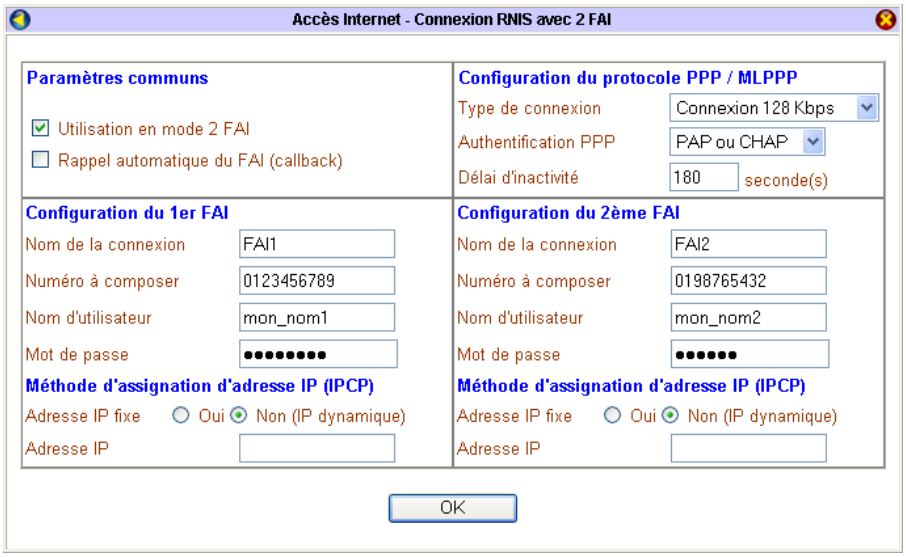
Connexion avec 2 FAI

Le VPN Booster 32 i vous permet également de configurer un double accès à Internet pour établir une connexion à 64 Kbps pour chacun d'entre eux.

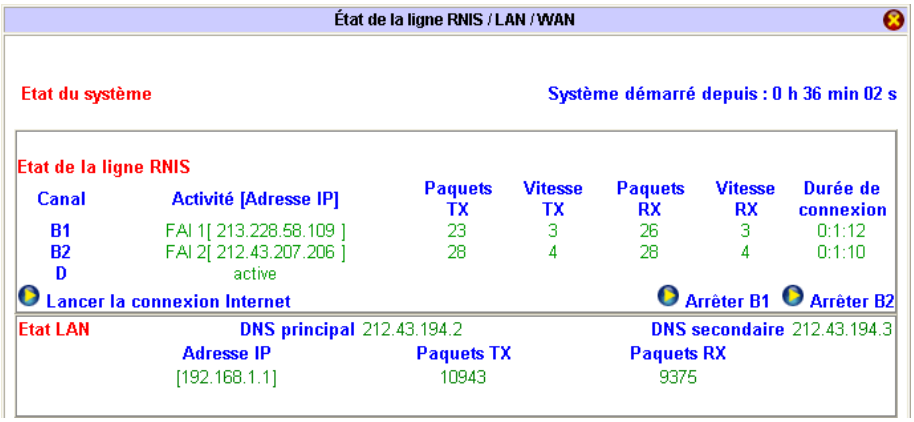
Certains FAI ne proposant pas de compte d'accès à 128 Kbps, dans ce cas précis, il peut être intéressant de souscrire à deux comptes différents chez un FAI afin d'établir une double connexion (2 x 64 Kbps).

Attention : la connexion en mode 2 FAI n'est pas possible si on utilise également une connexion xDSL.

1. Dans la partie **Paramètres communs**, cochez **Utilisation en mode 2 FAI**.
2. Saisissez les informations indiquées par les fournisseurs d'accès Internet (FAI) auprès desquels vous avez souscrit vos abonnements.
3. Dans la rubrique **Type de connexion**, sélectionnez **Connexion 128 Kbps**.



4. La configuration de votre accès Internet est terminée. Cliquez sur **OK** pour valider les informations.
5. Si vous désirez tester la connexion et ainsi vérifier l'exactitude des paramètres saisis, dans le menu **Diagnostics**, cliquez sur **Etat de la ligne RNIS / LAN / WAN**.
6. La fenêtre correspondante apparaît. Dans la partie **Etat de la ligne RNIS**, cliquez sur **Lancer la connexion Internet**. Un rafraîchissement a lieu toutes les 5 secondes. Sur le canal D, la signalisation RNIS devient active. Les noms de vos connexions doivent apparaître sur les deux canaux B si vous êtes connecté à 128 Kbps.



Votre connexion RNIS est établie. Vous pouvez désormais ouvrir une seconde fenêtre dans votre logiciel afin de naviguer sur Internet. Si vous désirez ensuite vérifier la durée de votre connexion ou avoir des informations sur les paquets transmis ou reçus, revenez dans la première fenêtre du navigateur sur la page **Etat de la ligne RNIS / LAN / WAN**.

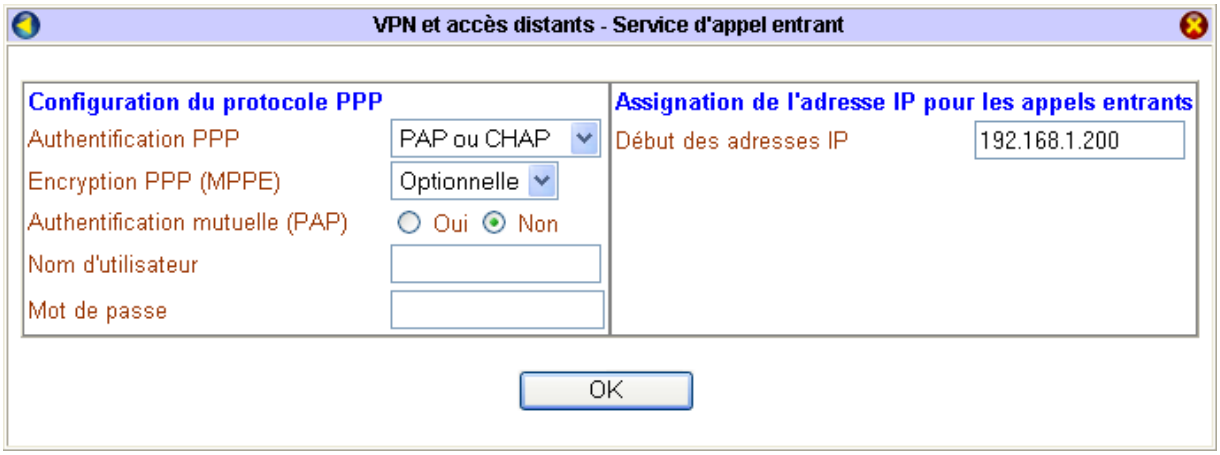
*Remarque : pour interrompre la connexion, cliquez sur **Arrêter B1** et/ou **Arrêter B2**.*

Connexion d'équipements distants (VPN Booster 32 i)

Connexion de postes isolés via RNIS

L'assistant de configuration d'appel entrant vous permet de configurer le VPN Booster 32 i afin que des équipements distants (ordinateurs, routeurs...) puissent se connecter à votre réseau local en toute sécurité. Cela ne s'applique que dans le cas où l'on effectue une connexion via un PC équipé d'un adaptateur RNIS.

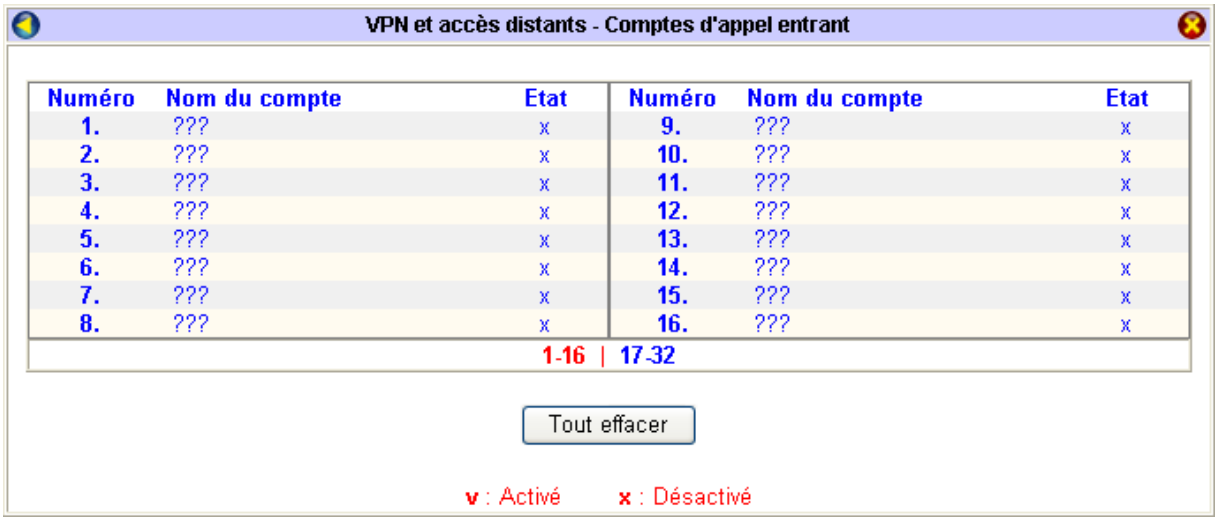
1. Dans le menu **Réglages Avancés**, cliquez sur **VPN et accès distants**, puis sur **Service d'appel entrant**.



2. Dans la rubrique **Authentification PPP** de la **Configuration du protocole PPP**, sélectionnez **PAP ou CHAP** ou **PAP seulement** en fonction du type d'authentification que vous souhaitez mettre en place.
3. L'activation de l'**Authentification mutuelle (PAP)** n'est pas indispensable. Par défaut, l'option **Non** est cochée. L'authentification mutuelle (PAP) constitue une sécurité supplémentaire. Si vous cochez l'option **Oui**, pour que l'appel entrant soit accepté, les 2 équipements distants doivent alors avoir des identifiants identiques (nom d'utilisateur et mot de passe).
4. Dans la rubrique **Début des adresses IP**, indiquez la première adresse IP à assigner aux équipements distants.

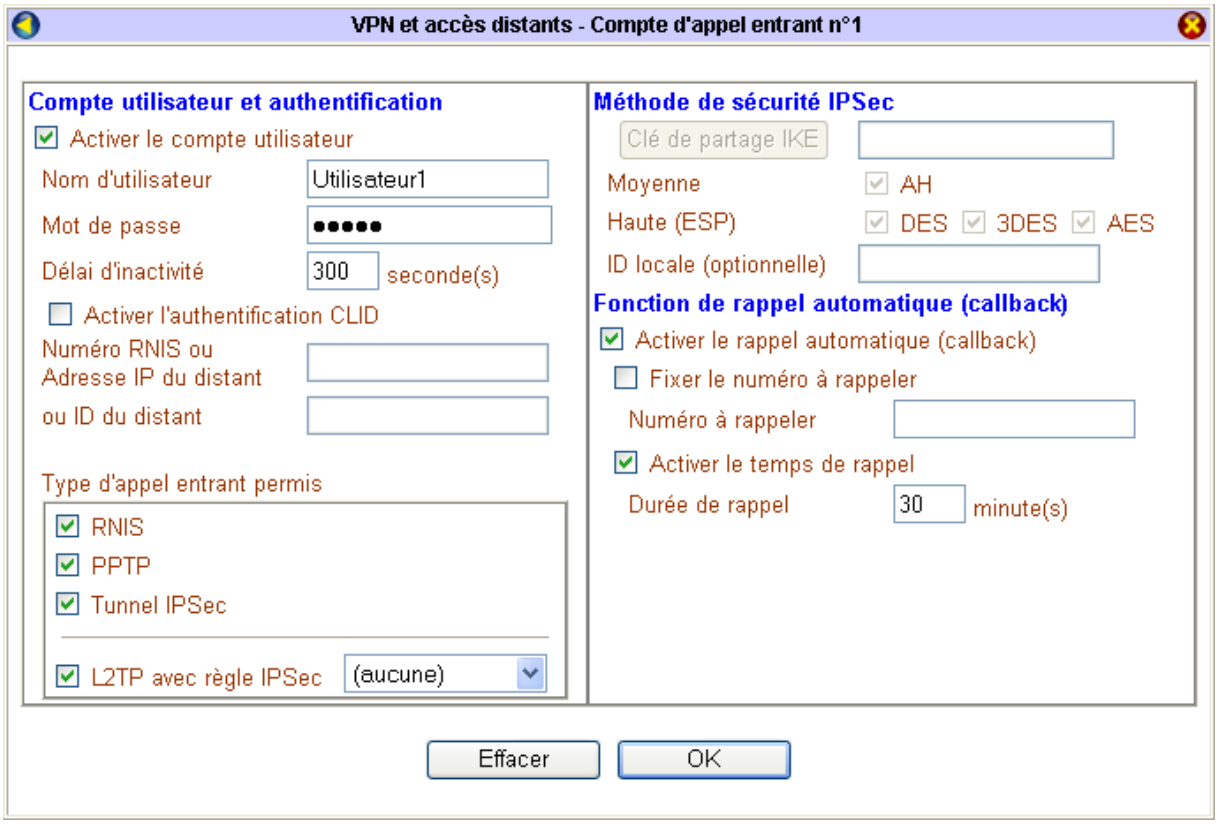
   Attention :

   - *Les équipements distants peuvent également spécifier des adresses IP fixes.*
   - *Qu'elles soient fixes ou allouées dynamiquement, les adresses IP des équipements distants doivent être compatibles avec le plan d'adressage du VPN Booster 32 i.*
5. Cliquez sur **OK**.
6. Cliquez ensuite sur **Comptes d'appel entrant**. La fenêtre suivante permet de configurer les comptes d'appel entrant et de les activer.



Le VPN Booster 32 i vous permet de paramétrer jusqu'à 32 comptes d'appel entrant. Toutefois, le nombre de connexions entrantes simultanées est limité au nombre de canaux B disponibles à un moment donné, soit deux au maximum (caractéristique de la ligne RNIS).

7. Pour paramétrer un compte, cliquez sur un numéro (si le compte n'a pas encore été paramétré, le nom du compte apparaît sous la forme **???**).
8. Pour activer le compte, cochez **Activer le compte utilisateur**.
9. Entrez un nom et un mot de passe dans les rubriques **Nom d'utilisateur** et **Mot de passe** (16 caractères maximum pour chacune des rubriques).
10. Dans la rubrique **Délai d'inactivité**, entrez le nombre de secondes au terme duquel la connexion sera automatiquement interrompue en cas d'inactivité.
11. Vous pouvez activer le système d'authentification CLID qui consiste à vérifier le numéro d'appel du correspondant. Pour cela, cochez **Activer l'authentification CLID**, puis indiquez le numéro RNIS du correspondant dans la rubrique correspondante.



12. Vous pouvez activer la fonction de rappel automatique (callback) afin que le correspondant soit rappelé par le routeur. Pour cela, cochez **Activer le rappel automatique (callback)**.

- Si le correspondant doit être rappelé à un numéro spécifique prédéterminé, cochez **Fixer le numéro à rappeler** et entrez le numéro à composer.

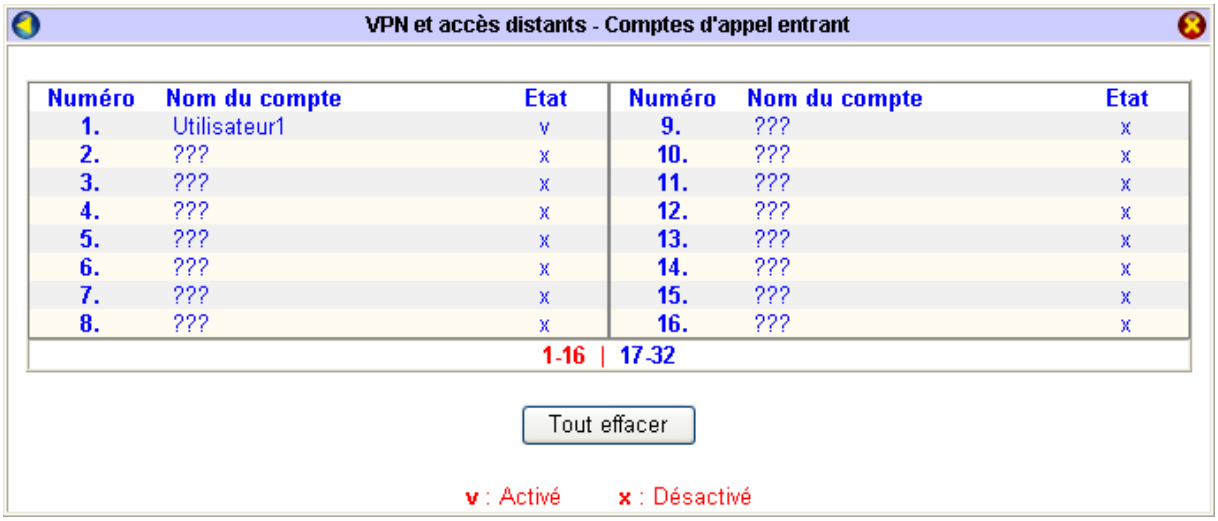
  Remarque : si cette option n'est pas cochée, le VPN Booster 32 i envoie une instruction à l'équipement distant afin que celui-ci indique le numéro à rappeler.

- Vous pouvez allouer un temps de rappel au correspondant en cochant **Activer le temps de rappel** et en indiquant une durée dans la rubrique **Durée de rappel**.

Remarque : le temps de rappel fonctionne comme un crédit de temps. La durée de chaque rappel est déduite. Lorsque le temps de rappel est épuisé, le VPN Booster n'effectue plus le rappel automatique. L'administrateur peut alors choisir d'allouer au correspondant un nouveau temps de rappel dans la rubrique ***Durée de rappel****.*

13. Cliquez sur **OK**.

La configuration du compte d'appel entrant est terminée. Dans la colonne **Etat**, le compte est indiqué *Activé* (« **v** »).



Procédez comme précédemment pour chacun des comptes que vous souhaitez paramétrer. Si vous avez paramétré et activé un ou plusieurs comptes, le VPN Booster 32 i peut désormais recevoir des appels entrants.

Remarque : n'oubliez pas de communiquer les paramètres de connexion à chacun de vos correspondants.

Interconnexion de réseaux via RNIS

Il est possible de connecter deux réseaux locaux distants via RNIS en utilisant 2 VPN Booster 32 i. Cette section vous indique comment configurer les profils de chacun des deux réseaux afin qu'ils puissent être interconnectés.

Attention :

- *Avant de paramétrer votre interconnexion, vérifiez que votre ligne RNIS est bien activée. Pour cela, dans le menu* ***Configuration Elémentaire****, cliquez sur* ***RNIS****. Par défaut, cette ligne est activée. Si ce n'est plus le cas, sélectionnez* ***Activée****, puis cliquez sur* ***OK*** *afin que ce paramètre soit pris en compte.*
- *Si vous désirez établir une communication à 128 Kbps avec le site distant, n'oubliez pas que votre correspondant doit également avoir sélectionné le même débit dans le paramétrage de l'appel entrant. Si tel n'est pas le cas, le routeur va essayer d'établir une connexion à 128 Kbps, mais n'ayant aucune réponse, la connexion ne s'effectuera que sur un seul canal à 64 Kbps. Pour paramétrer votre type de connexion, dans le menu* ***Réglages Avancés****, cliquez sur* ***Débit RNIS et options de rappel****.*

Il est nécessaire, pour que l'interconnexion soit établie, que les administrateurs des 2 sites distants s'échangent leurs paramètres de connexion (numéro RNIS, mot de passe,…).

Pour rendre plus claire cette section, nous avons documenté un cas d'application concret.

Voici les caractéristiques des deux réseaux de notre exemple :

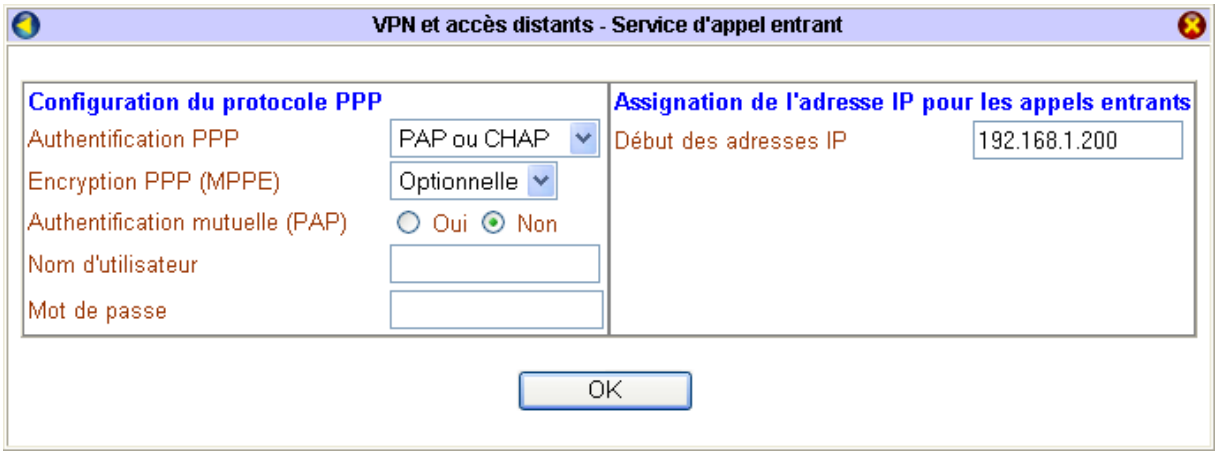
Nom du réseau	**Site A : Agence**	**Site B : Succursale**
Adresse IP du réseau	192.168.1.0	192.168.2.0
Adresse IP du routeur	192.168.1.1	192.168.2.1
Assignation de l'adresse IP pour les appels entrants	192.168.1.200	192.168.2.200
Numéro RNIS	0123456789	0198765432

Etape 1 : Paramétrage de l'appel entrant

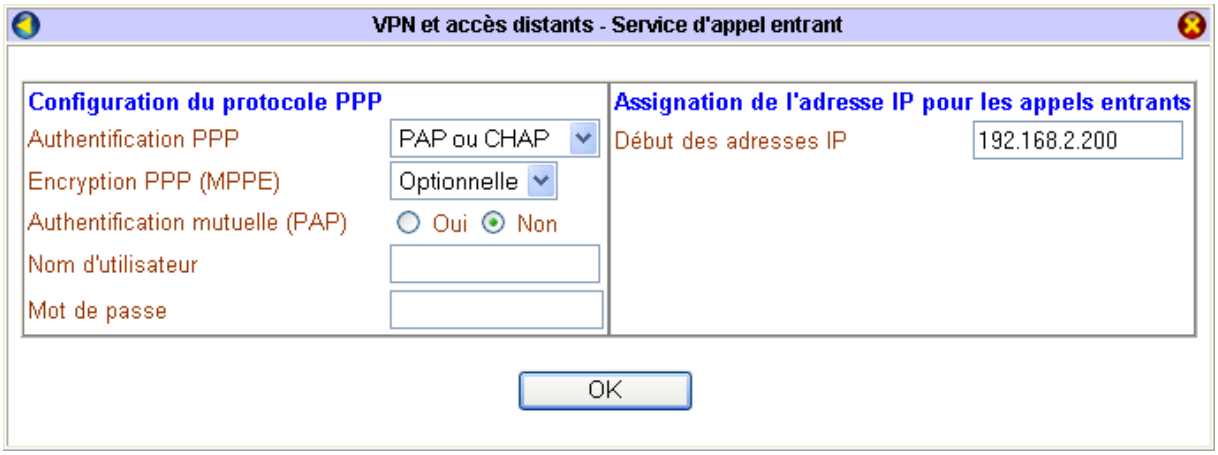
Afin que les deux réseaux puissent s'interconnecter, vous devez activer le service d'appel entrant. Cette activation doit être effective pour chacun des deux réseaux. Pour cela, il vous suffit d'activer un compte d'appel entrant. Procédez comme suit :

1. Dans le menu **Réglages Avancés**, cliquez sur **VPN et accès distants**, puis sur **Service d'appel entrant**.
2. Dans la rubrique **Authentification PPP** de la **Configuration du protocole PPP**, sélectionnez **PAP ou CHAP** ou **PAP seulement** en fonction du type d'authentification que vous souhaitez mettre en place.
3. L'activation de l'**Authentification mutuelle (PAP)** n'est pas indispensable. Par défaut, l'option **Non** est cochée. L'authentification mutuelle (PAP) constitue une sécurité supplémentaire. Si vous cochez l'option **Oui**, pour que l'appel entrant soit accepté, les 2 équipements distants doivent alors avoir des identifiants identiques (nom d'utilisateur et mot de passe).
4. Dans la rubrique **Début des adresses IP**, indiquez une adresse IP à assigner aux équipements distants.

Configuration sur le Site A, celui de l'Agence principale :



Configuration sur le Site B, celui de la Succursale :

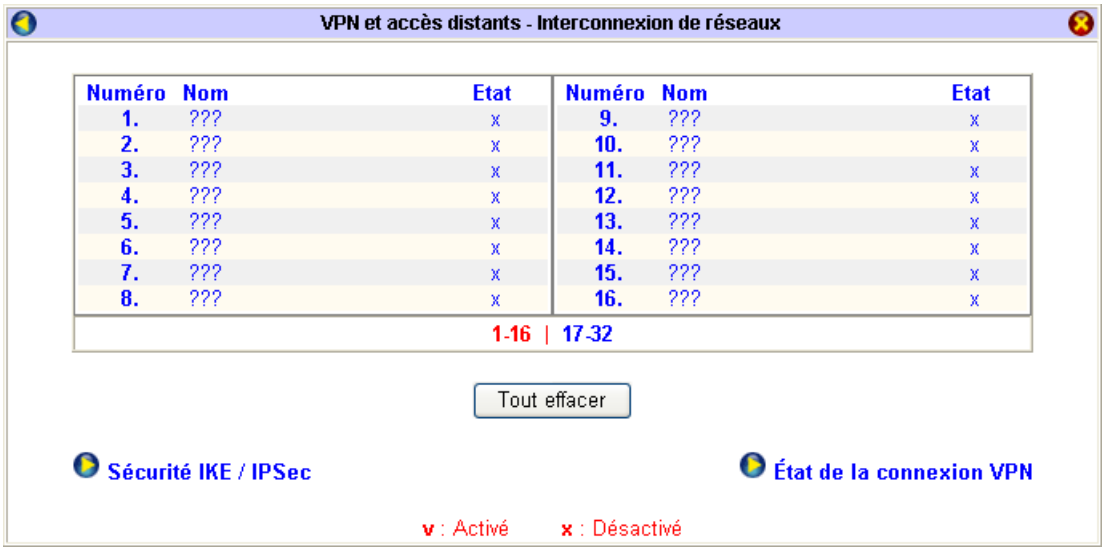


5. Cliquez sur **OK** pour valider ces informations.

Etape 2 : Création du profil des deux réseaux

Vous devez désormais créer sur chaque site un profil d'interconnexion afin d'établir les caractéristiques de la connexion avec le réseau distant.

1. Dans le menu **Réglages Avancés**, cliquez sur **VPN et accès distants**, puis sur **Interconnexion de réseaux**. L'écran suivant apparaît.



2. Cliquez sur un numéro dans la colonne **Numéro**.

   Remarques :

   - *Si un profil n'a pas encore été paramétré, son nom apparaît sous la forme* ***???****, indiquant qu'il est disponible.*
   - *Le VPN Booster 32 i vous permet de gérer jusqu'à 32 sites distants.*

3. Pour chaque profil d'interconnexion, vous devez renseigner quatre parties : Paramètres généraux, Paramètres d'appel sortant, Paramètres d'appel entrant, Paramètres TCP/IP de l'interconnexion de réseaux. Vous pouvez vous référer aux captures d'écrans suivantes. Procédez comme suit :

   Remarque : pour saisir le profil d'interconnexion, vous devez avoir en votre possession certains paramètres transmis par l'administrateur du site distant.

Partie 1 : Paramètres généraux

1. Pour activer le profil, sélectionnez l'option **Activer ce profil**.
2. Dans la rubrique **Nom du profil**, indiquez un nom qui soit clair pour vous (10 caractères maximum), correspondant à votre interconnexion.
3. En face de l'intitulé **Sens de l'appel**, sélectionnez la direction des appels pour ce profil :
   - **Entrant/sortant** : l'interconnexion peut s'établir aussi bien sur appels entrants que sur appels sortants.
   - **Entrant** : l'interconnexion ne peut s'établir que sur appels entrants.
   - **Sortant** : l'interconnexion ne peut s'établir que sur appels sortants.
4. Décochez **Rendre la connexion permanente**.
5. Dans la rubrique **Délai d'inactivité**, entrez le nombre de secondes d'inactivité au terme duquel votre interconnexion sera automatiquement interrompue si aucun ordinateur du réseau local ne l'utilise.

Partie 2 : Paramètres d'appel sortant

Dans cette partie, vous devez saisir les paramètres fournis par l'administrateur du réseau distant. Procédez comme suit :

1. Dans la partie **Type de serveur appelé**, sélectionnez le type **RNIS**.
2. Dans la rubrique **Numéro à composer**, saisissez le numéro que vous a fourni l'administrateur du site distant.
3. Dans la rubrique **Type de connexion**, sélectionnez le type de connexion souhaité :
   - **Connexion désactivée** : lorsque cette option est sélectionnée, la connexion est impossible.
   - **Connexion 64 Kbps** : la connexion s'établira sur un canal B à 64 Kbps.
   - **Connexion 128 Kbps** : la connexion s'établira sur deux canaux B agrégés à 128 Kbps.
   - **Connexion BOD** : la connexion s'établira initialement sur un seul canal B, mais le deuxième canal B pourra se connecter et se déconnecter en fonction du besoin en bande passante. Au cours d'une connexion, le débit pourra donc varier entre 64 et 128 Kbps afin d'optimiser le rapport confort/coût de communication.
4. Dans les rubriques **Nom d'utilisateur** et **Mot de passe**, entrez le nom (49 caractères maximum) et le mot de passe (24 caractères maximum) qui vous identifient sur le site distant.
5. Dans la rubrique **Authentification PPP**, sélectionnez **PAP ou CHAP** ou **PAP seulement**.

   Remarques :
   - *Si vous sélectionnez **PAP ou CHAP**, l'authentification pourra s'effectuer dans tous les cas.*
   - *Les protocoles d'authentification PPP acceptés dépendent du paramétrage du site distant. En cas de doute, contactez son administrateur.*

Partie 3 : Paramètres d'appel entrant

Dans cette partie, vous devez saisir les paramètres concernant le réseau distant. Procédez comme suit :

1. Dans la rubrique **Type d'appel entrant permis**, sélectionnez le type **RNIS**.
2. Dans les rubriques **Nom d'utilisateur** et **Mot de passe**, entrez un nom et un mot de passe (11 caractères maximum pour chacune des rubriques).

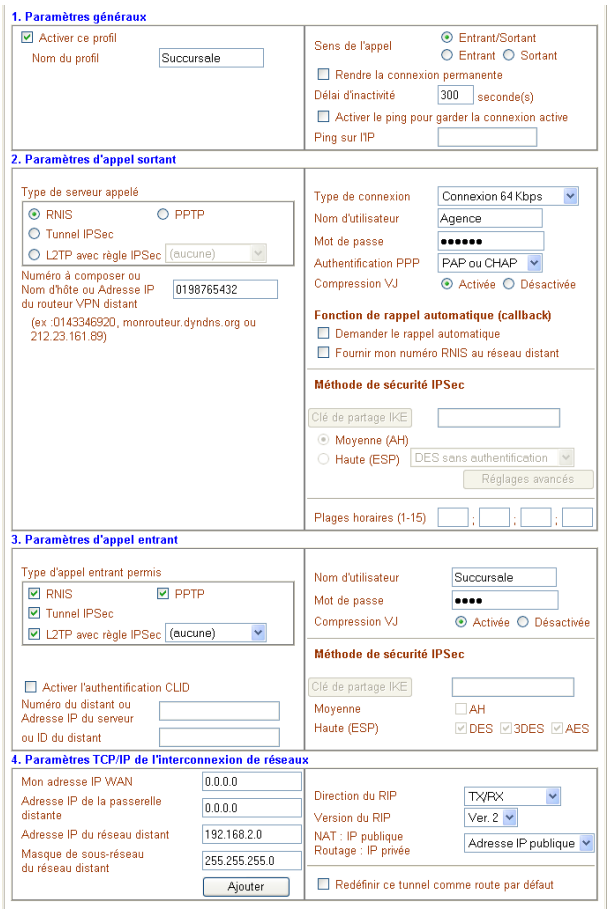
   Remarque : vérifiez que vos paramètres sont bien compatibles avec ceux enregistrés par le réseau distant.

Partie 4 : Paramètres TCP/IP de l'interconnexion de réseaux

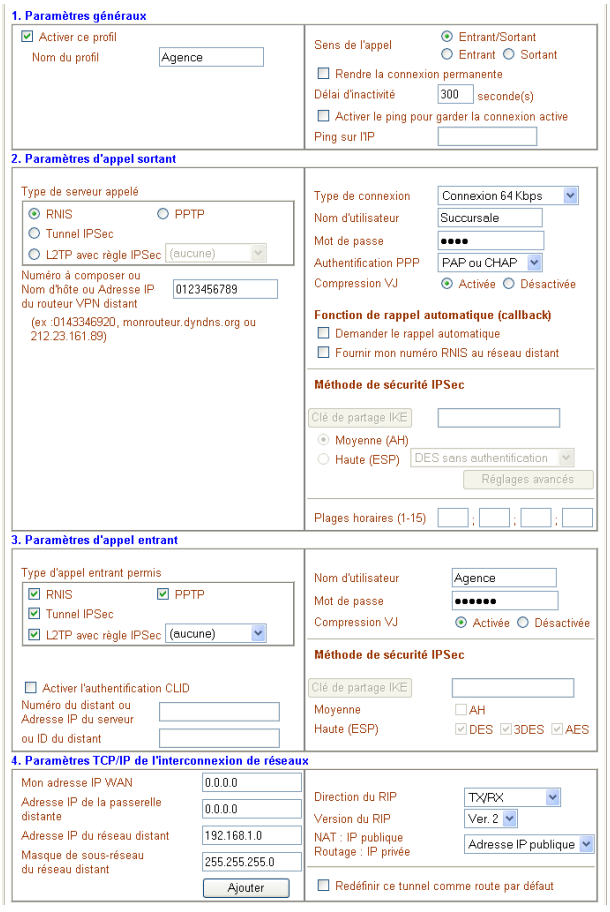
1. Dans la rubrique **Adresse IP du réseau distant**, entrez l'adresse IP du réseau avec lequel vous désirez établir une connexion.
2. Saisissez ensuite le masque de sous-réseau correspondant.
3. Sélectionnez la direction RIP :
   - **TX/RX** : Transmission/Réception : les informations RIP sont non seulement transmises vers le routeur distant mais aussi reçues ;
   - **TX** : Transmission seulement : les informations RIP sont transmises vers le routeur distant ;
   - **RX** : Réception seulement : les informations RIP sont reçues du routeur distant.

   *Remarque : le VPN Booster gère le RIP (**P**rotocole d'**I**nformation de **R**outage). Le RIP permet d'échanger les tables de routage sur les différents sites de façon dynamique. Pour visualiser les routes, dans le menu **Diagnostics**, cliquez sur **Table de routage**.*

Configuration sur le Site A, celui de l'Agence principale :

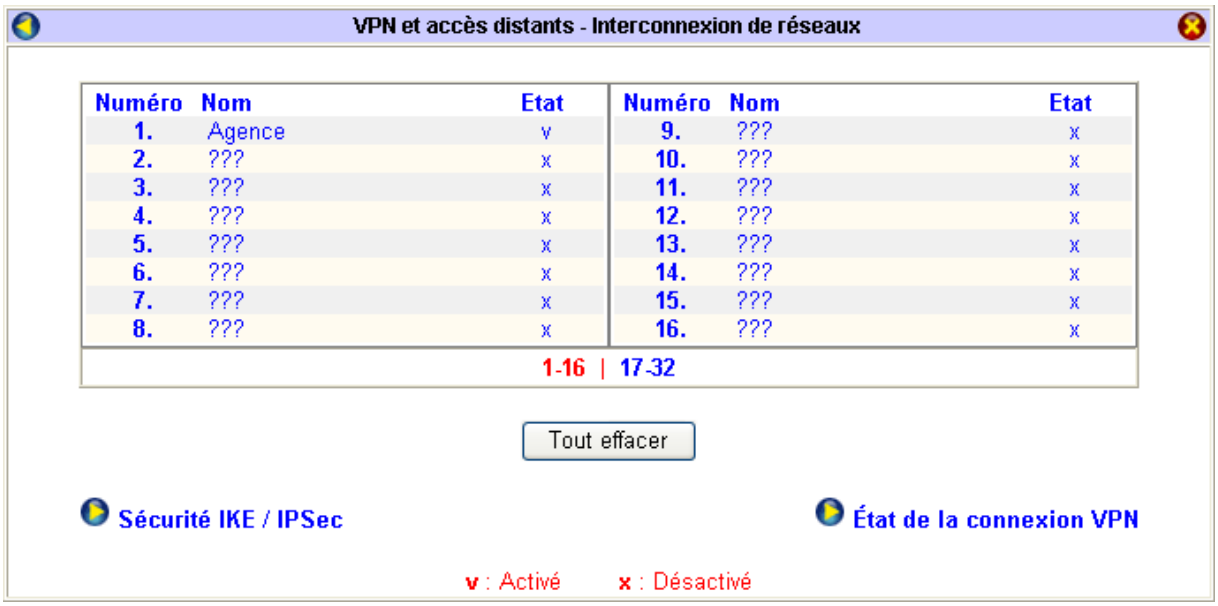


Configuration sur le Site B, celui de la Succursale :



4. Cliquez ensuite sur **OK** pour que les paramètres de votre interconnexion soient pris en compte. Une fois ces paramètres enregistrés, le profil créé est ajouté. Dans la colonne **Etat**, « v » signifie que le profil est activé.

Configuration sur le Site B, celui de la Succursale :



Remarques :

- Vous pouvez à tout moment modifier la configuration des profils créés. Pour cela, dans la colonne **Numéro**, sélectionnez le profil que vous voulez modifier. **Attention :** n'oubliez pas de bien transmettre les nouveaux paramètres à votre correspondant. Si ces changements ne sont pas répercutés chez le site distant, la connexion n'aura pas lieu.
- Vous avez la possibilité de supprimer chacun des profils, un par un, ou de supprimer la totalité des profils en une seule manipulation.
  - ✓ Si vous désirez supprimer un seul profil, dans la colonne **Numéro**, sélectionnez le profil que vous désirez supprimer. Dans la page de configuration du profil, cliquez sur **Effacer**. Une fenêtre de confirmation apparaît. Cliquez alors sur **OK**. Ce profil est supprimé.
  - ✓ Si vous souhaitez supprimer la totalité des vos profils, cliquez sur le bouton **Tout effacer**. Dans la fenêtre de confirmation, cliquez sur **OK**. Tous les profils sont alors supprimés.

Configuration du VPN

Le VPN (***V**irtual **P**rivate **N**etwork*) est une liaison sécurisée entre 2 parties via un réseau public, en général Internet. Il vous permet d'envoyer et de partager des données ou des ressources entre des sites distants.

Les réseaux privés virtuels (VPN) permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Grâce à un principe de tunnel (tunnelling) dont chaque extrémité est identifiée, les données transitent après avoir été chiffrées. C'est la méthode utilisée pour faire transiter des informations privées sur un réseau public. Cette technique assure donc l'authentification des 2 parties, l'intégrité des données et le chiffrage de celles-ci.

Pour communiquer au travers du VPN, plusieurs protocoles peuvent être utilisés : le PPTP (***P**oint to **P**oint **T**unneling **P**rotocol*), le protocole L2TP (***L**ayer **2** **T**unneling **P**rotocol*) et enfin le protocole IPSec.

Il existe deux modes de VPN distincts :

- le **Mode Tunnel** : il crée des tunnels en encapsulant chaque trame dans une enveloppe qui protège tous les champs de la trame. Il est utilisé entre 2 équipements gérant l'interconnexion (exemple : la connexion VPN entre deux routeurs ou passerelles). Les données peuvent être chiffrées (mode ESP) ou non (mode AH).
- le **Mode Transport** : il protège le contenu d'une trame IP en ignorant l'en-tête. Ce mode est généralement utilisé entre deux équipements dont au moins un de type terminal (exemple : la connexion VPN d'un utilisateur isolé 'SoHo' vers une passerelle ou un routeur).

En fonction du mode VPN choisi et du protocole de connexion sélectionné, différentes configurations sont possibles. Tout d'abord, avant que la connexion VPN ne puisse s'établir, il est nécessaire que les administrateurs des 2 sites distants s'échangent leurs paramètres de connexion (nom d'utilisateur, mot de passe, nom d'hôte ou adresse IP du serveur, voire clé IPSec…).

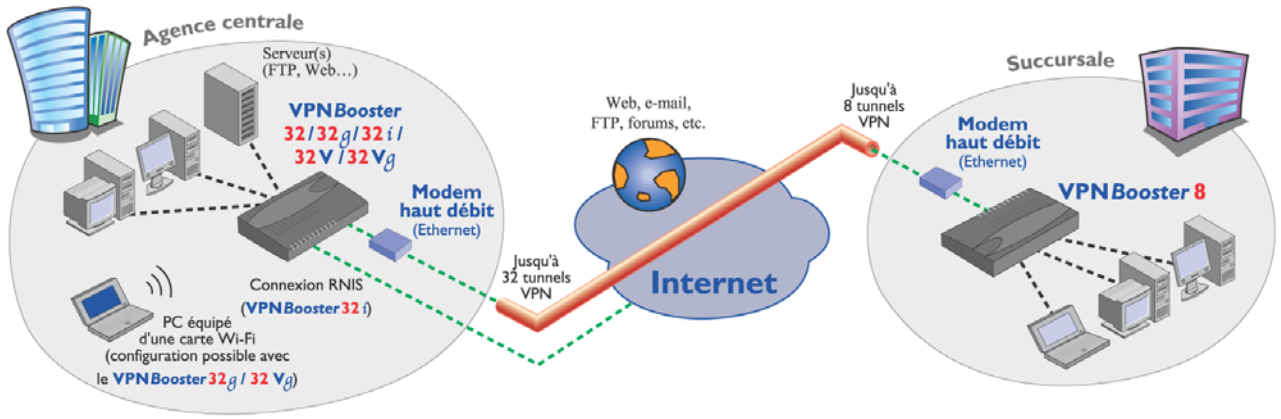
Préalable à l'établissement d'une connexion VPN : Paramétrage de la connexion Internet

⚠ *Très important : Avant la création de votre connexion VPN, vous devez préalablement avoir configuré et lancé votre connexion Internet. Reportez-vous pour cela au chapitre « Accès à Internet » page 79.*

*Attention : si vous utilisez une connexion Internet via RNIS (VPN Booster 32 i), avant de saisir vos paramètres de connexion, vérifiez que votre ligne RNIS est bien activée. Pour cela, dans la section **Configuration Elémentaire**, cliquez sur **RNIS**. Par défaut, cette ligne est activée. Si ce n'est plus le cas, sélectionnez **Activée**, puis cliquez sur **OK** afin que ce paramètre soit pris en compte.*

Configuration d'un VPN entre deux routeurs VPN Booster (mode Tunnel)

La figure suivante schématise une connexion VPN entre 2 sites d'une société :



Selon le protocole attribué à votre connexion VPN, les paramètres à renseigner ne sont pas obligatoirement les mêmes. Voici donc les paramètres que vous devez connaître selon la configuration que vous avez choisie. Vérifiez lors du paramétrage de votre connexion que vous avez bien en votre possession tous les éléments en fonction des exemples ci-dessous.

Configuration 1 : Connexion via PPTP ou L2TP (sans règle IPSec)

	Routeur 1	**Routeur 2**
Nom du réseau	Agence principale	Succursale
Adresse IP du routeur	192.168.1.1	192.168.3.1
Adresse IP du réseau	192.168.1.0	192.168.3.0
Nom d'utilisateur	VPN1	VPN2
Mot de passe	VPN1	VPN2
IP Internet	81.56.xx.xx	IP dynamique
Nom de domaine	vpn1.dyndns.org	vpn2.dyndns.org
IP assignée pour les appels	192.168.1.200	192.168.3.200

Configuration 2 : Connexion via L2TP avec règle IPSec (recommandée ou obligatoire)

	Routeur 1	**Routeur 2**
Nom du réseau	Agence principale	Succursale
Adresse IP du routeur	192.168.1.1	192.168.3.1
Adresse IP du réseau	192.168.1.0	192.168.3.0
Nom d'utilisateur	VPN1	VPN2
Mot de passe	VPN1	VPN2
IP Internet	81.56.xx.xx	IP dynamique
Nom de domaine	vpn1.dyndns.org	vpn2.dyndns.org
Clé IKE sortante	ABCABCABCABC	DEFDEF
Clé IKE entrante	DEFDEF	ABCABCABCABC
IP assignée pour les appels	192.168.1.200	192.168.3.200

Configuration 3 : Connexion via Tunnel IPSec

	Routeur 1	**Routeur 2**
Nom du réseau	Agence principale	Succursale
Adresse IP du routeur	192.168.1.1	192.168.3.1
Adresse IP du réseau	192.168.1.0	192.168.3.0
IP Internet	81.56.xx.xx	IP dynamique
Nom de domaine	vpn1.dyndns.org	vpn2.dyndns.org
Clé IKE sortante	ABCABCABCABC	DEFDEF
Clé IKE entrante	DEFDEF	ABCABCABCABC

Etape 1 : Configuration de l'appel entrant

***Attention** : la configuration de l'appel entrant est nécessaire uniquement pour les protocoles PPTP, L2TP ou L2TP IPSec.*

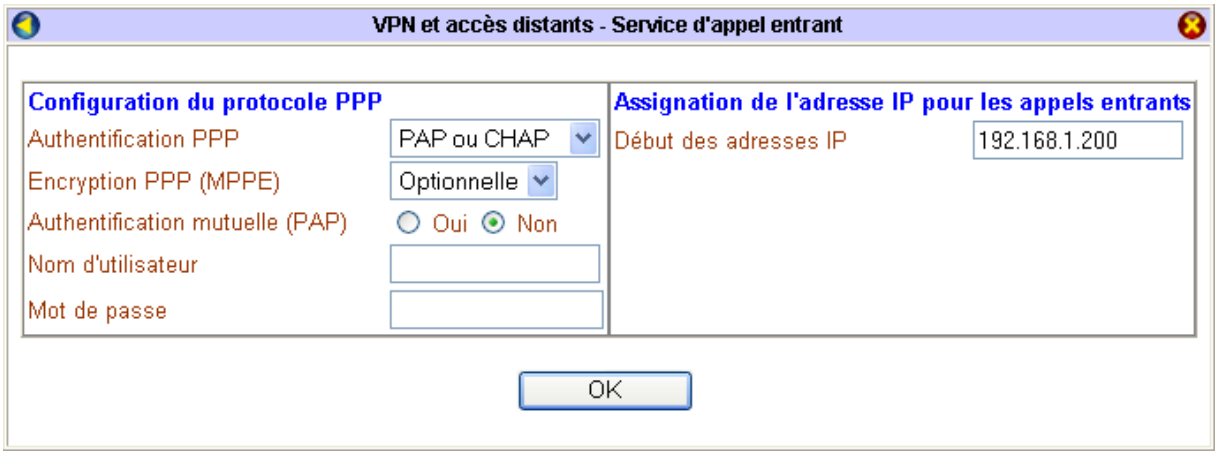
Afin que deux réseaux puissent s'interconnecter, vous devez activer le service d'appel entrant. Pour cela, il vous suffit d'activer un compte d'appel entrant. L'appel entrant vous permet de configurer le routeur afin qu'un équipement distant (passerelle, autre routeur...) puisse se connecter à votre réseau local en toute sécurité. Cette activation doit être effective pour chaque routeur qui souhaite recevoir des appels.

1. Dans le menu **Réglages Avancés**, cliquez sur **VPN et accès distants**, puis sur **Service d'appel entrant**.
2. Dans la rubrique **Début des adresses IP**, indiquez la première adresse IP à assigner aux équipements distants.

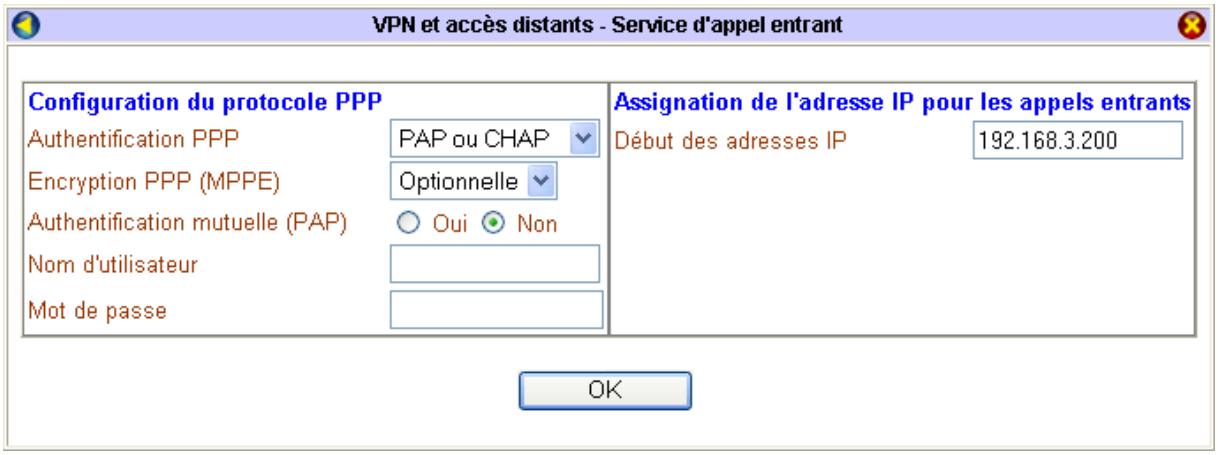
   Attention :

   - *Les équipements distants peuvent également spécifier leurs adresses IP. Dans ce cas, mettez « 0.0.0.0 » dans cette rubrique.*
   - *Qu'elles soient fixes ou allouées dynamiquement, les adresses IP des équipements distants doivent être disponibles et compatibles avec le plan d'adressage du réseau local.*

Paramétrage du routeur situé dans l'Agence principale :



Paramétrage du routeur situé dans la Succursale :



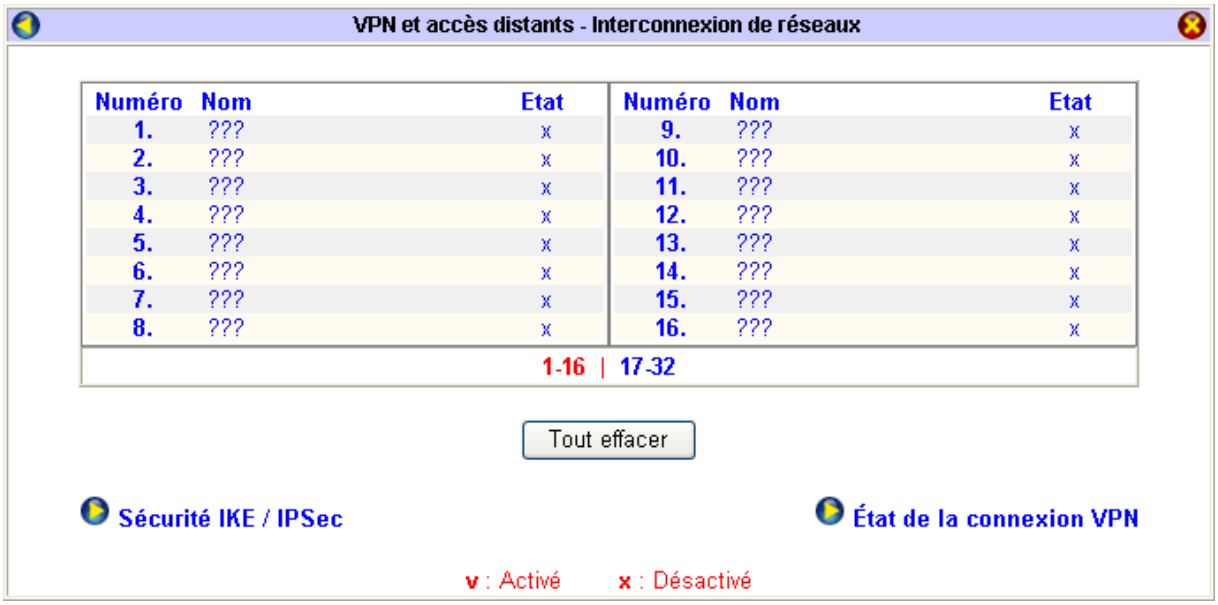
3. Cliquez sur **OK** pour valider les informations.
4. Pour chacun des routeurs, cliquez ensuite sur **Interconnexion de réseaux** afin d'établir votre fiche d'interconnexion et de créer le lien VPN entre les deux routeurs.

Etape 2 : Création du profil VPN

Pour relier les deux réseaux privés (les deux routeurs), vous devez désormais créer sur chaque site un profil d'interconnexion afin de saisir les caractéristiques de la connexion VPN avec le réseau distant.

Remarque : pour saisir le profil d'interconnexion, vous devez avoir en votre possession certains paramètres transmis par l'administrateur du routeur distant (nom d'utilisateur, mot de passe, IP Internet ou nom de domaine,…).

1. Dans le menu **Réglages Avancés**, cliquez sur **VPN et accès distants**, puis sur **Interconnexion de réseaux**. L'écran suivant apparaît.



2. Cliquez sur un numéro dans la colonne **Numéro**.

   Remarques :

   - *Si un profil n'a pas encore été paramétré, son nom apparaît sous la forme* ***???****, indiquant qu'il est disponible.*
   - *Le VPN Booster 8 vous permet d'établir jusqu'à 8 connexions VPN simultanément. Vous avez la possibilité d'établir 32 connexions si vous possédez un VPN Booster de la Série 32.*

3. Pour chaque profil d'interconnexion, renseignez les rubriques nécessaires. Vous pouvez vous référer aux captures d'écran suivantes. Procédez comme suit :

   Remarque : pour saisir le profil d'interconnexion, vous devez avoir en votre possession certains paramètres transmis par l'administrateur du site distant.

Partie 1 : Paramètres généraux

1. Pour activer le profil, sélectionnez l'option **Activer ce profil**.
2. Dans la rubrique **Nom du profil**, indiquez un nom qui soit clair pour vous (10 caractères maximum), correspondant à votre connexion VPN.
3. En face de l'intitulé **Sens de l'appel**, sélectionnez la direction des appels pour ce profil :
   - **Entrant/sortant** : l'interconnexion peut s'établir aussi bien sur appels entrants que sur appels sortants.
   - **Entrant** : l'interconnexion ne peut s'établir que sur appels entrants.
   - **Sortant** : l'interconnexion ne peut s'établir que sur appels sortants.
4. Si vous souhaitez bénéficier d'une connexion permanente, cochez la case correspondante. Dans ce cas, après une coupure, le routeur se reconnectera automatiquement.
5. Dans la rubrique **Délai d'inactivité**, entrez le nombre de secondes d'inactivité au terme duquel la connexion VPN sera automatiquement interrompue si aucun ordinateur du réseau local ne l'utilise.

   Remarque : si vous saisissez « 0 », vous pourrez bénéficier d'une connexion permanente. En revanche, après une coupure, le rétablissement de la connexion ne sera pas effectif.
6. Dans la rubrique **Ping sur l'IP**, saisissez l'adresse IP du routeur distant. C'est notamment indispensable quand la connexion est paramétrée avec une clé IPSec. En cas de coupure VPN par le distant, cette option permet de relancer la session VPN.

Partie 2 : Paramètres d'appel sortant

Dans cette partie, vous devez saisir les paramètres fournis par l'administrateur du réseau distant. Procédez comme suit :

1. Dans la partie **Type de serveur appelé**, sélectionnez le protocole utilisé pour établir la connexion VPN.
   - Si vous ne désirez pas ajouter le protocole IPSec au tunnel VPN, sélectionnez **PPTP** ou **L2TP (aucune règle IPSec)**.
   - Si vous désirez ajouter le protocole IPSec au tunnel VPN, sélectionnez **L2TP avec règle IPSec (recommandée ou obligatoire)** ou **Tunnel IPSec**.

     *Remarque : dans le cas où vous choisissez d'employer le protocole IPSec, sélectionnez ensuite votre niveau de sécurité dans la partie **Méthode de sécurité IPSec**. Différentes options sont proposées :*

Niveau de sécurité	Signification
Moyenne (AH)	l'en-tête des paquets IP est authentifié
Haute (ESP)	les données sont chiffrées et l'en-tête peut être authentifié selon le chiffrement DES ou AES sélectionné :
- DES sans authentification*	- les données sont chiffrées mais l'en-tête des paquets IP n'est pas authentifié
- DES avec authentification*	- les données sont chiffrées et l'en-tête des paquets IP est authentifié
- 3DES sans authentification*	- les données sont chiffrées mais l'en-tête des paquets IP n'est pas authentifié
- 3DES avec authentification*	- les données sont chiffrées et l'en-tête des paquets IP est authentifié
- AES sans authentification	- les données sont chiffrées mais l'en-tête des paquets IP n'est pas authentifié
- AES avec authentification	- les données sont chiffrées et l'en-tête des paquets IP est authentifié

* Méthodes de sécurité bénéficiant d'un chiffrement matériel (Série VPN Booster 32)

2. Dans la rubrique **Numéro à composer ou Nom d'hôte ou Adresse IP du routeur VPN distant**, saisissez le nom de domaine du site distant ou son adresse IP Internet fournie par l'administrateur.

3. Dans les rubriques **Nom d'utilisateur** et **Mot de passe**, entrez le nom (49 caractères maximum) et le mot de passe (24 caractères maximum) qui vous identifient sur le site distant.

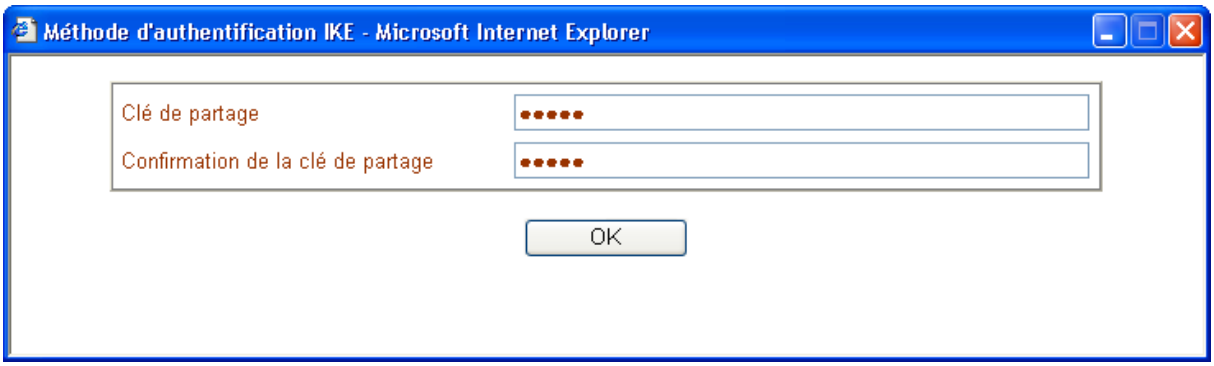
   *Remarque : si vous sélectionnez **Tunnel IPSec**, vous n'avez pas besoin de saisir un nom d'utilisateur ou un mot de passe. Ces identifiants ne sont pas pris en compte.*

4. Dans la rubrique **Authentification PPP**, sélectionnez **PAP ou CHAP** ou **PAP seulement**.

   Remarques :

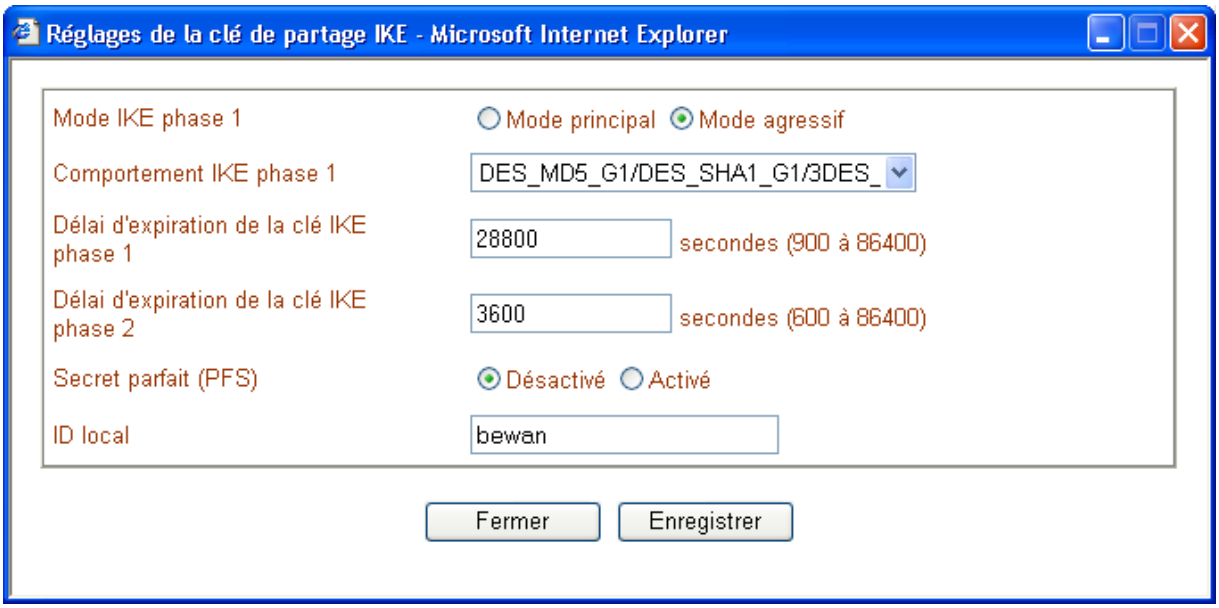
   - *Si vous sélectionnez **PAP ou CHAP**, l'authentification pourra s'effectuer dans tous les cas.*
   - *Les protocoles d'authentification PPP acceptés dépendent du paramétrage du site distant. En cas de doute, contactez son administrateur.*

5. Si vous avez sélectionné **L2TP avec règle IPSec** (recommandée ou obligatoire) ou **Tunnel IPSec** dans la partie **Type de serveur appelé**, vous pouvez attribuer une clé IPSec à ce profil en particulier. Le bouton **Clé de partage IKE** devient alors accessible. Saisissez-la, puis cliquez sur **OK**.



6. Si vous désirez gérer des heures de connexion en mode sortant, dans les rubriques des plages horaires, saisissez les numéros des plages horaires que vous souhaitez assigner à votre connexion VPN.

7. Le bouton **Réglages avancés** vous permet des paramétrer des options supplémentaires. Cliquez sur **Enregistrer** pour valider les informations.



- En activant le **Mode agressif**, vous avez la possibilité de saisir un **ID local** (47 caractères maximum). La définition d'un ID est utile si vous n'avez pas d'adresse IP fixe car elle permet précisément de remplacer l'authentification sur adresse IP tout en permettant l'utilisation d'une clé IKE spécifique à ce profil.
- Il est conseillé de conserver les délais d'expiration par défaut sauf si l'équipement distant possède des paramètres différents. Dans ce cas, les paramètres doivent être identiques des deux côtés.
- Le mode PFS permet une meilleure compatibilité avec certains serveurs VPN (serveurs Linux par exemple).

Partie 3 : Paramètres d'appel entrant

Dans cette partie, vous devez saisir les paramètres concernant le réseau distant.

Remarque : renseignez-vous auprès de l'administrateur du réseau distant afin de connaître ces paramètres et de permettre la compatibilité.

Procédez comme suit :

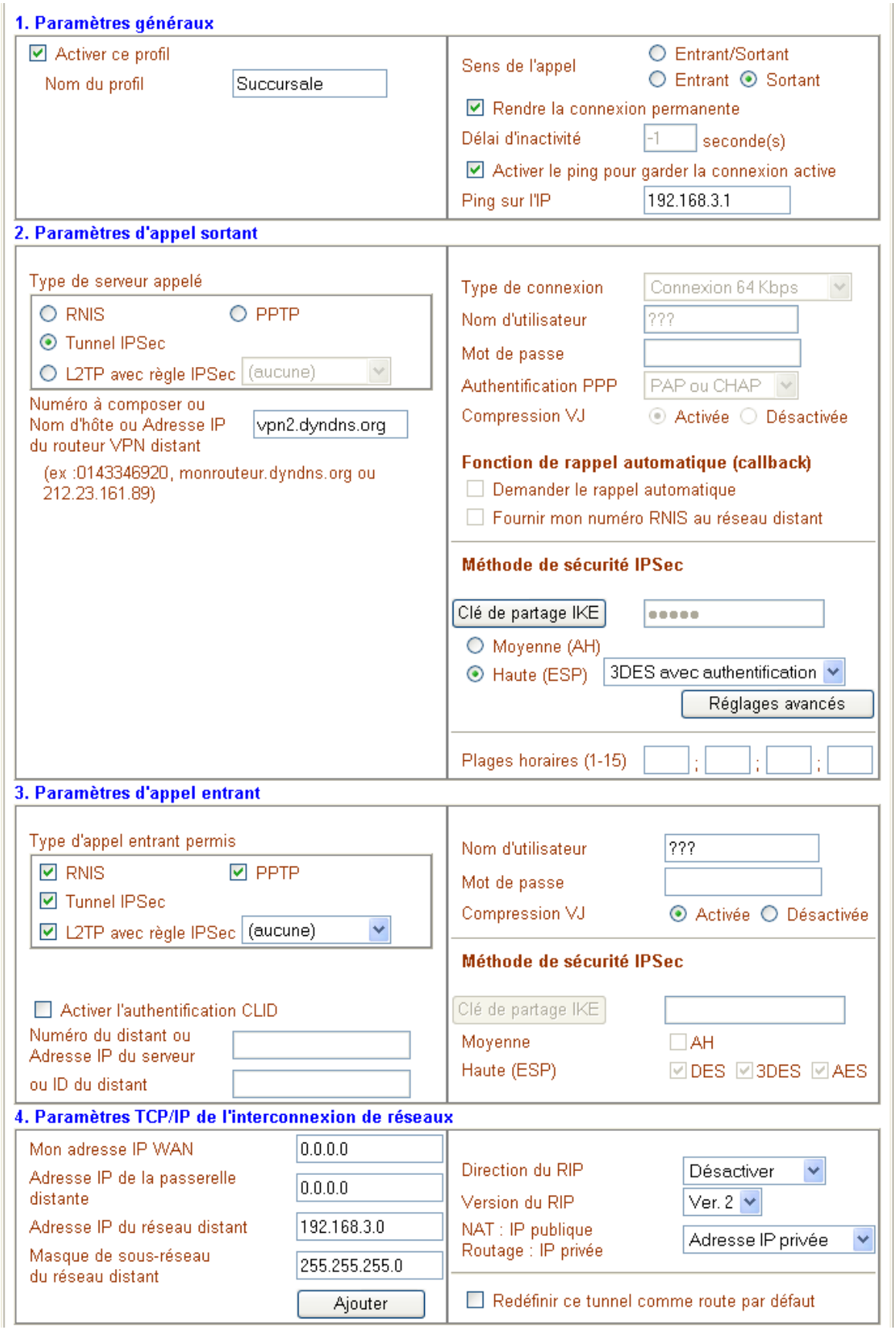
1. Dans la rubrique **Type d'appel entrant permis**, sélectionnez le type de protocole que vous allez accepter pour la connexion VPN.
2. Si, vous avez sélectionné le protocole Tunnel IPSec ou affecté une règle IPSec (recommandée ou obligatoire) au protocole L2TP, vous devez impérativement saisir une clé IPSec.
   - Si vous connaissez l'adresse IP fixe du serveur distant ou son ID (47 caractères maximum, configuré dans les **Paramètres d'appel sortant** du routeur distant), vous pouvez cocher **Activer l'authentification** (ou **Activer l'authentification CLID** si vous possédez le VPN Booster 32 i). Saisissez alors le paramètre du distant, puis entrez votre clé IPSec pour ce profil particulier en cliquant sur le bouton **Clé de partage IKE** qui est devenu accessible. Cette clé, une fois confirmée, ne sera active que pour ce profil.
   - Si vous ne connaissez pas les paramètres du distant, vous devez saisir une clé IPSec globale. Pour paramétrer cette clé, reportez-vous à la section « Etape 3 (facultative) : Paramétrage du protocole IPSec » page 108.
3. Dans les rubriques **Nom d'utilisateur** et **Mot de passe**, entrez un nom et un mot de passe (11 caractères maximum pour chacune des rubriques).

Partie 4 : Paramètres TCP/IP de l'interconnexion de réseaux

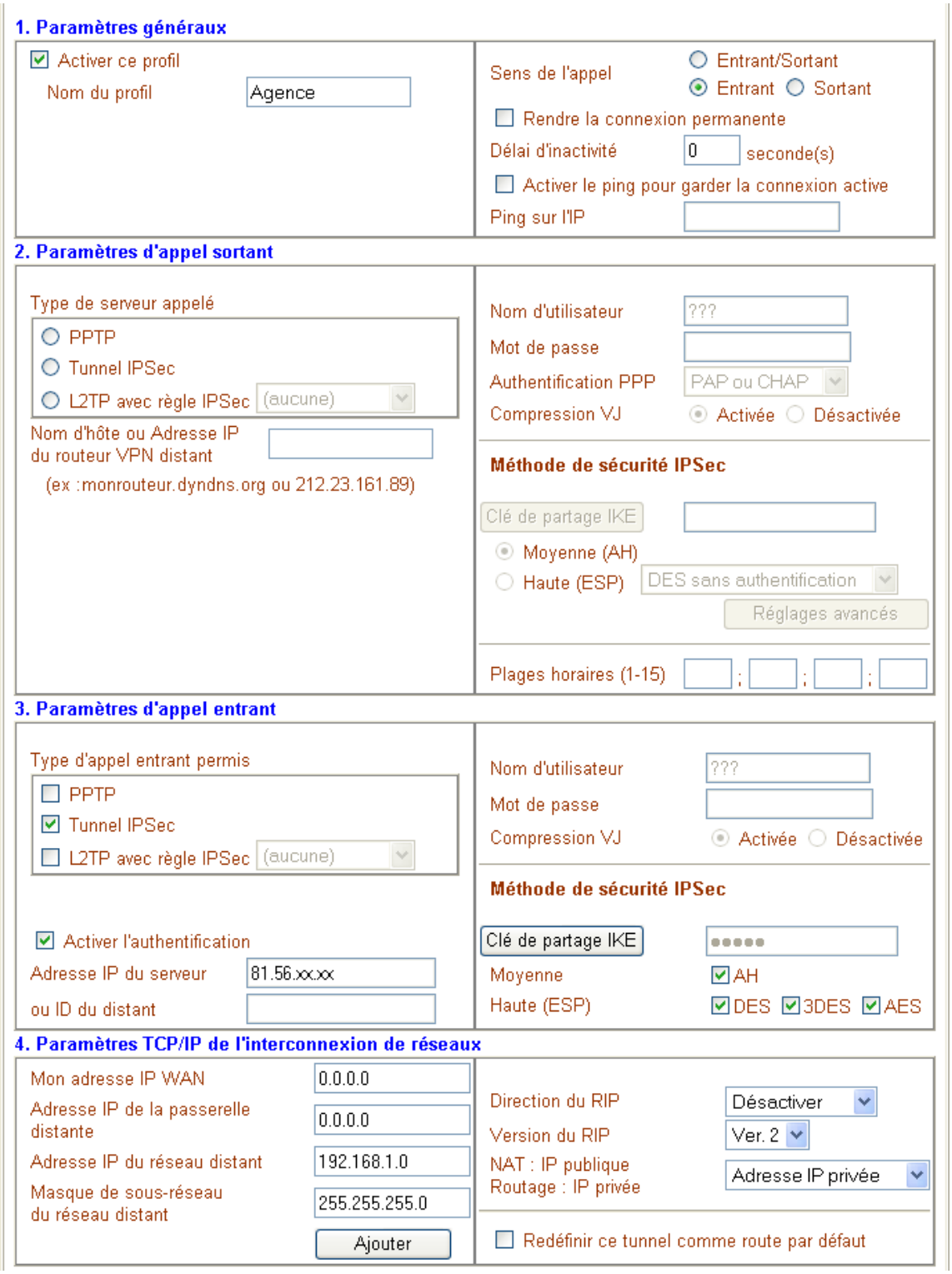
1. Dans la rubrique **Adresse IP du réseau distant**, entrez l'adresse IP du réseau avec lequel vous désirez établir une connexion.
2. Saisissez ensuite le masque de sous-réseau correspondant.
3. Sélectionnez la direction RIP :
   - **TX/RX** : Transmission/Réception : les informations RIP sont non seulement transmises vers le routeur distant mais aussi reçues ;
   - **TX** : Transmission seulement : les informations RIP sont transmises vers le routeur distant ;
   - **RX** : Réception seulement : les informations RIP sont reçues du routeur distant.

   *Remarque : le VPN Booster gère le RIP (**P**rotocole d'**I**nformation de **R**outage). Le RIP permet d'échanger les tables de routage sur les différents sites de façon dynamique. Pour visualiser les routes, dans le menu **Diagnostics**, cliquez sur **Table de routage**.*

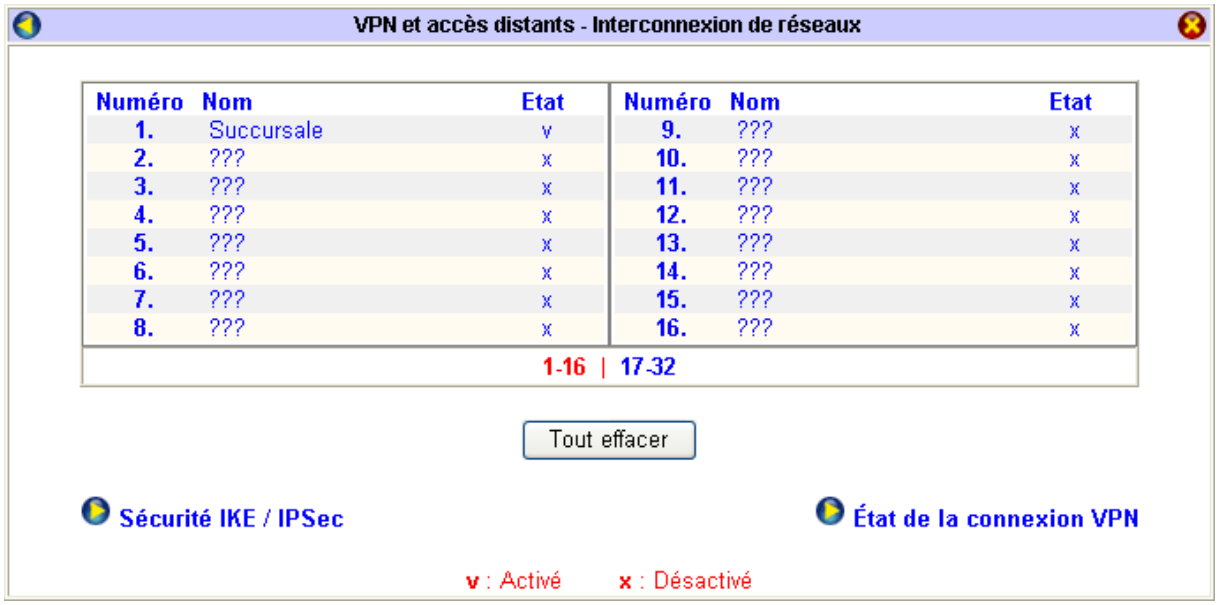
Paramétrage du routeur situé dans l'Agence principale (VPN Booster 32 i) :



Paramétrage du routeur situé dans la Succursale (VPN Booster 8) :



4. Cliquez ensuite sur **OK** pour que les paramètres de votre interconnexion soient pris en compte. Une fois ces paramètres enregistrés, le profil créé est ajouté. Dans la colonne **Etat**, « v » signifie que le profil est activé.



5. Vous venez de paramétrer une connexion VPN en Tunnel IPSec entre les deux VPN Booster. Cliquez sur **Etat de la connexion VPN** afin d'établir le lien VPN. Reportez-vous à la section « Etape 4 : Etat de la connexion VPN » page 109.

   Remarque : comme nous avons pu le constater lors de la description des rubriques composant votre fiche d'interconnexion, vous pouvez attribuer une clé IPSec par profil afin de sécuriser chaque connexion VPN. Néanmoins, si par exemple vous désirez simplifier la gestion de vos connexions VPN, vous avez également la possibilité d'attribuer une clé IPSec globale pour toutes vos connexions VPN entrantes. Pour paramétrer cette clé unique, cliquez sur ***Sécurité IKE / IPSec****. Reportez-vous à la section suivante « Etape 3 (facultative) : Paramétrage du protocole IPSec ».*

Etape 3 (facultative) : Paramétrage du protocole IPSec

Introduction

Le protocole IPSec vise à sécuriser les échanges au niveau de la couche réseau. L'utilisation de ce protocole permet :

- la gestion et l'échange de clés entre routeurs,
- l'authentification des paquets IP (méthode de sécurité AH : Authentication Header),
- le chiffrement des paquets IP (méthode de sécurité ESP : Encapsulating Security Payload).

Ce paramétrage est obligatoire si, dans votre fiche d'interconnexion, vous avez sélectionné soit Tunnel IPSec, soit le protocole L2TP avec règle IPSec recommandée ou obligatoire.

Ces deux protocoles (Tunnel IPSec et L2TP avec règle IPSec) nécessitent l'emploi d'une clé d'encryption (IKE : ***I**nternet **K**ey **E**xchange*) et le choix du niveau de sécurité (AH ou ESP).

Attention : la clé d'encryption et le niveau de sécurité doivent alors correspondre sur les deux routeurs qui souhaitent s'interconnecter.

Configuration IPSec

Pour réaliser le paramétrage IPSec, procédez comme suit :

1. Dans le menu **Réglages Avancés**, cliquez sur **VPN et accès distants**, puis sur **Sécurité IKE / IPSec** afin de saisir les paramètres de sécurité.

   Remarque : vous devez avoir en votre possession les paramètres de sécurité communiqués par l'administrateur du site distant (clé de partage, niveau de sécurité DES, 3DES ou AES).

2. Dans la rubrique **Clé de partage**, saisissez le code transmis par l'administrateur distant, puis tapez-le une seconde fois.

3. Sélectionnez ensuite le niveau de sécurité. Cochez en fonction du niveau de sécurité IPSec sélectionné dans la fiche d'interconnexion. Voici un récapitulatif des correspondances qui peuvent exister entre deux routeurs :

Fiche d'interconnexion : Différentes possibilités IPSec	**Paramétrage IPSec : Paramètres à sélectionner**
L2TP (recommandée ou obligatoire) / Tunnel IPSec : ➔ Moyenne (AH)	*Moyenne (AH)*
L2TP (recommandée ou obligatoire) / Tunnel IPSec : ➔ Haute (DES sans authentification)	*Haute (ESP) : DES* ou *Haute (ESP) : DES et 3DES*
L2TP (recommandée ou obligatoire) / Tunnel IPSec : ➔ Haute (DES avec authentification)	*Moyenne (AH)* **et** *Haute (ESP) : DES* ou *Haute (ESP) : DES et 3DES*
L2TP (recommandée ou obligatoire) / Tunnel IPSec : ➔ Haute (3DES sans authentification)	*Haute (ESP) : 3DES* ou *Haute (ESP) : DES et 3DES*
L2TP (recommandée ou obligatoire) / Tunnel IPSec : ➔ Haute (3DES avec authentification)	*Moyenne (AH)* **et** *Haute (ESP) : 3DES* ou *Haute (ESP) : DES et 3DES*
L2TP (recommandée ou obligatoire) / Tunnel IPSec : ➔ Haute (AES sans authentification)	*Haute (ESP) : AES* ou *Haute (ESP) : DES, 3DES et AES*
L2TP (recommandée ou obligatoire) / Tunnel IPSec : ➔ Haute (AES avec authentification)	*Moyenne (AH)* **et** *Haute (ESP) : AES* ou *Haute (ESP) : DES, 3DES et AES*

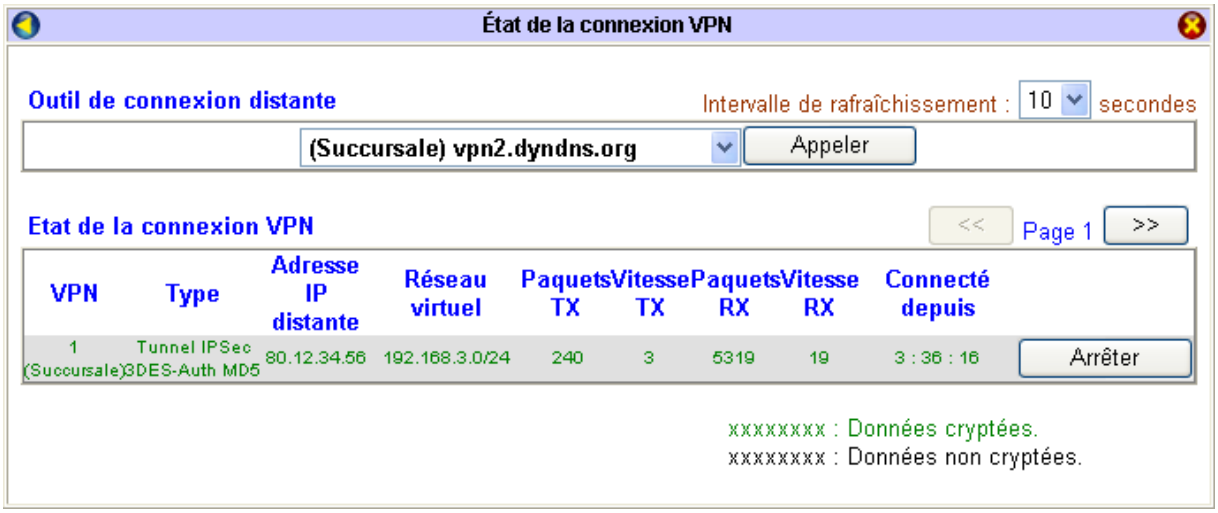
   Exemple de non connexion : si, dans sa fiche d'interconnexion, le routeur 1 a sélectionné le protocole L2TP avec règle IPSec recommandée et un niveau de sécurité Moyenne (AH), le routeur 2, dans la partie Appel entrant de son paramétrage IPSec, ne pourra pas sélectionner Haute (ESP). La connexion ne pourra pas s'établir.

4. Cliquez sur **OK** afin de valider les paramètres de connexion. Cliquez ensuite sur **Etat de la connexion VPN** afin de constater le bon fonctionnement du lien VPN.

Etape 4 : Etat de la connexion VPN

Après avoir établi votre fiche d'interconnexion, vérifiez désormais que votre lien VPN est bien établi.

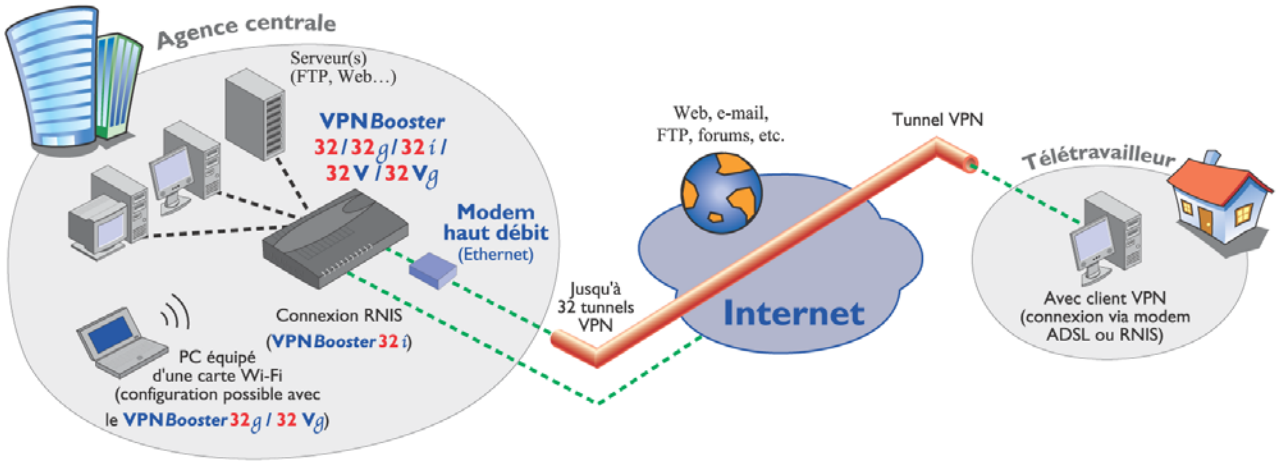
1. Cliquez sur **Etat de la connexion VPN**.
2. Dans la liste, sélectionnez le lien VPN avec lequel vous désirez établir la connexion, puis cliquez sur **Appeler**. Les paramètres de la connexion doivent alors apparaître dans **Etat de la connexion VPN**.



3. Pour interrompre la connexion VPN, cliquez sur **Arrêter**.

Configuration d'un VPN entre un routeur VPN Booster et un utilisateur isolé (mode Transport)

La figure suivante schématise une connexion VPN entre un hôte distant (par exemple, un télé-travailleur) et un routeur (situé au siège de sa société) avec lequel il souhaite établir une connexion VPN :



Voici à la fois les caractéristiques de l'hôte distant et celles du routeur qu'il faut prendre en compte :

Paramètres de connexion du routeur :

	Routeur
Adresse IP du routeur	192.168.1.1
Adresse IP du réseau	192.168.1.0
Nom d'utilisateur	télétravailleur
Mot de passe	bewan
Adresse IP WAN (Internet)	81.56.xx.xx*
IP assignée pour les appels	192.168.1.200

* Adresse IP indiquée dans la partie **Etat WAN** de **Etat LAN / WAN** (VPN Booster 8 / 32 / 32 g / 32 V / 32 Vg) ou **Etat de la ligne RNIS / LAN / WAN** (VPN Booster 32 i)
Cette adresse peut aussi être fixe ou remplacée par un nom de domaine dynamique.

Paramètres de connexion de l'hôte distant :

	Hôte (utilisateur distant)
Nom de connexion	Connexion VPN
Nom d'utilisateur	télétravailleur
Mot de passe	bewan
IP du routeur VPN distant	80.12.34.56
Adresse IP WAN (Internet)	IP dynamique *

* ou Adresse IP fixe. Dans ce cas, afin de sécuriser la connexion VPN, dans le paramétrage du compte d'appel entrant sur le routeur, il vous est possible de cocher **Activer l'authentification** (ou **Activer l'authentification CLID**) si vous possédez le VPN Booster 32 i). Indiquez ensuite l'adresse IP dans la rubrique correspondante.

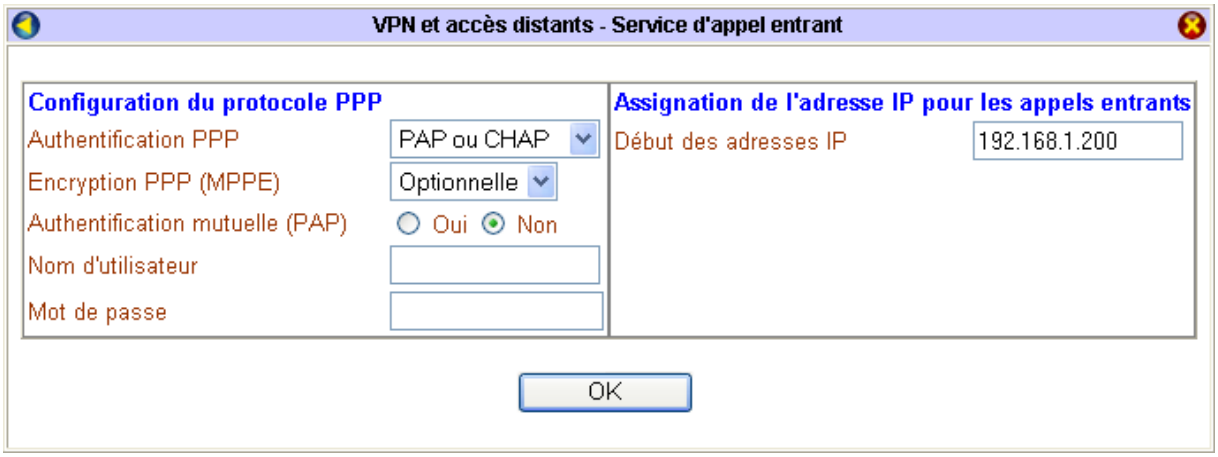
Etape 1 : Configuration de l'appel entrant sur le routeur

Afin que l'utilisateur distant puisse se connecter au réseau via le routeur, l'administrateur doit au préalable activer le service d'appel entrant. En mode Transport, le routeur est uniquement serveur VPN (connexion à l'initiative de l'hôte VPN distant).

1. Dans le menu **Réglages Avancés**, cliquez sur **VPN et accès distants**, puis sur **Service d'appel entrant**.
2. Dans la rubrique **Début des adresses IP**, indiquez la première adresse IP à assigner aux équipements distants.

   Attention :

   - *Les équipements distants peuvent également spécifier des adresses IP fixes.*
   - *Qu'elles soient fixes ou allouées dynamiquement, les adresses IP des équipements distants doivent être disponibles et compatibles avec le plan d'adressage du réseau local.*



3. Cliquez sur **OK** pour valider les informations.
4. Cliquez ensuite sur **Comptes d'appel entrant** afin d'établir un compte d'appel entrant pour que l'utilisateur distant puisse se connecter au réseau via un lien VPN.

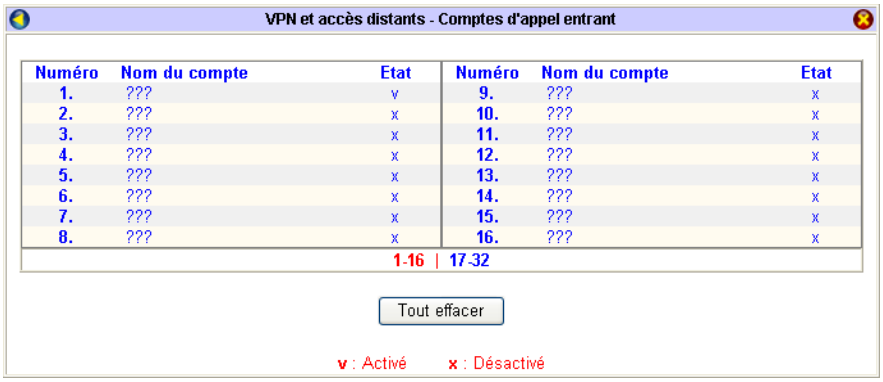
Etape 2 : Paramétrage du profil VPN

Nous indiquons ici les paramétrages à effectuer sur le routeur ainsi que ceux à saisir par l'utilisateur distant.

Remarque : n'oubliez pas de communiquer les paramètres de connexion à votre correspondant. Par exemple, le nom d'utilisateur et le mot de passe doivent être saisis de manière identique des deux côtés de la connexion VPN.

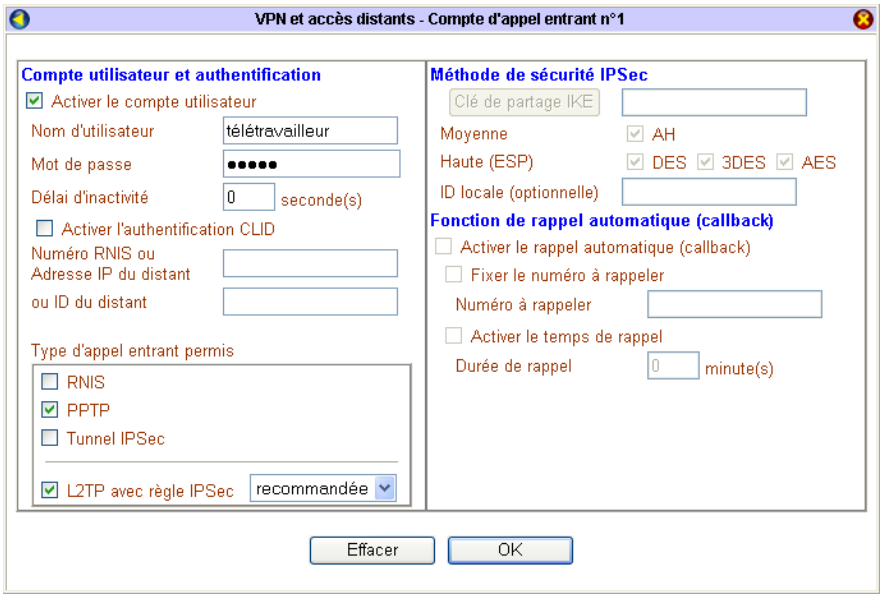
Paramétrage à effectuer sur le routeur

1. Configurez un compte d'appel entrant. Pour paramétrer un compte, cliquez sur un numéro (si le compte n'a pas encore été paramétré, le nom du compte apparaît sous la forme **???**). Le VPN Booster vous permet de gérer jusqu'à 16 comptes d'appel entrant si vous disposez du VPN Booster 8, et jusqu'à 32 comptes si vous possédez un VPN Booster de la série 32.



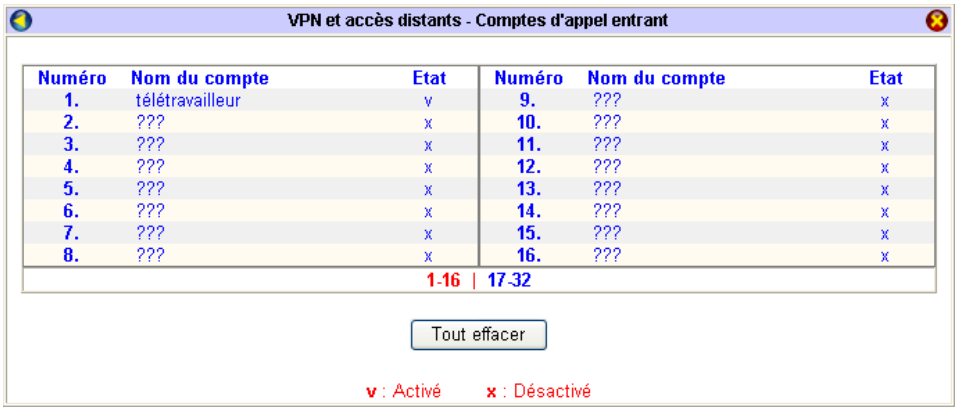
2. Pour activer le compte, cochez **Activer le compte utilisateur**.
   - Entrez un nom et un mot de passe dans les rubriques **Nom d'utilisateur** et **Mot de passe** (16 caractères maximum). Ceux-ci doivent être les mêmes identifiants que ceux saisis par l'hôte distant.
   - Dans la rubrique **Délai d'inactivité**, entrez le nombre de secondes au terme duquel la connexion sera automatiquement interrompue en cas d'inactivité.
   - Dans la partie **Type d'appel entrant permis**, cochez les protocoles que le routeur va autoriser pour ce compte. Le choix du protocole peut s'effectuer selon le système utilisé par l'utilisateur distant. A titre d'exemple, un utilisateur sous Windows 98 ou Me ne pourra réaliser qu'une connexion VPN en PPTP. En effet, les protocoles VPN ne sont pas disponibles sur tous les systèmes Windows (voir « Paramétrage à effectuer chez l'hôte distant » page 114). En revanche, si l'utilisateur distant est sous Windows 2000 ou XP, une connexion VPN sera possible en L2TP (avec ou sans règle IPSec).

     Remarque : si vous suivez notre exemple, vous pouvez en conclure que tous les systèmes peuvent accéder au routeur puisque le protocole minimum (PPTP) est coché.



- Si, vous avez sélectionné le protocole Tunnel IPSec ou affecté une règle IPSec (recommandée ou obligatoire) au protocole L2TP, vous devez impérativement saisir une clé IPSec.
  - ✓ Si vous connaissez l'adresse IP fixe du serveur distant ou si votre client VPN permet la gestion d'un ID, vous pouvez cocher **Activer l'authentification** (ou **Activer l'authentification CLID** si vous possédez le VPN Booster 32 i). Saisissez alors le paramètre du distant, puis entrez votre clé IPSec pour ce profil particulier en cliquant sur le bouton **Clé de partage IKE** qui est devenu accessible. Cette clé, une fois confirmée, ne sera active que pour ce profil.
  - ✓ Si vous ne connaissez pas les paramètres du distant, vous devez saisir une clé IPSec globale. Pour paramétrer cette clé, reportez-vous à l'encadré ci-dessous.

3. Cliquez sur **OK** afin de valider les informations. La configuration du compte d'appel entrant est terminée. Dans la colonne **Etat**, le compte est indiqué *Activé* (« **v** »).

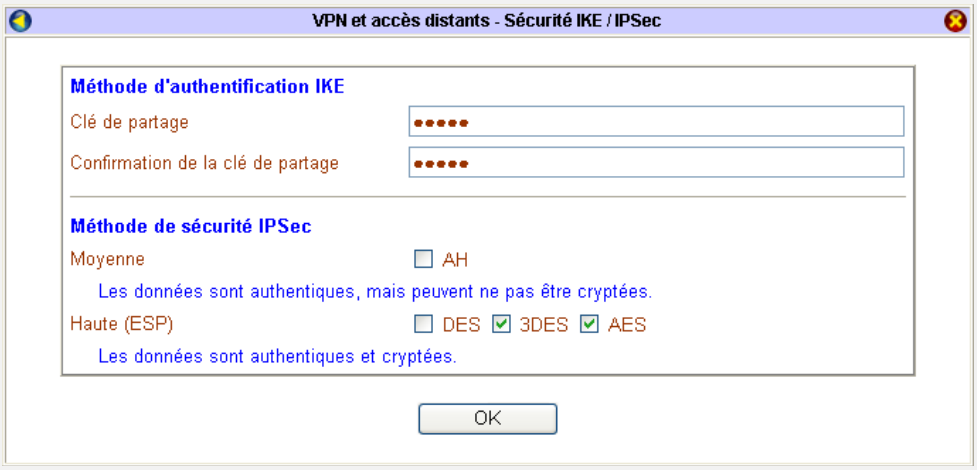


Remarques :

- *Pour que la connexion VPN puisse s'établir, vous devez évidemment au préalable avoir configuré et lancé votre connexion Internet. Reportez-vous pour cela au chapitre « Accès à Internet » page 79.*
- *Le VPN Booster 8 vous permet d'établir jusqu'à 8 connexions VPN simultanément. Vous avez la possibilité d'établir 32 connexions si vous possédez un VPN Booster de la Série 32.*

Comment paramétrer la règle IPSec sur le routeur si vous choisissez le protocole L2TP avec IPSec ?

1. Dans le menu **Réglages Avancés**, cliquez sur **VPN et accès distants**, puis sur **Sécurité IKE / IPSec**.
2. Saisissez la même clé de partage et le même niveau de sécurité que ceux saisis dans le configurateur VPN de l'utilisateur distant.



3. Cliquez sur **OK** pour valider les paramètres.

Paramétrage à effectuer chez l'hôte distant

Comme nous avons pu le voir plus haut, le choix du protocole dépend du système d'exploitation utilisé. Nous allons donc développer différents cas de figure selon l'environnement sur lequel se trouve l'utilisateur isolé.

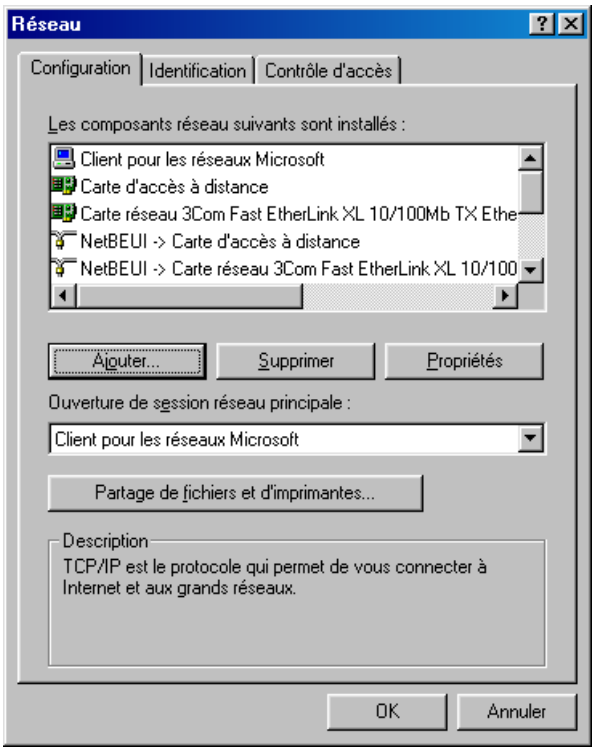
Si la carte réseau Ethernet de l'hôte est activée, son adresse IP ne doit pas être dans le même plan d'adressage que le réseau du routeur VPNBooster distant.

Environnement utilisé par l'hôte distant	*Windows 98 et Me*	*Windows NT*	*Windows 2000 et Windows XP*
Protocoles disponibles	PPTP	PPTP et L2TP	PPTP, L2TP sans ou avec règle IPSec

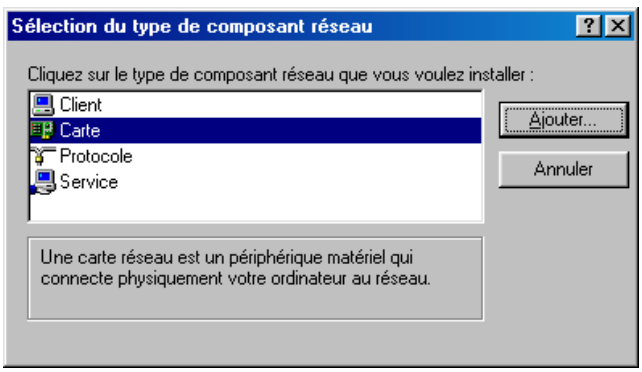
Important : pour que la connexion VPN puisse s'établir avec le routeur, tout comme lui, vous devez avoir une connexion Internet configurée et active (par exemple, via un modem ADSL).

Sous Windows 98/Me

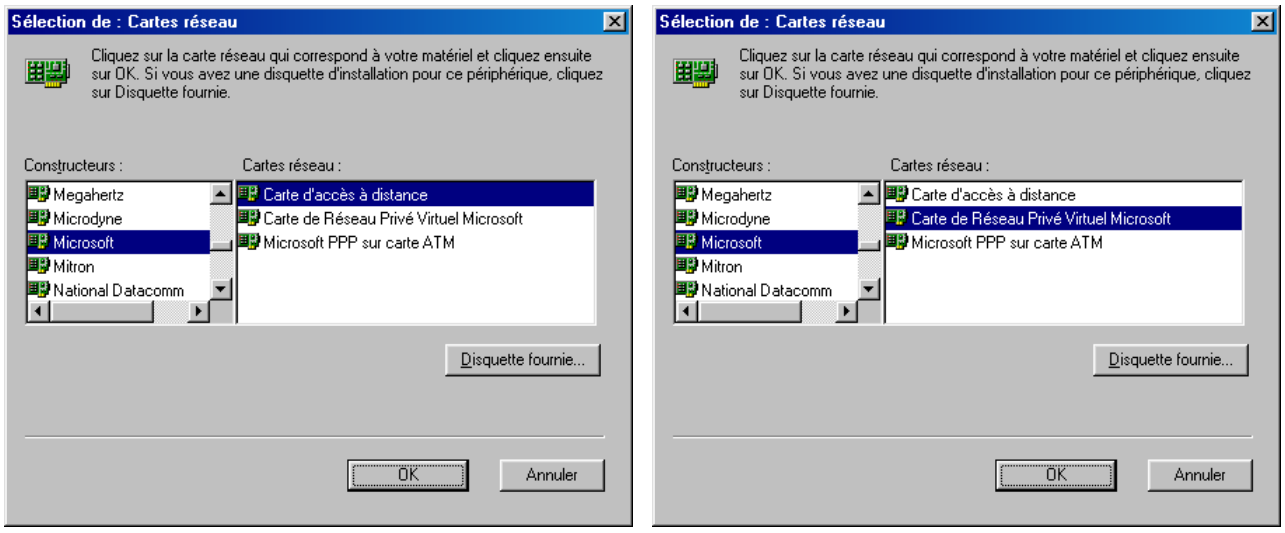
1. Cliquez sur **Démarrer**, pointez sur **Paramètres**, puis cliquez sur **Panneau de configuration**. Effectuez ensuite un double-clic sur l'icône **Réseau**.
2. Dans l'onglet **Configuration** de la fenêtre **Réseau**, cliquez sur le bouton **Ajouter…**.



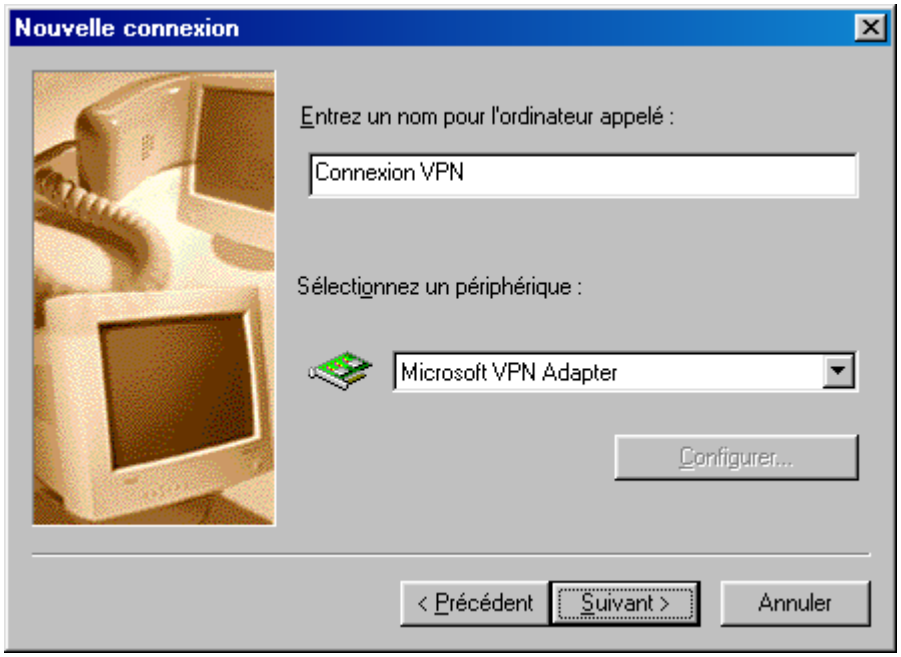
3. La fenêtre **Sélection du type de composant réseau** apparaît. Sélectionnez **Carte**, puis cliquez sur le bouton **Ajouter…**.



4. Paramétrage de l'hôte la même procédure pour installer la **Carte de Réseau Privé Virtuel Microsoft**.



5. Cliquez ensuite sur **OK** dans chacune des fenêtres et suivez les instructions à l'écran afin de valider les modifications.
6. Cliquez sur **Démarrer**, pointez sur **Programmes**, **Accessoires**, **Communications**, puis cliquez sur le dossier **Accès réseau à distance**.
7. Effectuez un double-clic sur l'élément **Nouvelle connexion**. Une fenêtre **Nouvelle connexion** s'ouvre (voir ci-dessous).

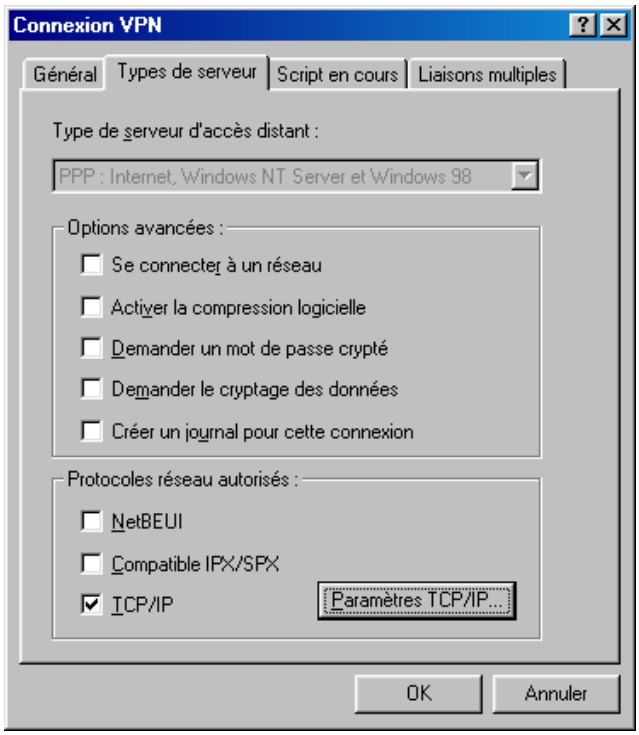


8. Saisissez un nom dans la rubrique **Entrez un nom pour l'ordinateur appelé**.

   Remarque : ce nom ne joue aucun rôle dans la connexion. Il permet seulement d'identifier le fichier créé sur votre disque. Son choix est donc arbitraire. Nous vous conseillons de choisir un nom qui restera clair pour vous (ex. : nom de l'équipement distant).

9. Dans la liste déroulante **Sélectionnez un périphérique**, sélectionnez **Microsoft VPN Adapter** pour une connexion VPN. Cliquez sur **Suivant**.
10. Une fois votre connexion créée, effectuez un clic droit sur celle-ci, puis sélectionnez **Propriétés** dans le menu.
11. Si vous êtes sous Windows 98, cliquez sur l'onglet **Types de serveur** (ou sur l'onglet **Mise en réseau** si vous êtes sous Windows Me). Dans la partie **Options avancées**, décochez toutes les options. Dans les **Protocoles réseau autorisés**, cochez seulement **TCP/IP**.

12. Cliquez sur **Paramètres TCP/IP**, puis décochez **Utiliser la passerelle par défaut pour le réseau distant**.

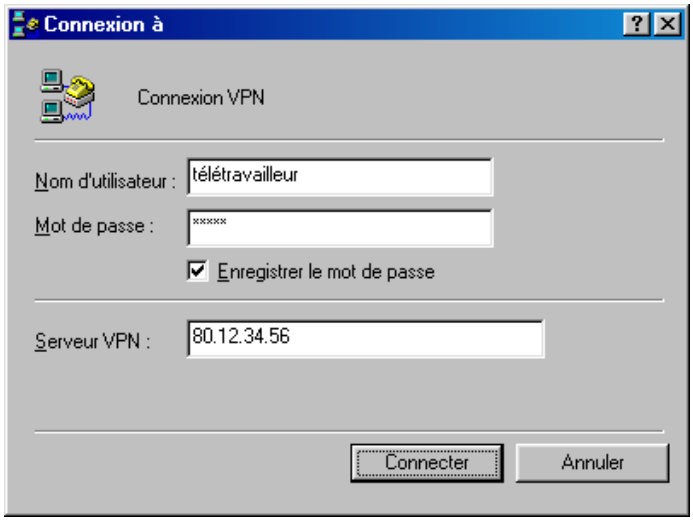


13. Cliquez sur **OK** pour valider les réglages et refermer la fenêtre.
14. Pour établir la connexion, effectuez un double-clic sur votre connexion. La fenêtre de connexion correspondante s'ouvre.
15. Dans les rubriques **Nom d'utilisateur** et **Mot de passe**, vous n'avez plus qu'à saisir vos identifiants.

    Rappel : ces paramètres d'identification sont les mêmes que ceux saisis dans le compte d'appel entrant du routeur.
16. Si vous ne souhaitez pas ressaisir votre mot de passe à chaque connexion, cochez **Enregistrer le mot de passe**.

    Attention : dans ce cas, toute personne pouvant accéder à votre PC sera en mesure d'utiliser votre connexion VPN.
17. Dans la rubrique **Serveur VPN**, saisissez l'adresse IP du serveur distant ou un nom de domaine dynamique.
18. Cliquez ensuite sur **Connecter** dans la fenêtre de connexion. La connexion s'effectue et vos paramètres d'identification sont vérifiés.

    Remarque : vous devez déjà lancer la connexion xDSL avant de vous connecter au serveur VPN du réseau distant.



19. Si ces paramètres sont exacts, la connexion s'établit en quelques secondes. La fenêtre de connexion disparaît automatiquement. A droite de la barre des tâches, l'indicateur d'accès distant apparaît également.

Sous Windows 2000 ou XP

Outre le protocole PPTP, vous pouvez également utiliser le protocole L2TP sans ou avec règle IPSec. Le protocole IPSec vise à sécuriser les échanges au niveau de la couche réseau. L'utilisation de ce protocole permet :

- la gestion et l'échange de clés entre routeurs,
- l'authentification des paquets IP (méthode de sécurité AH : Authentication Header),
- le chiffrement des paquets IP (méthode de sécurité ESP : Encapsulating Security Payload)

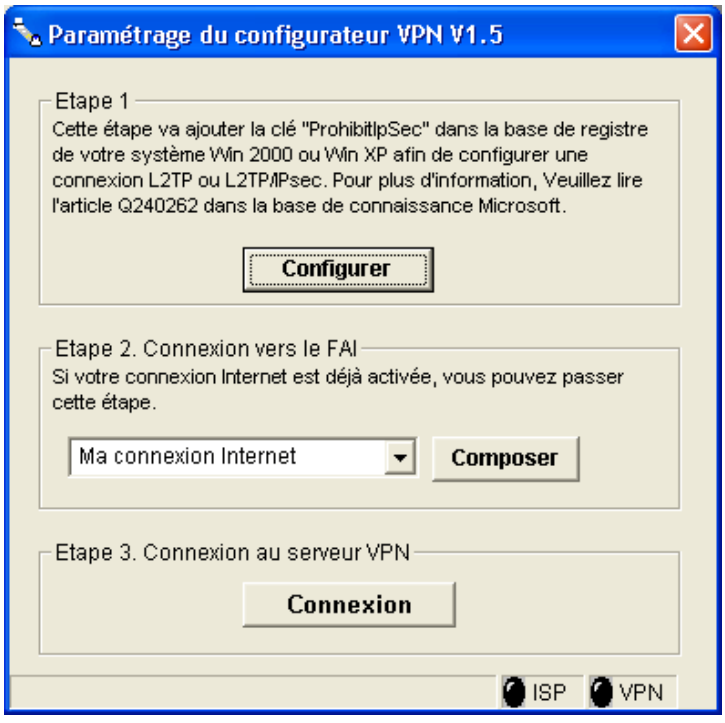
Pour créer une connexion VPN entre un hôte distant (sous Windows 2000 ou XP) et un routeur, afin de faciliter la configuration, un utilitaire est fourni sur le CD-ROM Routeurs VPN Booster. Installez ce configurateur VPN sur le poste distant.

1. Insérez le CD-ROM Routeurs VPN Booster dans le lecteur du PC. Si la configuration du PC l'autorise, le programme d'installation est lancé automatiquement. Si le lancement n'est pas automatique, exécutez le programme **autorun.exe** qui se trouve à la racine du CD-ROM.
2. Cliquez sur **Débuter l'installation**, **Série 6100 x**, puis sur votre modèle de VPN Booster. Cliquez sur **Utilitaires**, puis sur **Configurateur VPN**.
3. Suivez ensuite le programme d'installation de l'utilitaire jusqu'à son terme.

Après l'installation de l'utilitaire sur votre PC, procédez comme suit :

1. Cliquez sur **démarrer**, pointez sur **Tous les programmes**, puis cliquez sur **Configurateur VPN BeWAN**. La fenêtre de paramétrage apparaît. Lors de la première utilisation du configurateur VPN, cliquez sur **Configurer** afin d'ajouter la clé nécessaire dans la base de registre.

   Remarque : avant de procéder au paramétrage de votre connexion VPN et afin de vous connecter au serveur VPN du réseau distant, vous devez déjà être connecté à Internet. Si ce n'est pas le cas, sélectionnez votre connexion Internet que vous avez configurée, puis cliquez sur ***Composer****. Si cette connexion Internet n'existe pas encore, vous ne pourrez pas poursuivre la configuration de la connexion VPN.*



2. Cliquez ensuite sur **Connexion**.
3. Saisissez l'adresse IP du serveur distant (adresse IP WAN du routeur VPN Booster distant) ou le nom de domaine dynamique.
4. Dans les rubriques **Nom d'utilisateur** et **Mot de passe**, vous n'avez plus qu'à saisir vos identifiants.

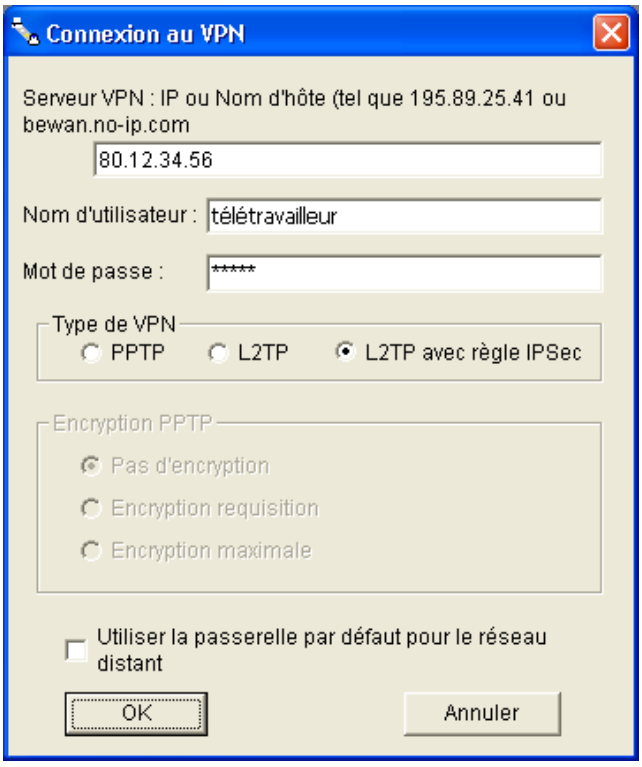
   Rappel : ces paramètres d'identification, connus par l'administrateur du routeur distant, sont les mêmes que ceux saisis dans le compte d'appel entrant du VPN Booster.

5. Dans la rubrique **Type de VPN**, sélectionnez le protocole que vous allez utiliser lors de votre connexion VPN (PPTP, L2TP ou L2TP avec règle IPSec), puis cliquez sur **OK**.

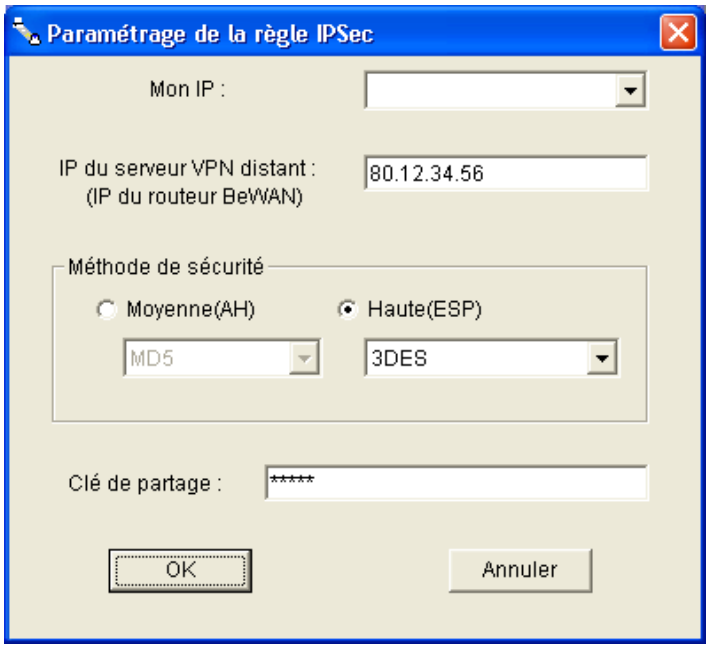
   Remarque : si vous sélectionnez le protocole PPTP, vous pouvez lui attribuer des niveaux d'encryption basés sur le protocole MPPE de Microsoft. ***Encryption requisition*** *correspond à une encryption de 40 bits.* ***Encryption maximale*** *correspond à une encryption de 128 bits.*

   Attention : si du côté du routeur distant, dans la partie ***Service d'appel entrant****, l'encryption PPP (MPPE) est déclarée* ***Obligatoire****, sur le Configurateur VPN, vous devez nécessairement cocher l'option* ***Encryption maximale*** *afin d'établir le lien VPN. Renseignez-vous éventuellement auprès de l'administrateur du distant.*

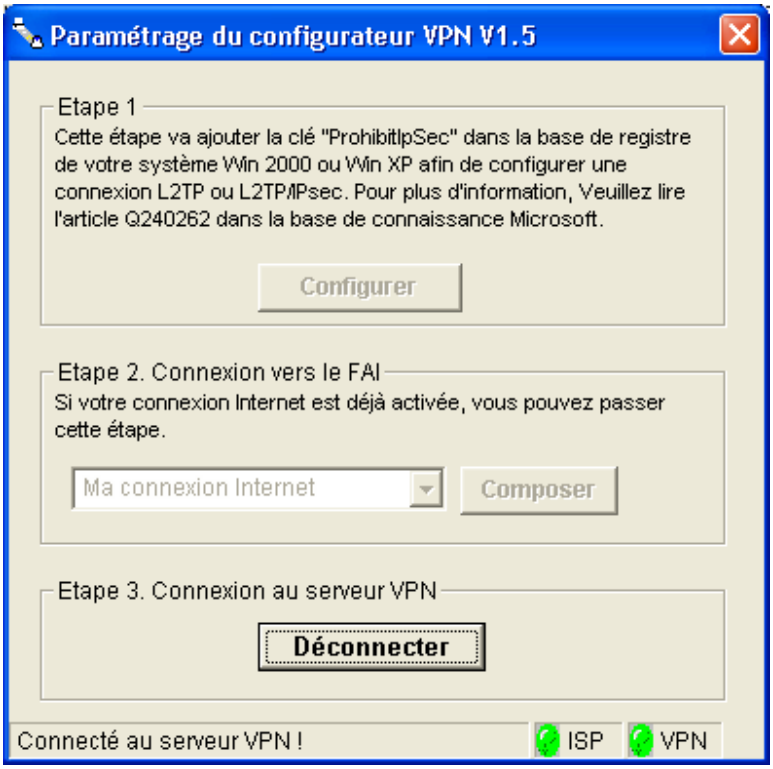
6. Décochez **Utiliser la passerelle par défaut pour le réseau distant**.



7. Si vous sélectionnez L2TP avec règle IPSec comme indiqué sur l'image ci-dessus, vous devez sélectionner ensuite une clé de partage ainsi qu'un niveau de sécurité. Attention : ces paramètres doivent être également saisis à l'identique du côté du routeur distant. Cliquez ensuite sur **OK**.

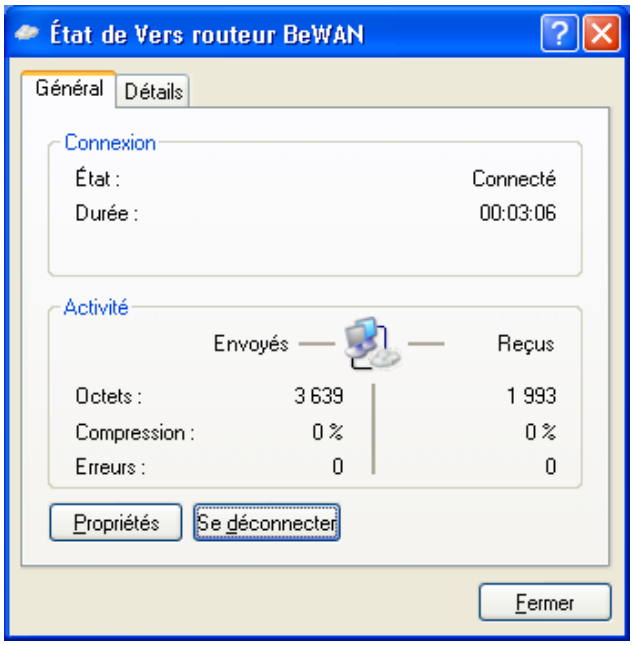


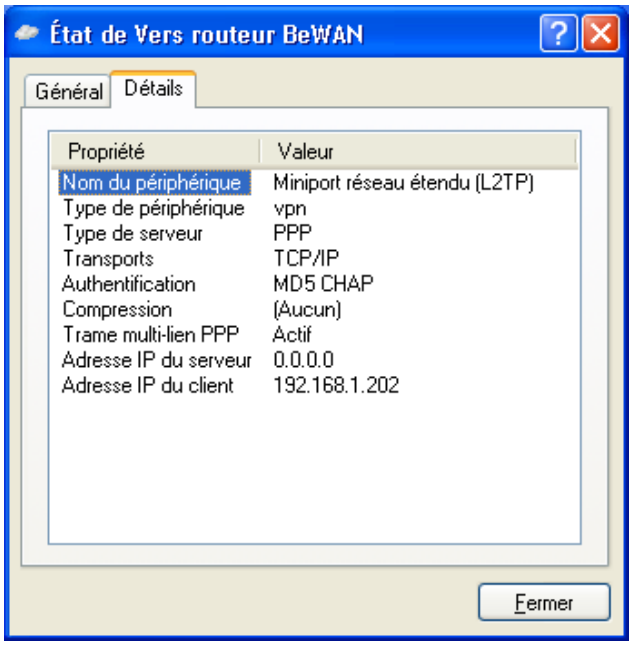
8. La connexion s'effectue et vos paramètres d'identification sont vérifiés. Si ces paramètres sont exacts, la connexion s'établit en quelques secondes. La fenêtre de connexion disparaît automatiquement. A droite de la barre des tâches, l'indicateur d'accès distant apparaît également.



9. Le voyant ISP vous indique que votre connexion Internet est bien établie. Le voyant VPN vert fait état de l'établissement de la connexion VPN.

10. L'indicateur d'accès distant situé dans la barre des tâches confirme que la connexion est établie. Si vous effectuez un double-clic sur cet indicateur, une fenêtre s'ouvre présentant les principaux paramètres de connexion (débit, durée de connexion…). Un bouton **Se déconnecter** vous permet d'interrompre la connexion VPN.

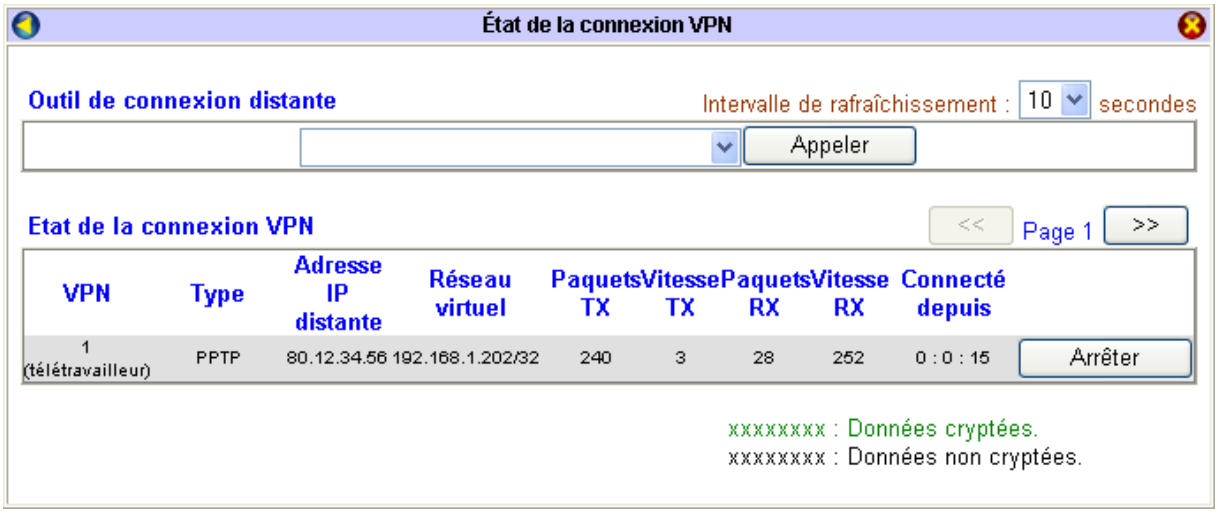




Etape 3 : Etat de la connexion VPN sur le routeur

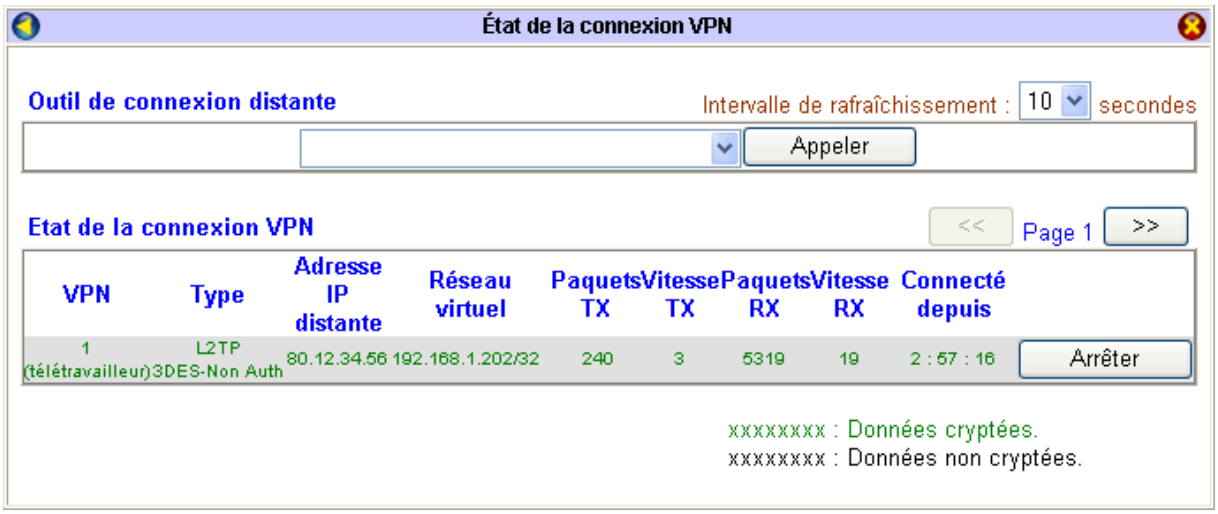
Etat de la connexion si l'hôte distant est sous Windows 98 ou Me

Si les paramétrages ont été correctement effectués sur le routeur et chez l'hôte isolé, votre lien VPN doit s'établir. Cliquez sur **Etat de la connexion VPN**. Les paramètres de la connexion doivent alors apparaître. Sous Windows 98 ou Me, comme l'indique l'image ci-dessous, la connexion VPN ne s'effectue que par le protocole PPTP.



Etat de la connexion si l'hôte distant est sous Windows 2000 ou XP

Si les paramétrages ont été correctement effectués sur le routeur et chez l'hôte isolé, votre lien VPN doit s'établir. Cliquez sur **Etat de la connexion VPN**. Les paramètres de la connexion doivent alors apparaître. Comme cela est possible sous Windows 2000 ou XP, votre connexion VPN apparaît cryptée.



Configuration d'un VPN sur le LAN ou WLAN

Ce mode de configuration permet de sécuriser la connexion d'un poste du réseau local. Il est notamment recommandé pour la liaison de postes sans fil.

Les protocoles possibles sont PPTP, L2TP avec ou sans règle IPSec.

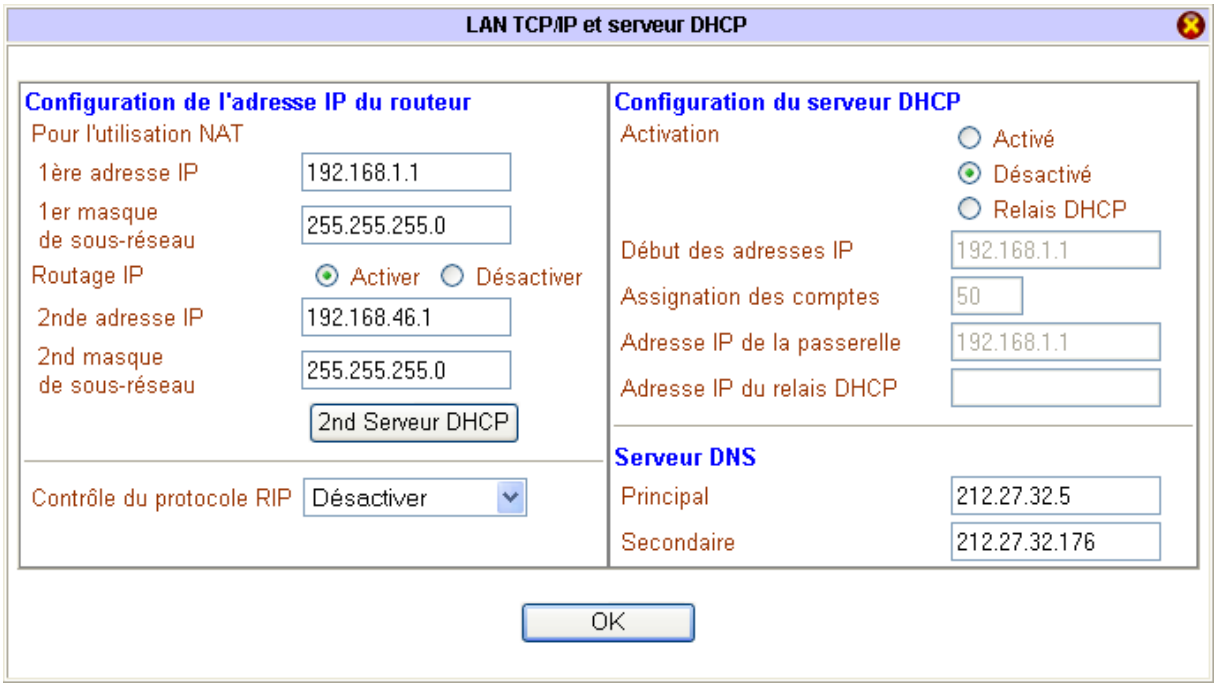
Pour mettre en place cette connexion VPN, sur le PC (client local sous Windows 2000 ou XP), on doit utiliser le Configurateur VPN BeWAN.

Etape 1 : Configuration des paramètres TCP/IP

La première étape consiste à affecter au routeur une seconde adresse IP et au poste client une adresse IP figurant dans la même plan d'adressage.

Sur le VPN Booster

1. Dans le menu **Configuration Elémentaire**, cliquez sur **LAN TCP/IP et serveur DHCP**.
2. En face de l'intitulé **Routage IP**, sélectionnez l'option **Activer**.
3. Affectez ensuite une seconde adresse IP au routeur qui ne doit pas se trouver pas dans le même plan d'adressage que votre réseau. Saisissez le masque de sous-réseau correspondant.



4. Une fois ces informations saisies, cliquez sur **OK** pour valider.
5. Le routeur doit redémarrer pour prendre en compte les nouveaux paramètres. Sélectionnez **Conserver la configuration actuelle**, puis cliquez sur **OK**. Attendez 5 secondes pour que le redémarrage soit terminé.

   Attention : n'éteignez surtout pas le VPN Booster pendant cette phase de redémarrage. Vous risqueriez d'endommager sa mémoire et de le rendre inutilisable (dommage non couvert par la garantie).
6. Une nouvelle fenêtre apparaît. Cliquez sur la première adresse http, qui est en fait l'adresse IP de votre routeur, afin de retourner sur le configurateur du VPN Booster.

Sur le poste client

1. Cliquez sur **démarrer**, puis sur **Panneau de configuration**.
2. Cliquez sur **Connexions réseau et Internet**, puis sur **Connexions réseau**.
3. Avec le bouton droit de la souris, cliquez sur **Connexion au réseau local**, puis sélectionnez **Propriétés** dans le menu.
4. Sélectionnez l'élément **Protocole Internet (TCP/IP)**, puis cliquez sur **Propriétés**.
5. Sélectionnez **Utiliser l'adresse IP suivante**.
6. Dans la rubrique **Adresse IP**, entrez l'adresse IP que vous avez décidé d'attribuer au PC.

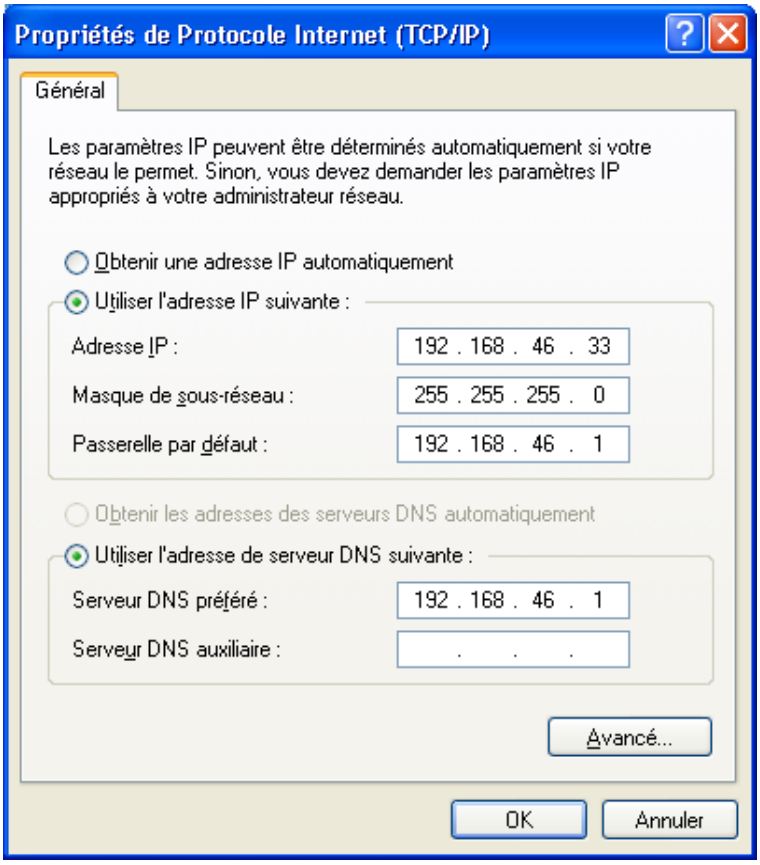
   Important :

   - *L'adresse IP du PC doit impérativement se situer dans la même plage que la deuxième adresse IP que vous venez d'affecter au VPN Booster (dans notre exemple, le routeur possède l'adresse IP « 192.168.46.1 » et le PC « 192.168.46.33 »).*
   - *L'adresse IP du PC doit être unique, c'est-à-dire différente de celle des autres équipements présents sur le réseau local (ordinateurs, VPN Booster …).*
7. Dans la rubrique **Masque de sous-réseau,** entrez la valeur du masque de sous-réseau du VPN Booster, soit « 255.255.255.0 ».
8. Dans la rubrique **Passerelle par défaut**, entrez la seconde adresse IP attribuée au VPN Booster.
9. Sélectionnez l'option **Utiliser l'adresse de serveur DNS suivante**.

   Saisissez de préférence l'adresse IP du routeur. De cette façon, vous utilisez la fonction Proxy DNS du routeur qui vous permet d'optimiser la navigation.

   Sinon, vous pouvez également saisir l'adresse de serveur DNS indiquée par votre FAI (pour cela, reportez-vous à la documentation fournie par celui-ci lors de la souscription de l'abonnement).

   Rappel : les serveurs DNS permettent la résolution des noms symboliques sur Internet.



10. Cliquez sur **OK** afin de valider les modifications.

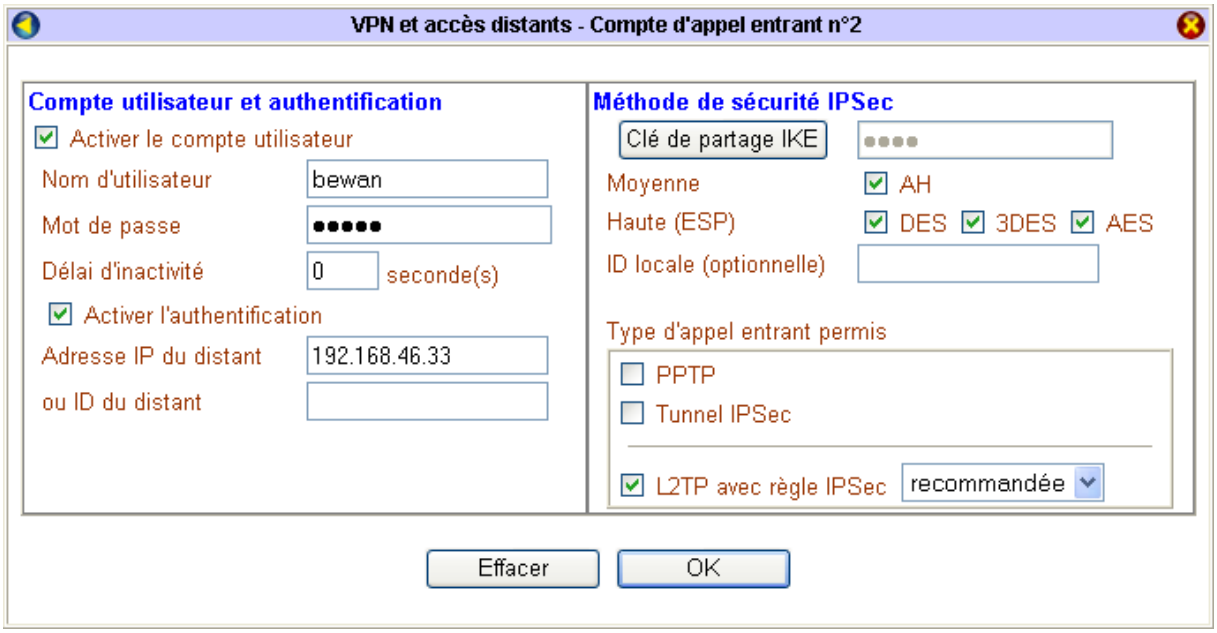
Etape 2 : Configuration du VPN

Sur le VPN Booster

1. Dans le menu **Réglages Avancés**, cliquez sur **VPN et accès distants**, puis sur **Compte d'appel entrant**.
2. Pour paramétrer un compte, cliquez sur un numéro (si le compte n'a pas encore été paramétré, le nom du compte apparaît sous la forme ???).
3. Pour activer le compte, cochez **Activer le compte utilisateur**.
4. Entrez un nom et un mot de passe dans les rubriques **Nom d'utilisateur** et **Mot de passe** (16 caractères maximum pour chacune des rubriques). Ceux-ci doivent être les mêmes identifiants que ceux saisis par l'hôte distant.
5. Dans la rubrique **Délai d'inactivité**, entrez le nombre de secondes au terme duquel la connexion sera automatiquement interrompue en cas d'inactivité.

   Remarque : indiquez « 0 » seconde afin que le routeur ne coupe pas la liaison après une période d'inactivité.
6. Dans la partie **Type d'appel entrant permis**, cochez le(s) protocole(s) que le routeur va autoriser pour ce compte.

   *Attention : vous pouvez décochez le protocole **Tunnel IPSec**. En effet, le configurateur VPN que vous allez utiliser pour établir votre lien VPN ne vous permet pas d'utiliser ce mode de sécurité.*
7. Si vous avez sélectionné le protocole **L2TP avec règle IPSec** (recommandée ou obligatoire), vous devez impérativement saisir une clé IPSec :
   - Cochez **Activer l'authentification** (ou **Activer l'authentification CLID** si vous possédez le VPN Booster 32 i).
   - Saisissez l'adresse IP du poste client.
   - Saisissez ensuite votre clé IPSec pour ce profil particulier en cliquant sur le bouton **Clé de partage IKE** qui est devenu accessible. Cette clé, une fois confirmée, ne sera active que pour ce compte utilisateur.



8. Cliquez sur **OK** afin de valider les informations. La configuration du compte d'appel entrant est terminée. Dans la colonne **Etat**, le compte est indiqué *Activé* (« **v** »).

Sur le poste client

1. Cliquez sur **démarrer**, pointez sur **Tous les programmes**, puis cliquez sur **Configurateur VPN BeWAN**.

   Remarque : le configurateur VPN est fourni sur le CD-ROM du routeur. Pour l'installer, une fois votre CD-ROM inséré, cliquez sur ***Débuter l'installation****, puis sur le modèle VPN Booster dont vous disposez. Cliquez sur* ***Utilitaires****, puis sur* ***Configurateur VPN****. Suivez ensuite le programme d'installation de l'utilitaire jusqu'à son terme.*

2. Cliquez sur **Connexion**.
3. Saisissez la seconde adresse IP affectée au VPN Booster.
4. Dans les rubriques **Nom d'utilisateur** et **Mot de passe**, vous n'avez plus qu'à saisir vos identifiants.

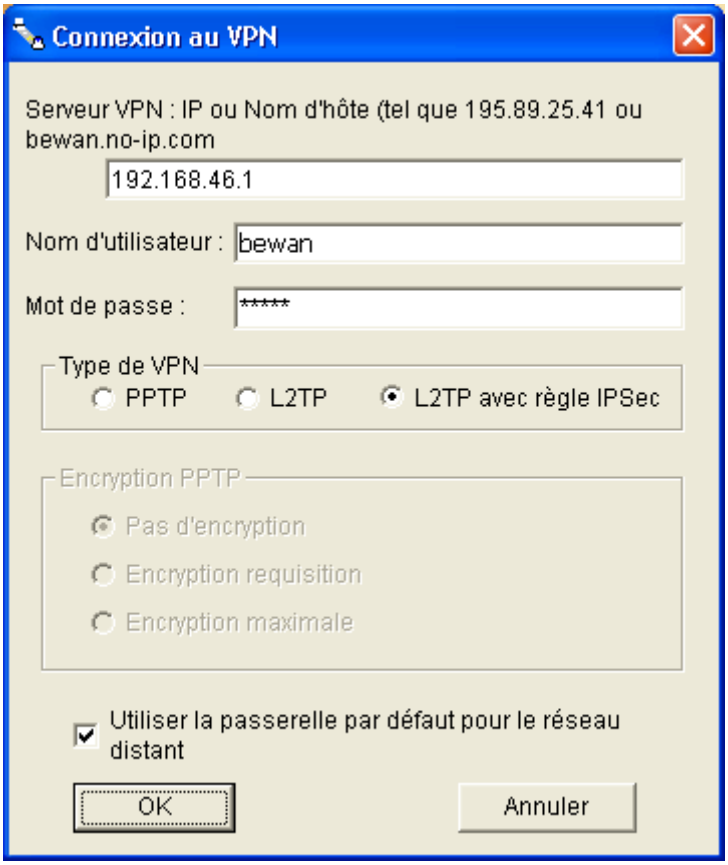
   Rappel : ces paramètres d'identification, connus par l'administrateur du routeur distant, sont les mêmes que ceux saisis dans le compte d'appel entrant du VPN Booster.

5. Dans la rubrique **Type de VPN**, sélectionnez le protocole que vous allez utiliser pour établir votre connexion VPN (dans notre exemple, L2TP avec règle IPSec), puis cliquez sur **OK**.

   Remarque : si vous sélectionnez le protocole PPTP, vous pouvez lui attribuer des niveaux d'encryption basés sur le protocole MPPE de Microsoft. ***Encryption requisition*** *correspond à une encryption de 40 bits.* ***Encryption maximale*** *correspond à une encryption de 128 bits.*

   Attention : si du côté du routeur, dans la partie ***Service d'appel entrant****, l'encryption PPP (MPPE) est déclarée* ***Obligatoire****, sur le Configurateur VPN, vous devez nécessairement cocher l'option* ***Encryption maximale*** *afin d'établir le lien VPN. Renseignez-vous auprès de l'administrateur réseau.*

6. Cochez **Utiliser la passerelle par défaut pour le réseau distant**.

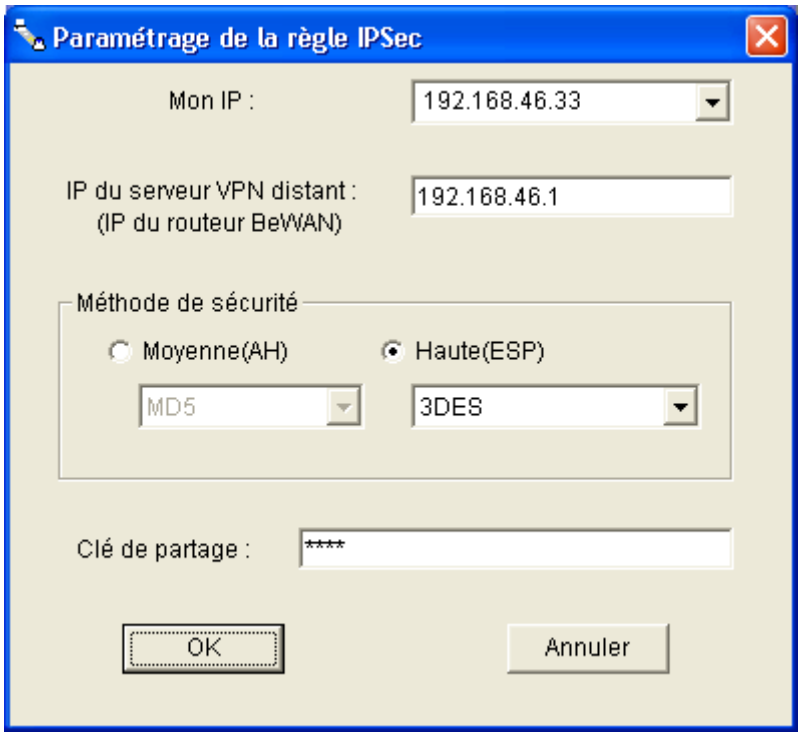


7. Cliquez sur **OK** pour valider.
8. Après avoir sélectionné **L2TP avec règle IPSec**, vous devez désormais choisir la **Méthode de sécurité** appropriée.

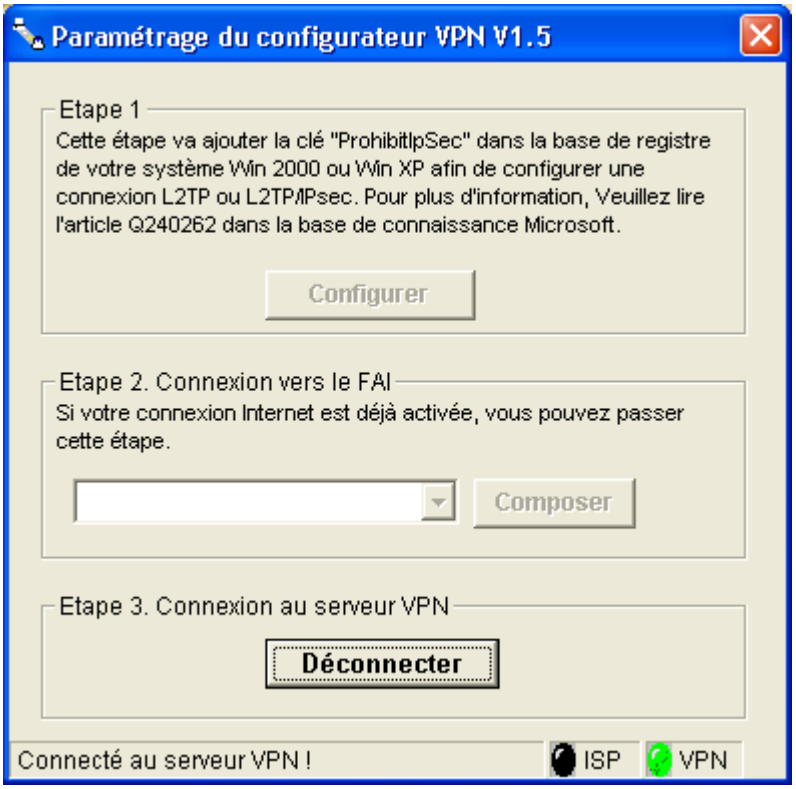
   Attention : veillez à ce que la méthode de sécurité choisie soit bien sélectionnée dans le compte d'appel entrant du VPN Booster.

9. Saisissez la même **Clé de partage** que celle renseignée dans le compte d'appel entrant du routeur.

   Attention : ce paramètre doit être également saisi à l'identique du côté du routeur distant.



10. Cliquez ensuite sur **OK**.
11. Une fois la connexion établie, vous devez obtenir l'écran suivant.



Le voyant VPN vert fait état de l'établissement de la connexion VPN. Votre poste est dorénavant connecté au VPN Booster sur le LAN ou WLAN.

Toutes les requêtes LAN ou WAN passeront exclusivement par le lien VPN.

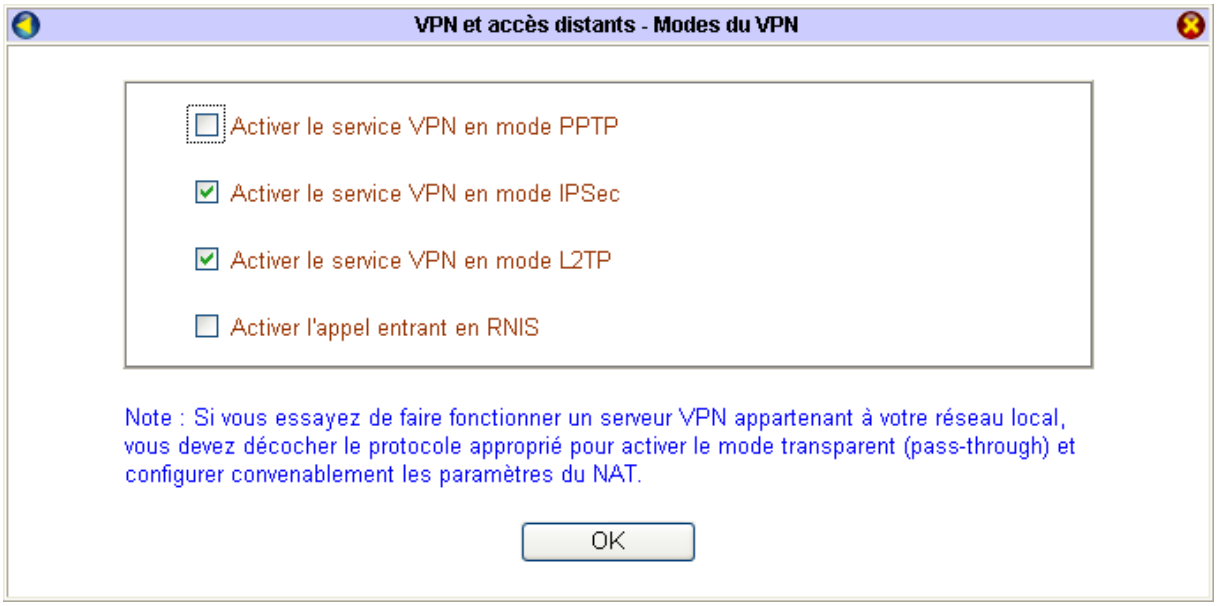
Configuration du mode Pass-Through

Si vous souhaitez gérer une connexion VPN via un autre équipement que le routeur, vous pouvez utiliser le mode VPN Pass-Through.

Le mode Pass-Through vous permet de désactiver la gestion native d'un ou de plusieurs modes VPN en associant une ouverture de port correspondant au mode VPN utilisé. Grâce à cette opération, le routeur redirige les requêtes VPN entrantes vers un serveur VPN du réseau local. Procédez en deux étapes :

1. Dans le menu **Réglages Avancés**, cliquez sur **VPN et accès distants**, puis sur **Modes du VPN**.
2. Décochez le service en question.

   Par exemple, si le serveur VPN fonctionne en mode PPTP, décochez **Activer le service VPN en mode PPTP**, puis cliquez sur **OK**. Vous devez ensuite redémarrer votre routeur.



3. Effectuez une ouverture de port correspondant au mode VPN utilisé. Cliquez sur **NAT** dans le menu **Réglages Avancés**, puis sur **Configuration de l'ouverture de ports**. Sélectionnez une fiche encore disponible. En fonction du mode choisi, sélectionnez le protocole et le port suivants :
   - **Mode PPTP** : protocole TCP/Port 1723
   - **Mode IPSec** : protocole UDP/Port 500
   - **Mode L2TP** : protocole TCP/Port 1701
4. Cliquez sur **OK**.

Filtres IP et Firewall

Le paramétrage des filtres IP et du Firewall vous permet d'empêcher l'intrusion de stations extérieures sur votre réseau local. Il vous permet également de restreindre l'accès à Internet.

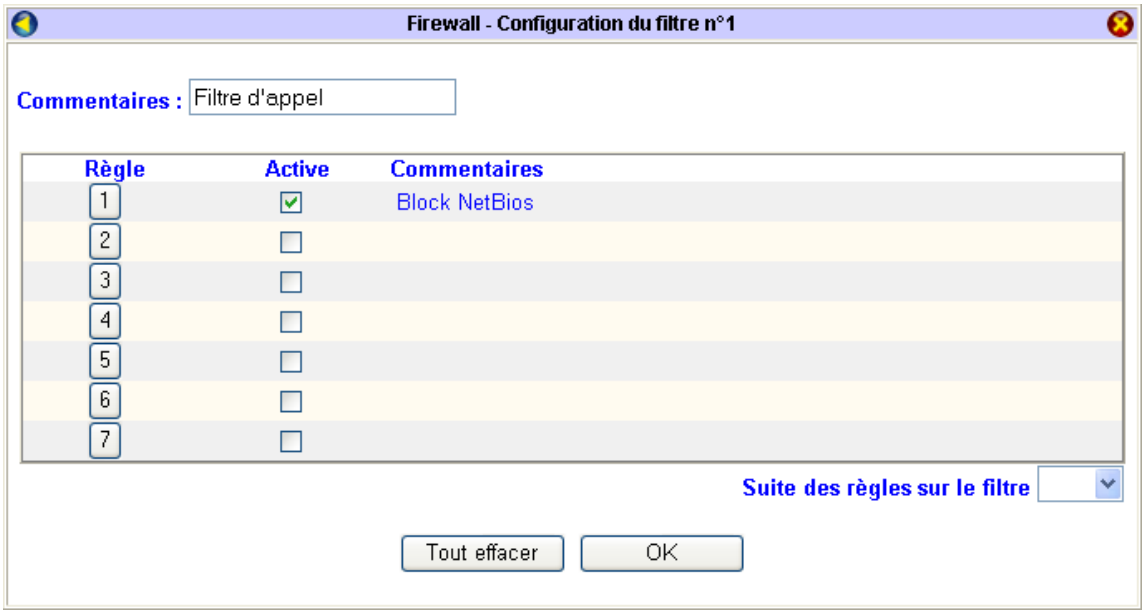
Le filtrage IP contient deux types de filtres : le filtre sur les appels et le filtre sur les données. Le premier donne la possibilité de bloquer ou de permettre l'accès des paquets avant que la connexion WAN soit établie. Le second est prévu pour bloquer ou permettre l'accès des données une fois la connexion WAN établie. C'est donc en fonction de l'état de la connexion WAN que le filtrage IP transférera le paquet vers le filtre sur les appels ou vers le filtre sur les données.

Paramétrage d'un filtre

Vous avez la possibilité de configurer 12 filtres. Procédez comme suit :

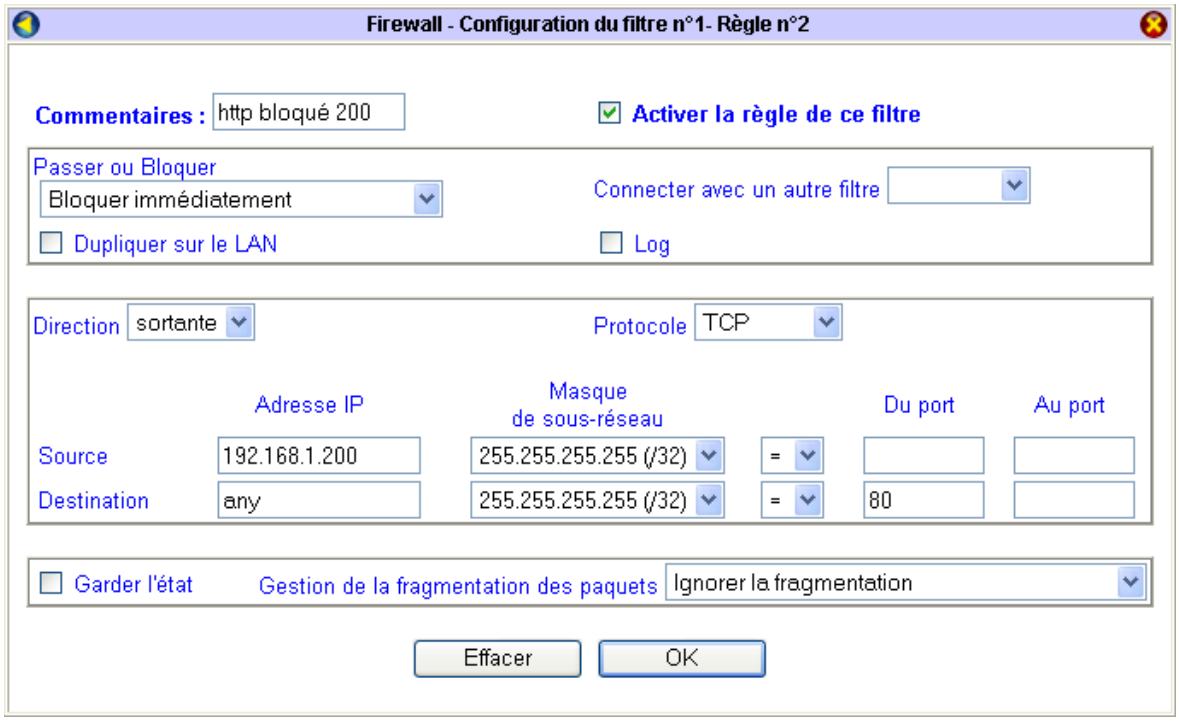
1. Dans le menu **Réglages Avancés**, cliquez sur **Firewall**.

2. Par défaut, le filtre sur les appels est défini dans le filtre 1 et le filtre sur les données dans le filtre 2. Sélectionnez le genre de filtre que vous désirez appliquer.



3. Pour chaque configuration d'un filtre, vous devez préciser des règles (un maximum de 7 règles par filtre). Cliquez sur un numéro de règle et renseignez les rubriques dans la nouvelle fenêtre. Pour illustrer le paramétrage d'une règle, nous avons choisi un exemple simple de restriction à l'accès Internet. Au travers de cet exemple, nous verrons également les autres options possibles lors d'une configuration.

   Dans ce cas présent, l'utilisateur qui possède l'adresse IP « 192.168.1.200 » n'est pas autorisé à accéder au service http sur Internet. Le port 80 correspond au port http.



4. Dans la rubrique **Commentaires**, entrez une information qui vous permettra d'identifier l'objet de cette règle.
5. Cochez **Activer la règle de ce filtre**.
6. Dans la rubrique **Passer ou Bloquer**, indiquez quelle action sur les paquets doit avoir cette règle. Vous avez le choix parmi 4 possibilités :
   - **Passer immédiatement** : laisse passer les paquets en fonction de la règle en question.
   - **Bloquer immédiatement** : bloque les paquets en fonction de la règle en question.
   - **Passer si plus de correspondance** : laisse passer les paquets en fonction non seulement de cette règle mais aussi en tenant compte des autres règles suivantes qui ont été paramétrées et activées. La vérification s'effectue à partir de la règle en question jusqu'à la dernière règle édictée et seulement dans cet ordre. Les règles sont donc mises en relation.
   - **Bloquer si plus de correspondance** : bloque les paquets en fonction non seulement de cette règle mais aussi en tenant compte des autres règles suivantes qui ont été paramétrées et activées. La vérification s'effectue à partir de la règle en question jusqu'à la dernière règle édictée et seulement dans cet ordre. Les règles sont donc mises en relation.
7. Si vous souhaitez récupérer une trace du filtrage effectué, cochez la rubrique **Log**. Vous pourrez visualiser cette trace en utilisant une session Telnet (référez-vous au chapitre « Commandes Telnet », section « Liste des sous-commandes LOG » page 188).
8. Dans la rubrique **Direction**, indiquez la direction des paquets sur laquelle doit s'appliquer la règle.

   Remarques :
   - *Si vous avez sélectionné le filtre sur les appels, cette rubrique n'est pas prise en compte. Quel que soit le paramètre sélectionné, la règle ne peut s'appliquer que sur les appels sortants. Ce filtre permettra le déclenchement ou le non déclenchement de la communication.*
   - *Concernant le filtrage sur les données, **Direction entrante** signifie que le filtrage se fait sur les paquets entrants sur le LAN (réseau local). **Direction sortante** signifie que le filtrage s'applique sur les paquets sortants sur le WAN (réseau distant).*

9. Sélectionnez le type de protocole auquel s'applique la règle. Quand vous effectuez un filtrage sur un port, veuillez utiliser l'un des choix suivants : *TCP*, *UDP* ou *TCP/UDP*.
10. Dans la rubrique **Source** de l'**Adresse IP**, saisissez l'adresse IP, puis le masque de sous-réseau.

    Remarques :

    - *Suivant le masque de sous-réseau choisi, vous pouvez sélectionnez une adresse en particulier ou un groupe d'adresses. Dans notre exemple, le masque de 255.255.255.255 (/32) inclut une seule adresse (192.168.1.200).*
    - *A titre indicatif, un masque de 255.255.255.0 (/24) inclurait les adresses de 192.168.1.1 à 192.168.1.254.*
11. Pour filtrer un service, si vous avez sélectionné le protocole TCP et/ou UDP, vous devez spécifier un opérateur logique (=, !=, < et >), puis un port ou une plage de ports :

    – **= (égal à)** : le filtrage s'applique au numéro de port ou à la plage de ports saisis,

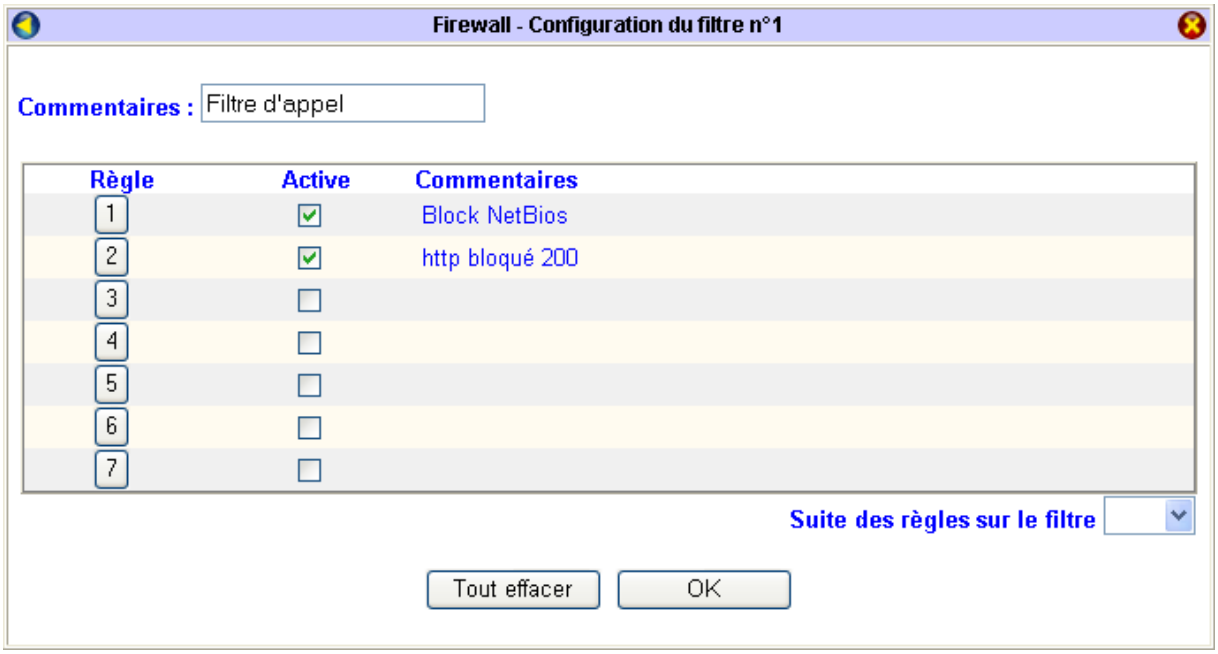
    – **!= (différent de)** : le filtrage s'applique à tous les ports sauf au numéro du port ou de la plage de ports saisis,

    – **< (inférieur à)** : le filtrage s'applique à tous les ports inférieurs au port saisi (de ce fait, vous ne devez rien saisir dans la rubrique **Au port**),

    – **> (supérieur à)** : le filtrage s'applique à tous les ports supérieurs au port saisi (de ce fait, vous ne devez rien saisir dans la rubrique **Au port**).

    Remarque : dans un processus client/serveur (ex. http, ftp,…), le port source du client est généralement un port libre supérieur à 1023 (port virtuel) alloué dynamiquement. Selon notre exemple, le filtrage doit donc s'effectuer sur le(s) port(s) de destination.
12. Dans la rubrique **Destination**, entrez l'adresse IP à laquelle n'a pas accès votre utilisateur.

    *Remarque : « **Any** » signifie que la règle s'applique à toutes les adresses IP.*
13. L'option **Garder l'état** permet de conserver des informations sur une session complète de communication TCP/UDP.
14. Dans la rubrique **Gestion de la fragmentation des paquets**, spécifiez le type de paquets sur lesquels vous souhaitez appliquer le filtrage.
15. Cliquez sur **OK** pour que les paramètres soient pris en compte. Vous venez de créer une nouvelle règle.



16. Une fois la règle édictée, elle devient active. Cliquez de nouveau sur **OK**. Vous revenez sur le tableau des filtres.

    *Remarque : pour la rendre inactive, décochez la case située dans la colonne **Active**, puis cliquez sur **OK**.*

Attention : *lorsque vous configurez un nouveau filtre, choisissez toujours le filtre immédiatement disponible après le dernier paramétré. En effet, si vous laissez un filtre libre entre deux filtres configurés, le(s) filtre(s) suivant le filtre laissé libre ne sera(seront) pas pris en compte (notamment en cas de suppression d'un filtre).*

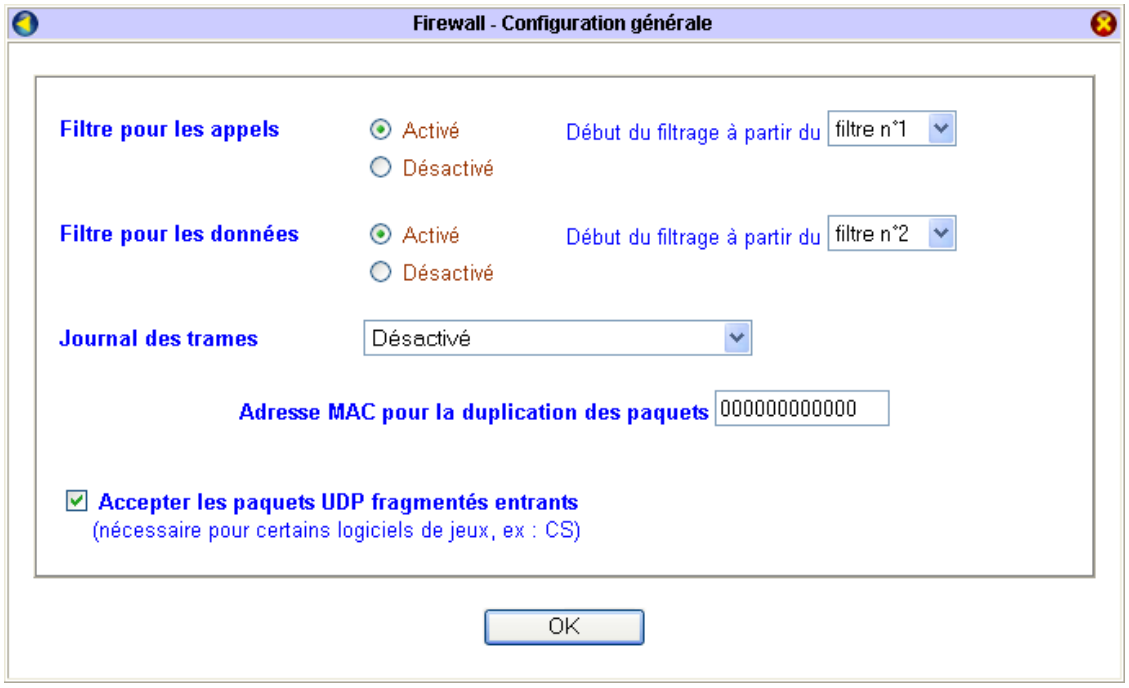
Pour que ce dernier soit pris en compte, vous devez le relier au filtre situé avant. Procédez comme suit :

- *Cliquez sur le numéro du filtre précédant le filtre laissé libre.*
- *Dans la rubrique* ***Suite des règles sur le filtre****, indiquez le numéro du filtre situé après le filtre laissé libre. De cette manière, la vérification s'effectuera sur tous les filtres configurés.*

Configuration générale des filtres

Dans une page de configuration générale, vous pouvez activer ou désactiver une partie ou la totalité des filtres sur les appels ou sur les données que vous avez préalablement créés. Pour cela, sélectionnez le numéro du filtre à partir duquel s'établira la vérification.

1. Dans la fenêtre **Paramétrage des filtres IP et du firewall**, cliquez sur **Configuration générale**. Sélectionnez le ou les filtres que vous désirez activer.



2. Vous pouvez ensuite activer ou non un journal des trames.

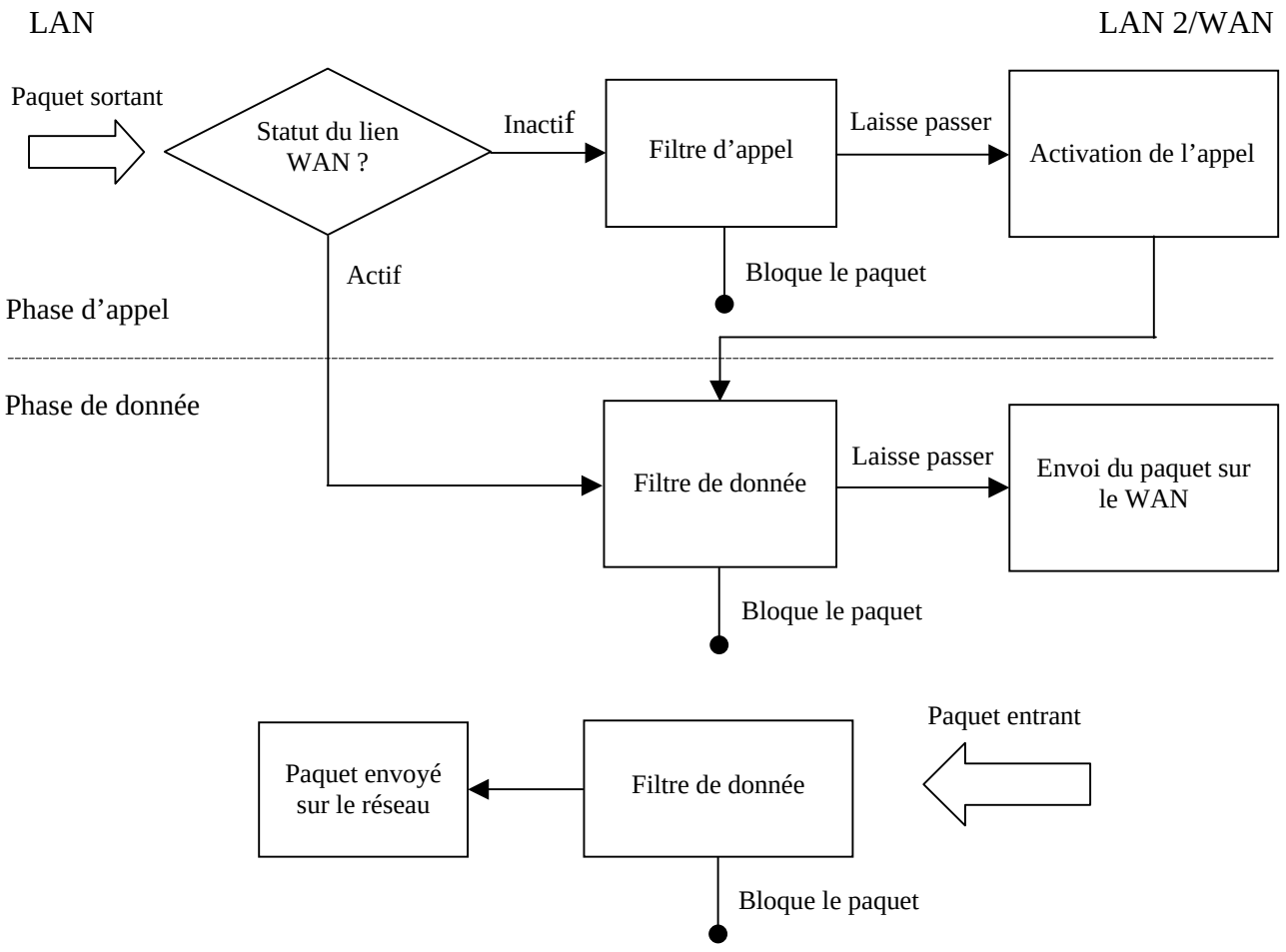
   Remarque : le journal des trames permet de dupliquer les paquets filtrés ou non filtrés par le routeur. Spécifiez alors l'adresse MAC du matériel (carte réseau d'un PC, firewall matériel, autre routeur,…) sur lequel seront renvoyés les paquets dont vous souhaitez avoir une trace. Pour que les informations soient renvoyées dans le journal des trames, cochez ***Dupliquer sur le LAN*** *dans la ou les régle(s) que vous souhaitez analyser.*

   - Si vous souhaitez désactiver le journal des trames, dans la rubrique **Journal des trames**, sélectionnez **Aucun**.
   - Si vous souhaitez au contraire avoir une trace des paquets filtrés ou non filtrés, plusieurs choix sont possibles dans la rubrique **Journal des trames** :
     - **Passer** : le journal des trames dupliquera tous les paquets autorisés par le(s) filtre(s),
     - **Bloquer** : le journal des trames dupliquera tous les paquets bloqués par le(s) filtre(s),
     - **Pas de correspondance** : le journal des trames dupliquera tous les paquets qui ne correspondent pas aux règles de filtrage.

3. Cliquez sur **OK** pour valider vos paramètres de filtrage.

Schéma du processus de filtrage

Voici un schéma qui résume la procédure du filtrage au niveau du routeur. Il faut que le filtre d'appel et le filtre de donnée soient activés :



Configuration des défenses DoS

Le VPN Booster dispose également des fonctionnalités de contrôle d'intrusion DoS (Denial of Service) pour contrer les tentatives d'intrusion vers votre réseau.

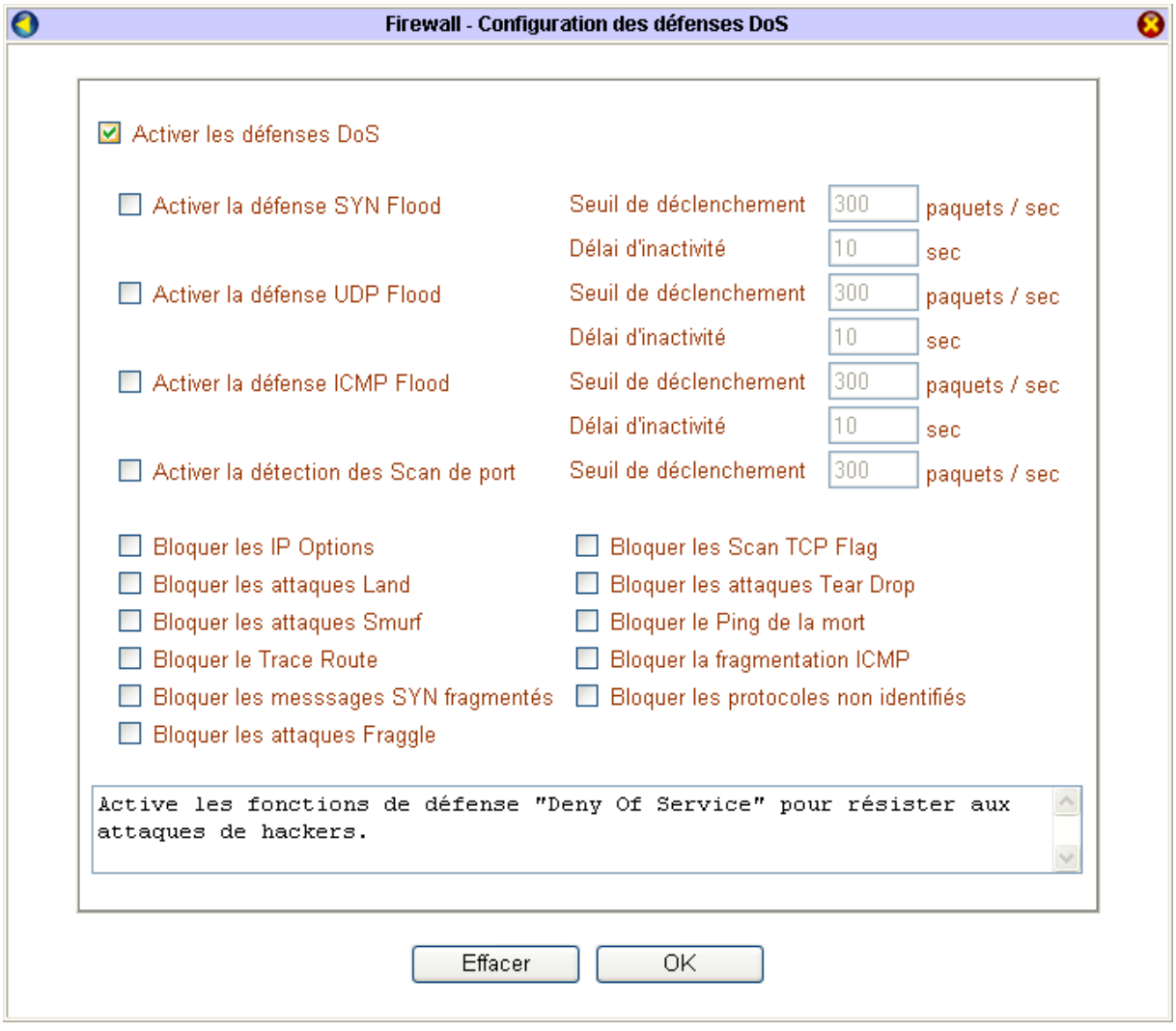
La défense DoS vous aide à détecter et atténuer les attaques de DoS. Ces attaques consistent à paralyser des équipements réseaux afin qu'ils ne puissent plus être utilisés temporairement. En général, le but de ces attaques n'est pas de récupérer ou d'altérer des données mais de rendre inaccessible un service aux utilisateurs légitimes. Ces attaques peuvent rendre inutilisables un ordinateur ou un réseau et donc provoquer des conséquences dramatiques.

On distingue donc des attaques de masse et des attaques de vulnérabilité. Les attaques de masse tentent d'épuiser toutes les ressources de votre système tandis que les attaques de vulnérabilité essaient de paralyser le système en attaquant les failles caractéristiques des protocoles ou des systèmes d'exploitation.

Le moteur de la défense DoS inspecte chaque paquet entrant selon sa base de données de signatures d'attaque à sa disposition. N'importe quel paquet identifié comme potentiellement dangereux ou destabilisant pour le système est bloqué. Lorsque le client Syslog est activé, tous les messages correspondants lui sont envoyés. Le format de message commence par le mot-clé représentant une signature DoS suivi du nom qui réfère à quelle attaque il correspond.

Il existe 15 types de défense pour la configuration de la défense DoS. Par défaut, la fonctionnalité de la défense DoS est désactivée. Une fois cette fonctionnalité activée, la valeur par défaut est placé à 300 paquets par seconde et le délai d'inactivité est de 10 secondes.

Remarque : veillez à ce que le seuil soit toujours supérieur à 150 paquets par seconde et que le délai d'inactivité soit supérieur à 5 secondes.



Configuration du filtrage de contenu

Le VPN Booster dispose de la fonction de filtrage de contenu.

Par exemple, pour les établissements scolaires ou les entreprises qui le souhaitent, il est possible d'interdire l'accès des élèves à des sites non souhaitables, mais également d'interdire certains sites (en fonctionnant par mot-clé) ne correspondant pas aux besoins de l'entreprise.

Grâce à des puissants filtres par mots-clés, vous pouvez restreindre l'accès à des sites Web et ainsi les sites indésirables peuvent être inaccessibles de votre réseau. L'administrateur se sert d'une liste pré-définie afin de bloquer l'accès aux sites comportant un contenu répréhensible ou non désiré (pages pornographiques, jeux d'argent, …). Ce filtrage est opéré sur la base de l'URL demandée.

Attention : si vous disposez du VPN Booster 8, seules les restrictions URL et WEB sont paramétrables.

Restriction URL

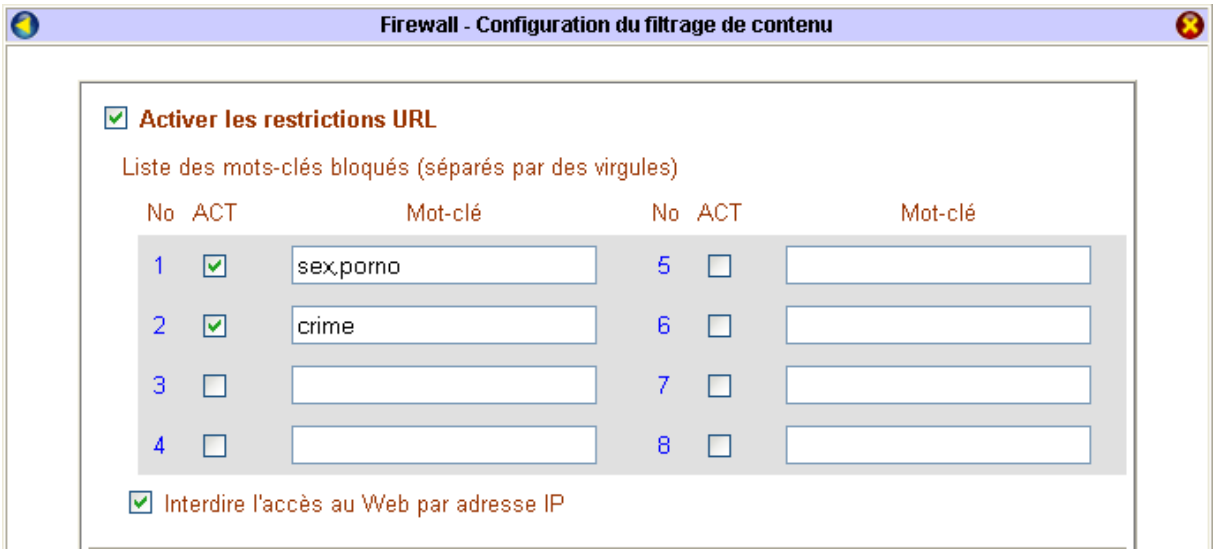
Pour bloquer l'accès à certains sites, procédez comme suit :

1. Cochez la case **Activer les restrictions URL**.
2. Cochez la case **ACT** d'une ou plusieurs des 8 listes disponibles, puis saisissez le nom du site ou un ensemble de mots-clés dans la zone de texte.

   Si une adresse de site saisie par un utilisateur contient l'un de ces mots-clés, la page concernée ne sera pas affichée. Dans l'exemple ci-dessous, nous avons décidé de bloquer les sites dont l'adresse contient les caractères 'sex' ou 'porno'.

   Important à savoir : en précisant l'expression 'sex', vous interdisez également l'accès aux noms de sites comportant les mots comme 'sexe', 'sexologie', 'sexy', 'sexualité' ou encore 'sextant', c'est-à-dire tous les mots constitués de ces trois lettres.

   Remarque : quand plusieurs mots composent une liste, veuillez les séparer par une espace, une virgule ou un point virgule pour qu'ils soient pris en compte.



3. Cliquez sur **OK** pour enregistrer les changements.

Remarque : en activant le filtrage URL, vous avez la possibilité de cocher l'option ***Interdire l'accès au Web par adresse IP****. De cette manière, l'utilisateur doit obligatoirement taper un nom de domaine pour accéder à un site.*

Restriction WEB

Outre des URL spécifiques, le routeur peut également rejeter certains types de code comme ActiveX, des applets Java, des cookies…

1. Cochez la case **Activer les restrictions WEB**.
2. Cochez ensuite les applications que vous souhaitez bloquer.

   Dans l'exemple ci-dessous, nous avons décidé de bloquer pour tout utilisateur le téléchargement de fichiers '.exe' (option **Fichiers exécutables**) ou de fichiers '.zip' (option **Fichiers compressés**).

   Attention : ces restrictions ne concernent pas le téléchargement via le protocole FTP, mais uniquement le téléchargement via le protocole http.

3. Cliquez sur **OK** pour valider ces restrictions.

Plage horaire des restrictions

Par défaut, dès que vous activez l'une des deux restrictions précédentes (URL ou WEB), ces filtrages sont permanents puisque l'option **Blocage permanent** est sélectionnée. Néanmoins, vous avez également la possibilité de leur attribuer une plage horaire spécifique. Procédez comme suit :

1. Sélectionnez l'option **Blocage de**.
2. Indiquez l'heure à laquelle vous souhaitez que le filtrage démarre ainsi que l'heure à laquelle il doit se terminer.
3. Déterminez ensuite les jours concernés par ces restrictions.

   Selon l'exemple montré ci-dessous, les restrictions que nous avons attribuées ne sont pas effectives le samedi et le dimanche. De plus, en semaine, l'accès est autorisé de 17h31 à 9h.

4. Cliquez sur **OK**.

Autorisations exceptionnelles

La Série VPN Booster 32 gère une table des adresses IP qui, sous forme de liste de contrôle, autorisera l'accès aux sites interdits. Vous avez donc la possibilité, malgré les interdictions précédentes (Restriction URL ou Restriction WEB), d'autoriser certaines adresses IP qui composent votre réseau à accéder néanmoins aux sites prohibés. Ces autorisations sont donc prioritaires par rapport aux interdictions. Pour cela, procédez comme suit :

1. Cochez la case **Ignorer les restrictions pour les clients suivants**.
2. Saisissez l'adresse IP (et le masque de sous réseau correspondant) du client pour lequel les interdictions préalablement établies ne seront pas prises en compte. Seule cette adresse IP validée et configurée peut accéder aux sites interdits.

   Dans l'exemple ci-dessous (en correspondance avec les exemples précédents), nous avons décidé d'autoriser l'ordinateur dont l'adresse IP est '192.168.1.20' à accéder aux noms de sites composés des caractères 'sex', et à télécharger des fichiers '.exe' ou des fichiers '.zip'.

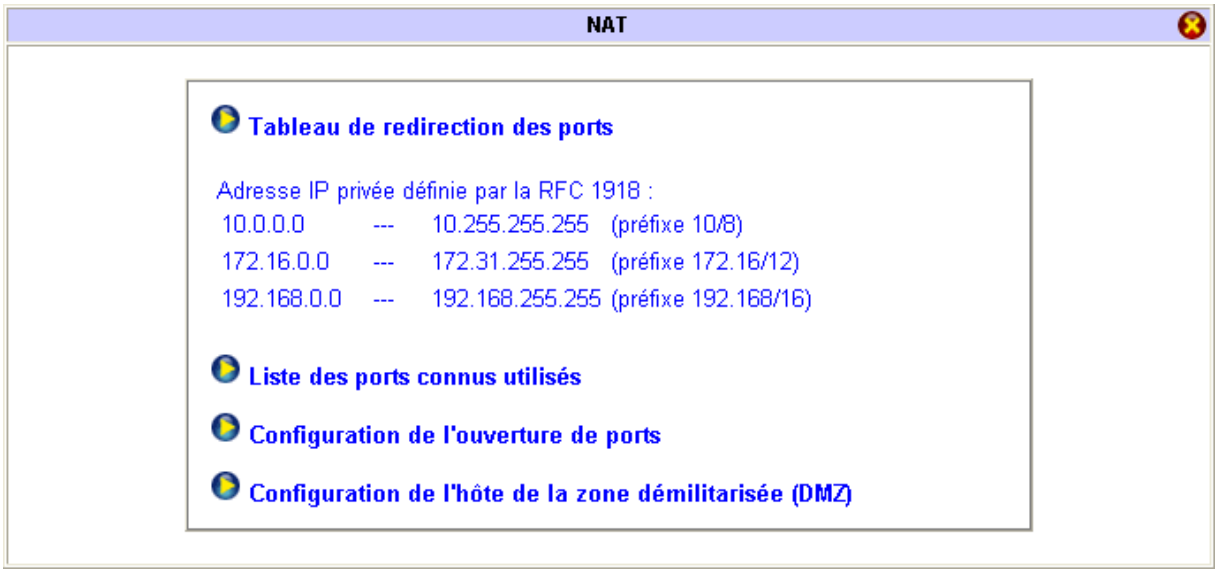
3. Cliquez sur **OK** pour valider.

NAT / Ouverture de ports / DMZ

Translation d'adresses (NAT)

L'utilisation classique du NAT permet de remplacer l'adresse privée des stations du réseau par l'adresse publique attribuée par le fournisseur d'accès au routeur.

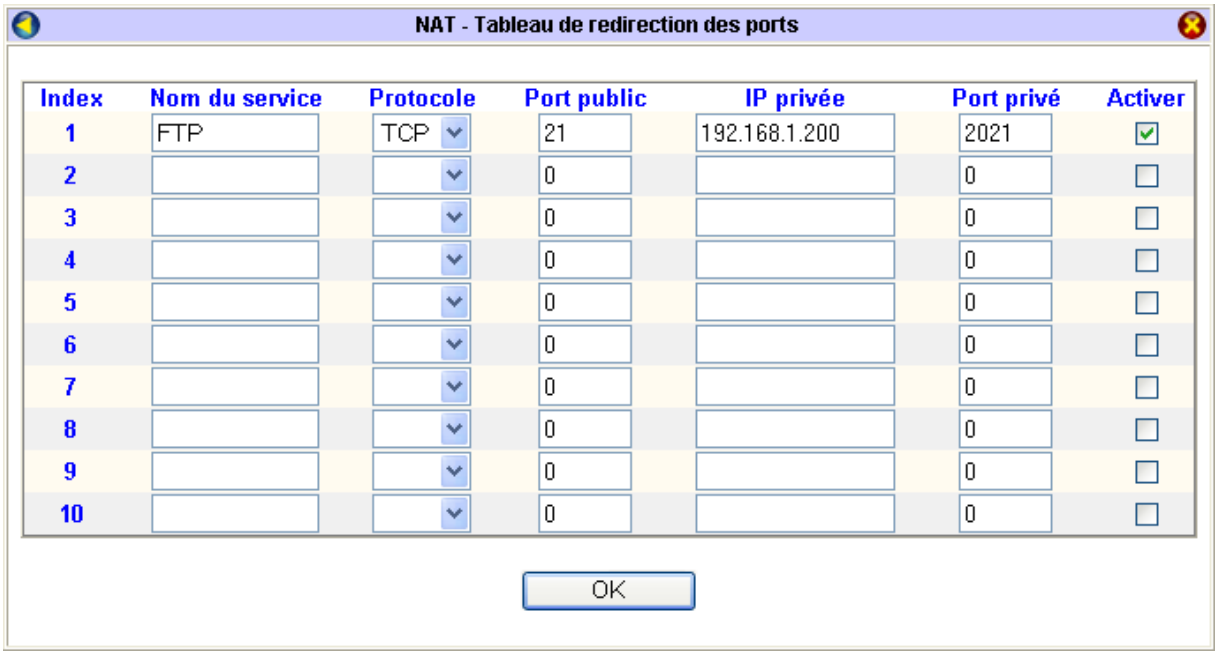
Dans le menu **Réglages Avancés**, cliquez sur **NAT**. L'écran suivant apparaît.



Exposer un serveur sur Internet

Avec certaines applications, vous pouvez utiliser le tableau de redirection des ports afin de permettre l'accessibilité de ces applications à tous les internautes.

L'exemple suivant vous montre un serveur FTP présent sur le LAN et accessible sur Internet. L'adresse du serveur FTP sur le réseau local est « 192.168.1.200 ». Le serveur FTP a été reconfiguré avec un port 2021 (le port standard du service FTP est normalement le port 21).



Le tableau permet la redirection de 10 ports.

Dans la colonne **Nom du service**, saisissez le nom du service concerné par cette redirection de port.

Dans la colonne **Protocole**, indiquez le type de protocole.

Dans la colonne **Port public**, indiquez le port qui doit être redirigé sur le service interne.

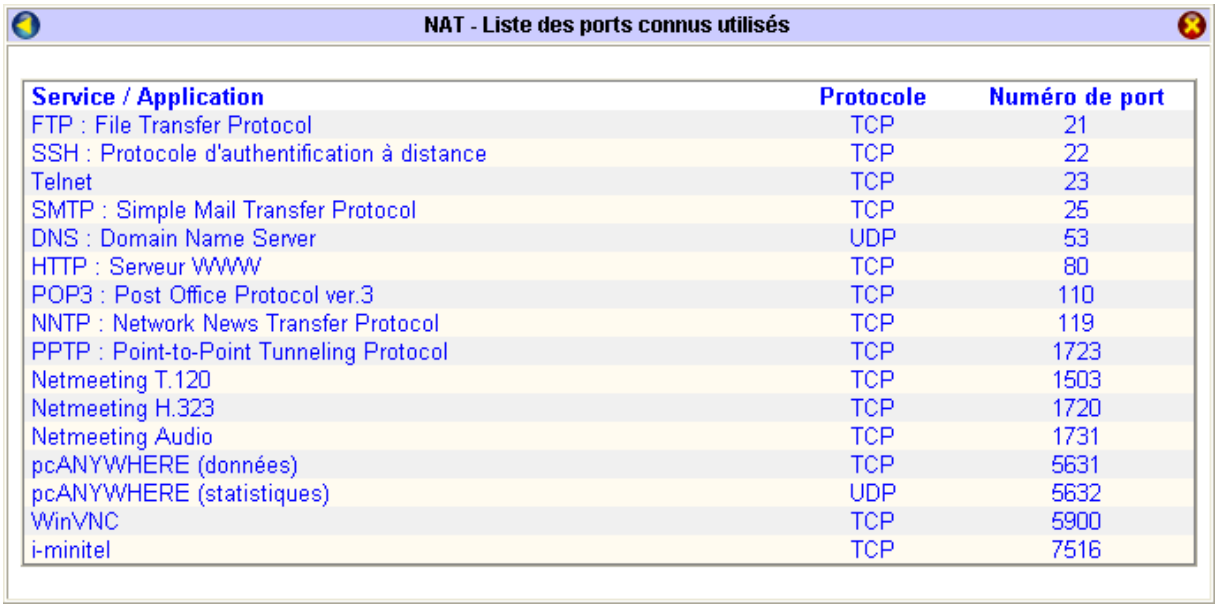
Dans la colonne **IP privée**, indiquez sur quelle adresse privée doit être redirigée la requête.

Dans la colonne **Port privé**, indiquez sur quel port privé doit être redirigée la requête.

Dans la colonne **Activer**, en cochant la case, vous validez la ligne concernée. Cliquez ensuite sur **OK**. Cette redirection de port est activé (le signe « v » est présent dans le tableau de la fenêtre de confirmation).

Tableau des ports les plus connus

Dans le menu **Réglages Avancés**, cliquez sur **NAT**, puis sur **Liste des ports connus utilisés**. Le tableau suivant apparaît, récapitulant le numéro des ports standards par service.



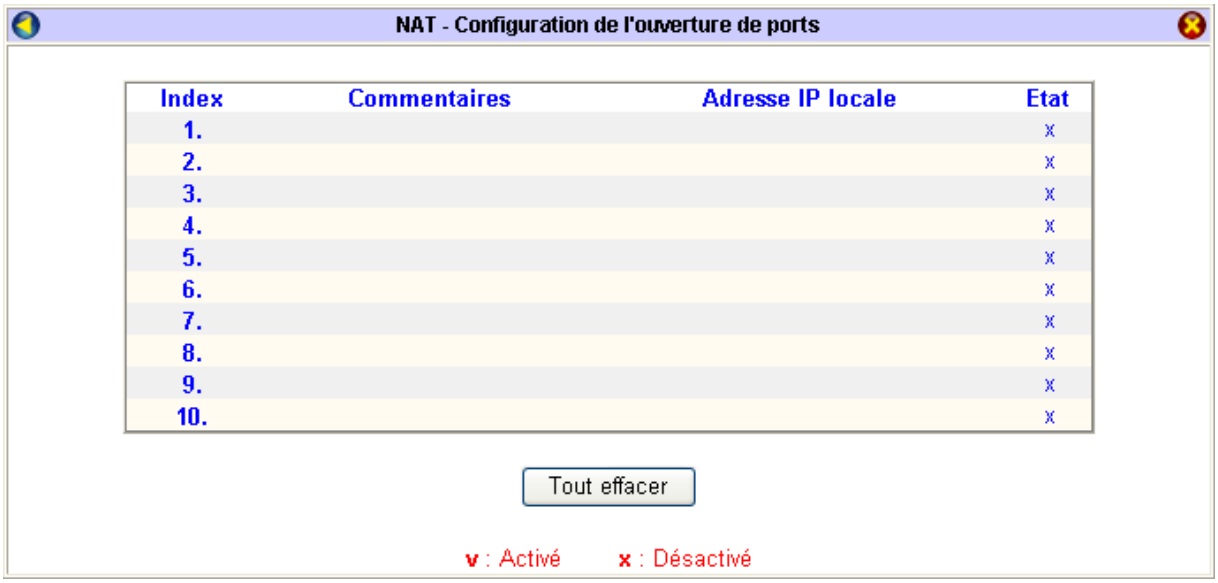
Service / Application	Protocole	Numéro de port
FTP : File Transfer Protocol	TCP	21
SSH : Protocole d'authentification à distance	TCP	22
Telnet	TCP	23
SMTP : Simple Mail Transfer Protocol	TCP	25
DNS : Domain Name Server	UDP	53
HTTP : Serveur WWW	TCP	80
POP3 : Post Office Protocol ver.3	TCP	110
NNTP : Network News Transfer Protocol	TCP	119
PPTP : Point-to-Point Tunneling Protocol	TCP	1723
Netmeeting T.120	TCP	1503
Netmeeting H.323	TCP	1720
Netmeeting Audio	TCP	1731
pcANYWHERE (données)	TCP	5631
pcANYWHERE (statistiques)	UDP	5632
WinVNC	TCP	5900
i-minitel	TCP	7516

Ouverture de ports

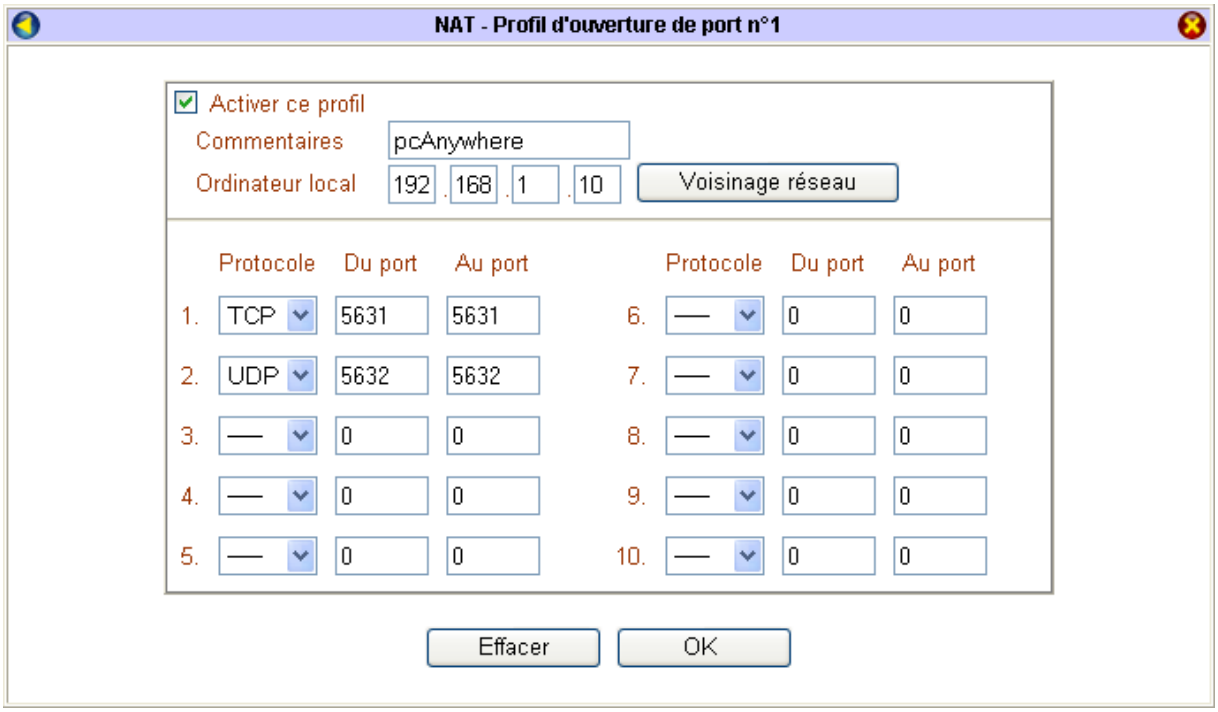
Certaines applications (pcAnywhere, NetMeeting, jeux…) nécessitent l'utilisation de ports spécifiques. Pour que les machines du réseau local (un maximum de 10) aient accès à ces applications, vous pouvez rediriger ces dernières en utilisant l'ouverture de ports si vous connaissez les ports utilisés. Contrairement au NAT, l'ouverture de ports peut s'appliquer à plusieurs ports successifs. Vous pouvez ainsi rediriger un maximum de 10 plages de ports par machine.

Dans l'exemple suivant, afin de documenter cette fonction, nous considérons une machine destinée à être administrée à distance avec l'application pcAnywhere ou WinVNC (référez-vous à la liste des ports connus utilisés page 137).

1. Dans le menu **Réglages Avancés**, cliquez sur **NAT**.
2. Cliquez ensuite sur **Configuration de l'ouverture de ports**.

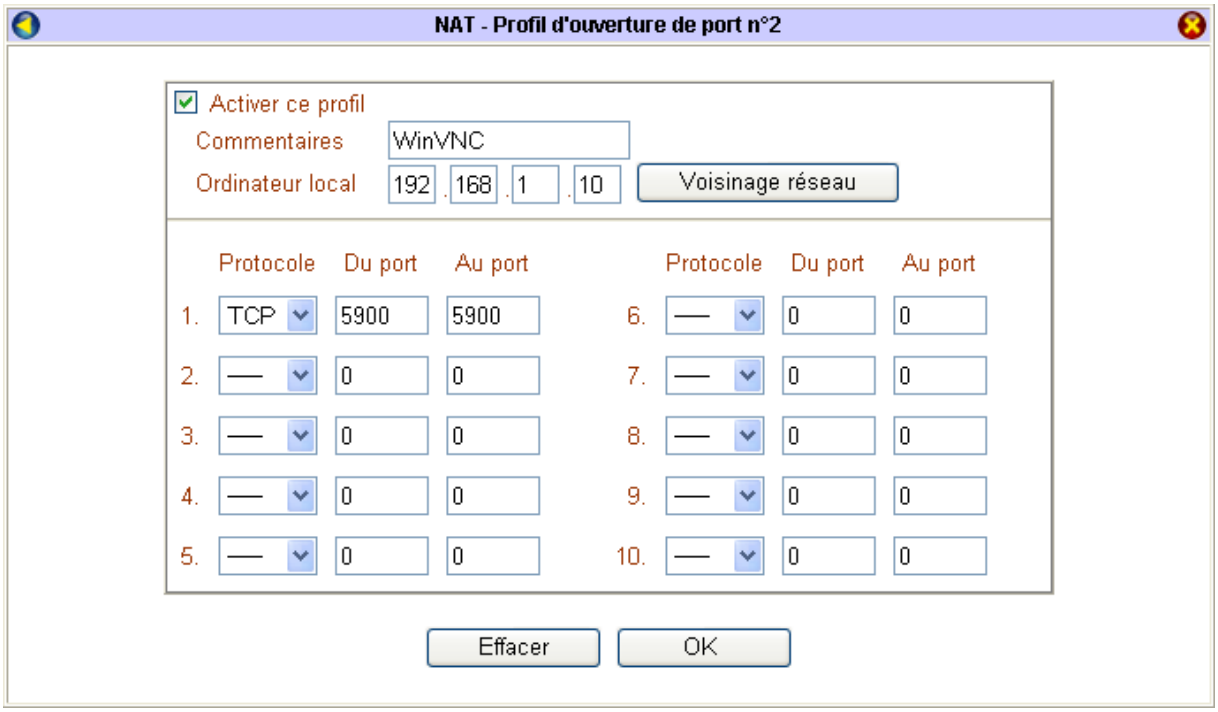


3. Cliquez sur un numéro dans la colonne **Index**.
4. Dans l'écran suivant, cochez **Activer ce profil**.

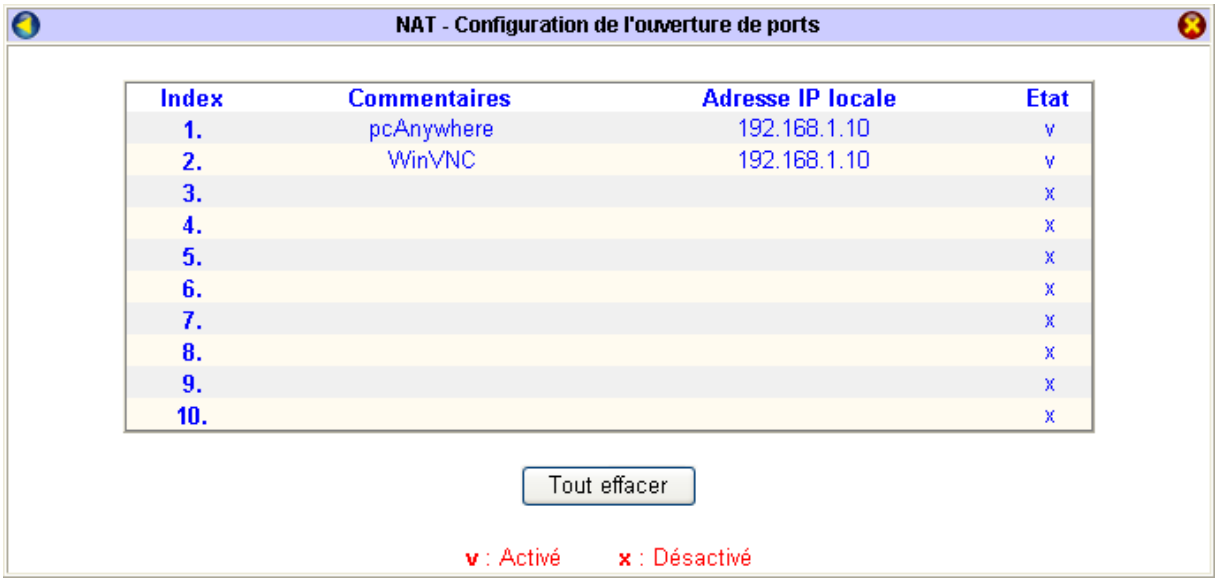


5. Dans la rubrique **Commentaires**, entrez une information qui vous permettra d'identifier l'objet de ce profil.

6. Cliquez ensuite sur **Voisinage réseau**, puis sélectionnez l'adresse IP de la machine sur laquelle sera dirigée l'ouverture de ports.
7. Indiquez les ports utilisés et le protocole associé.
8. Cliquez sur **OK** afin de valider le profil.
9. Effectuez la même opération pour l'application WinVNC.



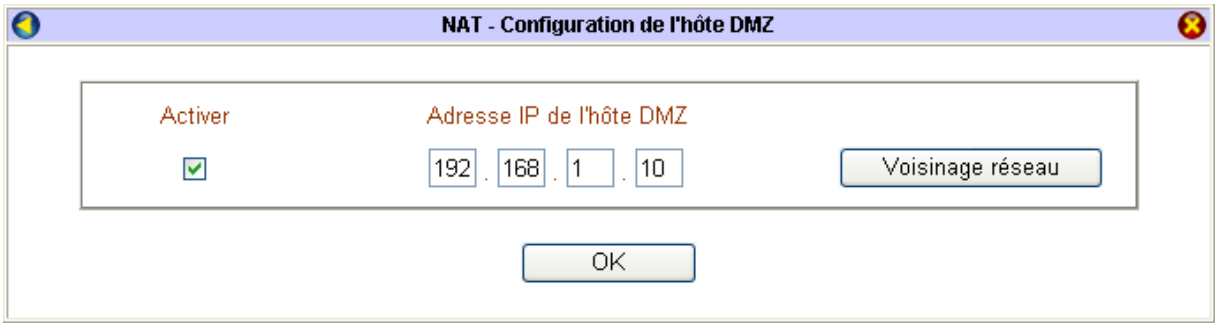
10. Dans la colonne **Etat**, « v » signifie que l'ouverture de ports concernée est activée.



DMZ

Si les applications utilisent des ports inconnus ou non standards, on utilisera la zone DMZ. Celle-ci vous permet d'ouvrir tous les ports non définis précédemment (NAT ou ouverture de ports) vers une seule machine du réseau local. La DMZ vous permet d'exposer une machine sur Internet sans restriction d'utilisation des ports.

1. Dans le menu **Réglages Avancés**, cliquez sur **NAT**.
2. Cliquez ensuite sur **Configuration de l'hôte de la zone démilitarisée (DMZ)**.
3. Cochez **Activer**.
4. Cliquez sur **Voisinage réseau**, puis sélectionnez l'adresse IP de la machine sur laquelle sera utilisée l'application.
5. Cliquez sur **OK** pour valider.



6. Après avoir lancé l'application sur la machine hôte, dans le menu **Diagnostics**, cliquez sur **Etat du trafic** afin de connaître les ports utilisés par l'application. En effet, le routeur redirige tous les ports non définis.

Vous pouvez de cette manière spécifier ces ports dans l'ouverture de ports après avoir désactivé la DMZ. Ceci vous permet d'optimiser la sécurité en n'ouvrant que les ports nécessaires à l'application.

Remarque sur une autre utilisation de la DMZ :

Si vous souhaitez utiliser un logiciel firewall pour constater les différentes tentatives d'intrusions sur le réseau local, installez tout d'abord ce logiciel sur une des machines du réseau, puis configurez ensuite cette machine en hôte DMZ. De cette manière, toutes les tentatives d'accès sur des ports non standards ne seront pas bloquées par le routeur, mais redirigées sur la machine DMZ.

Gestion des plages horaires

Le VPN Booster vous permet de gérer les heures de connexion Internet.

Vous pouvez spécifier des plages horaires pendant lesquelles vous interdisez ou autorisez au routeur la connexion vers l'extérieur.

Réglage de l'heure du routeur

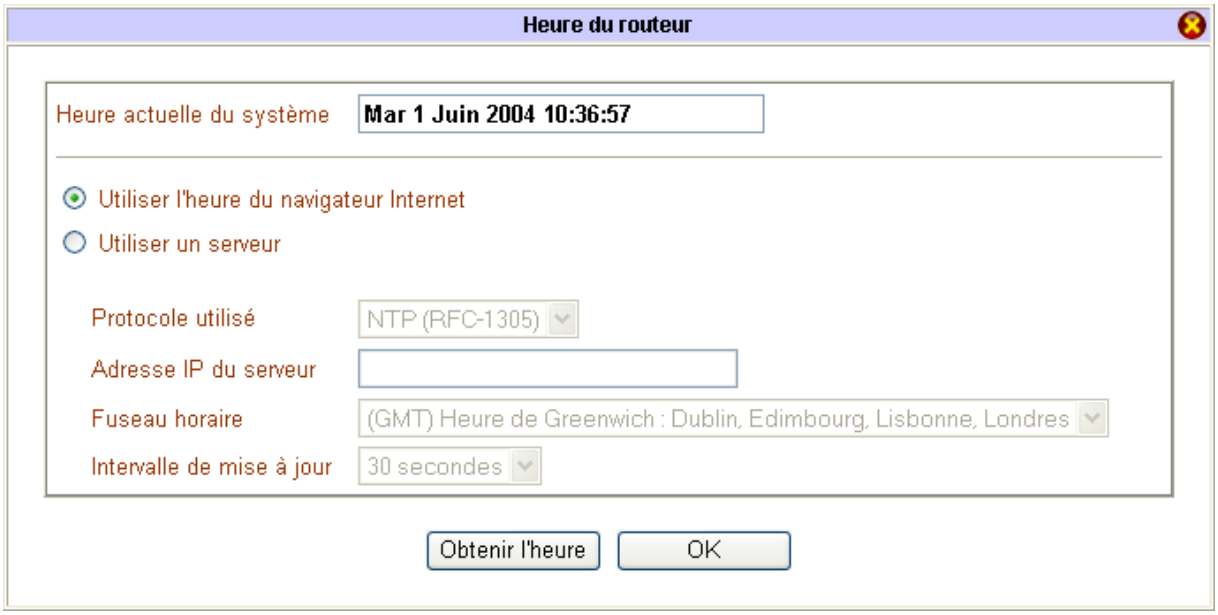
Attention :

- *Les données concernant l'heure du routeur seront effacées en cas de redémarrage. N'oubliez pas de régler l'heure du routeur à chaque redémarrage afin que les plages horaires activées soient correctement prises en compte.*
- *Le passage à l'heure d'été n'est pas pris en compte par le routeur. Si vous sélectionnez* ***Utiliser un serveur*** *afin de régler l'heure, choisissez alors un fuseau horaire en GMT+02:00.*

1. Dans le menu **Réglages Avancés**, cliquez sur **Heure du routeur**.
2. Cliquez ensuite sur **Obtenir l'heure**.

- Si vous sélectionnez **Utiliser l'heure du navigateur Internet**, l'heure prise en compte sera celle du PC d'administration sur lequel le navigateur est utilisé.
- Si vous sélectionnez **Utiliser un serveur**, le routeur va chercher l'heure sur une machine du réseau local sur laquelle est installé un logiciel serveur NTP (Network Time Protocol). Ce logiciel (non fourni sur le CD-ROM) se connecte sur des sites afin de récupérer l'heure.
  - ✓ Dans la rubrique **Adresse IP du serveur**, saisissez l'adresse IP de l'ordinateur dédié sur lequel est installé le logiciel serveur NTP.
  - ✓ Indiquez le fuseau horaire dans la rubrique correspondante.
  - ✓ Dans la rubrique **Intervalle de mise à jour**, indiquez le délai de récupération de l'heure entre le routeur et l'ordinateur dédié.

  Remarque : nous vous conseillons d'installer le logiciel NTP sur une machine allumée en permanence.

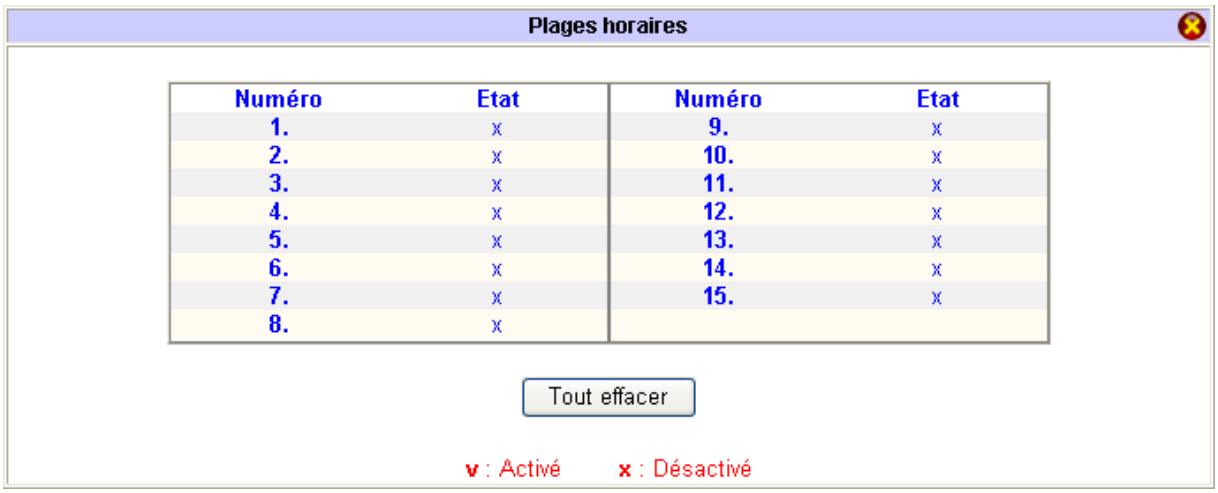


3. Cliquez sur **OK** pour valider les paramètres de l'heure.

Paramétrage des plages horaires

Toutes les plages horaires que vous allez désormais configurer, puis activer, vont prendre comme référence l'heure du routeur que vous venez de paramétrer dans la section précédente.

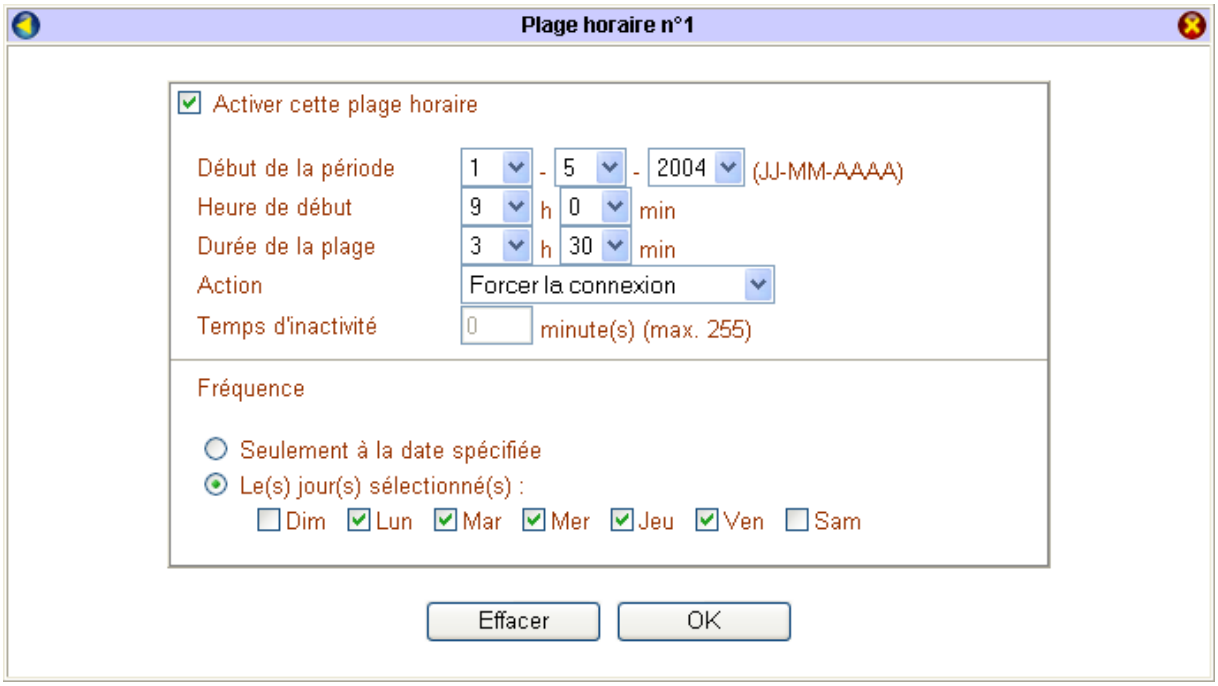
1. Dans le menu **Réglages Avancés**, cliquez sur **Plages horaires**. L'écran suivant apparaît.



2. Cliquez sur un numéro dans la colonne **Numéro** et renseignez les rubriques dans la nouvelle fenêtre.

   Remarques : le VPN Booster vous permet de paramétrer jusqu'à 15 plages horaires. Cependant, vous ne pourrez attribuer que 4 plages horaires à chaque type de connexion.

3. Cochez **Activer cette plage horaire**.



4. Dans la rubrique **Début de la période**, indiquez la date à partir de laquelle la plage horaire devra être prise en compte par le routeur.
5. Indiquez ensuite l'heure de début ainsi que la durée de la plage horaire.

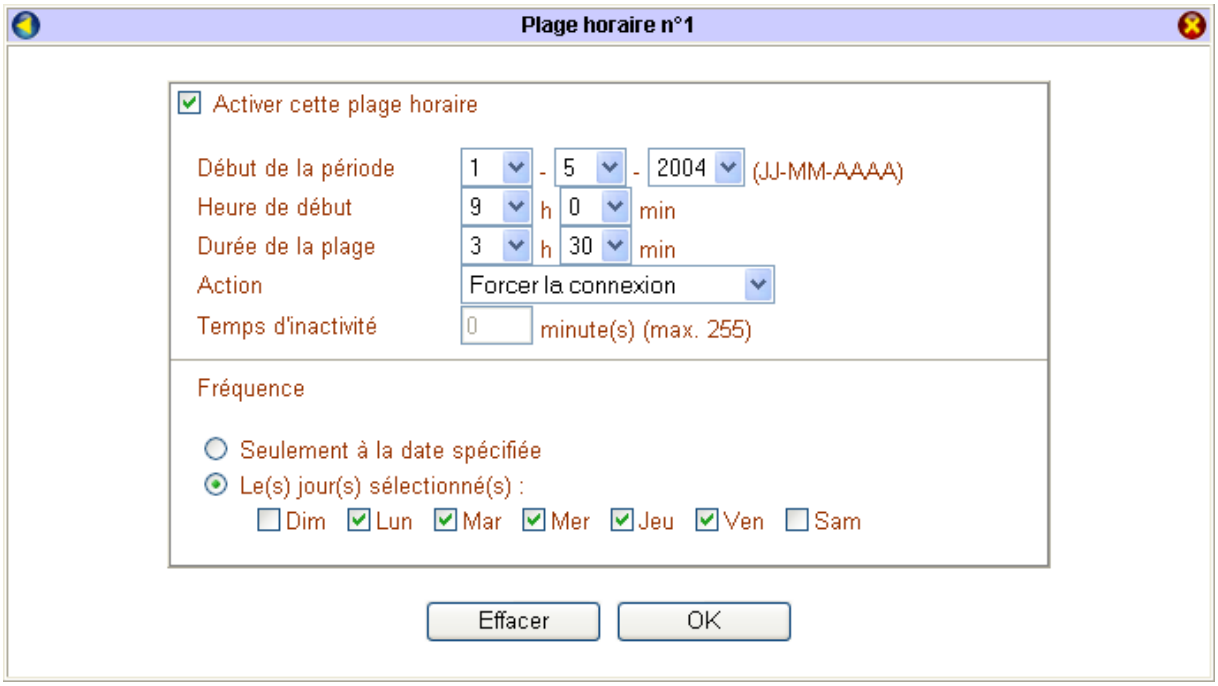
6. Dans la rubrique **Action**, indiquez quelle action la connexion doit avoir cette plage horaire. Vous avez le choix parmi 4 possibilités :
   - **Forcer la connexion** : autorise la connexion suivant les heures établies.
   - **Forcer la déconnexion** : interdit la connexion suivant les heures établies.
   - **Activer à la demande** : autorise les connexions si une requête est envoyée. La connexion reste ensuite active en fonction du temps d'inactivité indiqué dans la rubrique correspondante.
   - **Désactiver à la demande** : si une connexion est déjà en cours, autorise la poursuite de la connexion tant que le trafic est permanent. En revanche, une fois le délai d'inactivité dépassé, toute reconnexion est impossible.
7. Sélectionnez ensuite la fréquence.
   - Si vous désirez que la prise en compte de la plage horaire soit ponctuelle, sélectionnez **Seulement à la date spécifiée**.
   - Si vous désirez que cette plage horaire s'applique à plusieurs jours, sélectionnez **Le(s) jour(s) sélectionné(s)**, puis cochez ceux qui seront concernés.
8. Cochez ensuite sur **OK** afin de valider cette plage horaire.

Exemple de paramétrage de plages horaires

Nous prenons l'exemple d'une société qui ne désire autoriser l'accès à Internet via ADSL que pendant ses heures d'ouverture : de 9h00 à 12h30 et de 14h-18h30 sur cinq jours, du lundi au vendredi.

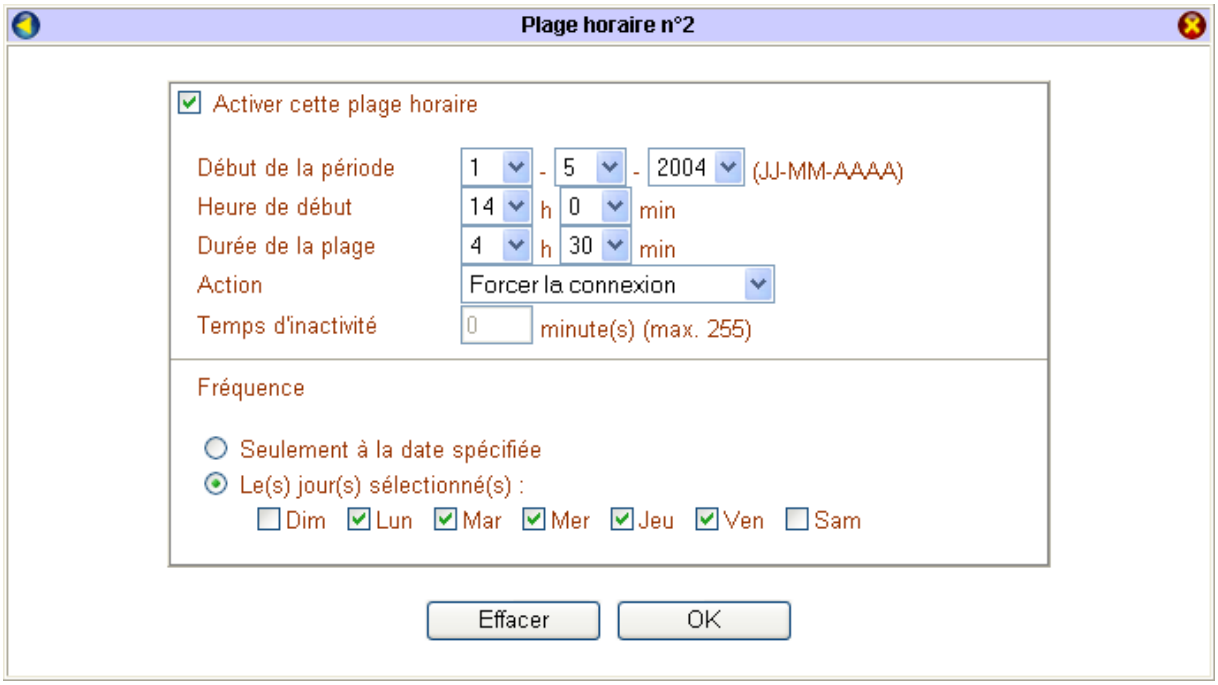
Plage horaire n°1 : Activer la plage horaire, puis sélectionnez **Forcer la connexion** pour autoriser la connexion de 9h00 à 12h30.

Cochez les jours concernés par le paramétrage, puis cliquez sur **OK** afin de valider l'information.



Plage horaire n°2 : Activer la plage horaire, puis sélectionnez **Forcer la connexion** pour autoriser la connexion de 14h00 à 18h30.

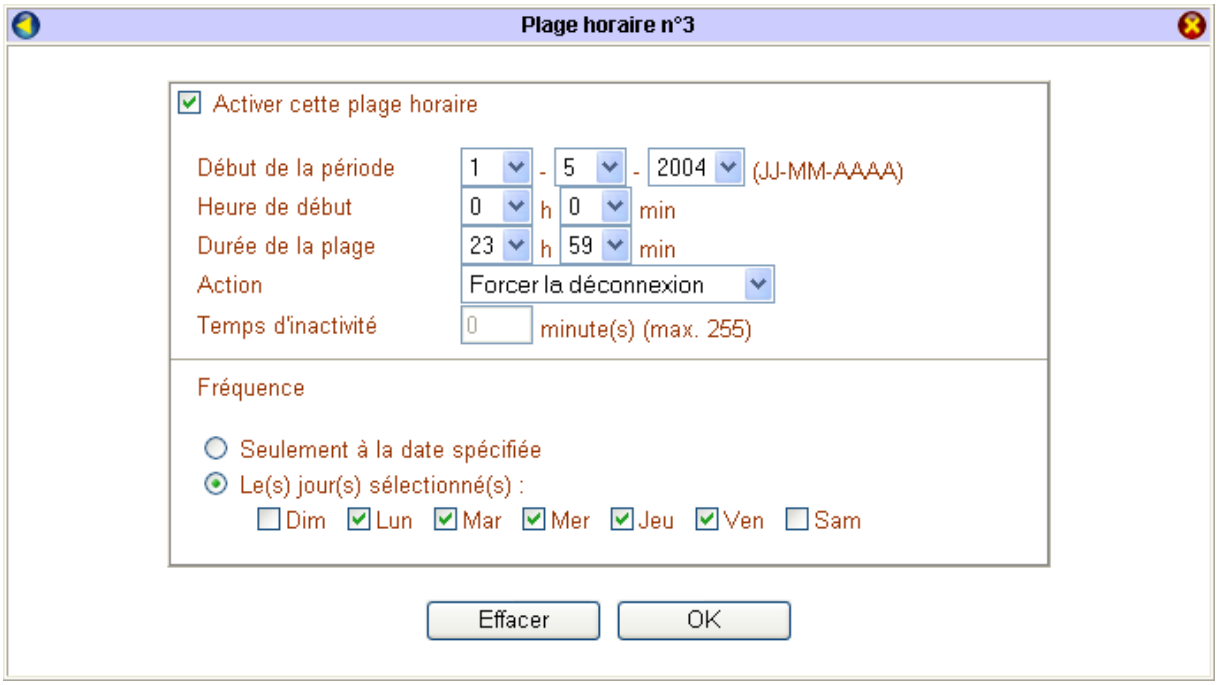
Cochez les jours concernés par le paramétrage, puis cliquez sur **OK** afin de valider l'information.



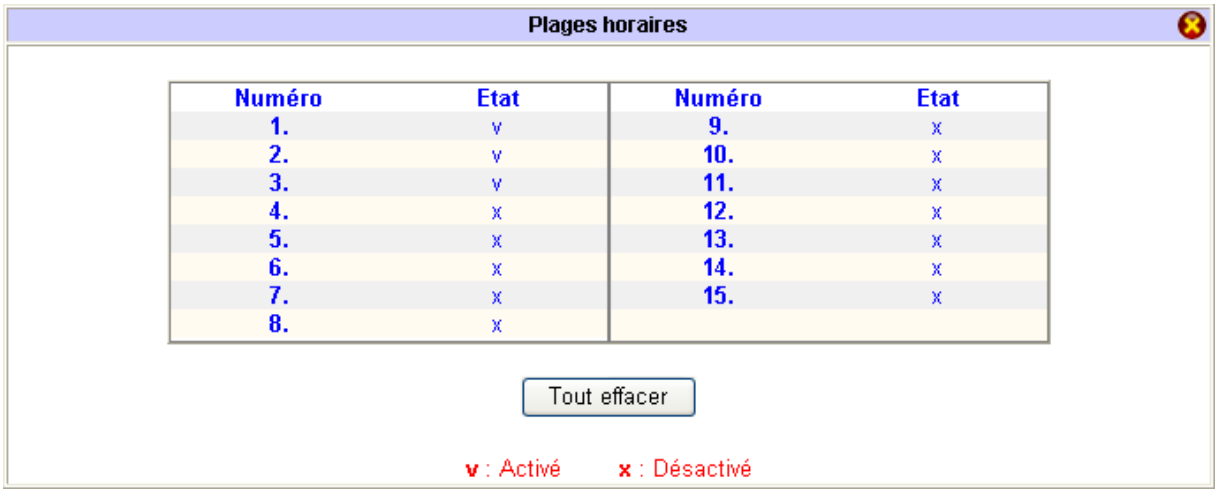
Plage horaire n°3 : Activer la plage horaire, puis sélectionnez **Forcer la déconnexion** pour interdire la connexion pendant les autres périodes de la journée c'est-à-dire de 00h00 à 8h59, de 12h31 à 13h59 et de 18h31 à 23h59.

Cochez les jours concernés par le paramétrage, puis cliquez sur **OK** afin de valider l'information.

Remarque : cela concerne également le samedi et le dimanche.

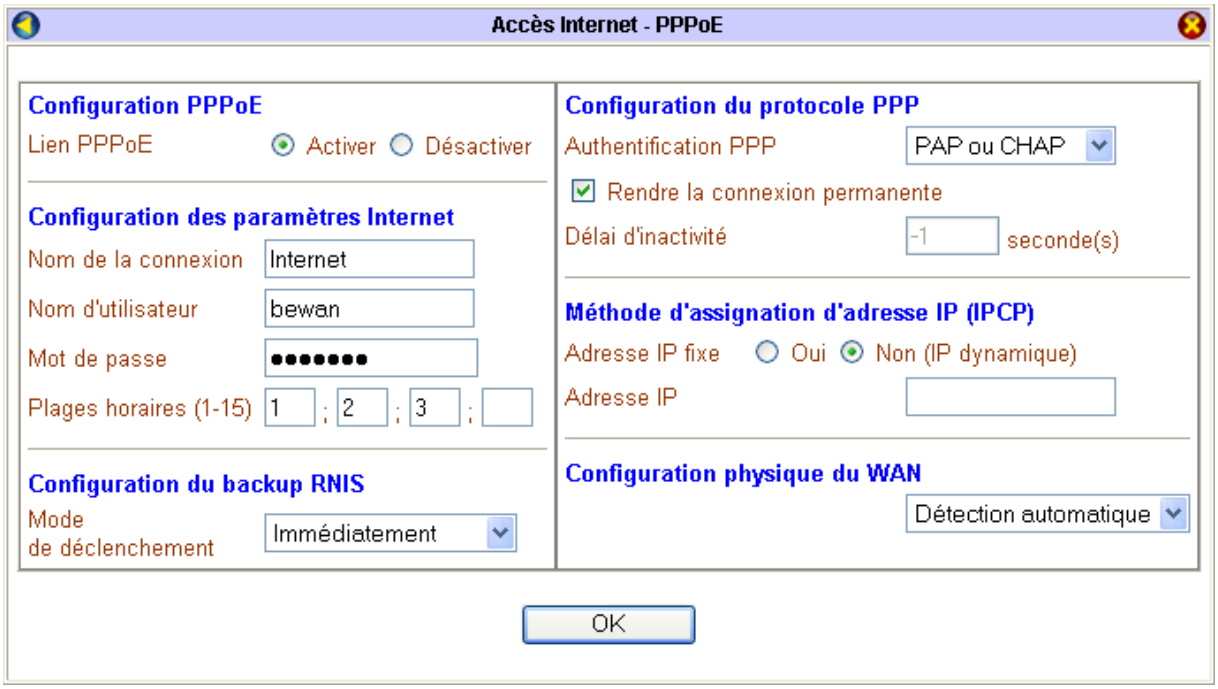


Dans la colonne **Etat**, « v » signifie que les plages horaires concernées sont activées.



Il vous suffit ensuite de retourner dans la fenêtre des paramètres de votre connexion Internet. Dans les rubriques **Plages horaires (1-15)**, saisissez les numéros des plages horaires que vous désirez attribuer à votre connexion.

Attention : veillez toujours à saisir le numéro de la plage la plus restrictive en dernier, en l'occurrence la plage n°3 dans notre exemple.



Paramétrage du DNS Dynamique

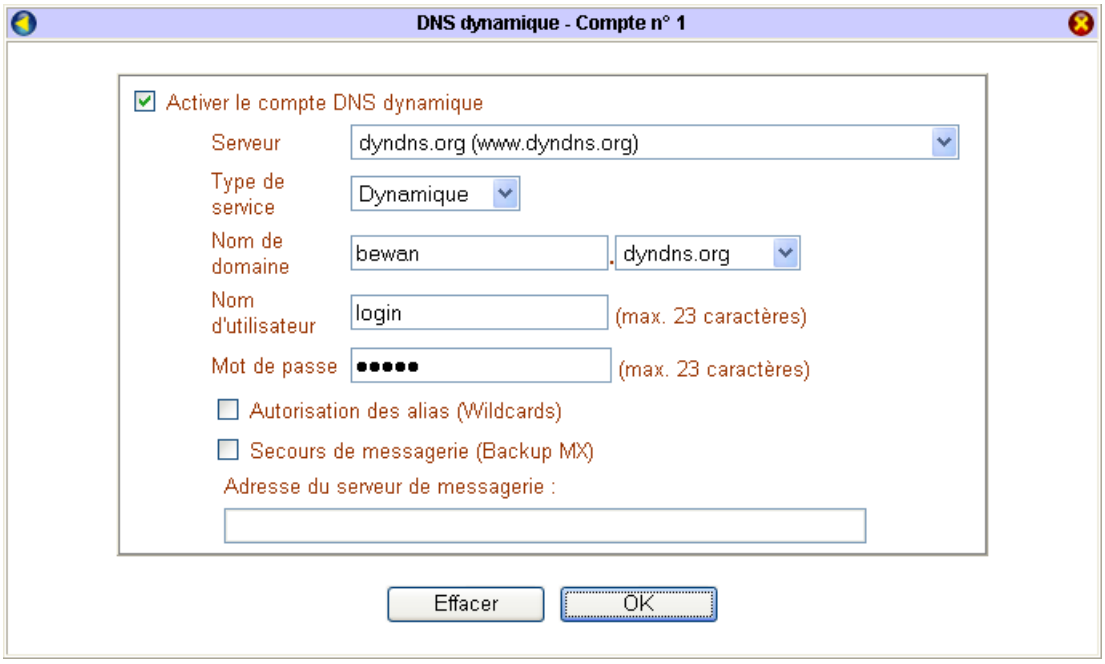
La fonction DNS dynamique vous permet d'obtenir un nom de domaine qui pointe en permanence vers votre machine lorsqu'elle est connectée à Internet. Le DNS dynamique fait donc correspondre un nom de domaine constant avec une adresse IP variable. Si vous utilisez une adresse IP dynamique, cela vous offre ainsi un accès permanent aux ressources utilisées via le routeur (applications serveur qui passent derrière le routeur : serveur FTP, serveur web, serveur de messagerie…).

Au préalable, avant de procéder au paramétrage du DNS dynamique via l'interface du routeur, vous devez avoir ouvert un compte chez un des fournisseurs de noms de domaine dynamique actuellement supportés par le routeur. Ce compte une fois ouvert vous permettra de créer un lien dynamique entre le nom de domaine et l'adresse IP obtenue lors de chacune de vos connexions. Cela évite ainsi de fournir à chaque fois son adresse IP à un correspondant qui veut se connecter en ftp ou http par exemple sur votre serveur.

Il suffit ensuite de remplacer l'adresse IP par le nom « bewan.dyndns.org » par exemple, pour obtenir directement la connexion.

Activation du DNS dynamique

1. Dans le menu **Réglages Avancés**, cliquez sur **DNS dynamique**.
2. Dans la colonne **Comptes**, cliquez sur l'un des trois numéros.
3. Dans la fenêtre de paramétrage du compte, cochez **Activer le compte DNS dynamique**.
4. Dans la rubrique **Serveur**, sélectionnez un nom de serveur correspondant à celui que vous avez choisi lorsque vous avez ouvert un compte.
5. Dans la rubrique **Nom de domaine**, saisissez le nom choisi lors de la création de votre compte.
6. Saisissez ensuite le nom d'utilisateur que vous avez choisi ainsi que le mot de passe fourni par dyndns.org (dans notre exemple) sauf si vous avez modifié ce mot de passe.

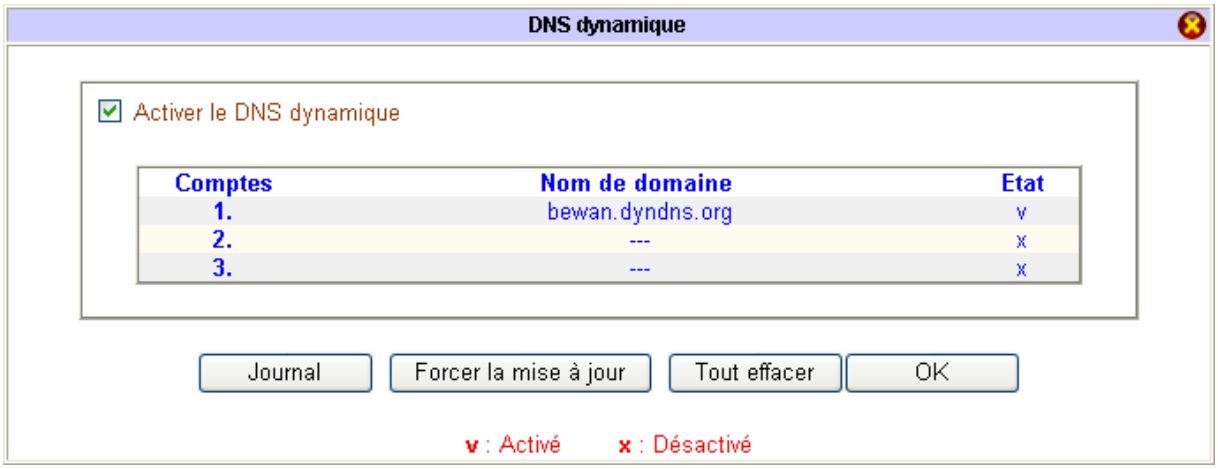


Remarques :

- *La rubrique **Autorisation des alias (Wildcards)** vous permet de rendre votre nom de domaine accessible même si vous ajoutez un alias (ex. : dupont@bewan.dyndns.org). Cela peut notamment se révéler utile si vous avez un serveur de messagerie derrière le routeur.*
- *Les rubriques **Secours de messagerie (Backup MX)** et **Adresse du serveur de messagerie** ne sont valables que si vous avez souscrit une donation auprès du serveur.*

7. Cliquez sur **OK** afin d'activer ce compte.

8. Votre compte est activé mais vous devez désormais activer la fonction même du DNS dynamique. Après avoir coché **Activer le DNS dynamique**, cliquez de nouveau sur **OK**.

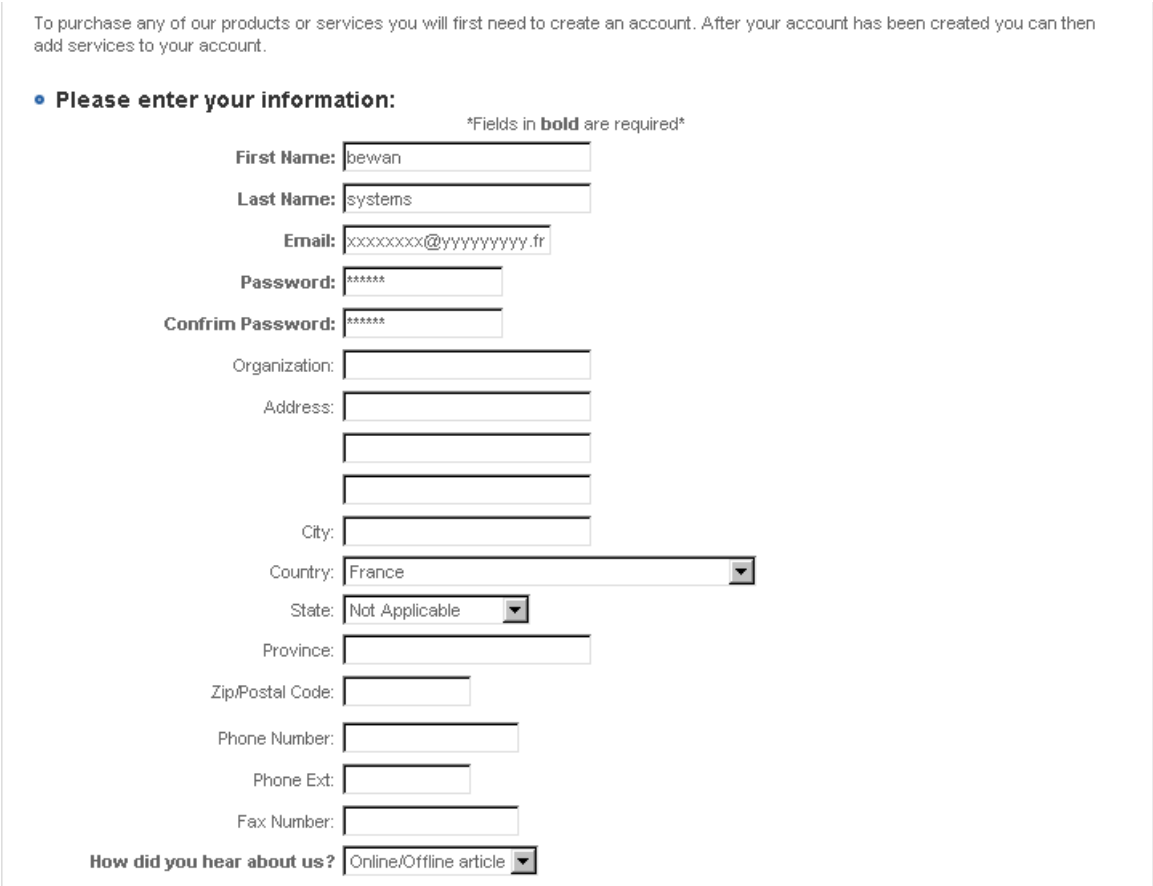


*Remarque : si vous cliquez sur le bouton **Journal**, vous pouvez vérifier que la mise à jour a bien été effectuée.*

Exemples de création de comptes DNS dynamiques

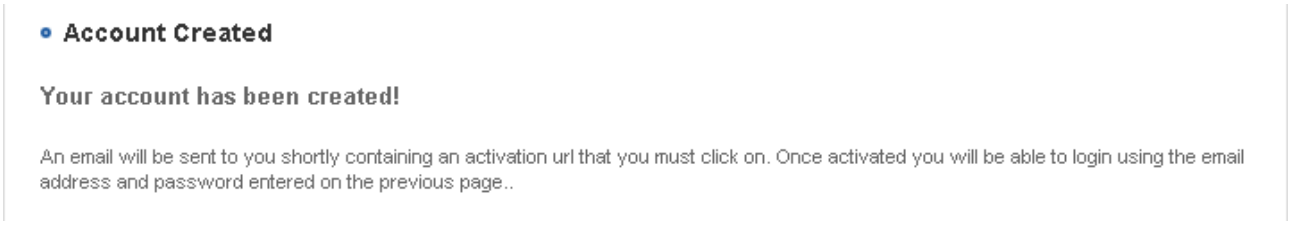
Ouvrir un compte sur no-ip.com

1. Connectez-vous sur le site http://www.no-ip.com
2. Une fois sur la page d'accueil, cliquez sur **Sign up Free!**.
3. Renseignez les champs obligatoires affichés en gras. Il vous faut bien sûr indiquer une adresse e-mail valide.

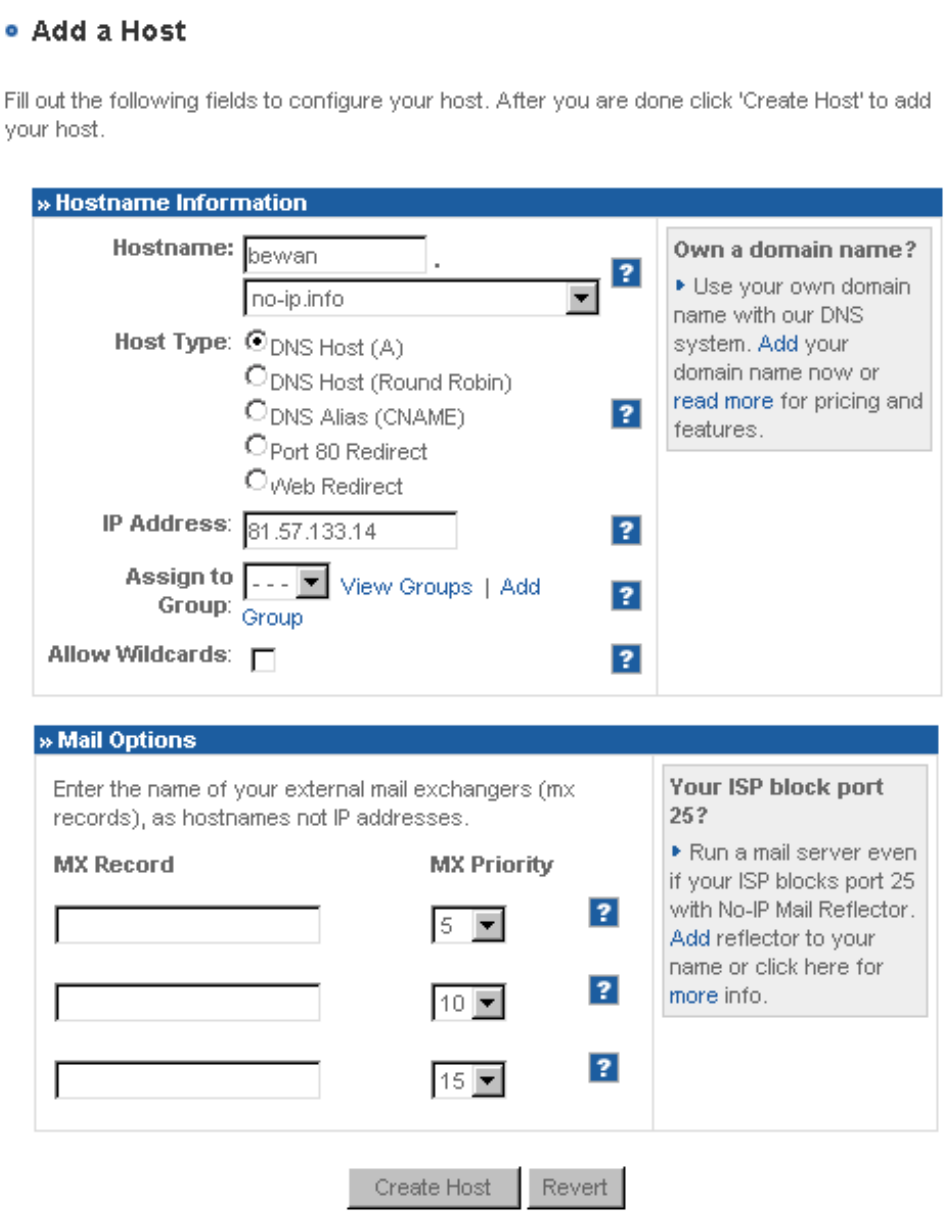


4. Cliquez sur le bouton **SIGN UP NOW**.

5. Un écran vous confirme que l'enregistrement du compte utilisateur a bien été validé. No-IP.com envoie un message à l'adresse email indiquée.

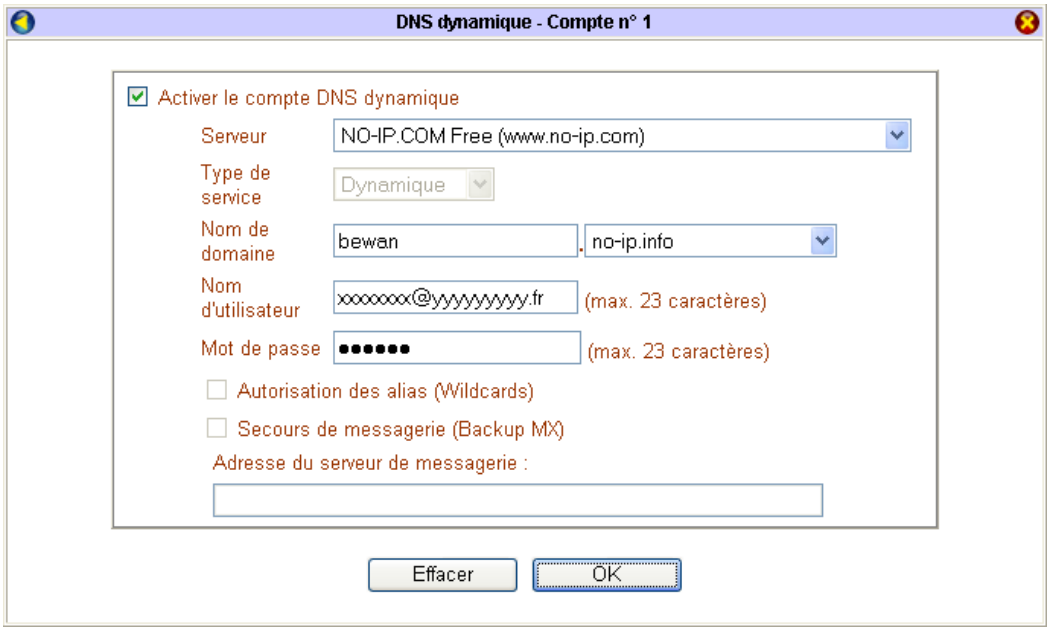


6. Une fois connecté sur votre messagerie, activez ensuite votre compte. Retournez ensuite sur la page d'accueil afin de vous authentifier.
7. Dans le menu de gauche, saisissez votre adresse e-mail, puis votre mot de passe. Cliquez alors sur **Login**.
8. Toujours dans le menu de gauche, dans la rubrique **Hosts / Redirects**, cliquez maintenant sur **Add** afin de créer un nom de domaine : bewan.no-ip.info. Attention : avant de choisir l'extension du nom de domaine, assurez-vous qu'elle soit implémentée sur votre routeur.

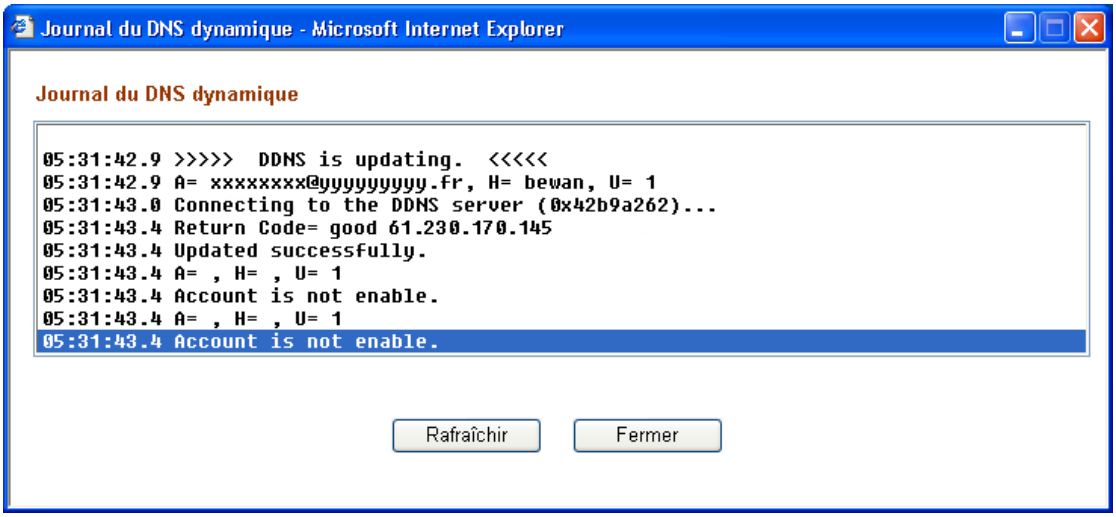


9. L'adresse IP qui apparaît correspond à l'adresse IP de la connexion Internet que vous utilisez actuellement. Inutile de s'en préoccuper pour l'instant. Cliquez sur **Create Host**.

10. Dans le menu **Configuration Elémentaire** du routeur, cliquez sur **LAN TCP/IP et serveur DHCP**. Renseignez les champs **Serveur DNS** en indiquant les DNS du FAI.
11. Dans le menu **Réglages Avancés**, cliquez sur **DNS dynamique**.
12. Cliquez sur un compte disponible, puis cochez **Activer le compte DNS dynamique**.
13. Indiquez ensuite :
    - le Serveur utilisé (**no-ip.com**)
    - le Nom de domaine (**bewan**) et l'extension **no-ip.info**
    - le Nom d'utilisateur et le Mot de passe : adresse e-mail que vous avez utilisée pour vous inscrire sur le site no-ip et le mot de passe.



14. Cliquez sur **OK** afin d'activer ce compte.
15. Dans la fenêtre de paramétrage du compte, cochez **Activer le DNS dynamique**, puis cliquez de nouveau sur **OK**.
16. Il est possible de **Forcer la mise à jour** et de vérifier, grâce au **Journal**, que la mise à jour s'est bien effectuée. Les deux messages *"Account is not enable"* correspondent aux deux comptes (2 et 3) qui ne sont pas renseignés.



Remarques :

- *"A" représente le nom d'utilisateur et "H" le nom de domaine sans l'extension.*
- *Si le message "Http request error" s'affiche, vérifiez que les DNS ont bien été saisis sur le routeur.*

17. Vous pouvez maintenant :
    - Soit effectuer un ping sur bewan.no-ip.info afin de retrouver l'adresse IP de la connexion Internet du routeur,
    - Soit utiliser le compte bewan.no-ip.info.

Ouvrir un compte sur dyndns.org

1. Connectez-vous sur le site http://www.dyndns.org
2. Une fois sur la page d'accueil, cliquez sur **Sign Up Now**.
3. Lisez les informations, puis cochez la case **I have read and agree to the Acceptable Use Policy above**.
4. Renseignez les champs suivants :
    - **Username** : saisissez un nom d'utilisateur.
    - **E-mail Address** : indiquez votre adresse e-mail, puis confirmez cette adresse.
    - **Password** : indiquez votre mot de passe, puis confirmez-le.
5. Cliquez sur le bouton **Create Account**.
6. Connectez-vous ensuite sur votre messagerie et allez sur l'adresse URL indiquée dans le message transmis par dyndns.org.
7. Saisissez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **Login**.
8. Cliquez sur l'onglet **Services**, sur **Dynamic DNS**, puis sur **Add Host**.
9. Choisissez un nom de domaine, puis cliquez sur le bouton **Add Host**.

    Remarque : le nom de domaine est composé d'un nom d'hôte que vous avez choisi et d'un nom de serveur répertorié dans la liste des adresses. Avant de choisir l'extension du nom de domaine, assurez-vous qu'elle soit implémentée sur votre routeur. Voici un exemple de nom de domaine : bewan.dyndns.org
10. Reportez vos paramètres dans la partie du routeur consacrée au paramétrage du DNS dynamique.

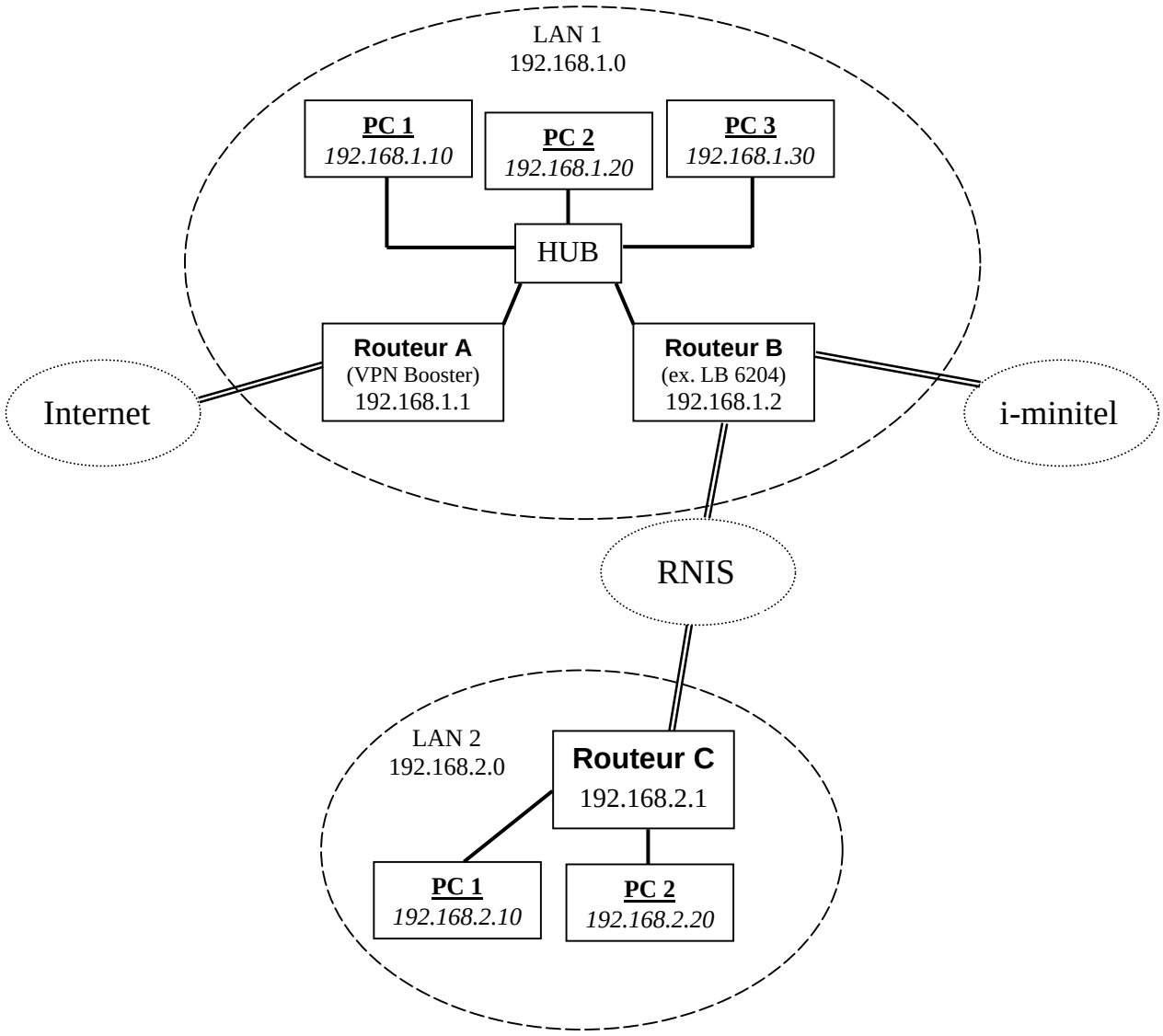
Paramétrage des routes statiques

L'implémentation des routes statiques permet de spécifier un chemin et ainsi d'orienter des paquets IP vers différentes passerelles capables de joindre les réseaux de destination souhaités. Si votre réseau comporte au minimum 3 passerelles (routeurs, serveurs NT,…), il vous est alors possible d'établir des routes statiques. Sont nécessaires :

- une passerelle par défaut (en général la passerelle qui permet l'accès Internet) ; c'est aussi le routeur sur lequel va être implémentée la route statique,
- une passerelle intermédiaire par laquelle vont transiter les paquets et qui va les envoyer vers la passerelle de destination,
- une passerelle de destination.

Sur le VPN Booster, vous pouvez paramétrer jusqu'à 10 routes statiques.

Nous allons illustrer cette section en prenant pour référence le type de configuration suivant. A noter dans l'exemple, que toutes les passerelles sont en réseau de classe C.



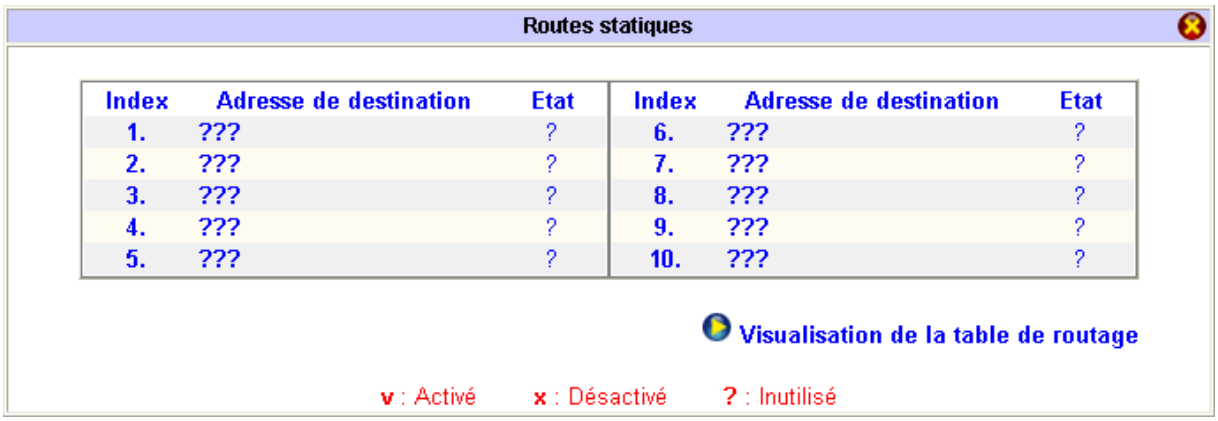
A partir du routeur A (VPN Booster), nous désirons :

- accéder au LAN 2 ;
- faire de l'i-minitel au travers du routeur B.

Remarques préalables :

- *Des fiches d'interconnexion (sur les routeurs B et C) doivent être paramétrées.*
- *Sur les PC du LAN 1, vous devez déclarer le routeur A comme passerelle par défaut.*

1. Dans le menu **Réglages Avancés**, cliquez sur **Routes statiques**. L'écran suivant apparaît.



2. Pour paramétrer une route, cliquez sur une adresse de destination (si la route n'a pas encore été paramétrée, dans la colonne **Etat**, le signe « **?** » apparaît, indiquant qu'elle est encore disponible).
3. Vous allez paramétrer la première route statique : le routeur A va pouvoir accéder au routeur C.

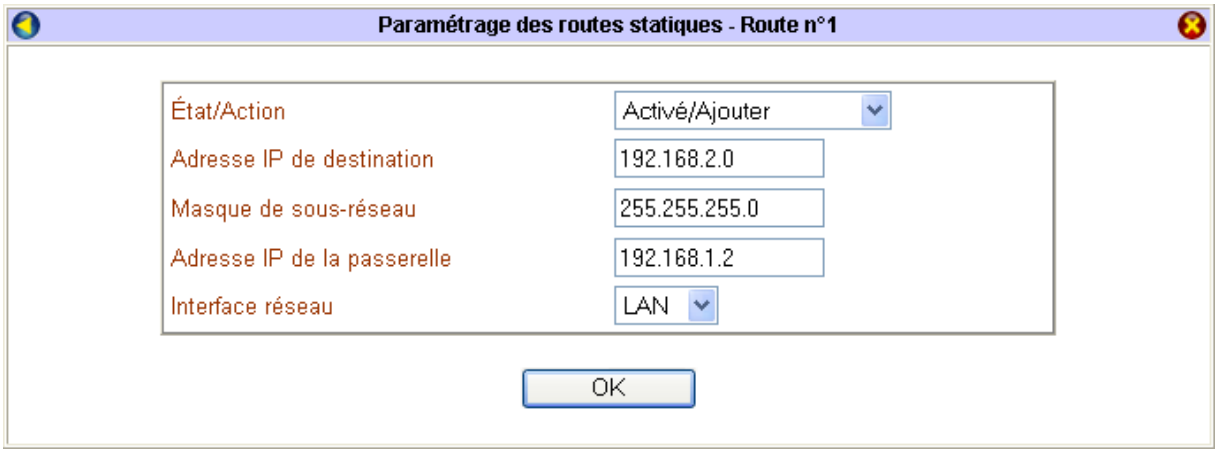
   Dans la rubrique **Etat/Action**, sélectionnez l'option **Activé/Ajouter**.

   Remarques :

   - *L'option **Vide/Effacer** vous permet de supprimer une route statique déjà existante. Cliquez sur **OK**.*
   - *L'option **Désactivé/Désactiver** vous permet de désactiver provisoirement une route statique. Cliquez sur **OK**.*

   Dans la rubrique **Adresse IP de destination**, spécifiez l'adresse du réseau auquel vous voulez accéder. Dans notre exemple, nous désirons accéder au LAN 2, donc à l'adresse réseau 192.168.2.0. Indiquez également le masque de sous-réseau correspondant.

   Dans la rubrique **Adresse IP de la passerelle**, spécifiez l'adresse du routeur qui va faire le lien avec le réseau de destination. Dans notre exemple, pour accéder au LAN 2, nous allons mettre le routeur B en passerelle.

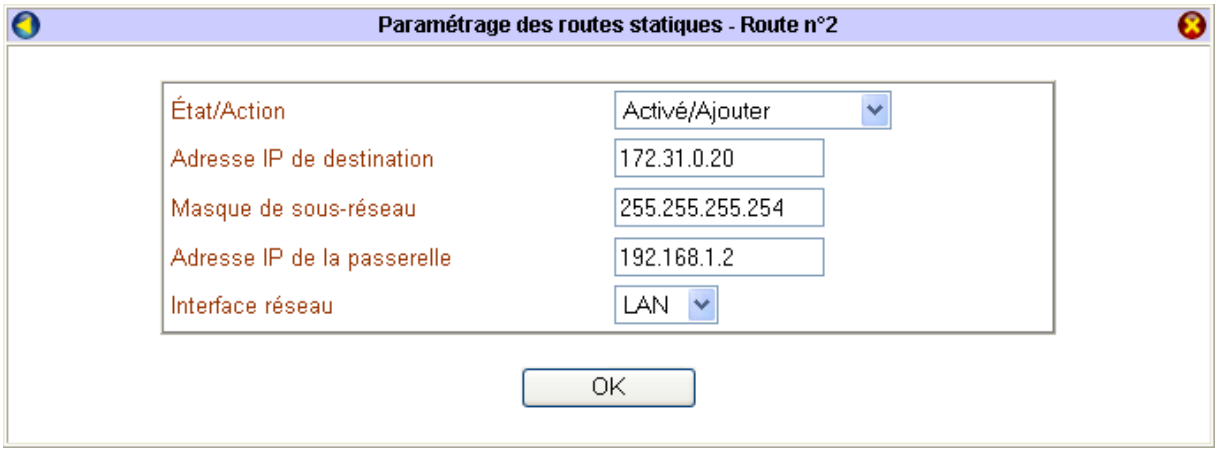


4. Cliquez sur **OK** afin de valider cette route statique.
5. Dans la ligne 2, cliquez sur **???** afin de paramétrer la seconde route statique : le routeur A pourra joindre le serveur i-minitel par le routeur B.

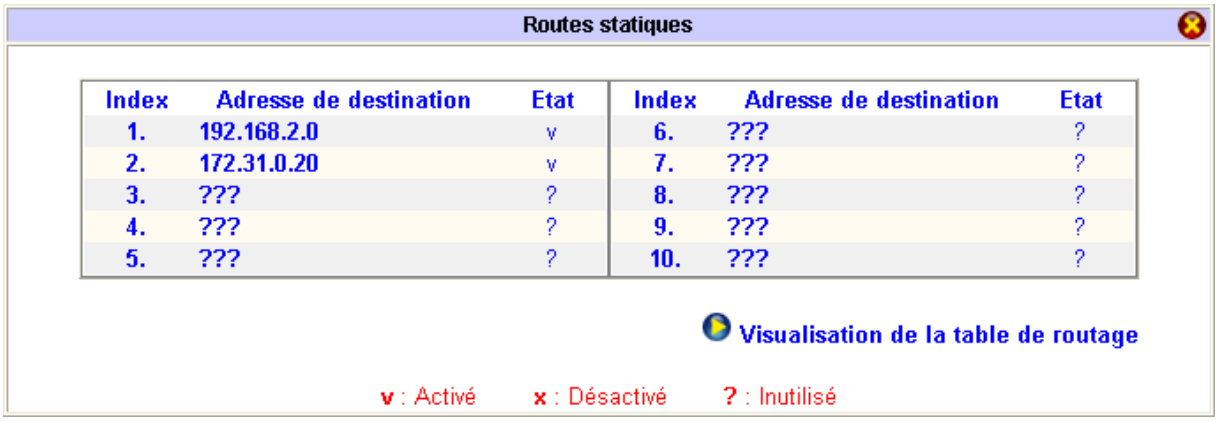
Dans la rubrique **Etat/Action**, sélectionnez l'option **Activé/Ajouter**.

Dans la rubrique **Adresse IP de destination**, spécifiez l'adresse de l'application à laquelle vous voulez accéder. Dans notre exemple, nous désirons accéder à l'i-minitel, donc à l'adresse 172.31.0.20. Indiquez également le masque de sous-réseau correspondant.

Dans la rubrique **Adresse IP de la passerelle**, spécifiez l'adresse du routeur qui va faire le lien avec le réseau de destination. Dans notre exemple, pour accéder à l'i-minitel, nous allons mettre le routeur B en passerelle.



6. Cliquez sur **OK** afin de valider cette seconde route statique. L'écran récapitulatif apparaît.



Dans la colonne **Etat**, « v » signifie que les routes statiques concernées sont activées.

Attention : si votre routeur est en classe A ou en classe B, la première adresse IP ne gère que le NAT. Vous devez alors activer le routage IP en indiquant une seconde adresse IP qui prendra le relais de la première pour toutes les fonctions autres que le NAT (routage). Dans le menu ***Configuration Elémentaire****, cliquez sur* ***Paramètres LAN TCP/IP et serveur DHCP****. Activez le routage IP, puis saisissez la seconde adresse qui doit se trouver sur la même plage que la première.*

Client RADIUS

L'intérêt est toujours de protéger les accès au serveur par identification des utilisateurs. Le VPN Booster vous permet de configurer jusqu'à 10 comptes d'appels entrants. Si vous désirez paramétrer des comptes supplémentaires, il vous faut donc utiliser un serveur central (appelé serveur RADIUS).

RADIUS (***R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice*) est un protocole client/serveur destiné à permettre au VPN Booster (qui fait alors office de « client » RADIUS) de communiquer avec une base de données centralisée regroupant en un point l'ensemble des utilisateurs distants. RADIUS va authentifier les utilisateurs et leur autoriser l'accès à telle ou telle ressource du routeur, ceci allant dans le sens d'une sécurité accrue.

Quand un utilisateur distant appelle un serveur d'accès (routeur), il leur est demandé un nom d'utilisateur et un mot de passe. RADIUS authentifie et autorise l'accès des utilisateurs distants au moyen d'un dialogue entre le routeur et le serveur RADIUS.

Le serveur crée un paquet de données à partir de ces informations appelé « demande d'authentification », qui est faite à partir des informations collectées. Le serveur demande l'authentification, le port utilisé pour la connexion, le nom d'utilisateur et le mot de passe. Le serveur envoie ces informations au serveur qui possède les informations enregistrées dans sa base.

Une fois que l'utilisateur a été authentifié, si le nom d'utilisateur et le mot de passe sont corrects, le routeur transmet un message d'authentification incluant les informations relatives au système et aux services demandés par l'utilisateur et lui donne donc accès aux services appropriés du réseau. Si le nom d'utilisateur et le mot de passe sont incorrects le serveur RADIUS transmet un message de rejet d'authentification au routeur et l'utilisateur se voit refuser l'accès au réseau.

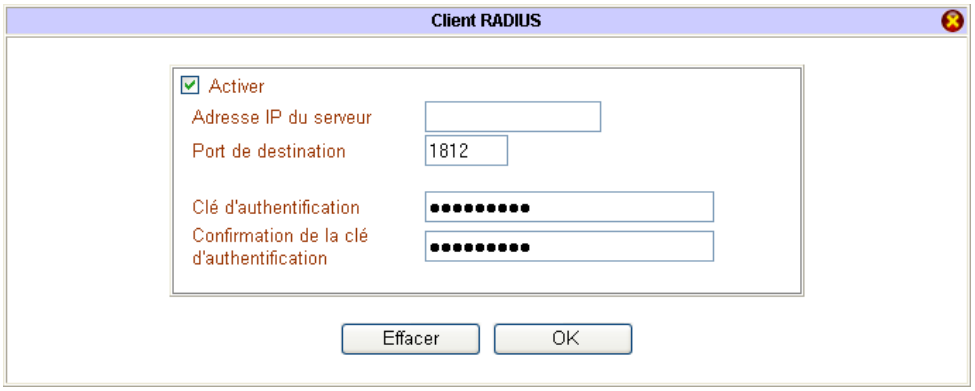
RADIUS contrôle l'accès des sites distants au VPN Booster en fonction des comptes clients enregistrés dans sa base de données. Par conséquent, le système RADIUS se décompose en deux entités :

- un client RADIUS, qui correspond donc au VPN Booster, qui se charge, suivant la configuration, de demander l'accord au serveur "d'authentification" pour les accès pupitres, et les accès de communication de données entrants, de demander l'enregistrement des données recueillies au serveur "d'accounting".
- un ou plusieurs serveurs RADIUS (possibilité de séparer la partie "authentification" de la partie "accounting") destiné(s) à recevoir les requêtes des clients, à gérer des données liées aux serveurs eux-mêmes, à fournir des réponses aux clients.

Pour paramétrer le client RADIUS, procédez comme suit :

1. Dans le menu **Réglages Avancés** du routeur, cliquez sur **Client RADIUS**.
2. Cochez **Activer**.
3. Dans la rubrique **Adresse IP du serveur**, indiquez l'adresse IP de votre serveur RADIUS pour faire pointer le routeur vers le serveur.

   Remarque : le port de destination 1812 présent par défaut correspond au port standard RADIUS. Si vous le modifiez, veillez bien à en faire de même du côté « serveur ».
4. Indiquez le mot de passe secret partagé échangé entre le serveur et le client RADIUS, puis confirmez-le. Demandez-le à votre administrateur RADIUS si vous ne le connaissez pas. Le mot de passe doit être identique sur le serveur RADIUS et le routeur.

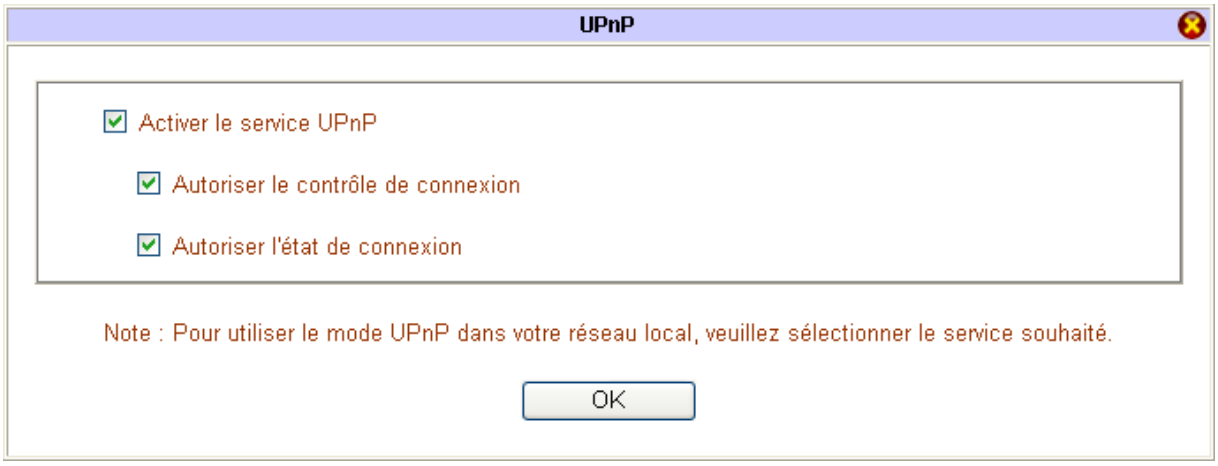


5. Cliquez sur **OK** pour valider les informations. Le routeur doit ensuite redémarrer.

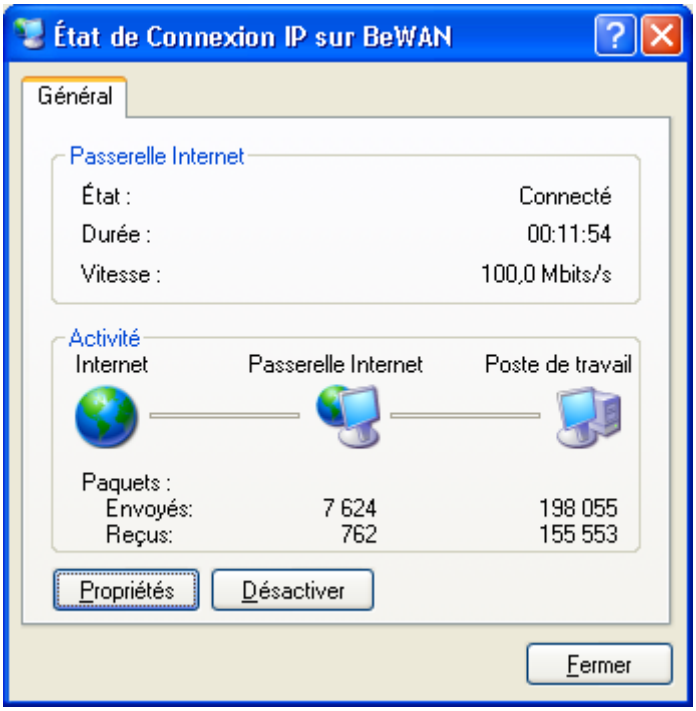
Paramétrage du service UPnP

Lorsqu'une application de fonctionne pas en utilisation normale, vous pouvez vous servir de la fonction UPnP (Universal Plug and Play). Le VPN Booster offre une gestion complète de l'UPnP sous Windows XP. Lorsque cette fonction est activée, les ordinateurs du réseau détectent l'état de connexion du routeur et gèrent automatiquement l'ouverture et la fermeture des ports TCP/UDP lors de l'utilisation d'applications compatibles UPnP. Ceci permet d'éviter des paramétrages complexes. Cette fonction fournit ainsi la meilleure solution permettant aux utilisateurs de pouvoir profiter des jeux en ligne, des vidéo conférences et autres applications dites « peer-to-peer ».

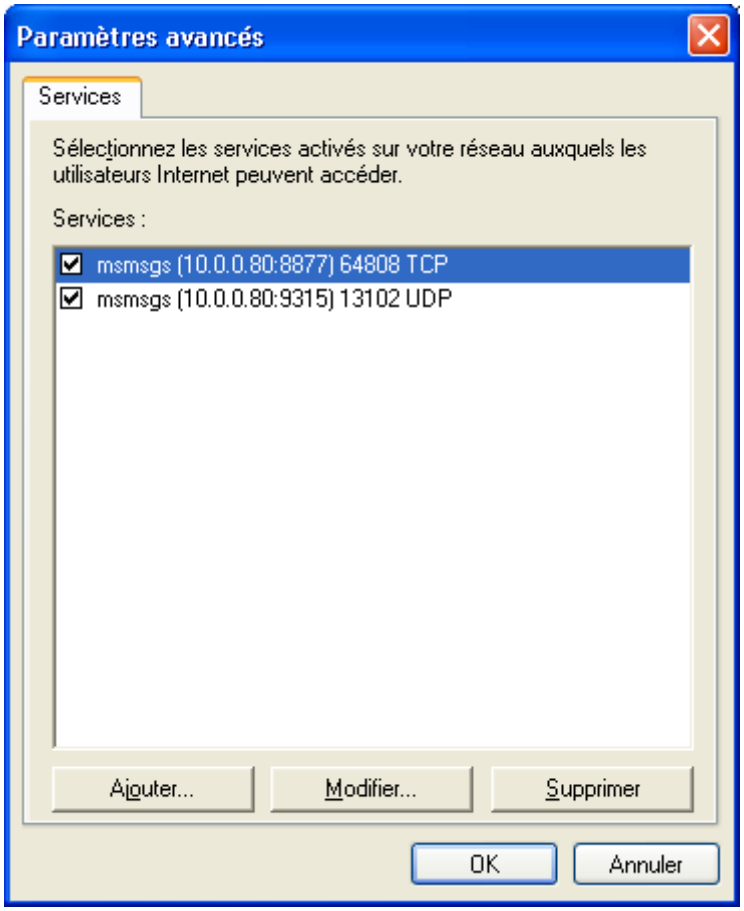
1. Dans le menu **Réglages Avancés**, cliquez sur **UPnP**.
2. Cochez **Activer le service UPnP**, puis les deux options **Autoriser le contrôle de connexion** et **Autoriser l'état de connexion**.



3. Lancez votre connexion Internet, puis lancez l'application souhaitée (MSN Messenger, dans notre exemple).
4. Cliquez sur **démarrer**, puis sur **Panneau de configuration**. Cliquez sur **Connexions réseau et Internet**, puis sur **Connexions réseau**.
5. Dans la partie **Passerelle Internet**, l'élément **Connexion IP sur BeWAN** apparaît (si votre type de connexion Internet est **IP statique ou dynamique**). Effectuez un double clic sur celui-ci. La fenêtre suivante s'affiche.



6. Cliquez sur **Propriétés**. Cochez la case **Afficher une icône dans la zone de notification une fois la connexion établie** afin de faire apparaître une icône dans la barre des tâches pour suivre l'état de connexion.
7. Pour intervenir plus précisément sur la gestion des ports, après avoir cliqué sur **Propriétés**, cliquez ensuite sur **Paramètres…**.



8. Cliquez sur **OK** pour valider toute modification.

Configuration du VLAN

Un VLAN (***V**irtuel **L**ocal **A**rea **N**etwork*) est une option de gestion de réseau permettant de répartir et d'organiser les éléments du réseau par regroupement logique des utilisateurs. Sur le VPN Booster, la méthode de construction du VLAN s'effectue par port.

Un VLAN est obtenu en associant chaque port du VPN Booster à un VLAN. L'administrateur peut ainsi parfaire les performances de communication et optimiser l'utilisation des ressources. Les avantages du VLAN peuvent être les suivants :

- la réduction de la diffusion du trafic. En créant des VLAN ou des groupes d'utilisateurs destinés à ne travailler qu'entre eux sur le réseau local, vous contrôlez les échanges entre les différents LAN, les messages de diffusion étant limités à l'intérieur de chaque VLAN.
- une meilleur utilisation de la bande passante.
- l'amélioration de la sécurité.

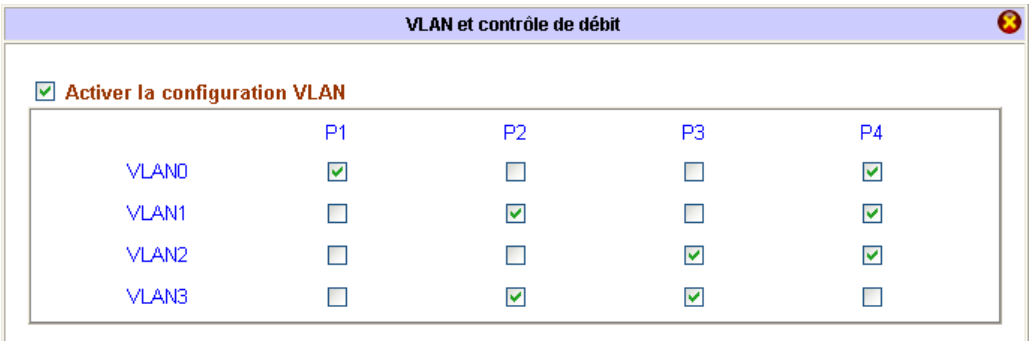
Activation du VLAN

Vous pouvez créer 4 VLAN au maximum, qui seront constitués par groupes d'utilisateurs, et favoriser ou non l'un d'entre eux. En groupant plusieurs ports dans un VLAN, vous permettez à des paquets d'être envoyés aux ports constituant le même VLAN sans générer de trafic sur les autres ports, améliorant ainsi l'utilisation des ressources du réseau et sa sécurité. N'importe quel port peut faire partie d'un VLAN et un port peut appartenir à des VLAN différents.

Afin de configurer un VLAN et d'en comprendre le concept, vous pouvez suivre l'exemple suivant. Dans une société, considérons que nous regroupons :

- ✓ le service Comptabilité sur le port 1,
- ✓ le service Commercial sur le port 2,
- ✓ le service Marketing sur le port 3,
- ✓ un serveur de fichiers et de messagerie sur le port 4, où chaque utilisateur possède un répertoire propre avec ses dossiers courants.

1. Créez les VLAN suivants :
   - un VLAN associant le port 1 et le port 4,
   - un autre les ports 2 et 4,
   - un troisième les ports 3 et 4,
   - et enfin un dernier réunissant les ports 2 et 3.



2. Cliquez sur **OK** pour valider.

En paramétrant ainsi votre routeur, vous autorisez :

- la communication entre chacun des services et le port 4 qui est constitué des serveurs.
- la diffusion d'informations uniquement entre le service Marketing et le service Commercial.

En revanche, par exemple, la communication entre les postes du service Comptabilité (port 1) et du service Marketing (port 3) est impossible.

Activation du contrôle de débit

Le contrôle de débit vous permet de contrôler l'allocation de la bande passante entre les services et ainsi d'optimiser l'utilisation des ressources réseau, offrant ainsi la possibilité de privilégier certains services au détriment d'autres et de faire bénéficier aux services prioritaires de la bande passante la plus large pour une meilleure fluidité.

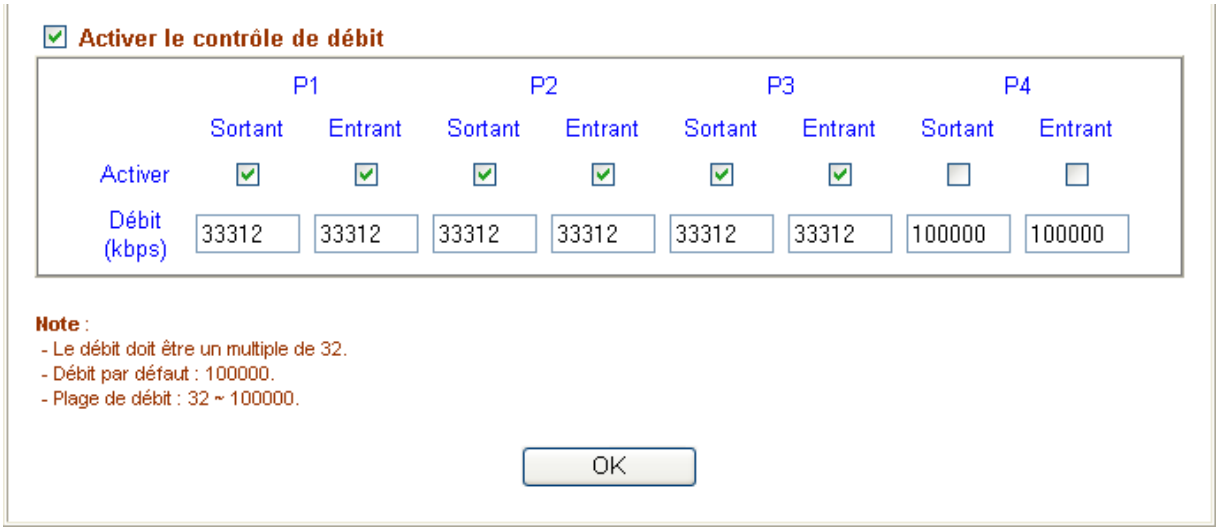
Par exemple, il sera pratique d'allouer plus de bande passante à un VLAN utilisant des services de téléphonie, de transfert de fichiers plutôt qu'à un VLAN regroupant des utilisateurs de connexion Internet.

Lorsque vous cochez **Activer le contrôle de débit**, vous avez la possibilité de spécifier un débit maximum sortant ou entrant par port. C'est utile pour réduire au minimum l'impact d'un utilisateur qui monopoliserait l'intégralité de la bande xDSL (par exemple en jouant à des jeux ou en téléchargeant des dossiers volumineux à partir d'un serveur de fichiers) sur les autres utilisateurs.

Pour chacun des ports LAN (P1, P2, P3 ou P4), vous pouvez choisir de limiter la largeur de la bande en entrée ou en sortie.

Sous le numéro de port correspondant, sur le ligne **Activer**, cliquez sur **Sortant** ou **Entrant**, puis indiquez la bande passante que vous désirez allouer à chaque port.

Reprenons l'exemple évoqué lors de l'activation du VLAN. L'intérêt, en fonction de la structure de la société, est de permettre à chaque service un accès constant au serveur de fichiers et au serveur de messagerie. Pour cette raison, vous ne limiterez pas le niveau de bande passante sur le port 4, et rendrez ainsi son utilisation prioritaire. En revanche, pour que chaque service puisse profiter de la même manière de l'accès au serveur, vous partagerez la bande passante entre les 3 services concernés.



Cliquez sur **OK**.

Contrôle QoS (Série VPN Booster 32)

Introduction

La fonction QoS (***Q**uality **o**f **S**ervice* ou Qualité de Service) désigne un ensemble de paramètres vous permettant de garantir un trafic de données en contrôlant l'allocation des ressources réseau, et notamment le débit alloué à certaines applications. Cette fonction fixe des règles de priorités entre les différents flux pour optimiser l'acheminement des données. Pour configurer la QoS, il convient donc au préalable de bien identifier les besoins du réseau afin de déterminer les applications prioritaires. Cela nécessite une analyse pertinente et régulière afin de se protéger des pointes de trafic et de prévoir d'éventuelles saturations.

L'allocation des ressources réseau permet de privilégier certains utilisateurs ou services ou de garantir une bande passante suffisante pour certaines applications, telles la Voix sur IP ou les jeux en ligne.

Afin de garantir cette qualité de service, plusieurs protocoles se sont imposés. Celui utilisé par les routeurs VPN Booster est le protocole Diffser (***Diff**erentiated **Ser**vices*). Ce protocole assure une distinction des paquets par classes de flux. Les données sont identifiées grâce à un marquage dans le champ ToS (***T**ype **o**f **S**ervice*, champ spécifique réservé dans l'en-tête IP de 8 bits), qui fixe les priorités.

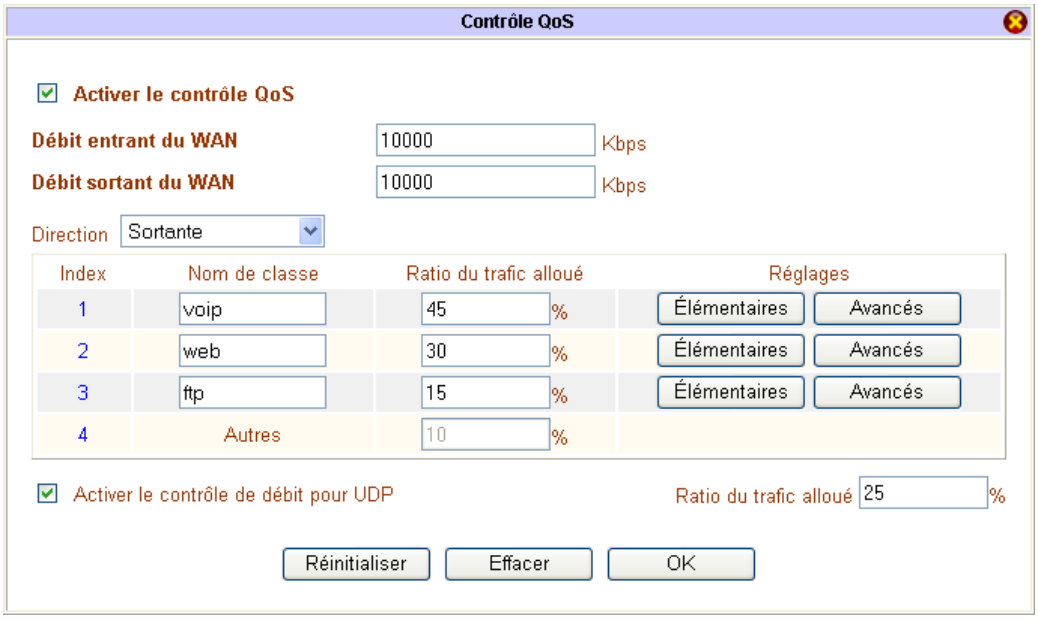
Configuration du QoS

Procédez comme suit :

1. Dans le menu **Réglages Avancés**, cliquez sur **Contrôle QoS**.
2. Cochez la case **Activer le contrôle QoS**.
3. Dans les champs **Débit entrant du WAN** et **Débit sortant du WAN**, spécifiez la partie de la bande passante allouée à votre routeur par le FAI.

   Remarque : nous vous recommandons de ne pas spécifier plus de 90 % de la bande passante afin de tenir compte des pics d'utilisations.
4. Définissez le sens de la direction de la QoS : **Entrante**, **Sortante** ou **Entrante / Sortante**.
5. Renseignez ensuite les informations sur les classes. Seules les trois premières peuvent être définies par les utilisateurs.
   - Pour les index 1 à 3, renseignez les rubriques **Nom de classe** (différents types de service).
   - Spécifiez le pourcentage de bande passante que vous souhaitez leur octroyer dans la colonne **Ratio du trafic alloué**.

   Remarque : l'index 4 prend automatiquement le pourcentage du trafic restant pour tous les autres protocoles.



*Remarque : **Activer le contrôle de débit pour UDP** avec un ratio de **25 %** est recommandé afin que les paquets UDP ne puissent dépasser le pourcentage indiqué si leur volume devenait trop important. En effet, les performances peuvent être améliorées en séparant les trafics TCP et UDP. Le ratio est pris sur la totalité de la bande passante spécifiée dans les rubriques **Débit entrant du WAN** et **Débit sortant du WAN**.*

Sur les routeurs VPN Booster, il existe ensuite deux manières de configurer la Qualité de Service :

- les réglages **Elémentaires**, qui correspond à une bonne majorité des utilisations.
- les réglages **Avancés**, pour affiner les réglages sur un réseau plus conséquent.

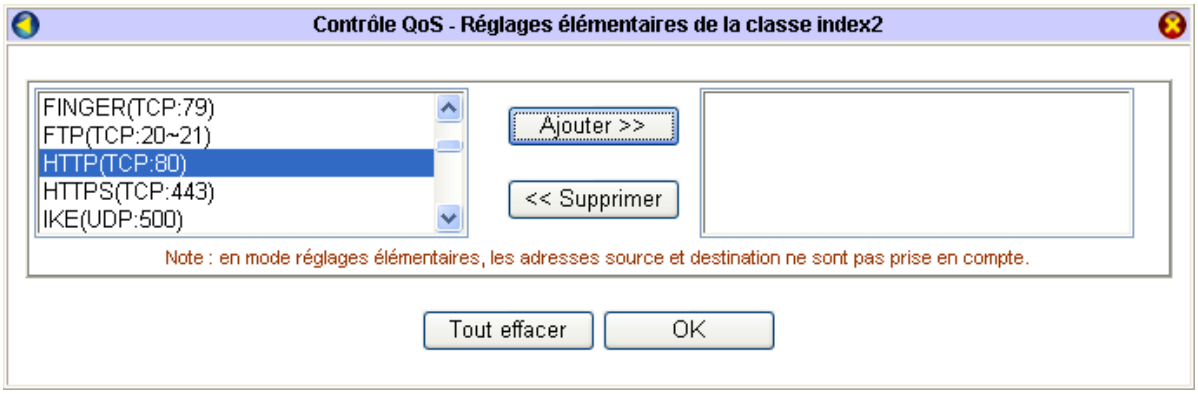
Paramétrage avec les réglages Elémentaires

Comme cela est indiqué dans notre exemple, nous désirons allouer un pourcentage du trafic aux services VoIP, Web et FTP.

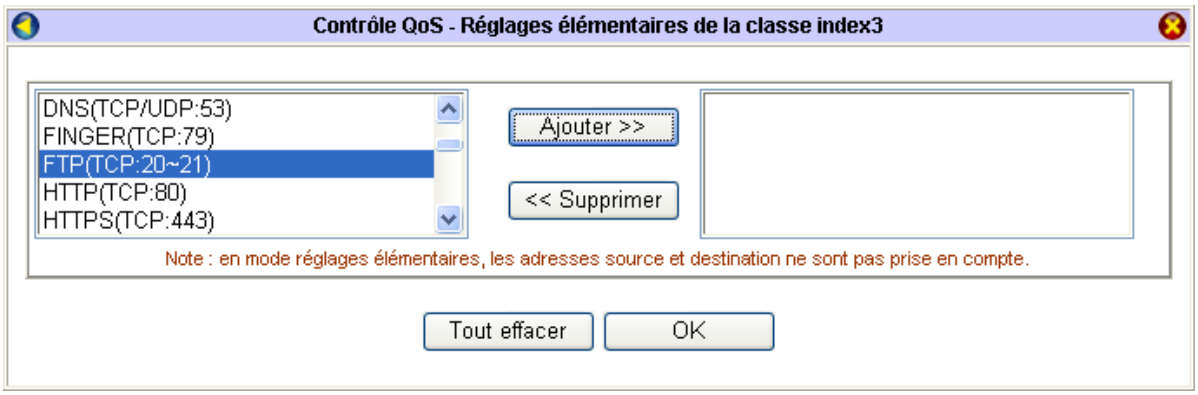
1. Pour chaque index, cliquez sur le bouton **Elémentaires**.
2. Dans la liste, sélectionnez le protocole recherché, cliquez sur **Ajouter** puis validez par **OK**.

Remarque : Le trafic alloué à un protocole non-utilisé est redistribué sur les autres classes.

Ainsi, pour faire référence à notre exemple, pour le service Web, sélectionnez le protocole HTTP.



Pour le service FTP, sélectionnez le protocole FTP.

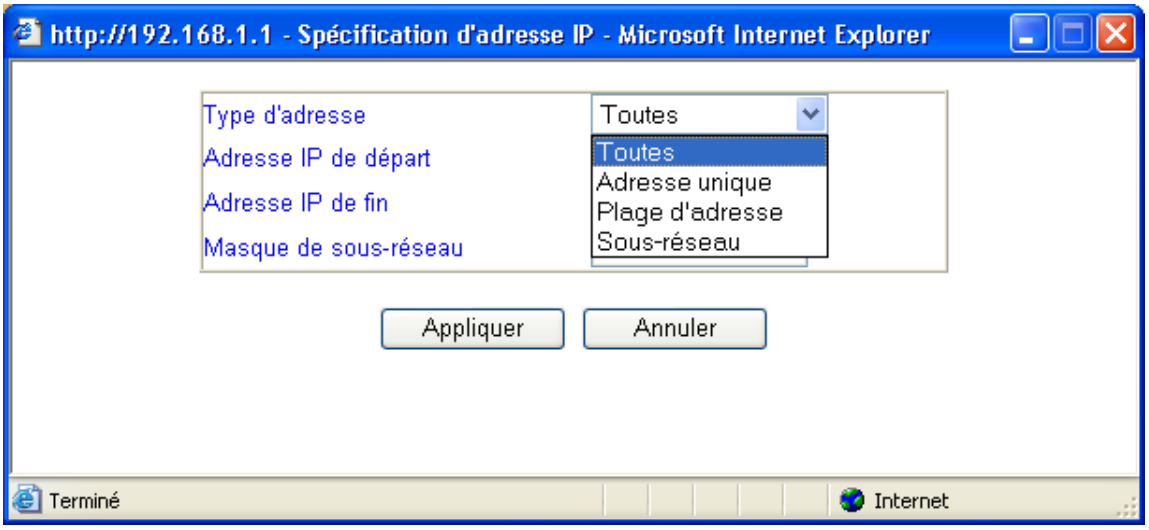


Paramétrage avec les réglages Avancés

Le bouton **Avancés** vous permet d'affiner le contrôle QoS en spécifiant une adresse IP, un réseau, un sous-réseau en adresse source ou destination, voire un codage de priorité. Procédez comme suit :

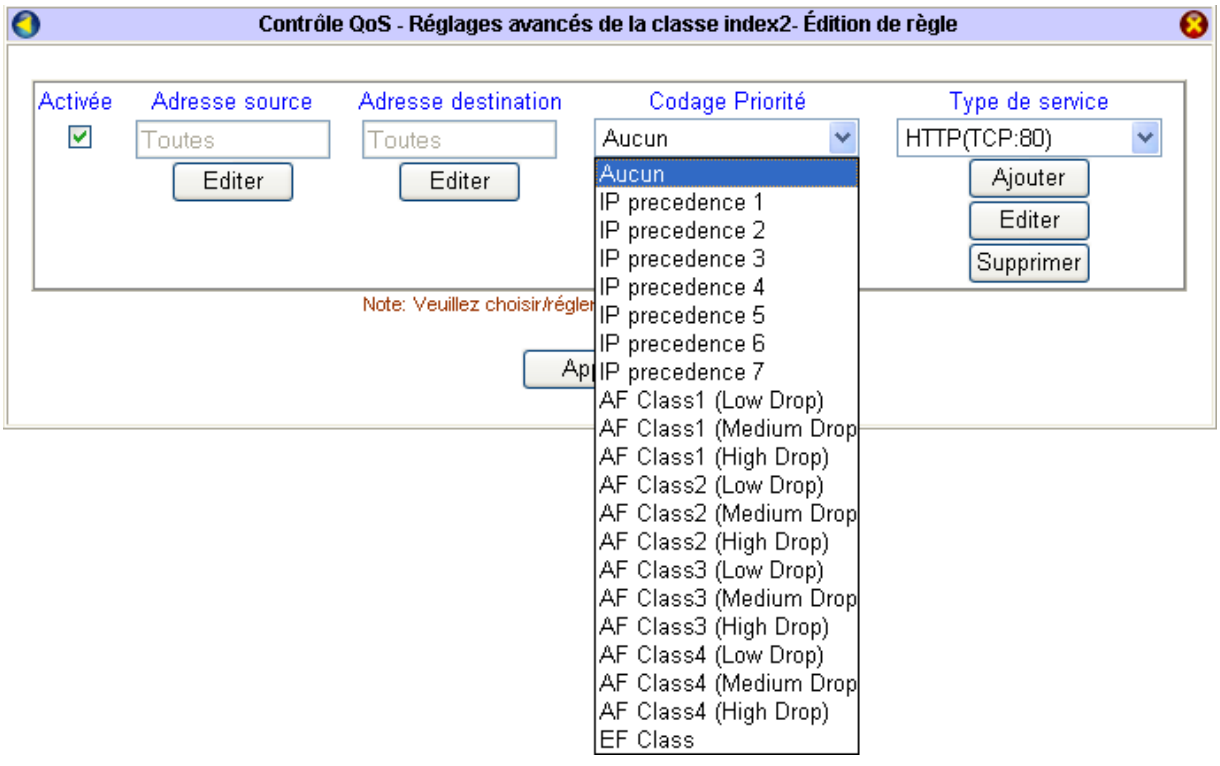
1. Pour chaque index, cliquez sur le bouton **Avancés**.
2. Cliquez sur le bouton **Insérer**.
3. Cochez la case **Activée**.
4. Sélectionnez le service dans la liste **Type de service**.

5. Renseignez si nécessaire les rubriques **Adresse source** et **Adresse destination** qui correspondent aux adresses IP des machines concernées. Vous pouvez définir une adresse unique, une plage d'adresse ou un sous-réseau.



6. La rubrique **Codage de priorité** permet de définir un niveau de priorité appliqué au paquet. Les routeurs gérant ces paquets doivent avoir les mêmes règles de QoS. On y retrouve les paquets de type :

   - **IP precedence** : définit la priorité de traitement des paquets (7 étant le plus prioritaire, 1 le moins prioritaire).
   - **AF** (***A**ssured **F**orwarding*) : garantit la transmission des données sans tenir compte des délais. Quatre classe AF sont disponibles dans lesquels sont définis 3 niveaux de priorité d'ordre de rejet [de Low Drop (faible rejet) à High Drop (rejet élevé)] dans un routeur en cas de congestion du réseau. Il n'existe aucune priorité entre ces différentes classes.
   - **EF** (***E**xpedited **F**orwarding*) : correspond à la priorité maximale. Cette classe a pour but de garantir une bande passante avec des taux de perte et de délit (latence) faibles. Elle réalise le transfert de flux à fortes contraintes temporelles comme la visio-conférence ou la téléphonie sur IP par exemple. Elle est donc destinée aux paquets nécessitant une haute disponibilité.
   - **Aucun** doit être utilisé pour les flux Internet qui ne nécessitent pas un trafic en temps réel.



7. Cliquez sur **Appliquer** pour valider votre règle.

Configuration de la Voix sur IP (VPN Booster 32 V / 32 Vg)

La Voix sur IP ou VoIP est une technique permettant de faire dialoguer deux postes téléphoniques via un réseau IP.

Le principe de la voix sur IP est de faire circuler sur Internet, grâce au protocole IP, des paquets de données correspondant à des échantillons de voix numérisée que le routeur a compressés. Internet permet ensuite l'acheminement de ces paquets à leur destinataire. Cette technologie vous permet donc de communiquer à moindre coût avec une personne se trouvant à l'autre bout du monde. La VoIP offre également une qualité de transmission de la voix ainsi qu'une fiabilité comparable au réseau téléphonique classique.

La téléphonie sur réseau de données par paquets est constituée de plusieurs étapes. Voici comment transite la voix par IP :

1. **Numérisation de la voix** (par exemple à 64 Kbps comme en téléphonie numérique) : les communications issues de téléphones traditionnels sont converties en données binaires.
2. **Compression du signal numérique** correspondant (pour diminuer son débit, donc la quantité d'informations à transmettre).
3. **Découpage du signal** obtenu, puis encapsulation du flux de données en paquets IP.
4. **Transmission des paquets** vers son destinataire à travers Internet sur un réseau de données utilisant la même technologie.

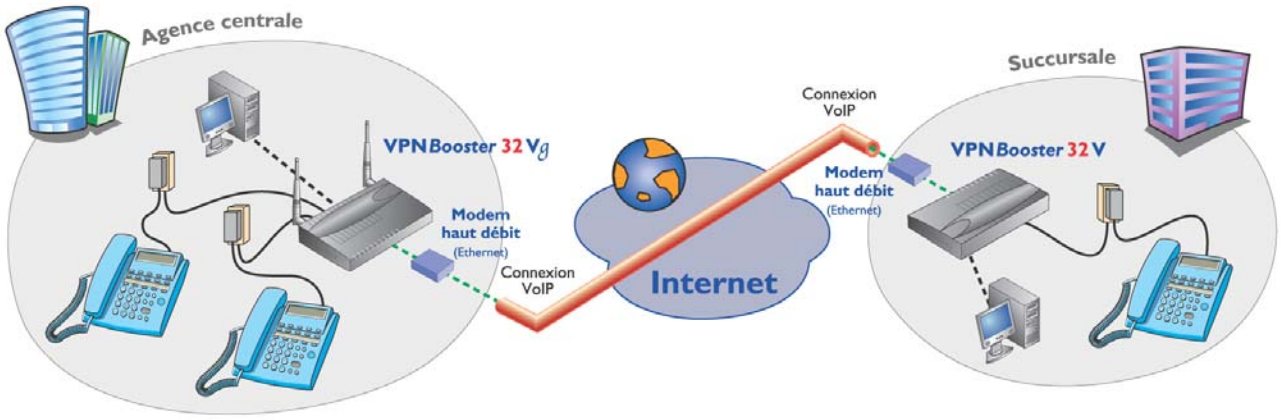
A l'arrivée, le routeur récupère les paquets pour reconstituer la voix. Ces paquets acheminés sont ré-assemblés. Le signal de données ainsi obtenu est décompressé, puis converti en signal analogique pour restitution sonore à l'utilisateur (transformation inverse : des paquets vers la voix).

Préalable à l'établissement de la connexion VoIP

⚠ *Avant la mise en place de votre communication, vous devez avoir configuré et lancé votre connexion Internet. Reportez-vous pour cela au chapitre « Accès à Internet » page 79.*

Il est nécessaire que les 2 correspondants aient échangé leurs paramètres de connexion Internet (exemple : adresse IP WAN ou DNS dynamique).

La figure suivante schématise une connexion VoIP entre 2 sites d'une société :



L'utilisation de la Voix sur IP n'est possible que si les deux correspondants sont connectés chacun à un VPN Booster qui gère alors la communication, y compris la signalisation avec le réseau téléphonique et les conversions à l'entrée et à la sortie du réseau IP. Cette passerelle est l'élément central permettant des conversations VoIP impliquant un téléphone comme origine ou destination de l'appel. Il suffit donc de brancher le combiné téléphonique sur l'un des ports FXS de votre routeur.

Remarque : que la fiche de votre combiné téléphonique soit moulée ou non, nous vous conseillons de toujours utiliser l'adaptateur fourni avec le VPN Booster 32 V / 32 Vg.

Considérons une connexion VoIP entre deux sites d'une société. Chaque correspondant possède un VPN Booster VoIP. Après avoir pris connaissance des paramètres du distant (Adresse IP ou Nom de domaine), les deux interlocuteurs doivent chacun saisir les paramètres suivants :

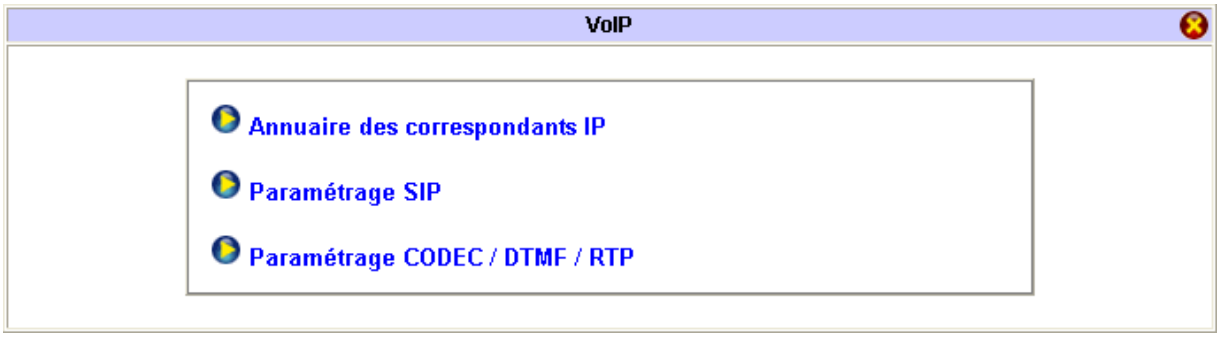
Cas de figure 1 : les deux sites possèdent une adresse IP fixe ou un DNS dynamique

	Paramètres de la Succursale	Paramètres de l'Agence principale
Annuaire du correspondant IP		
Numéro d'appel :	**1234**	**6789**
Nom :	**Agence**	**Succursale**
Adresse IP / Nom de domaine :	**80.12.34.56**	**203.xx.xx.xx**
Paramétrage SIP		
Port SIP :	**5060** (conservez le port par défaut)	
Enregistrement :	(Ne remplissez pas ce champ)	
Paramétrage des ports :	Choisissez **Port 1** (cela signifie que le téléphone est branché sur le port *FXS1 à l'arrière du routeur*)	
Méthode d'enregistrement :	Sélectionnez l'option **Aucun**	
Nom :	**Succursale**	**Agence**
Mot de passe :	(Ne remplissez pas ce champ)	
Délai d'expiration :	**10 minutes** (conservez le paramètre par défaut)	
Paramétrage CODEC / DTMF / RTP	Conserver les paramètres par défaut	

Cas de figure 2 : les deux sites utilisent une adresse SIP obtenue auprès d'un service d'enregistrement (dans notre exemple : iptel.org)

	Paramètres de la Succursale	Paramètres de l'Agence principale
Annuaire du correspondant IP		
Numéro d'appel :	**1234**	**6789**
Nom :	**Agence**	**Succursale**
Adresse IP / Nom de domaine :	**iptel.org**	**iptel.org**
Paramétrage SIP		
Port SIP :	**5060** (conservez le port par défaut)	
Enregistrement :	**iptel.org** (nom du serveur)	
Paramétrage des ports :	Choisissez **Port 1** (cela signifie que le téléphone est branché sur le port *FXS1 à l'arrière du routeur*)	
Méthode d'enregistrement :	Sélectionnez l'option **Automatique**	
Nom :	**Succursale**	**bewan**
Mot de passe :	***** (Saisissez le mot de passe)	
Délai d'expiration :	**10 minutes** (conservez le paramètre par défaut)	
Paramétrage CODEC / DTMF / RTP	Conservez les paramètres par défaut	

Dans le menu **Réglages Avancés**, cliquez sur **VoIP**.



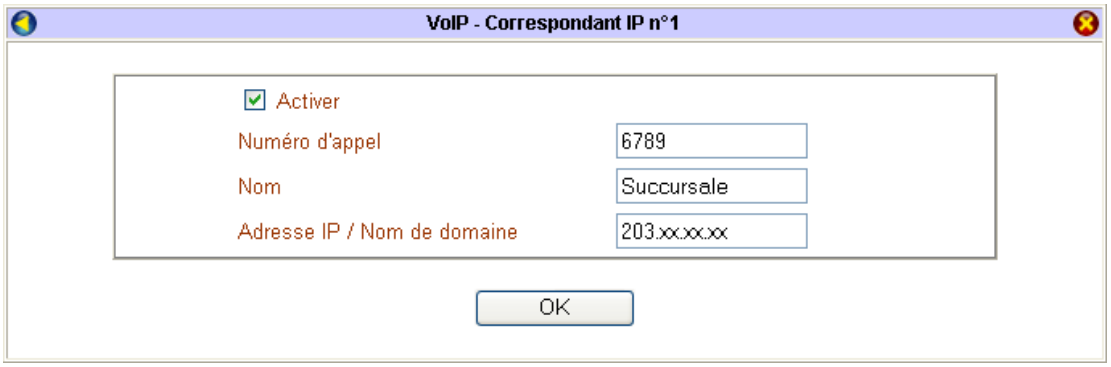
Etape 1 : Annuaire des correspondants IP

Vous avez la possibilité de répertorier jusqu'à 60 correspondants. Procédez comme suit :

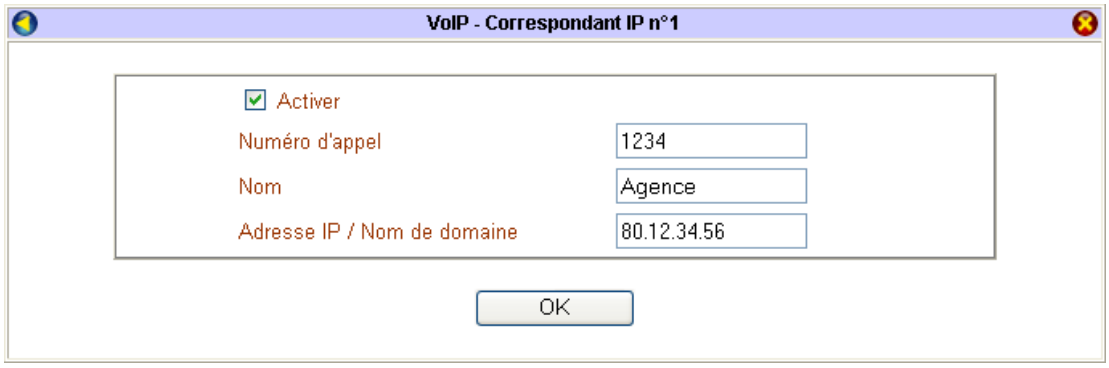
1. Cliquez sur un numéro dans la colonne **Index**. La fiche concernant votre futur interlocuteur apparaît alors.
2. Cochez la case **Activer**.
3. Dans la rubrique **Numéro d'appel**, saisissez le numéro qui sera attribué pour la communication avec le correspondant en question. Le choix de ce numéro est libre (26 caractères maximum).
4. Dans la rubrique **Nom**, saisissez le nom de votre correspondant. Il peut s'agir aussi bien d'un nombre que d'un nom (23 caractères maximum). Ce nom doit être le même que celui présent dans la configuration du distant.
5. Dans la rubrique **Adresse IP / Nom de domaine**, précisez l'adresse IP WAN utilisé par votre correspondant (ou DNS dynamique).

   Si votre interlocuteur ne possède pas d'adresse IP fixe, vous devez saisir le nom du serveur qui gère votre abonnement SIP. Ce serveur fait correspondre un nom de domaine constant avec une adresse IP variable.

   Paramétrage du routeur situé dans l'Agence principale :



   Paramétrage du routeur situé dans la Succursale :



6. Cliquez sur **OK** pour valider les informations.

Etape 2 : Paramétrage SIP

En matière de codage et de restitution de la voix, le VPN Booster utilise le protocole SIP (***S**ession **I**nitiation **P**rotocol*). C'est un protocole de signalisation simple pour les applications de téléphonie qui s'occupe uniquement de l'établissement, de la gestion et de la terminaison des sessions. Le protocole de signalisation SIP est optimisé pour fournir une meilleure qualité de voix.

Le protocole est bâti sur une architecture Client/Serveur et utilise des messages textuels. Les messages sont transportés par les protocoles de transport réseaux TCP ou UDP. Le message possède un en-tête et un corps. L'en-tête définit les paramètres nécessaires au routage du message et à l'établissement de la session. Le corps définit les caractéristiques de la session à l'aide d'un protocole de description de session.

Le protocole SIP spécifie comment établir sur Internet des appels téléphoniques :

- localisation du terminal appelé,
- la gestion des mécanismes d'établissement et de libération de l'appel,
- authentification de l'appelant / de l'appelé.

Cas de figure 1 : les deux sites possèdent une adresse IP fixe ou un DNS dynamique

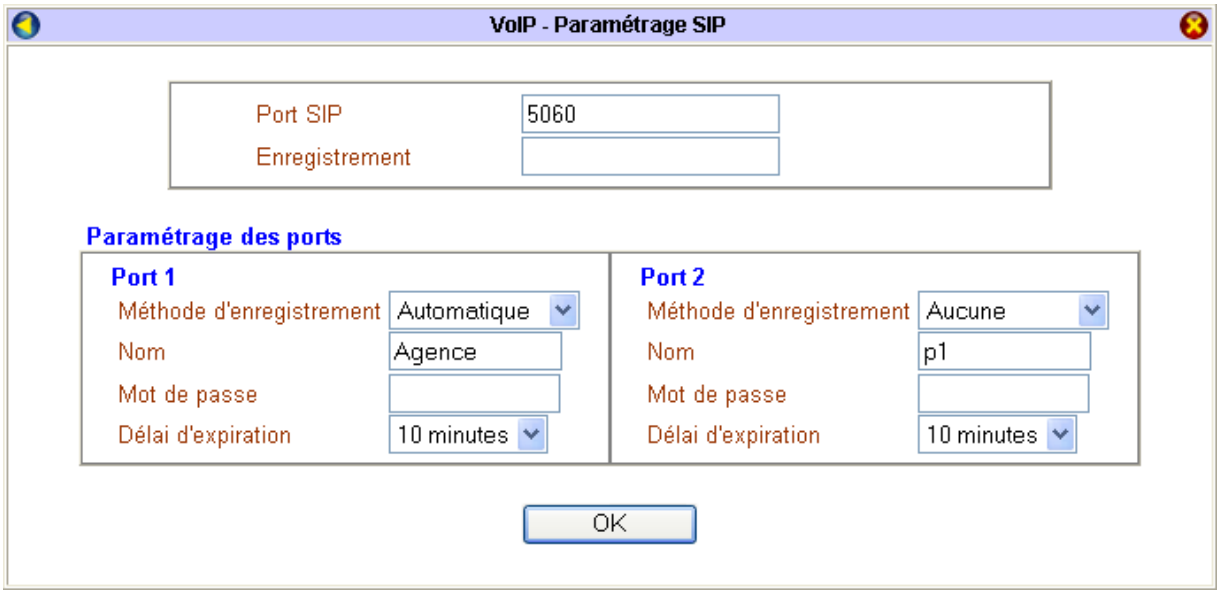
Attention : si les deux interlocuteurs possèdent une adresse IP fixe, il n'est pas nécessaire de posséder une adresse SIP. Ils peuvent se joindre directement sans utiliser ce type d'adresse.

Sur la page du **Paramétrage SIP**, selon vos paramètres, il n'est pas nécessaire de remplir toutes les rubriques.

1. Dans la rubrique **Port SIP**, le numéro de port est utilisé pour établir une session. La valeur par défaut est 5060. Vous pouvez modifier le numéro, mais il faut bien vérifier que votre interlocuteur change également ce paramètre sur son routeur.
2. Dans la partie **Paramétrage des ports**, sélectionnez l'un des ports.

   *Remarque : si vous avez branché votre téléphone sur le **Port FXS1** situé à l'arrière du routeur, sélectionnez **Port 1**. A l'inverse, si vous l'avez branché sur le **Port FXS2**, sélectionnez **Port 2**.*
3. Cochez la case **Activer**.
4. Dans la rubrique **Nom**, indiquez un nom de votre choix. Ce nom doit être le même que celui qui se trouve dans l'annuaire de votre correspondant.

Paramétrage du routeur situé dans l'Agence principale :



5. Cliquez sur **OK** pour valider les informations.

Cas de figure 2 : les deux sites utilisent une adresse SIP obtenue auprès d'un service d'enregistrement (dans notre exemple : iptel.org)

Pour entamer une communication, le téléphone doit en référer à un serveur (nécessité de créer un compte SIP) chargé de l'identification, de la gestion de la bande passante et du routage d'appels. Une fois l'autorisation délivrée, les paquets IP porteurs de voix transitent par le routeur qui dispose d'interfaces analogiques de type FXS *(**F**oreign e**X**change **S**tation)* nécessaires.

Pour obtenir une adresse SIP, vous devez vous inscrire sur un serveur d'enregistrement. Les adresses SIP se présentent sous la forme suivante : **sip:utilisateur@domaine**.

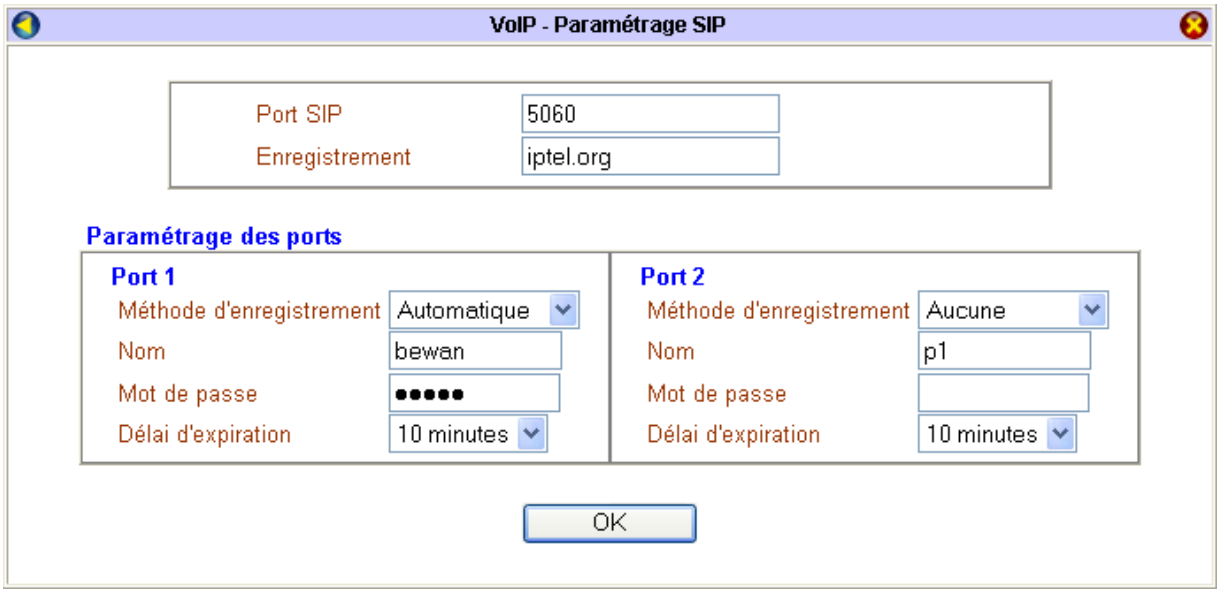
- Utilisateur = mot de passe ou numéro de téléphone
- Domaine = nom de domaine (xxx.fr) ou adresse IP

Ainsi, la définition du numéro de téléphone pour joindre un utilisateur ressemble à une adresse de type e-mail, généralement constituée d'un nom d'utilisateur et d'un domaine séparé par un « @ ». Il est donc nécessaire de connaître son adresse SIP pour dialoguer.

1. Dans la rubrique **Port SIP**, le numéro de port est utilisé pour établir une session. La valeur par défaut est 5060. Vous pouvez modifier le numéro, mais il faut bien vérifier que votre interlocuteur change également ce paramètre sur son routeur.
2. Dans la rubrique **Enregistrement**, afin de pouvoir joindre une personne à partir de son adresse SIP, saisissez le nom de domaine ou l'adresse IP du serveur d'enregistrement SIP sur lequel vous vous êtes abonné. Ce serveur permet de maintenir une correspondance entre l'adresse IP et le nom de domaine SIP. Par exemple, iptel.org ou 80.xx.xx.xx sont identiques.
3. Dans la partie **Paramétrage des ports**, sélectionnez l'un des ports.

   *Remarque : si vous avez branché votre téléphone sur le **Port FXS1** situé à l'arrière du routeur, sélectionnez **Port 1**. A l'inverse, si vous l'avez branché sur le **Port FXS2**, sélectionnez **Port 2**.*
4. Dans la rubrique **Méthode d'enregistrement**, sélectionnez **Activer**.
5. Dans la rubrique **Nom**, indiquez le nom que vous vous êtes attribué sur le serveur d'enregistrement. Ce nom doit être le même qui celui qui se trouve dans l'annuaire de votre correspondant.
6. Dans la rubrique **Mot de passe**, saisissez le mot de passe que vous avez choisi lors de votre inscription sur le site.

Paramétrage du routeur situé dans l'Agence principale :



7. Cliquez sur **OK** pour valider les informations.

Etape 3 : Paramétrage CODEC / DTMF / RTP

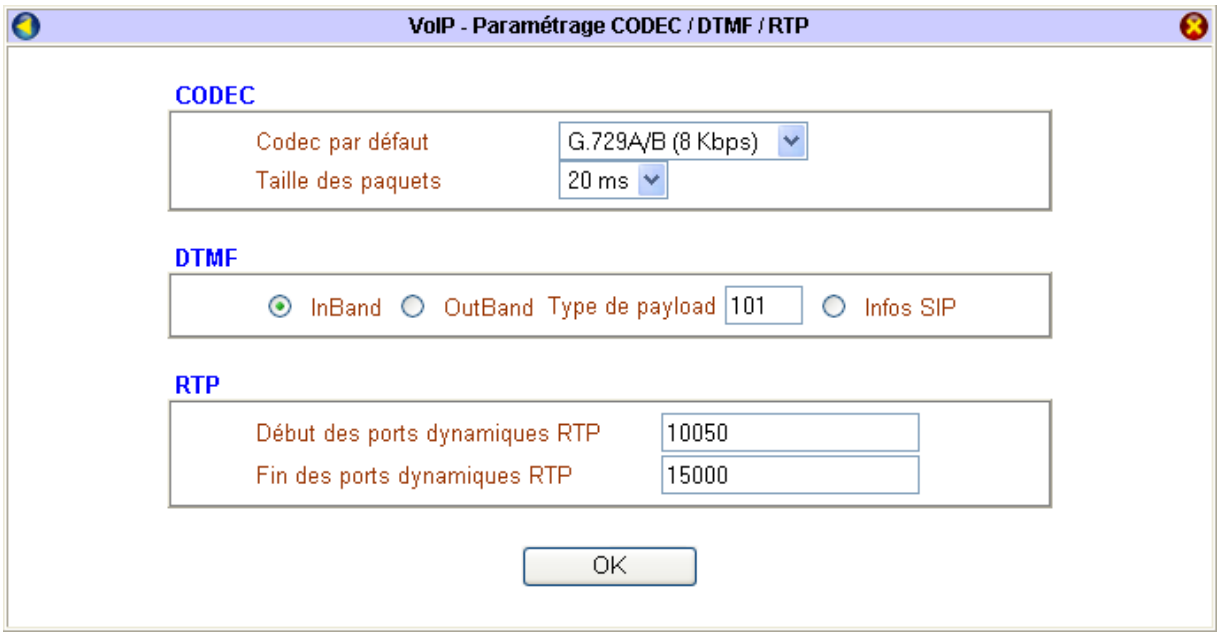
Dans une transmission vocale ordinaire, un Codec (Codeur-Décodeur) convertit les ondes de la voix en paquets numérisés. Ces paquets sont mis en forme pour être transmis sur le réseau. Les paquets VoIP acheminent de tout petits échantillons de la conversation, généralement à 20 ms afin que certaines pertes n'affectent pas l'intelligibilité de la conversation.

A l'émission, la voix est segmentée, codée, puis compressée afin d'être encapsulée dans un paquet IP. La détermination de la taille du paquet est un compromis entre la réduction du délai de transmission et l'utilisation optimale de la bande passante.

Il existe 5 Codec différents : G.711MU (64 Kbps), G.711A (64 Kbps), G.729A/B (8 Kbps), G.723 (6.4 Kbps) et G.726_32 (32 Kbps). La qualité de service de la transmission de la voix sur IP peut être déterminée par ce paramètre. Le Codec choisi peut être utilisé du moment que votre interlocuteur à l'extrémité de la communication le supporte également.

Le Codec par défaut est le Codec G.729A/B. Celui-ci occupe moins de bande passante tout en offrant une voix de bonne qualité.

Remarque : si votre ligne ADSL fonctionne en Upload à 64 Kbps, n'utilisez pas le Codec G.711.



Outre le protocole SIP, d'autres protocoles sont sollicités comme le protocole RTP (***R**eal-time **T**ransport **P**rotocol*) pour le transport des données et la gestion des flux multimédias sur IP. Il est utilisé pour optimiser (sans la garantir) la livraison de l'information dans l'ordre approprié d'un expéditeur à un récepteur. Il privilégie ainsi l'enchaînement du son, plutôt que l'intégrité des données.

RTP fournit un service de transport de bout en bout pour des applications incluant de la voix. Son rôle principal consiste à mettre en oeuvre des numéros de séquence de paquets IP pour reconstituer les informations de voix, même si le réseau sous-jacent change l'ordre des paquets.

RTP permet :

- d'identifier le type de codage et l'information transportée,
- d'ajouter des marqueurs temporels et des numéros de séquence,
- de détecter les pertes de paquets et d'en informer la source,
- d'identifier le contenu des paquets pour leur transmission sécurisée,
- de contrôler l'arrivée à destination des paquets.

Intégré à RTP, RTCP (***R**eal-time **T**ransport **C**ontrol **P**rotocol*) permet d'avoir des informations sur la qualité des données transmises.

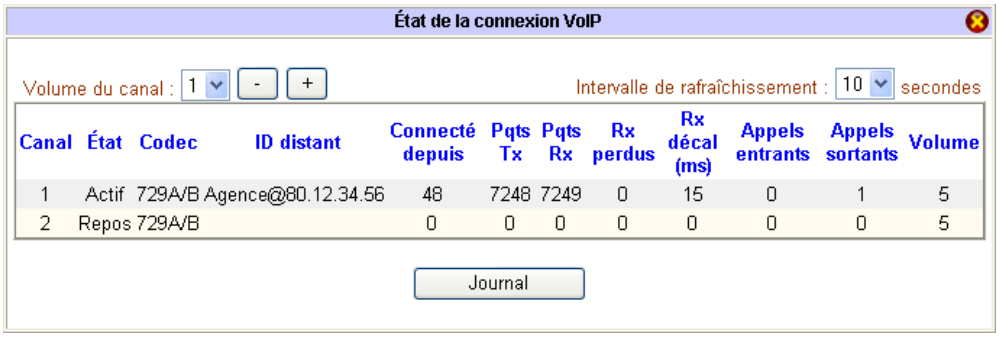
Etape 4 : Etat de la connexion VoIP

Pour appeler l'Agence principale, la Succursale doit composer le numéro 1234 sur son téléphone. A l'inverse, lorsque l'Agence principale veut appeler la Succursale, elle compose le numéro 6789.

Dans le menu **Diagnostics**, cliquez sur **Etat de la connexion VoIP**.

- **Canal :** si vous avez connecté deux téléphones sur les ports FXS1 et FXS2, la ligne 1 ou 2 vous indique celui qui est actuellement en communication.
- **Etat :** si vous êtes en communication le message *Actif* est visible.
  - ✓ *Repos* : cela signifie qu'aucune communication n'est en cours
  - ✓ *Collecte* : votre téléphone est en réception d'appel
  - ✓ *Actif* : vous avez décroché et vous êtes en communication
  - ✓ *Raccroché* : vous avez raccroché votre téléphone
- **Codec :** indique le Codec paramétré pour votre connexion VoIP.
- **ID distant :** indique l'interlocuteur qui vous appelle ou que vous appelez.
- **Connecté depuis :** le temps écoulé depuis le début de la connexion (temps en secondes).
- **Pqts TX / Pqts RX :** le nombre de paquets envoyés et reçus depuis le début de la connexion.
- **RX perdus :** le délai de transmission dépend de la qualité de la ligne ainsi que de la dimension du réseau. Un taux de perte de paquets faible signifie que la retranscription de la voix est de bonne qualité. Les causes de pertes de paquets peuvent être dues à une mauvaise qualité du réseau IP. En effet, dans un tel cas, lorsque le routeur ne peut plus traiter les paquets entrants, ceux-ci sont simplement supprimés.
- **Appels entrants / Appels sortants :** comptabilise le nombre d'appels reçus et envoyés depuis le dernier redémarrage du routeur.

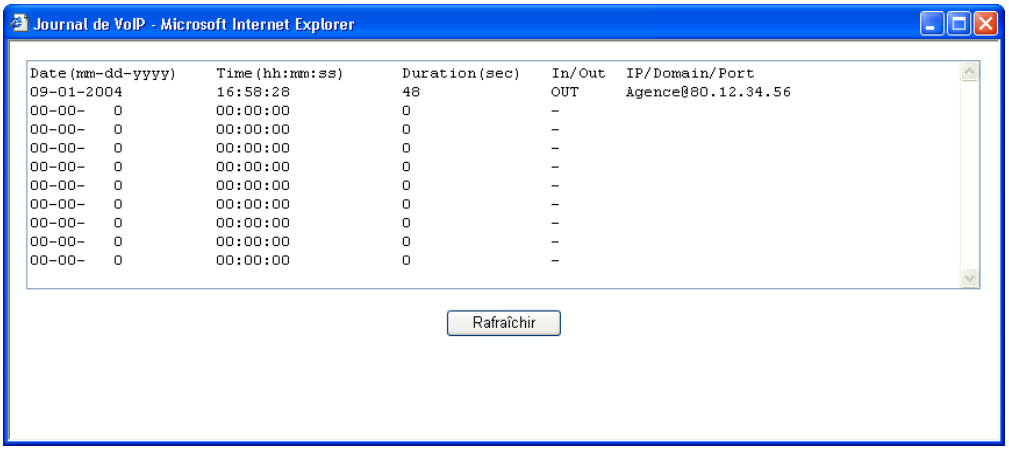
Etat de la connexion dans la Succursale



Canal	État	Codec	ID distant	Connecté depuis	Pqts Tx	Pqts Rx	Rx perdus	Rx décal (ms)	Appels entrants	Appels sortants	Volume
1	Actif	729A/B	Agence@80.12.34.56	48	7248	7249	0	15	0	1	5
2	Repos	729A/B		0	0	0	0	0	0	0	5

A noter : l'image précédente nous permet de déduire que c'est la Succursale qui est à l'origine de l'appel. L'ID distant correspond à l'adresse IP fixe de l'Agence.

En cliquant sur le bouton **Journal**, vous pouvez visualiser les derniers appels reçus ou envoyés.



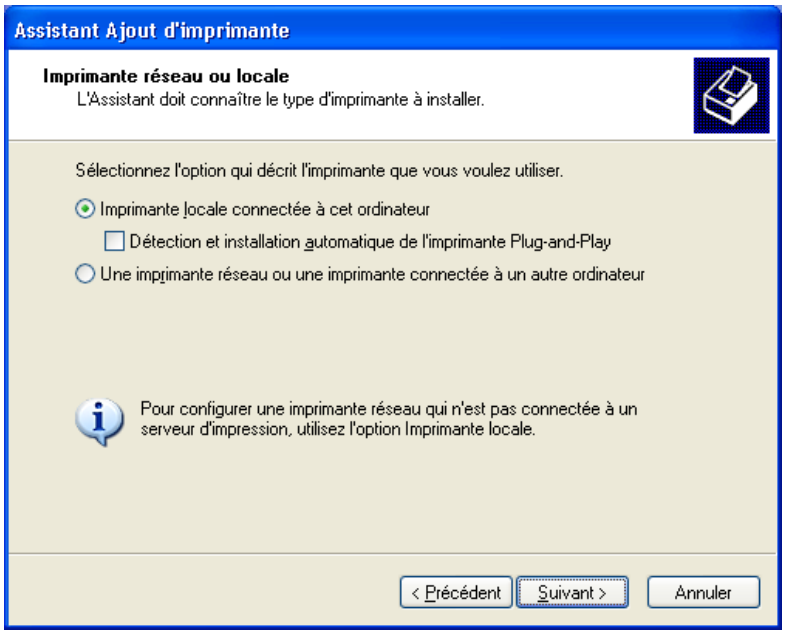
Date(mm-dd-yyyy)	Time(hh:mm:ss)	Duration(sec)	In/Out	IP/Domain/Port
09-01-2004	16:58:28	48	OUT	Agence@80.12.34.56
00-00- 0	00:00:00	0	-	
00-00- 0	00:00:00	0	-	
00-00- 0	00:00:00	0	-	
00-00- 0	00:00:00	0	-	
00-00- 0	00:00:00	0	-	
00-00- 0	00:00:00	0	-	
00-00- 0	00:00:00	0	-	
00-00- 0	00:00:00	0	-	
00-00- 0	00:00:00	0	-	

Partage de l'imprimante USB (Série VPN Booster 32)

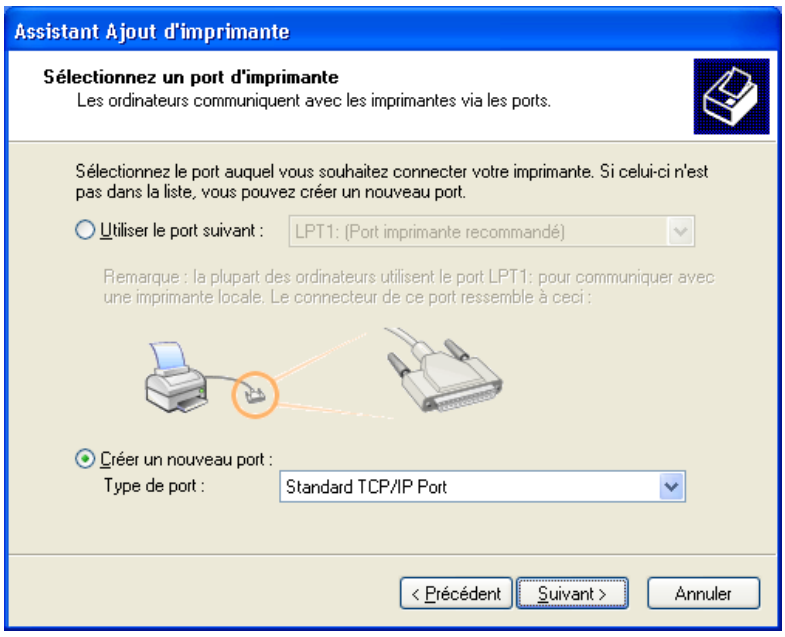
Le VPN Booster 32 permet de partager une imprimante et fait office de serveur d'impression. Après avoir correctement raccordé votre imprimante au VPN Booster 32 (dans le chapitre consacré aux raccordements du routeur du VPN Booster 32, reportez-vous à la partie dédiée au raccordement de l'imprimante USB), vous devez désormais configurer les ordinateurs de votre réseau local en installant sur chaque poste les pilotes de votre imprimante. Pour cela, procédez comme suit :

Attention : l'utilisation de l'imprimante via le VPN Booster 32 n'est possible que si vous êtes sous Windows 2000 ou Windows XP.

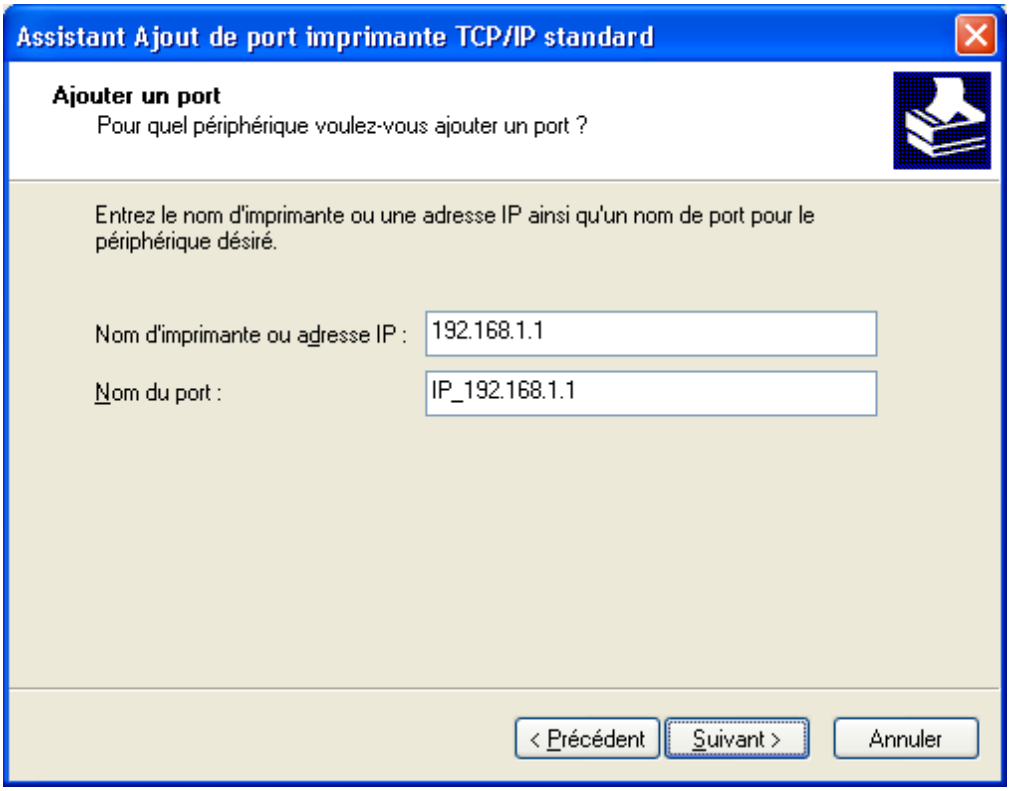
1. Cliquez sur **démarrer**, **Paramètres**, **Imprimantes et télécopieurs**.
2. Effectuez un double-clic sur **Ajouter une imprimante**.
3. L'**Assistant Ajout d'imprimante** apparaît. Cliquez sur **Suivant**.
4. Sélectionnez **Imprimante locale connectée à cet ordinateur**, puis cliquez sur **Suivant**.



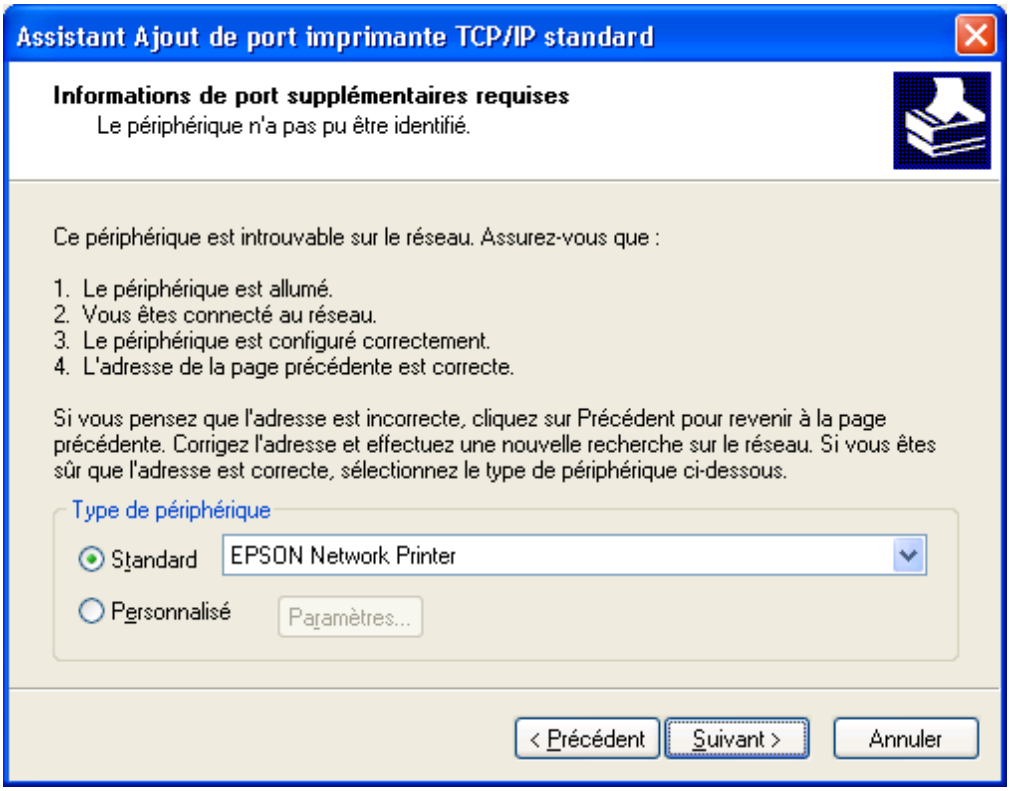
5. Sélectionnez **Créer un nouveau port**, puis dans la rubrique **Type de port**, sélectionnez **Standard TCP/IP Port**.



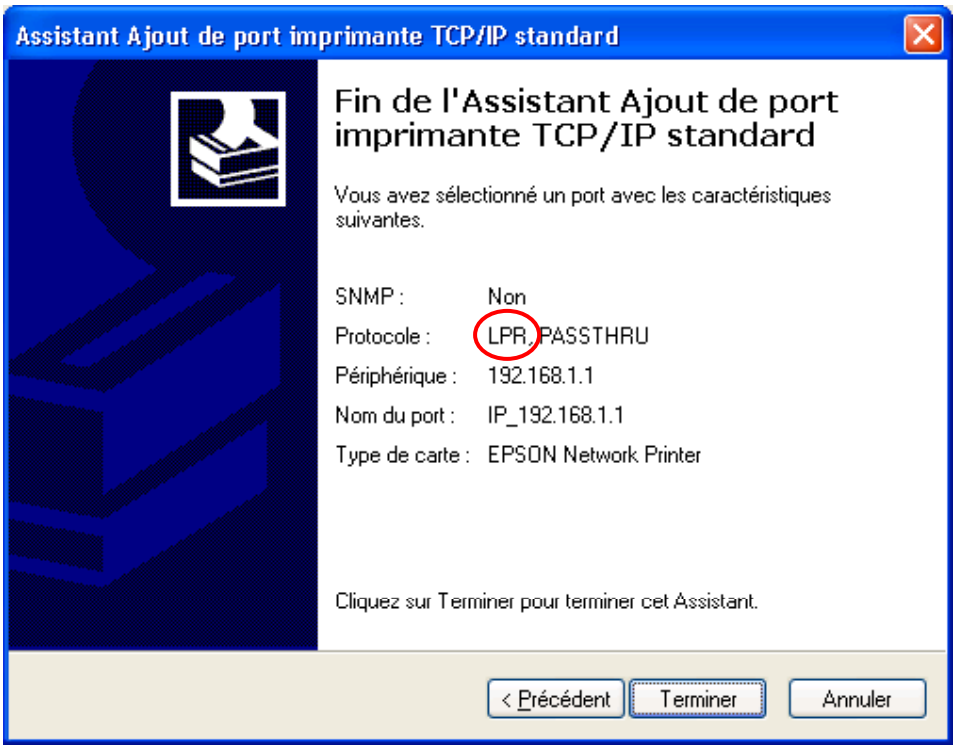
6. Vous allez désormais ajouter un port pour votre imprimante. Cliquez sur **Suivant**.
7. Dans la rubrique **Nom d'imprimante ou adresse IP**, saisissez l'adresse IP de votre routeur. Le nom du port est automatiquement créé. Cliquez sur **Suivant**.



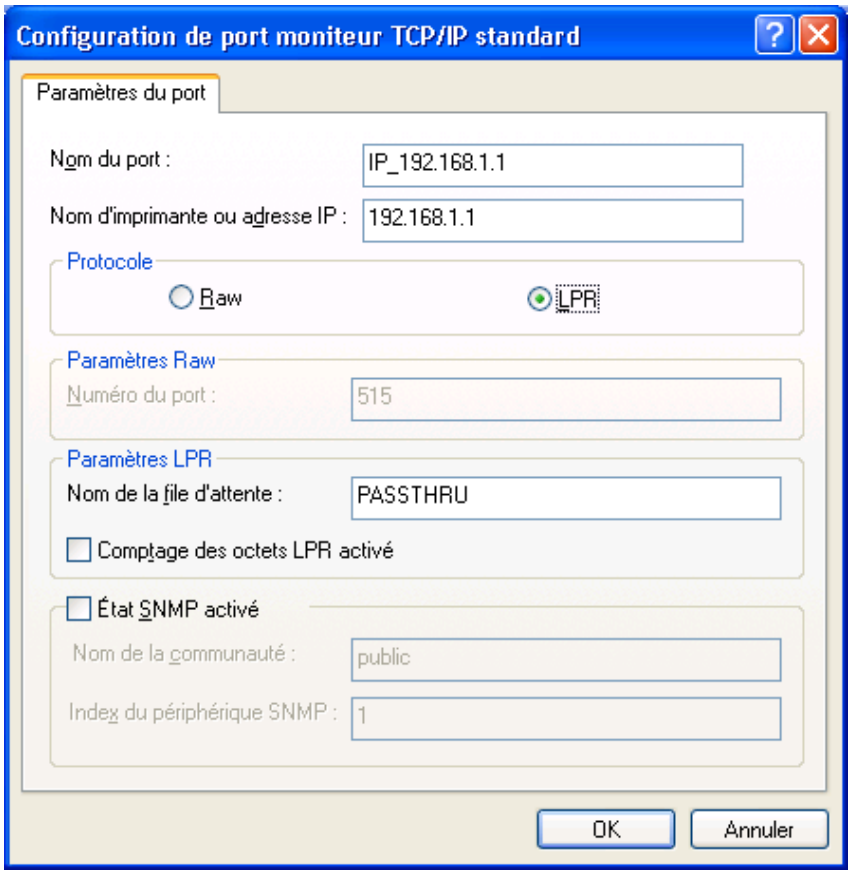
8. Dans la partie **Type de périphérique**, sélectionnez **Standard**, puis votre type de matériel. Cliquez sur **Suivant**.



9. Votre port imprimante a bien été ajouté. Cliquez alors sur **Terminer**.



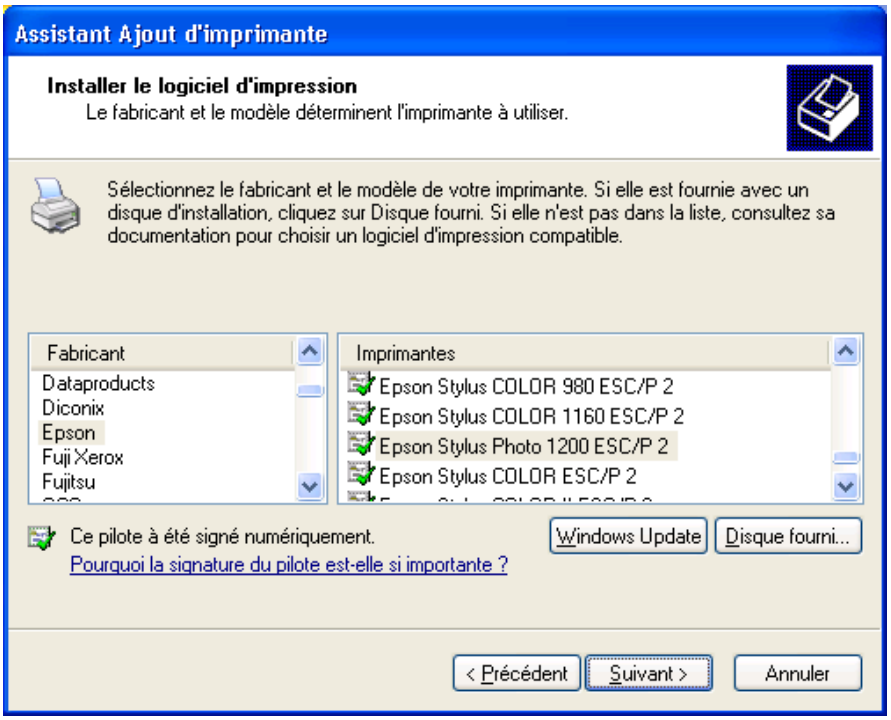
*Attention : vérifiez que le protocole **LPR** soit bien sélectionné par défaut. Si ce n'est pas le cas, cliquez sur le bouton **Précédent**. Dans la partie **Type de périphérique**, sélectionnez **Personnalisé** à la place de **Standard**, puis cliquez sur **Paramètres…**. La fenêtre suivante apparaît. Dans la partie **Protocole**, sélectionnez **LPR**, puis cliquez sur **OK**.*



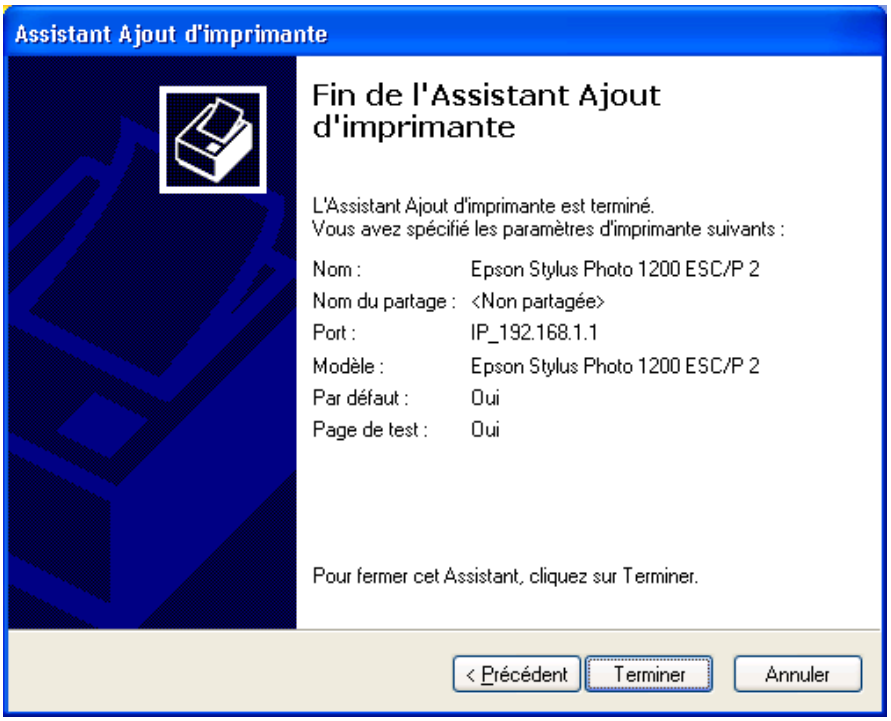
*Cliquez sur **Suivant**. Vous voici de nouveau dans la fenêtre récapitulant le type de port. Cliquez sur **Terminer**.*

10. Installez ensuite les pilotes de l'imprimante en sélectionnant tour à tour le fabricant, puis votre modèle d'imprimante. Cliquez sur **Suivant**.

    Remarque : si l'imprimante que vous souhaitez installer ne fait pas partie de cette liste, cliquez sur ***Disque fourni…****, puis installez les pilotes de votre imprimante grâce au CD-ROM du fabricant livré avec votre matériel.*

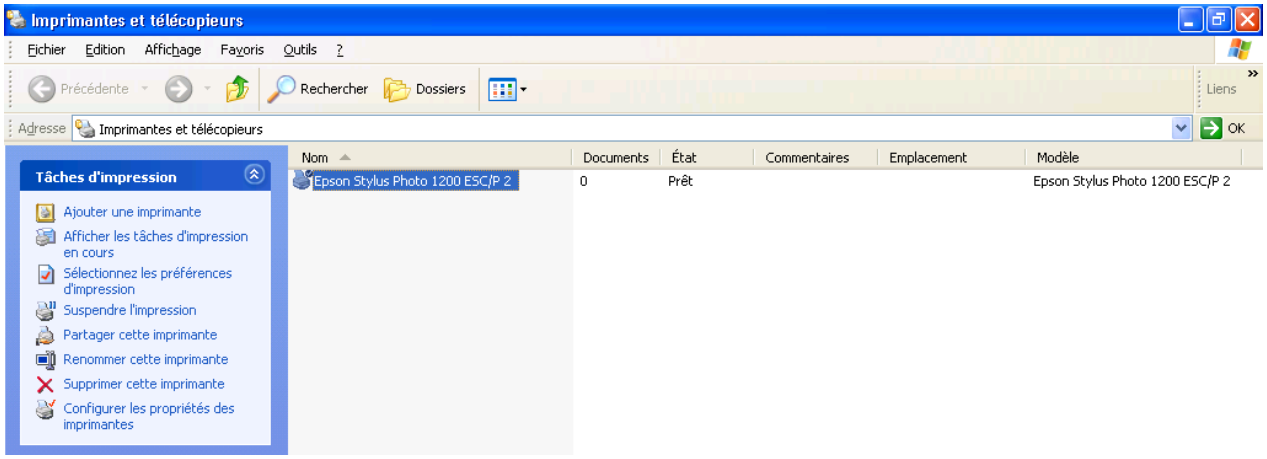


11. Sélectionnez **Conserver le pilote existant (recommandé)**, puis cliquez sur **Suivant**.
12. Si vous le souhaitez, modifiez le nom de votre imprimante, puis cliquez sur **Suivant**.
13. Dans la fenêtre consacrée au partage de l'imprimante, sélectionnez **Ne pas partager cette imprimante**, puis cliquez sur **Suivant**.
14. A la question *Voulez-vous imprimer une page de test ?*, sélectionnez **Oui**, puis cliquez sur **Suivant**.
15. Une fenêtre récapitulative apparaît. Cliquez sur **Terminer** pour fermer l'Assistant.



16. Votre page de test, si vous avez choisi de l'imprimer, va être envoyée à l'imprimante. Si cela fonctionne, cliquez sur **OK**.

17. L'imprimante est bien connectée à votre ordinateur, disponible et prête à répondre à vos requêtes d'impression.



Partie 4 :
Outils d'analyse et de contrôle

Outils de diagnostic

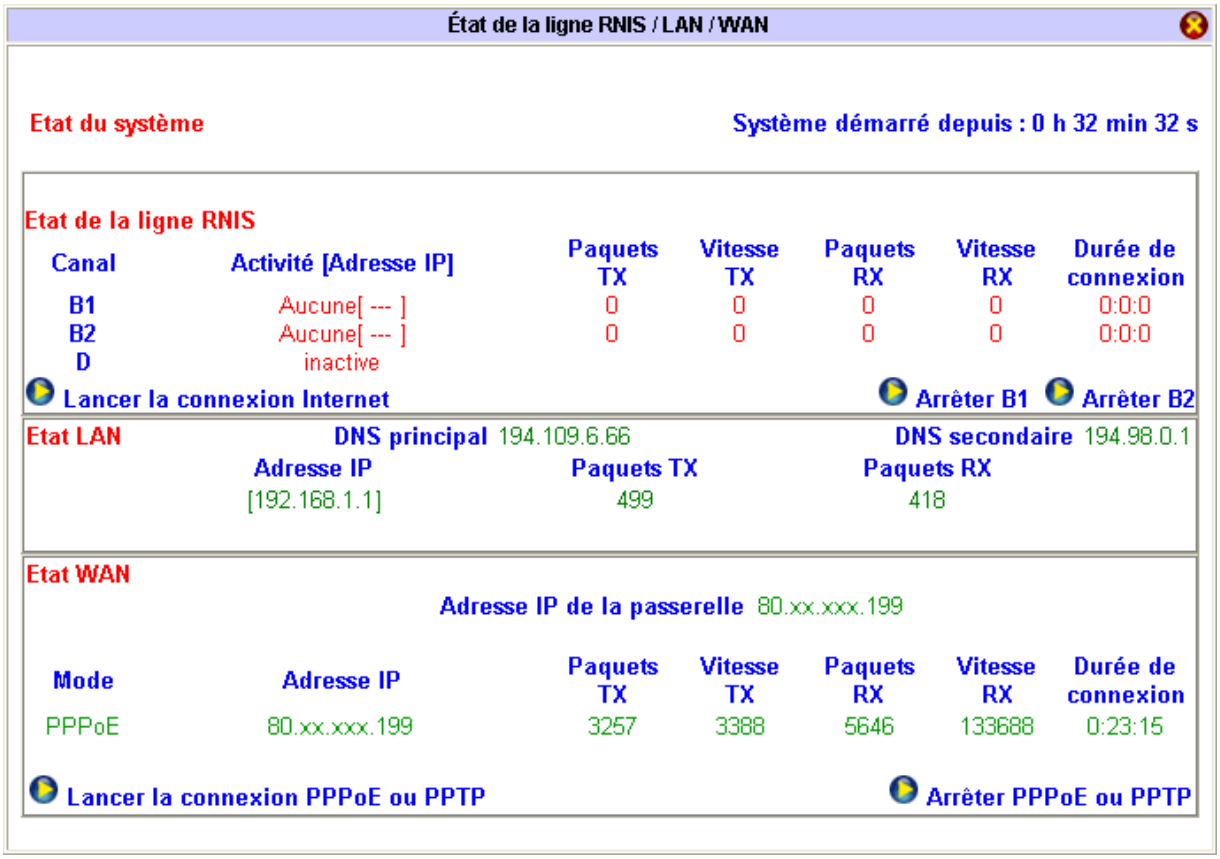
Le VPN Booster possède des outils d'analyse et de contrôle des connexions. En cliquant sur le menu **Diagnostics**, vous avez accès à ces fonctions de contrôle.

Etat de la connexion Internet

Cette page vous permet de suivre l'activité de votre liaison xDSL ou câble ainsi que l'activité de chaque canal B de votre ligne RNIS (VPN Booster 32 i uniquement). Elle indique également le nom de vos connexions.

Vous pouvez établir la connexion Internet en cliquant sur **Lancer la connexion PPPoE ou PPTP**. De la même manière, vous pouvez arrêter la liaison Internet en cliquant alors sur **Arrêter PPPoE ou PPTP**.

Si vous utilisez le module RNIS du VPN Booster 32 i, vous pouvez établir la connexion Internet en cliquant sur **Lancer la connexion Internet**. De la même manière, vous pouvez arrêter la connexion RNIS en cliquant alors sur **Arrêter B1** et/ou **Arrêter B2**.



La page HTML correspondant à cette rubrique vous permet de connaître l'état du réseau Ethernet. Elle est rafraîchie automatiquement toutes les 5 secondes.

Etat LAN

Vous pouvez connaître :

- l'adresse IP du routeur,
- le nombre de paquets envoyés et reçus par le routeur,
- les DNS utilisés.

Etat WAN

Dans cette partie, vous voyez apparaître le compte-rendu de votre liaison xDSL ou câble. Vous pouvez connaître :

- le protocole utilisé pour votre connexion (PPPoE, PPTP, Static IP ou DHCP Client),
- l'adresse IP de la passerelle,
- l'adresse IP attribuée par le fournisseur d'accès,
- le temps écoulé depuis le début de la connexion,
- le nombre de paquets envoyés et reçus depuis le début de la connexion.

Le bouton **Arrêter PPPoE ou PPTP** permet de déconnecter la liaison xDSL.

Etat de la ligne RNIS (VPN Booster 32 i)

Une activité sur le canal D est indispensable avant toute connexion.

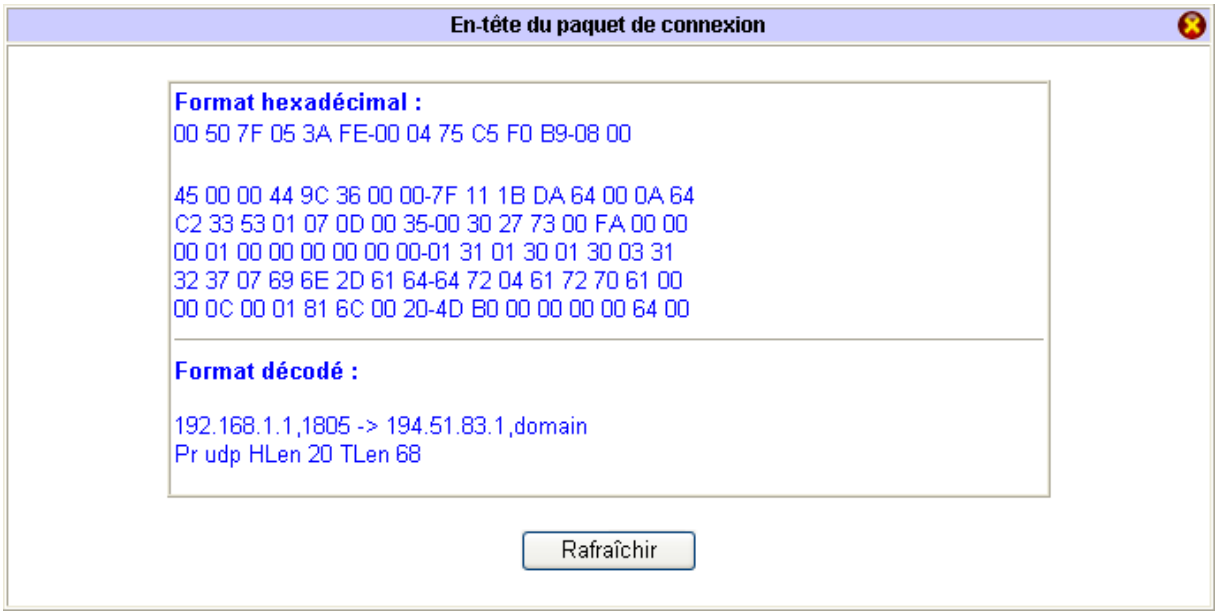
Pour chacun des canaux B de la ligne RNIS, vous pouvez connaître :

- l'activité,
  - **Aucune**, s'il n'y a pas de connexion,
  - le nom de la connexion s'il s'agit d'une connexion à Internet.
- l'adresse IP attribuée par le fournisseur d'accès,
- le temps écoulé depuis le début de la connexion,
- le nombre de paquets envoyés et reçus depuis le début de la connexion.

Les boutons **Arrêter B*n*** permettent de déconnecter les canaux concernés.

Visualisation de l'en-tête du paquet de connexion

Cette page vous permet de voir l'en-tête décodé du paquet qui a déclenché la dernière connexion (adresse IP, port utilisé, adresse DNS,…).

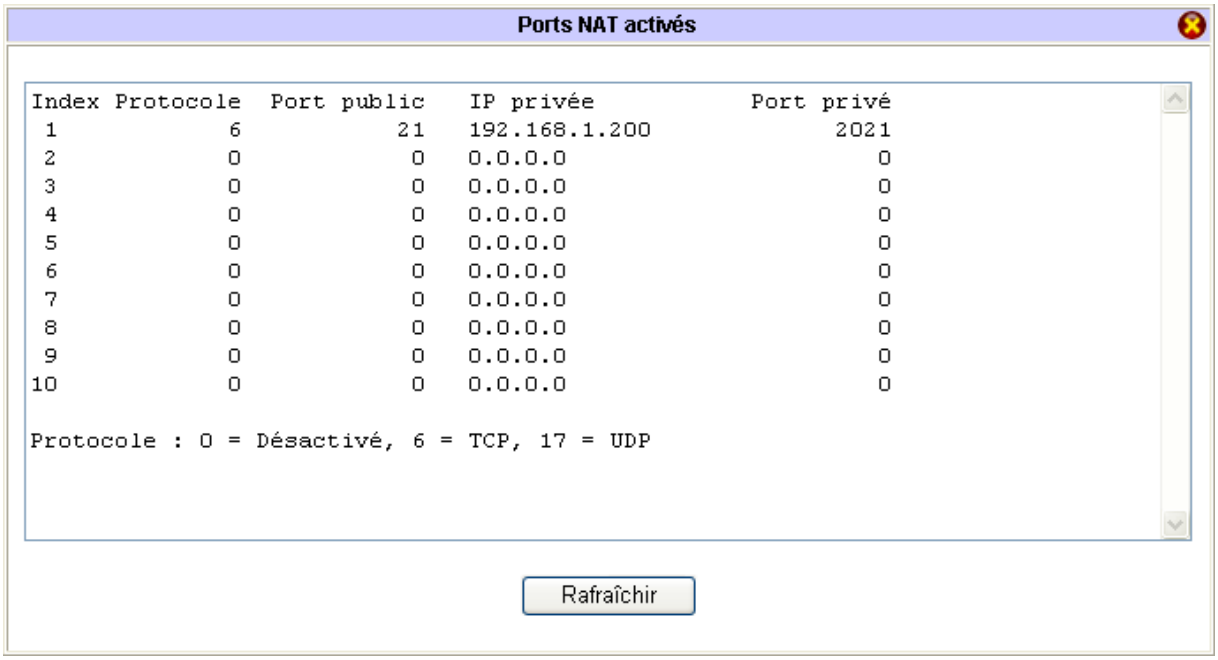


Visualisation de la table ARP

Cet outil vous permet de voir la correspondance entre l'adresse MAC et l'adresse IP des stations situées sur le réseau.

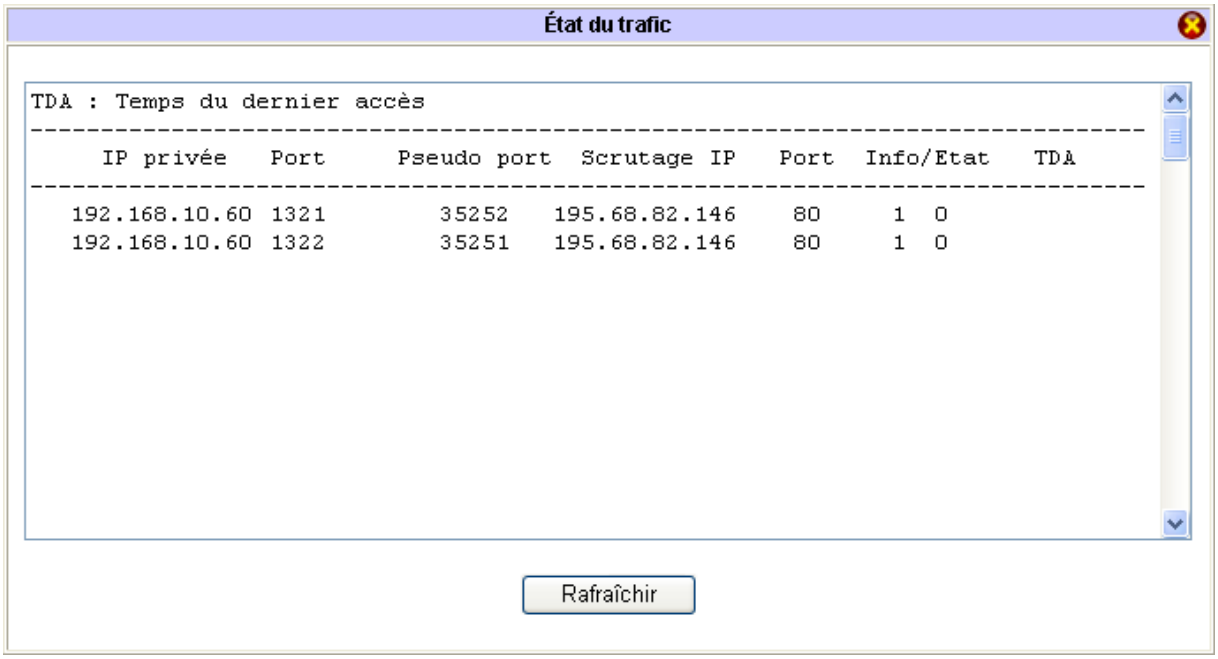
Visualisation de la table des ports NAT activés

Cet outil vous permet de voir toutes les redirections de port effectuées dans le paramétrage du NAT.



Etat du trafic

Cliquez sur **Etat du trafic**, puis sur **Rafraîchir**. La fenêtre indique la liste des requêtes formulées par chaque ordinateur à un moment donné avec le numéro de port concerné.



Paramétrage du Syslog

Mettre en service le Syslog permet de centraliser la réception de messages d'erreurs ou d'informations sur une machine de supervision. Syslog journalise ainsi les événements du système de façon continue sur ce que l'on nommera un serveur Syslog. Cette supervision permet de connaître les heures de connexion ainsi que l'adresse IP des machines qui déclenchent les appels. Les traces sont sauvegardées dans un fichier texte. Ceci signifie que le Syslog avertit mais ne filtre pas.

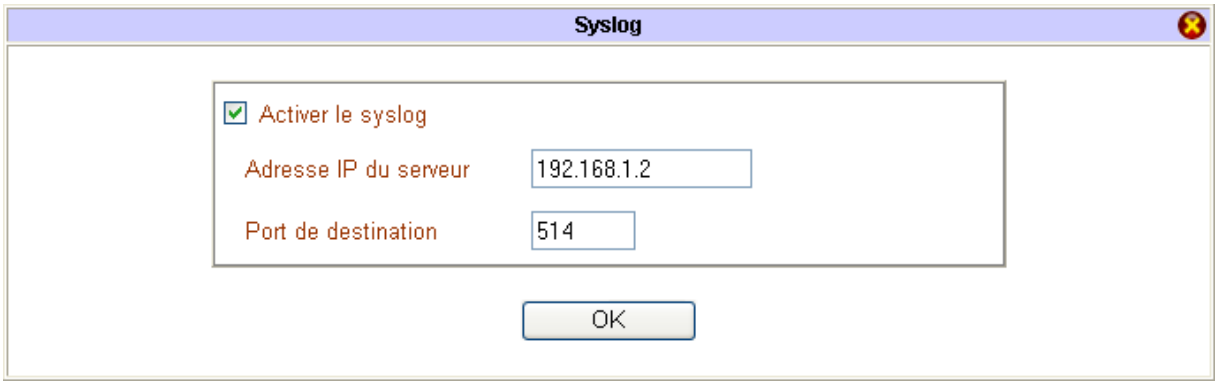
Vous devez réserver une machine de supervision dédiée à l'utilisation du BeWAN Syslog. Le logiciel BeWAN Syslog s'installe en même temps que les Utilitaires VPN Booster livrés sur le CD-ROM Routeurs VPN Booster.

Pour mettre en service le Syslog, procédez comme suit :

1. Installez tout d'abord sur la machine dédiée le logiciel BeWAN Syslog fourni sur le CD-ROM Routeurs VPN Booster. Cet utilitaire est présent avec les Utilitaires VPN Booster.
2. Dans le menu **Réglages Avancés** du configurateur Web du routeur, cliquez sur **Syslog**.
3. Cochez **Activer le syslog**.
4. Dans la rubrique **Adresse IP du serveur**, indiquez l'adresse IP de la machine dédiée sur laquelle est installé le BeWAN Syslog.

   Remarque : le port de destination 514 présent par défaut correspond au port standard Syslog. Si vous le modifiez, veillez bien à en faire de même du côté de la machine de supervision.

   Attention : sous Mac OS X, en raison du firewall interne qui, s'il est activé, bloque les ports 0 à 1023 inclus, le port standard du Syslog est le port 1028. Si vous utilisez donc le BeWAN Syslog sous ce système, veillez à bien changer le port de destination dans le configurateur Web du routeur.



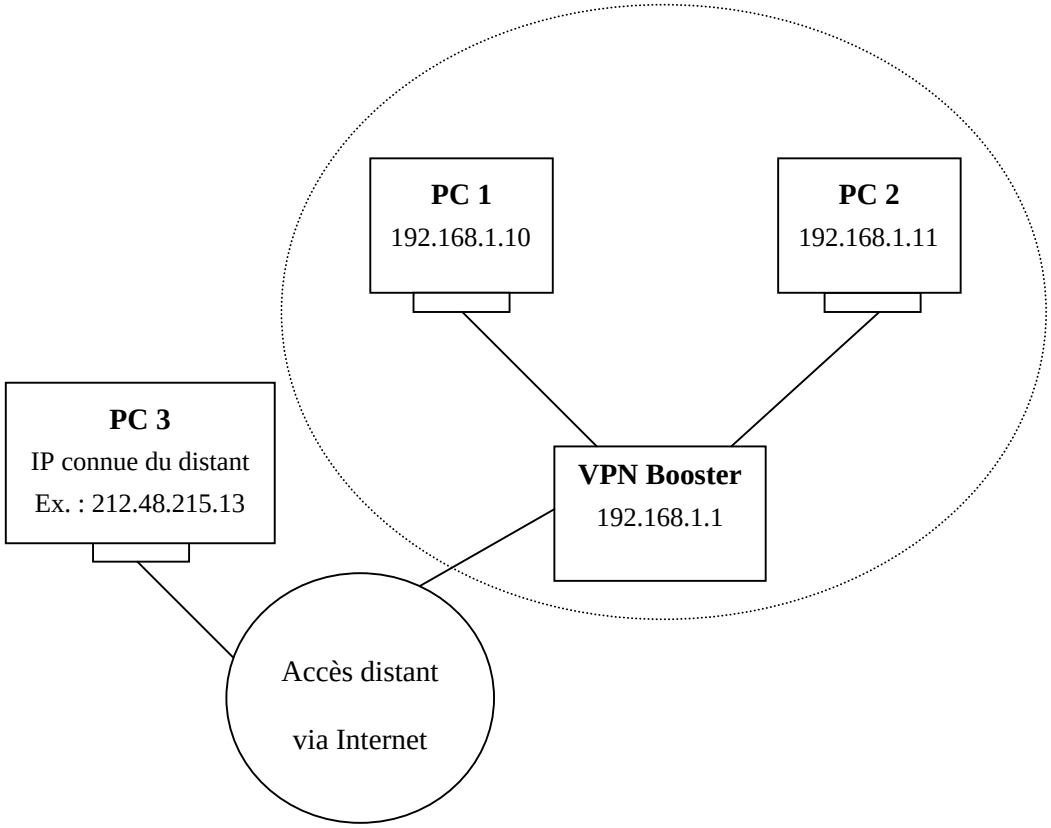
5. Cliquez sur **OK** pour valider les modifications.
6. Lancez ensuite l'utilitaire BeWAN Syslog à partir de la machine dédiée.
   - Si vous êtes sous Windows, cliquez sur **démarrer**, pointez sur **Tous les programmes**, **Utilitaires VPN Booster**, puis cliquez sur **BeWAN Syslog**.
   - Si vous êtes sous Mac OS 9, cliquez sur le menu **Pomme**, pointez sur **Tableaux de bord**, **Utilitaires VPN Booster**, puis cliquez sur **BeWAN Syslog**.
   - Si vous êtes sous Mac OS X, effectuez un double-clic sur le fichier **Utilitaires VPN Booster.dmg**. Un disque **Utilitaires VPN Booster** est créé sur le bureau de votre Macintosh. Effectuez un double clic sur ce disque. Lancez le BeWAN Syslog.

Maintenant, à chaque connexion, réinitialisation ou autre utilisation du routeur, un message Syslog sera envoyé sur la machine automatiquement.

Fonctionnalités d'administration

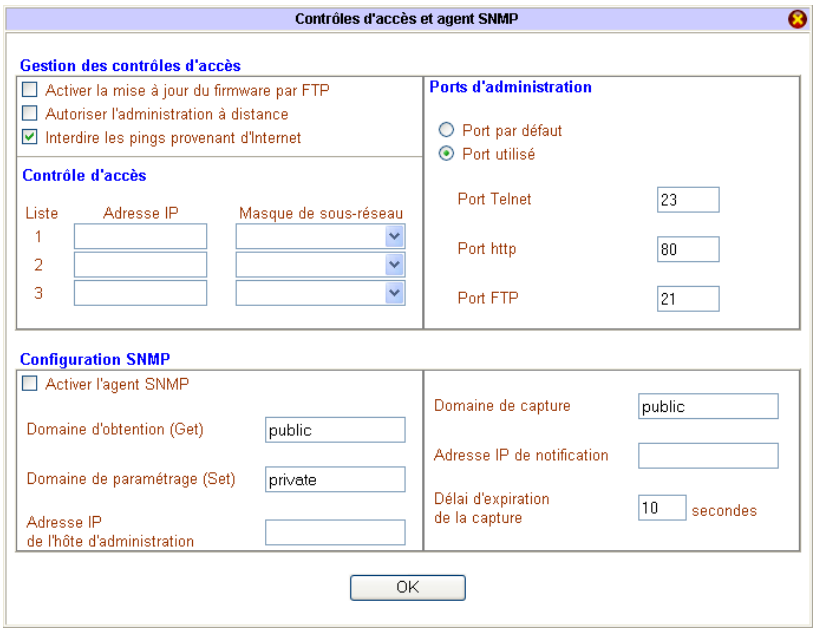
Gestion du contrôle d'accès

Le contrôle d'accès permet de gérer les utilisateurs autorisés à paramétrer le routeur. Pour saisir le principe, nous allons prendre un exemple concret. Dans le menu **Administration Système**, sélectionnez **Contrôles d'accès et agent SNMP**.



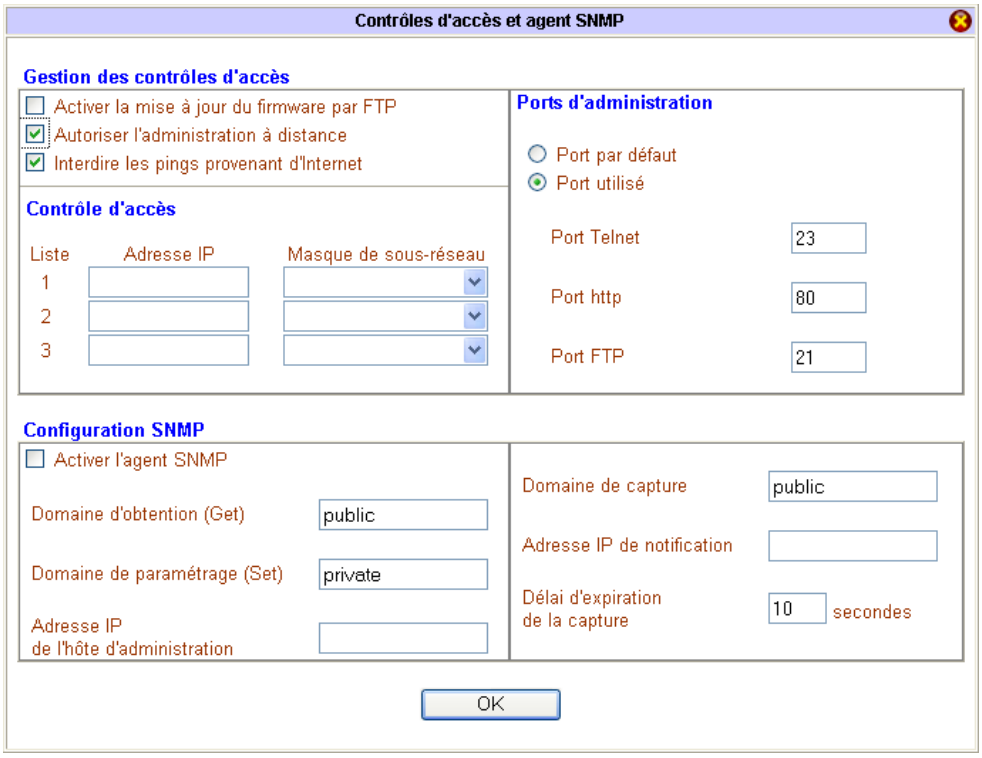
Cas numéro 1 : les PC 1 et 2 peuvent accéder au paramétrage du routeur après la vérification du nom d'utilisateur et du mot de passe.

*Remarque : par défaut, **Autoriser l'administration à distance** est décochée.*



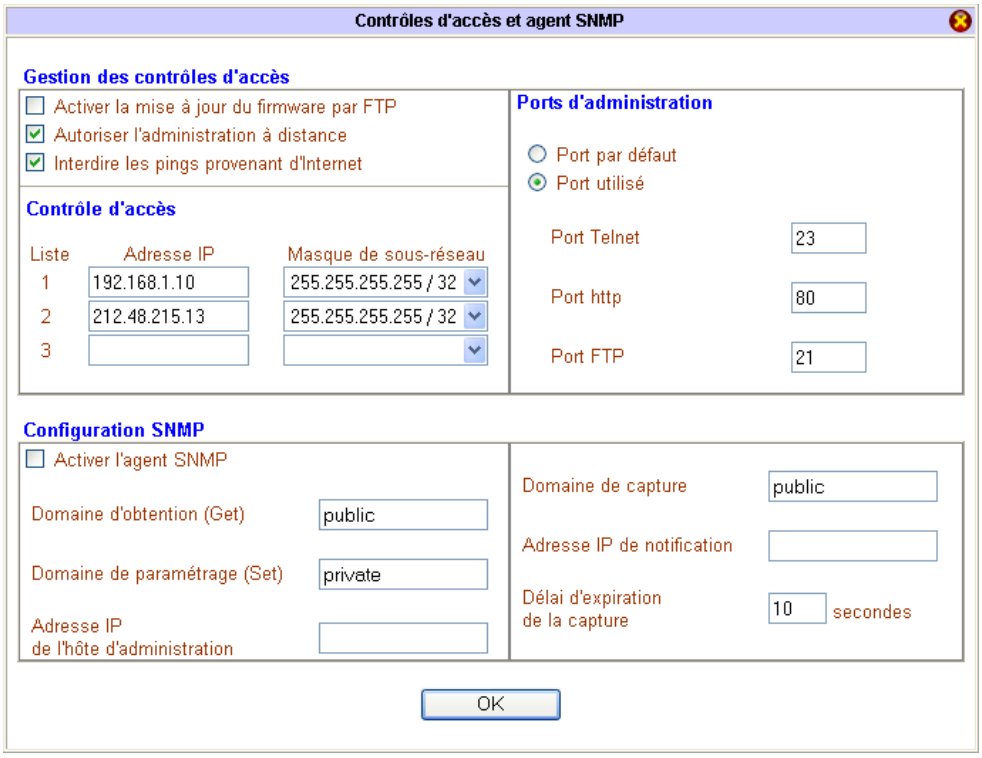
Cas numéro 2 : les PC 1, 2 et 3 peuvent accéder au paramétrage du routeur après la vérification du nom d'utilisateur et du mot de passe.

Cochez **Autoriser l'administration à distance**, puis cliquez sur **OK** pour valider.



Cas numéro 3 : les PC 1 et 3 peuvent accéder au paramétrage du routeur après la vérification du nom d'utilisateur et du mot de passe.

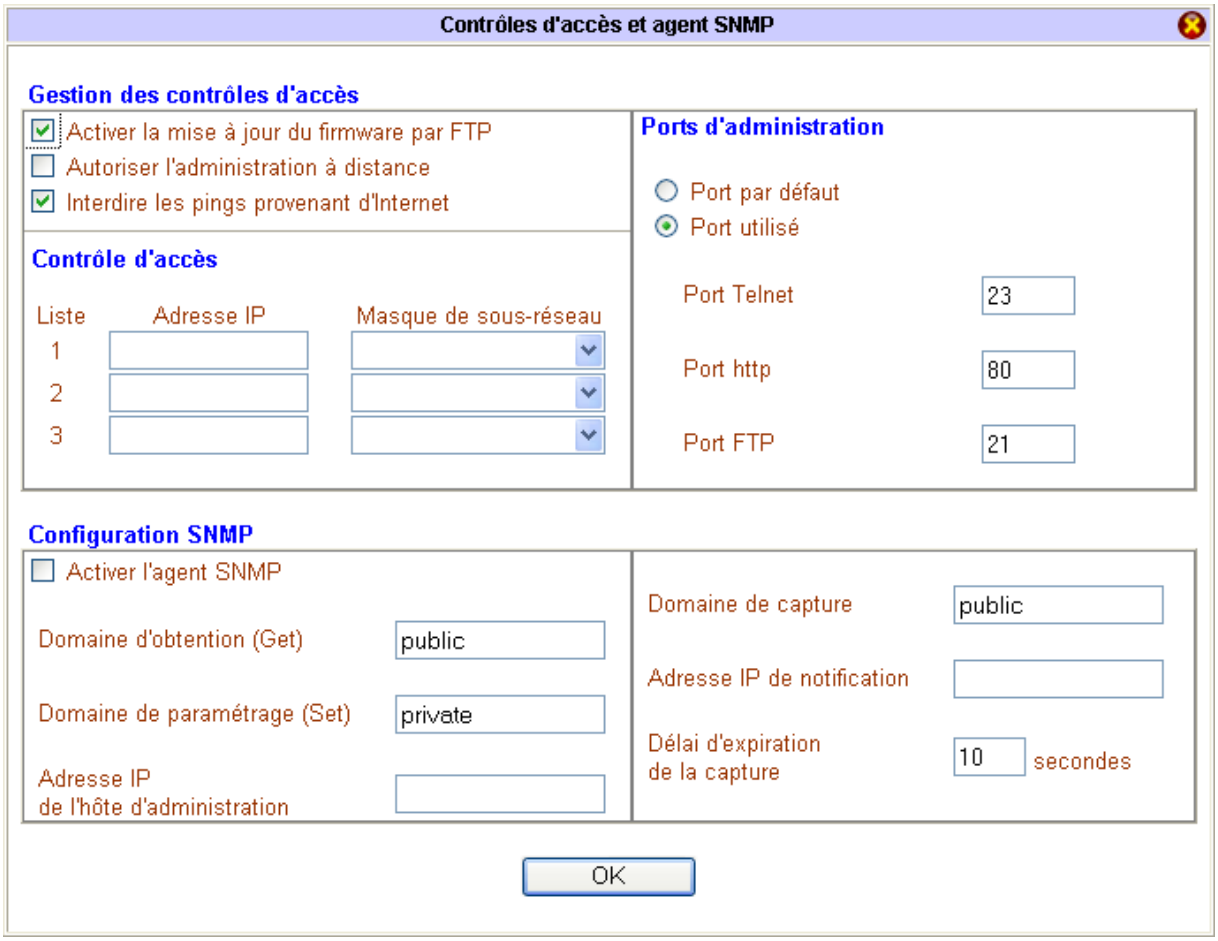
1. Cochez **Autoriser l'administration à distance**.
2. Dans la partie **Contrôle d'accès**, saisissez les adresses qui ont la possibilité de procéder à l'activation à distance, puis cliquez sur **OK** pour valider.



Mise à jour du firmware par FTP

Vous avez la possibilité de mettre à jour le firmware du VPN Booster par FTP. La mise à jour via FTP vous permet de remplacer le .ALL (fichier de mise à jour du firmware) ou le .CFG (fichier de mise à jour de la configuration). Pour effectuer ce mode de mise à jour, procédez comme suit :

1. Dans le menu **Administration Système**, sélectionnez **Contrôles d'accès et agent SNMP**.
2. Cochez **Activer la mise à jour du firmware par FTP**, puis cliquez sur **OK**.



3. Lancez le Client FTP dont vous disposez.
4. Saisissez l'adresse IP du routeur, le nom d'utilisateur et le mot de passe.
5. Une fois connecté au routeur, les fichiers .ALL et .CFG contenus dans la mémoire du routeur apparaissent directement dans le répertoire d'accueil de votre Client FTP.
6. Procédez à la mise à jour en téléchargeant via FTP les nouveaux fichiers de mise à jour.

Attention : pour que ce nouveau fichier de mise à jour (.ALL ou .CFG) soit pris en compte, il doit être nommé de la même manière que le fichier existant. Renommez donc le nouveau fichier à l'identique afin d'écraser celui présent dans la mémoire du VPN Booster.

Remarques :

- *La mise à jour ne provoque pas de redémarrage automatique. Il est donc conseillé de démarrer manuellement le routeur afin de prendre en compte les modifications apportées.*
- *Outre pour la mise à jour, vous pouvez également utiliser ce moyen pour récupérer les fichiers du VPN Booster en les copiant dans un dossier de votre disque dur.*

Commandes Telnet

Nous avons vu que le VPN Booster pouvait être configuré très simplement grâce à un configurateur Web.

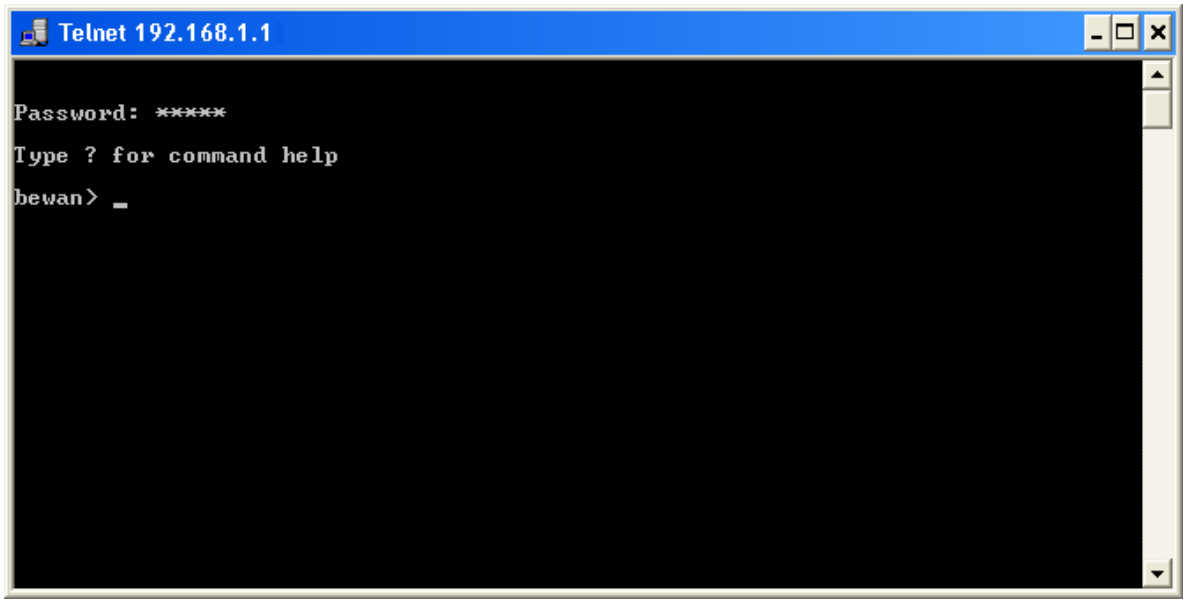
Vous pouvez également effectuer la configuration du VPN Booster via des commandes Telnet. Attention : la configuration de certains paramètres n'est pas possible en session Telnet.

Ouvrir une session Telnet

Pour démarrer le mode de configuration Telnet du VPN Booster à partir d'un PC sous Windows, procédez comme suit :

1. Cliquez sur **démarrer**, puis sur **Exécuter…**.
2. Tapez **telnet 192.168.1.1** (sauf si vous avez modifié l'adresse IP par défaut de votre VPN Booster).
3. Lorsque le libellé **Password** apparaît, entrez votre mot de passe d'accès au mode administrateur du VPN Booster, puis appuyez sur la touche **ENTRÉE**.

   Rappel : si vous ne l'avez pas encore modifié en mode HTML (voir « Modification des paramètres administrateur » page 69), le mot de passe par défaut du VPN Booster est « bewan ».



Principes de base de Telnet

Lorsque votre mot de passe a été vérifié, votre nom d'utilisateur apparaît suivi du caractère >.

***VotreNom*>**

Pour envoyer une commande Telnet au routeur, saisissez-la, puis appuyez sur la touche **ENTRÉE**.

Par exemple, pour obtenir la liste des commandes Telnet, tapez **?** puis appuyez sur la touche **ENTRÉE** :

***VotreNom*> ?**
% Valid commands are:
ddns ddos exit ip ipf isdn log mngt quit srv sys urlf wan

Pour obtenir une aide en ligne sur une commande Telnet particulière, entrez celle-ci, tapez **?**, puis appuyez sur la touche **ENTRÉE**. Voir l'exemple ci-dessous :

VotreNom> log ?

usage:

log [-cfhipstwx?][-F a|c|f|s|w]

-c for call log

-f for IP filter log

-F flush log buffer

- **a flush all logs**
- **c flush the call log**
- **f flush the IP filter log**
- **s flush the IP state log**
- **w flush the wan log**

-h for this usage help

-p for PPP/MP log

-s for IP state log

-t display to the end

-w for WAN log

-x for packet body hex dump

Les 20 dernières commandes Telnet que vous avez entrées sont mémorisées. Vous pouvez ainsi les faire défiler une à une en appuyant sur les touches FLÈCHE HAUT et FLÈCHE BAS. Vous pouvez également utiliser la commande **sys cmdlog** pour les lister.

Après 2 minutes d'inactivité, la session Telnet se déconnecte automatiquement.

Vous ne pouvez pas ouvrir deux sessions Telnet simultanément.

Pour toute information complémentaire sur le fonctionnement du logiciel Telnet, veuillez vous reporter à l'aide en ligne de Microsoft.

Liste des commandes principales

Pour configurer votre routeur, vous disposez des commandes Telnet suivantes :

Ddns	Consultation des paramètres DynDNS
Ddos	Configuration des défenses DoS
Exit	Fermeture de la session Telnet
Ip	Configuration du réseau TCP/IP : routage…
Ipf	Configuration des filtres IP
Isdn	Configuration de l'interface RNIS
Log	Fonctions de diagnostic
Mngt	Fonctionnalités d'administration
Quit	Fermeture de la session Telnet
Srv	Configuration des fonctions serveur : NAT, DHCP
Sys	Commandes système
Urlf	Configuration du filtrage de contenu
Wan	Modification du MTU

Liste des sous-commandes

Liste des sous-commandes DDNS

1. Obtenir des informations sur la configuration du DNS dynamique
   Etat de la mise à jour, login et mot de passe utilisés, nom d'hôte, adresse IP de connexion

   ***VotreNom*> ddns log**

Liste des sous-commandes DDOS

1. Activer le système des défenses DoS

   ***VotreNom*> ddos -A**

2. Désactiver le système des défenses DoS

   ***VotreNom*> ddos -D**

3. Afficher la liste des défenses DoS afin de visualiser leur activation ou non

   ***VotreNom*> ddos -V**

Liste des sous-commandes EXIT

1. Quitter la session Telnet

   ***VotreNom*> exit**

Liste des sous-commandes IP

1. Obtenir l'adresse IP actuelle du routeur

   ***VotreNom*> ip addr ?**
   % ip addr <IP address>
   % Now: 192.168.1.1

2. Changer l'adresse IP du routeur

   ***VotreNom*> ip addr <nouvelle adresse IP>**
   % Set IP address OK !!!

3. Effectuer un ping sur l'adresse IP

   ***VotreNom*> ip ping**
   % ip ping <IP address>

   Exemple : ***bewan*> ip ping 192.168.1.10**
   Pinging 192.168.1.10 with 64 bytes of Data:

   Receive reply from 192.168.1.10, time=10ms
   Receive reply from 192.168.1.10, time=10ms
   Receive reply from 192.168.1.10, time=10ms
   Receive reply from 192.168.1.10, time=10ms
   Receive reply from 192.168.1.10, time=10ms

   Packets: Sent = 5, Received = 5, Lost = 0 (0% loss)

4. Visualiser la liste de la table ARP du routeur

   ***VotreNom*> ip arp status**
   [ARP Table for Ethernet Interface]
   IP Address MAC Address
   192.168.1.75 00-00-E8-8F-B9-B5
   192.168.1.77 00-50-DA-3B-2C-85

5. Ajouter une entrée dans le cache ARP du routeur

   ***VotreNom*> ip arp add <IP Address> <MAC Address> <LAN or WAN>**

   Exemple : ***bewan*> ip arp add 192.168.1.76 00-50-7F-00-00-33 LAN**

6. Supprimer une entrée dans le cache ARP du routeur

   ***VotreNom*> ip arp del <IP Address>**

   Exemple : ***bewan*> ip arp del 192.168.1.76**
   IP Address MAC Address
   192.168.1.75 00-00-E8-8F-B9-B5
   192.168.1.77 00-50-DA-3B-2C-85

7. Ajouter une route statique

   ***VotreNom*> ip route add**
   % ip route add <dst> <netmask> <gateway> <iface> <rtype>

c'est-à-dire :	**dst**	Destination hôte/réseau
	netmask	Masque de sous-réseau de destination
	gateway	Passerelle à utiliser
	iface	0 : interface Ethernet
		3 : interface WAN
	rtype	S : routage statique

   Exemple : ***bewan*> ip route add 0.0.0.0 0.0.0.0 192.168.1.100 0 S**

8. Visualiser la table de routage IP du routeur

   ***VotreNom*> ip route status**
   Codes : C - connected, S - static, R - RIP, * - default
   S 0.0.0.0/ 0.0.0.0 via 192.168.1.100, IF0
   C 100.0.0.0/ 255.0.0.0 is directly connected, IF0

9. Supprimer une route statique du routeur

   ***VotreNom*> ip route del**
   % ip route del <dst> <netmask> <rtype>

   Exemple : ***bewan*> ip route del 0.0.0.0 0.0.0.0 S**

10. Libérer les paramètres du client DHCP du routeur

    ***VotreNom*> ip dhcpc release**

11. Renouveler les paramètres du client DHCP du routeur

    ***VotreNom*> ip dhcpc renew**

12. Afficher les paramètres du client DHCP du routeur

    ***VotreNom*> ip dhcpc status**

13. Spécifier une adresse IP WAN pour accéder à Internet via une passerelle

    ***VotreNom*> ip wanaddr**
    % ip wanaddr <IP address> <IP netmask>
    c'est-à-dire : **IP address** Adresse IP
    IP netmask Masque de sous-réseau
    % Set WAN IP address OK !!!

    Exemple : ***bewan*> ip wanaddr 192.168.2.1 255.255.255.0**

    Remarque : l'adresse IP WAN du routeur doit se trouver dans la plage d'adressage de la passerelle.

Liste des sous-commandes IPF

1. Obtenir la version du filtre

   ***VotreNom*> ipf -v**

2. Afficher le journal de filtrage

   ***VotreNom*> ipf view**

3. Effacer le journal de filtrage

   ***VotreNom*> ipf -z**

Liste des sous-commandes ISDN

1. Lancer manuellement une connexion Internet ou une interconnexion de réseaux

   ***VotreNom*> isdn dial <nom de la connexion>**
   Exemple : ***bewan*> isdn dial Wanadoo**

   Après avoir saisi la commande ci-dessus, le routeur établira la connexion Internet pour appeler Wanadoo.

2. Arrêter un canal B RNIS manuellement

   ***VotreNom*> isdn drop <B1 ou B2>**
   Exemple : ***bewan*> isdn drop B1**

   Cette commande coupe la connexion sur le canal B spécifié.

Liste des sous-commandes LOG

Ces commandes vous permettent de vérifier le processus de connexion. Pour déterminer le problème rencontré, nous vous conseillons au préalable de vider du « buffer » tous les éléments retenus en mémoire. Une fois cette action effectuée, vous pouvez lancer votre connexion. En cas d'appel au support technique, ces informations vous seront demandées afin de diagnostiquer le problème rencontré.

1. Obtenir des informations de connexion sur tous les derniers appels depuis le redémarrage du routeur

   ***VotreNom*> log -c**

2. Obtenir des informations sur toutes les dernières négociations PPP depuis le redémarrage du routeur

   ***VotreNom*> log -p**

3. Afficher une copie hexadécimale et ASCII des paquets d'appel

   ***VotreNom*> log -p -x**

4. Obtenir des informations sur toutes les dernières connexions WAN depuis le redémarrage du routeur

   ***VotreNom*> log -w**

5. Afficher une copie hexadécimale et ASCII des paquets WAN qui transitent par le routeur

   ***VotreNom*> log -w -x**

6. Supprimer toutes les mémoires de log du « buffer »

   ***VotreNom*> log -F a** (efface toutes les logs en mémoire)
   ***VotreNom*> log -F c** (efface tous les logs d'appel en mémoire)
   ***VotreNom*> log -F f** (efface tous les logs de filtrage en mémoire)
   ***VotreNom*> log -F w** (efface tous les logs des connexions WAN)

Liste des sous-commandes MNGT

1. Afficher le port FTP utilisé

   ***VotreNom*> mngt ftpport ?**

   Exemple : ***bewan*> mngt ftpport ?**
   % % mngt ftpport <FTP port>
   %% Current setting is 21

2. Changer le port FTP utilisé

   ***VotreNom*> mngt ftpport <FTP port>**

   Exemple : ***bewan*> mngt ftpport 43**
   % Set FTP server port to 43 done

3. Afficher le port http utilisé

   ***VotreNom*> mngt httpport ?**

   Exemple : ***bewan*> mngt httpport ?**
   %% mngt httpport <http port>
   %% Current setting is 80

4. Changer le port http utilisé

   ***VotreNom*> mngt httpport <http port>**

5. Afficher le port telnet utilisé

   ***VotreNom*> mngt telnetport ?**

   Exemple : ***bewan*> mngt telnetport ?**
   %% mngt telnetport <Telnet port>
   %% Current setting is 23

6. Changer le port telnet utilisé

   ***VotreNom*> mngt telnetport <Telnet port>**

7. Activer la mise à jour du firmware par FTP

   ***VotreNom*> mngt ftpserver enable**
   % FTP server has been enabled

8. Désactiver la mise à jour du firmware par FTP

   ***VotreNom*> mngt ftpserver disable**
   % FTP server has been disabled

9. Activer l'autorisation d'administration à distance

   ***VotreNom*> mngt rmtcfg enable**
   % Remote configure function has been enabled

10. Désactiver l'autorisation d'administration à distance

    ***VotreNom*> mngt rmtcfg disable**
    % Remote configure function has been disabled

11. Activer l'interdiction des pings provenant d'Internet

    ***VotreNom*> mngt echoicmp enable**
    %% Echo ICMP packet enabled

12. Désactiver l'interdiction des pings provenant d'Internet

    ***VotreNom*> mngt echoicmp disable**
    %% Echo ICMP packet disabled

Liste des sous-commandes QUIT

1. Quitter la session Telnet

   ***VotreNom*> quit**

Liste des sous-commandes SRV

1. Activer le serveur DHCP

   ***VotreNom*> srv dhcp on**

2. Désactiver le serveur DHCP

   ***VotreNom*> srv dhcp off**

3. Spécifier le nombre d'adresses à affecter au serveur DHCP

   ***VotreNom*> srv dhcp ipcnt <IP counts** (nombre de comptes assignés par le serveur DHCP)**>**

   Exemple : ***bewan*> srv dhcp ipcnt 43**

   *Remarque : le nombre maximal de comptes gérés ne peut pas dépasser 50. Après avoir tapé cette commande, vous devez taper la commande **sys reboot** pour redémarrer le routeur.*

4. Spécifier l'adresse IP de départ de la plage DHCP

   ***VotreNom*> srv dhcp startip <adresse IP de départ>**

5. Réserver une adresse IP fixe dans la plage DHCP pour une adresse MAC spécifique

   ***VotreNom*> srv dhcp fixip add <IP Addr> <MAC Addr XX-XX-XX-XX-XX-XX> <Host ID>**
   c'est-à-dire :

IP Addr	Adresse IP fixe désirée pour un hôte spécifique
MAC Addr	Adresse Mac de la carte réseau de l'hôte spécifique
Host ID	Identification de l'hôte

6. Supprimer une réservation d'adresse IP dans la plage DHCP

   ***VotreNom*> srv dhcp fixip del <adresse IP fixe à supprimer>**

7. Effacer toutes les réservations d'adresses IP dans la plage DHCP

   ***VotreNom*> srv dhcp fixip clr**

8. Visualiser les comptes DHCP assignés par le routeur

   ***VotreNom*> srv dhcp status**
   DHCP server: Running
   Default gateway: 192.168.1.1

Index	IP Address	MAC Address	Leased Time	HOST ID
1	192.168.1.1	00-50-7F-00-00-33	ROUTER IP	bewan

9. Spécifier le DNS principal

   ***VotreNom*> srv dhcp dns1 <DNS IP address>**

10. Spécifier le DNS secondaire

    ***VotreNom*> srv dhcp dns2 <DNS IP address>**

11. Forcer l'utilisation des DNS saisis dans les paramètres TCP/IP du routeur (Commande non disponible sur le VPN Booster 8)

    ***VotreNom*> srv dhcp frcdnsmanl on**
    % Domain name server now is using manual settings!

12. Ne pas forcer l'utilisation des DNS saisis dans les paramètres TCP/IP du routeur (Commande non disponible sur le VPN Booster 8)

    ***VotreNom*> srv dhcp frcdnsmanl off**
    % Domain name server now is using auto settings!

13. Changer la passerelle par défaut affectée aux clients DHCP (par défaut, il s'agit de l'adresse IP du routeur)

    ***VotreNom*> srv dhcp gateway <Gateway IP** (adresse IP de la nouvelle passerelle)**>**

14. Changer le délai d'expiration des comptes du serveur DHCP (bail)

    ***VotreNom*> srv dhcp leasetime <Lease Time (sec.)>**

    Exemple : ***bewan*> srv dhcp leasetime 9000**

15. Visualiser les entrées de la table NAT

    ***VotreNom*> srv nat status**
    % NAT server: Running

    NAT Port Redirection Running Table:

Index	Protocol	Public Port	Private IP	Private Port
1	0	0	0.0.0.0	0
2	0	0	0.0.0.0	0
3	0	0	0.0.0.0	0
4	0	0	0.0.0.0	0
5	0	0	0.0.0.0	0
…				
16	0	0	0.0.0.0	0
17	0	0	0.0.0.0	0
18	0	0	0.0.0.0	0
19	0	0	0.0.0.0	0
20	0	0	0.0.0.0	0

    Protocol: 0 = Disable, 6 = TCP, 17 = UDP

16. Ajouter une entrée dans la table NAT

    ***VotreNom*> srv nat portmap add**
    % srv nat portmap add <idx> <serv name> <proto> <pub port> <pri ip> <pri port>

    Exemple :***bewan*> srv nat portmap add 1 WWW 6 80 192.168.1.2 80**

    Pour vérifier que le port est bien redirigé dans la table de configuration, tapez la commande suivante :
    ***VotreNom*> srv nat portmap table**

    NAT Port Redirection Configuration Table:

Index	Service Name	Protocol	Public Port	Private IP	Private Port
1	WWW	6	80	192.168.1.2	80
2		0	0	0	0
3		0	0	0	0
4		0	0	0	0
5		0	0	0	0
6		0	0	0	0
7		0	0	0	0
8		0	0	0	0
9		0	0	0	0
10		0	0	0	0

    Protocol: 0 = Disable, 6 = TCP, 17 = UDP

    *Remarque : la commande **srv nat portmap table** équivaut à **srv nat status**.*

***VotreNom*> srv nat status**

% NAT server: Running

NAT Port Redirection Running Table:

Index	Protocol	Public Port	Private IP	Private Port
1	6	80	192.168.1.2	80
2	0	0	0.0.0.0	0
3	0	0	0.0.0.0	0
4	0	0	0.0.0.0	0
5	0	0	0.0.0.0	0
…				
16	0	0	0.0.0.0	0
17	0	0	0.0.0.0	0
18	0	0	0.0.0.0	0
19	0	0	0.0.0.0	0
20	0	0	0.0.0.0	0

Protocol: 0 = Disable, 6 = TCP, 17 = UDP

17. Supprimer une entrée dans la table NAT

***VotreNom*> srv nat portmap del**

% srv nat portmap del <idx>

Exemple : ***bewan*> srv nat portmap del 1**

Vérification du port supprimé dans la table de configuration

***VotreNom*> srv nat portmap table**

NAT Port Redirection Configuration Table:

Index	Service Name	Protocol	Public Port	Private IP	Private Port
1		0	0	0	0
2		0	0	0	0
3		0	0	0	0
4		0	0	0	0
5		0	0	0	0
6		0	0	0	0
7		0	0	0	0
8		0	0	0	0
9		0	0	0	0
10		0	0	0	0

Protocol: 0 = Disable, 6 = TCP, 17 = UDP

18. Activer une entrée NAT existante

***VotreNom*> srv nat portmap enable**

% srv nat portmap enable <idx> <proto>

c'est-à-dire : **idx** Index

proto Protocole (TCP ou UDP)

19. Désactiver une entrée NAT existante

***VotreNom*> srv nat portmap disable**

% srv nat portmap disable <idx>

20. Supprimer tous les index de la table NAT

***VotreNom*> srv nat portmap flush**

Liste des sous-commandes SYS

1. Afficher le nom de l'administrateur du routeur

   ***VotreNom*> sys admin ?**
   % sys admin <ASCII string>
   % Now: Pierre

2. Changer le nom de l'administrateur du routeur

   ***VotreNom*> sys admin <ASCII string>**

   Exemple : ***bewan*> sys admin Dominique**

3. Restaurer la configuration d'usine

   ***VotreNom*> sys cfg default**

4. Obtenir la liste des dernières commandes effectuées

   ***VotreNom*> sys cmdlog**

5. Indiquer l'état des interfaces LAN et WAN

   ***VotreNom*> sys iface**

6. Démarrer le serveur TFTP pour la mise à jour du routeur

   ***VotreNom*> sys tftpd**
   % Enable firmware upgrade TFTP server !!!

7. Obtenir l'identifiant de connexion actuel pour accéder au paramétrage du routeur

   ***VotreNom*> sys name ?**

8. Changer l'identifiant de connexion pour accéder au paramétrage du routeur

   ***VotreNom*> sys name <ASCII string>**

9. Obtenir le mot de passe actuel pour accéder au paramétrage du routeur

   ***VotreNom*> sys passwd < ASCII string>**

10. Changer le mot de passe pour accéder au paramétrage du routeur

    ***VotreNom*> sys passwd < ASCII string>**

11. Redémarrer le routeur en conservant la configuration actuelle

    ***VotreNom*> sys reboot**

12. Obtenir la version du firmware et des informations relatives au routeur

    ***VotreNom*> sys version**
    Router Model: VPN Booster Version: vX.XX
    Profile version: 0x2
    Router IP: 192.168.1.1 Netmask: 255.255.255.0
    Firmware Build Date/Time: Wed Feb XX HH:MM:SS.S Year

Liste des sous-commandes URLF

1. Activer les restrictions URL

   ***VotreNom*> urlf blist on**

2. Activer une liste de mots spécifique

   ***VotreNom*> urlf blist <INDEX (1-8)> -e <KEYWORD** (mot)>

   Exemple : ***bewan*> urlf blist 2 -e sex** (la liste 2 contenant le mot 'sex' est activée)
   On peut traduire '-e' par 'enable'.

   Remarque : si votre liste contient plusieurs termes, séparez-les par une virgule, un point ou un point virgule.

3. Désactiver une liste de mots

   ***VotreNom*> urlf blist <INDEX (1-8)> -d**
   On peut traduire '-d' par 'disable'.

4. Afficher l'état des restrictions URL (restrictions URL activées ou non et mots interdits)

   ***VotreNom*> urlf blist status**

5. Désactiver les restrictions URL

   ***VotreNom*> urlf blist off**

6. Activer l'interdiction au Web par adresse IP

   ***VotreNom*> urlf blist noip on**
   User can not surf webs with IP inside the URLs!!

7. Désactiver l'interdiction au Web par adresse IP

   ***VotreNom*> urlf blist noip off**
   User can surf webs with IP inside the URLs!!

8. Activer les restrictions WEB

   ***VotreNom*> urlf webf on**

9. Activer une restriction WEB spécifique

   ***VotreNom*> urlf webf -e [java] [activex] [zip] [exe] [mms] [cookie] [proxy]**

   Exemple : ***bewan*> urlf webf -e zip** (active la restriction des fichiers compressés).
   On peut traduire '-e' par 'enable'.

10. Désactiver une restriction WEB spécifique

    ***VotreNom*> urlf webf -d [java] [activex] [zip] [exe] [mms] [cookie] [proxy]**

    Exemple : ***bewan*> urlf webf -d exe** (désactive la restriction des fichiers exécutables).
    On peut traduire '-d' par 'disable'.

11. Afficher l'état des restrictions WEB (restrictions WEB activées ou non)

    ***VotreNom*> urlf webf status**

12. Désactiver les restrictions WEB

    ***VotreNom*> urlf webf off**

13. Restaurer les paramètres par défaut du filtrage de contenu (ce qui équivaut à effacer tous les filtres)

    ***VotreNom*> urlf setdefault**

14. Afficher la plage horaire des restrictions

    ***VotreNom*> urlf tschedule status**

15. Activer l'autorisation pour certaines adresses MAC

    ***VotreNom*> urlf esubnet on**

16. Activer l'autorisation pour une adresse MAC spécifique

    ***VotreNom*> urlf esubnet <INDEX (1-4)> -e <IP Address> <Subnet Mask>**

    Exemple : ***bewan*> urlf esubnet 1 -e 192.168.1.23 255.255.255.0** (autorise l'accès à l'adresse IP 1, 192.168.1.23 avec un masque de sous-réseau en 255.255.255.0)
    On peut traduire '-e' par 'enable'.

17. Désactiver l'autorisation pour une adresse MAC spécifique

    ***VotreNom*> urlf esubnet <INDEX (1-4)> -d**

    Exemple : ***bewan*> urlf esubnet 1 -d** (n'autorise pas l'accès à l'adresse IP 1)
    On peut traduire '-d' par 'disable'.

18. Désactiver l'autorisation pour certaines adresses MAC

    ***VotreNom*> urlf esubnet off**

Liste des sous-commandes WAN

1. Obtenir la taille actuelle du MTU (1442 par défaut)

   ***VotreNom*> wan mtu ?**

2. Spécifier un nouveau MTU

   ***VotreNom*> wan mtu <valeur entre 1000 et 1500>**

   Remarque : cette commande permet de changer la taille maximum du champ Datagramme des paquets qui transitent sur la partie WAN du routeur.

Partie 5 : Outils de maintenance

Mise à jour du routeur

Le VPN Booster dispose d'une mémoire (flash EPROM) qui contient son logiciel (firmware) et ses paramètres d'usine. Cette mémoire étant reprogrammable, le firmware et les paramètres d'usine du routeur peuvent être mis à jour.

Les informations concernant d'éventuelles mises à jour du VPN Booster sont consultables sur le site Web de BeWAN systems (http://www.bewan.com).

Pour effectuer une mise à jour du VPN Booster, vous devez disposer d'un fichier de mise à jour. Il existe 3 types de fichiers de mise à jour, distingués par leur extension :

Extension	Contenu du fichier de mise à jour
.CFG	fichier de sauvegarde de votre configuration créé par l'administrateur (voir « Sauvegarde d'une configuration » page 202). Pour la mise à jour de ce fichier, reportez-vous à la section « Restauration d'une configuration » page 203.
.ALL	programmes + pages HTML du configurateur
.RST	programmes + paramètres d'usine + pages HTML du configurateur

La procédure varie ensuite selon le type de fichier de mise à jour utilisé et selon le type d'ordinateur utilisé (PC ou Macintosh).

- Si vous désirez mettre à jour les fichiers .ALL et .RST, utilisez l'Assistant de mise à jour installé avec les Utilitaires VPN Booster.
- Si vous désirez mettre à jour le fichier .CFG, cliquez sur **Sauvegarde / Restauration de configuration** dans le menu **Administration Système**. Reportez-vous alors au chapitre « Sauvegarde / Restauration de configuration » page 202.

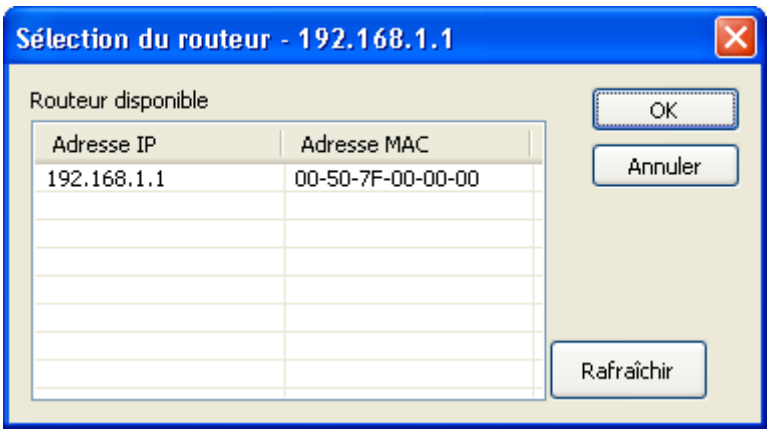
Mise à jour à partir d'un PC

La mise à jour s'effectue via l'Assistant de mise à jour installé avec les Utilitaires VPN Booster.

Remarque : le serveur TFTP est démarré automatiquement avec l'Assistant de mise à jour.

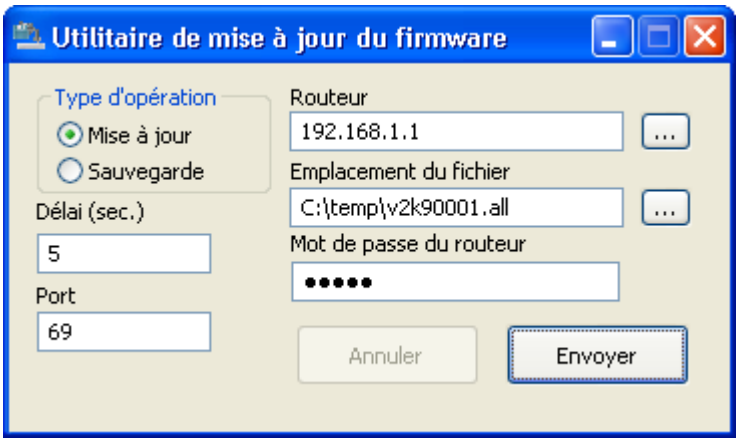
Procédez comme suit :

1. Cliquez sur **démarrer**, **Tous les programmes**, **Utilitaires VPN Booster**, puis sur **Assistant de mise à jour**. L'Assistant apparaît.
2. L'option **Mise à jour** est sélectionnée par défaut.
3. Dans la rubrique **Routeur**, cliquez sur **…** pour sélectionnez le routeur à mettre à jour (voir l'image ci-dessous) ou saisissez directement l'adresse IP du routeur si vous la connaissez.

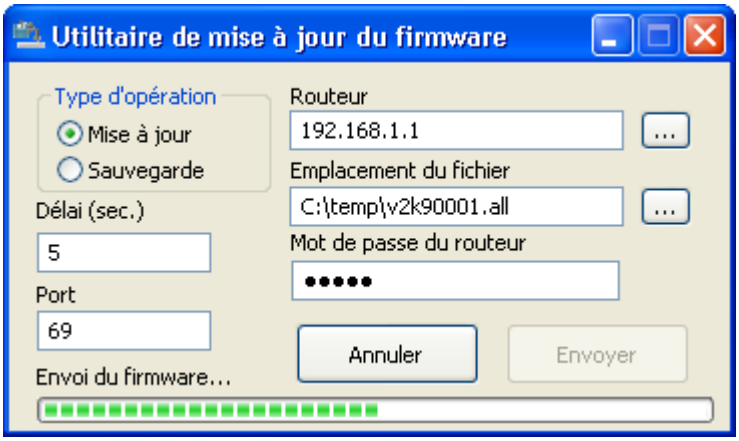


4. En face de la rubrique **Emplacement du fichier**, cliquez sur **…** afin d'indiquer le chemin d'accès du fichier de mise à jour.

5. Enfin, indiquez le mot de passe du routeur à mettre à jour.

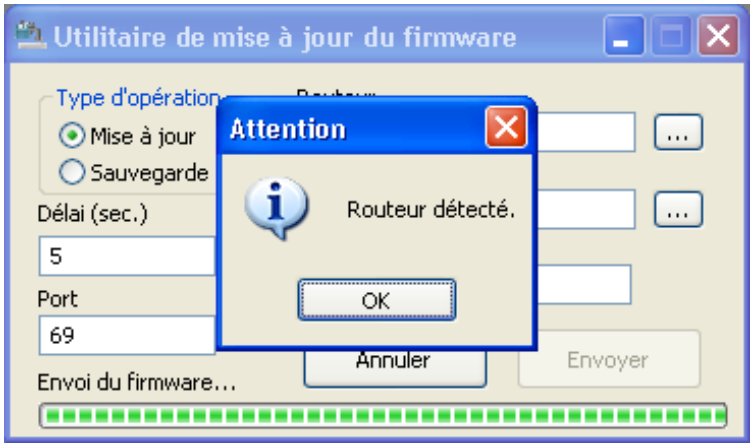


6. Cliquez ensuite sur le bouton **Envoyer** afin de charger le fichier de mise à jour dans la mémoire du VPN Booster.
7. Le fichier de mise à jour est alors en cours de chargement dans la mémoire du VPN Booster.



*Remarque : si le serveur TFTP qui permet d'effectuer la mise à jour du firmware, n'a pas démarré pendant cette phase, le bouton **Envoyer** devient alors accessible. Cliquez de nouveau sur celui-ci afin de relancer le serveur TFTP.*

8. Un message vous informe lorsque la mise à jour est effectuée. Cliquez sur **OK**.



Mise à jour à partir d'un Macintosh

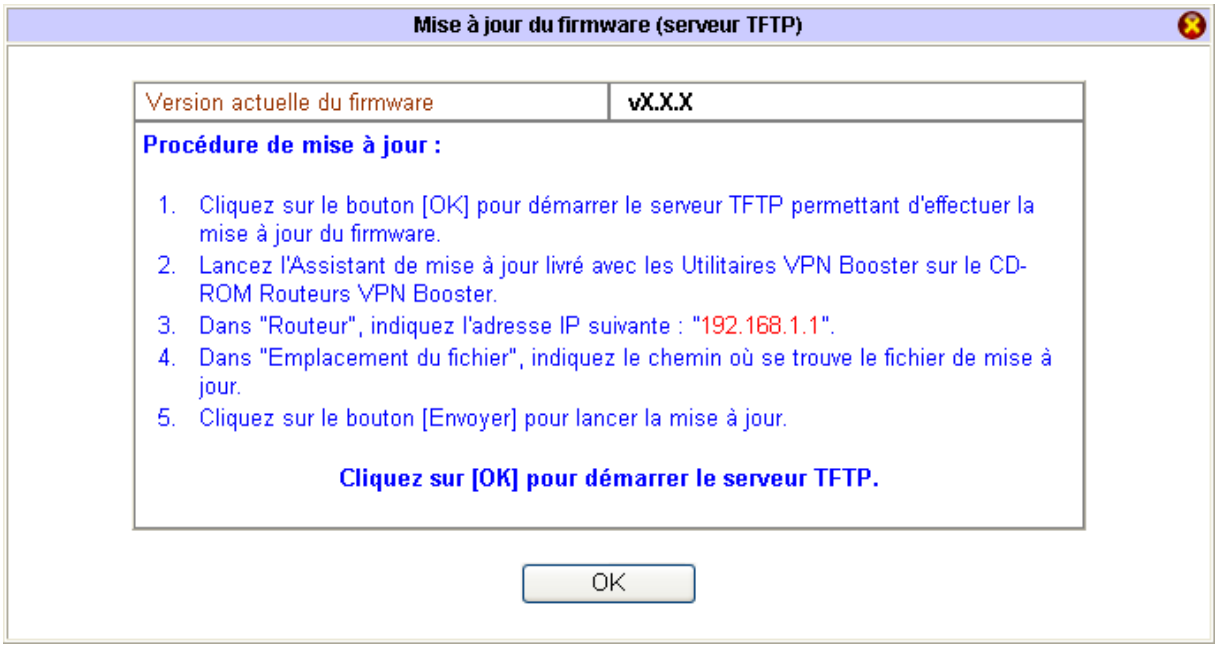
La mise à jour à partir d'un Macintosh (de Mac OS 9 à Mac OS X) s'effectue en 3 étapes :

1. Activation du serveur TFTP via le configurateur HTML du VPN Booster afin qu'il soit prêt à recevoir le fichier de mise à jour.
2. Téléchargement du fichier de mise à jour dans la mémoire du VPN Booster, grâce à l'Assistant de mise à jour.
3. Redémarrage du VPN Booster dans la nouvelle configuration.

Activation du serveur TFTP

Pour activer le serveur TFTP du VPN Booster en mode HTML, procédez comme suit :

1. Démarrez le configurateur HTML du VPN Booster.
2. Lorsque le configurateur HTML est démarré, dans le menu **Administration Système**, sélectionnez **Mise à jour du firmware (serveur TFTP)**. L'écran suivant rappelle la version de firmware actuellement utilisée.



3. Cliquez sur **OK**. Le serveur TFTP est démarré, vous pouvez maintenant utiliser l'Assistant de mise à jour pour télécharger le fichier de mise à jour dans la mémoire du VPN Booster. Reportez-vous pour cela à la section suivante « Mise à jour via l'Assistant de mise à jour ».

Mise à jour via l'Assistant de mise à jour

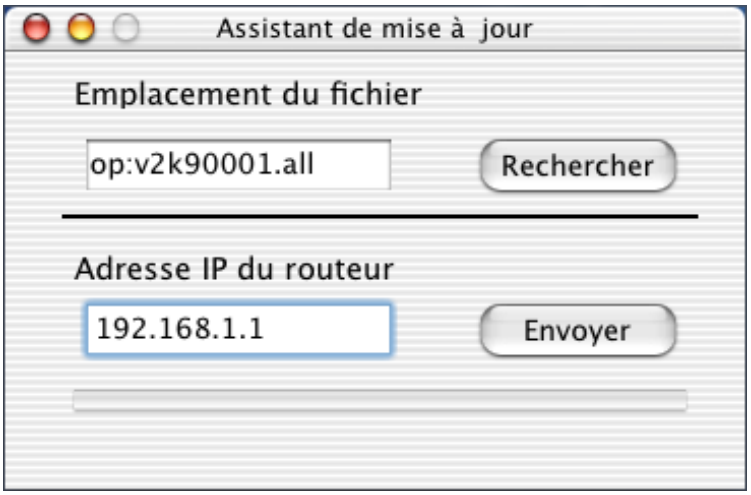
L'Assistant de mise à jour a été installé en même temps que les Utilitaires VPN Booster. Reportez-vous pour cela au chapitre « Installation et utilisation de l'Assistant de démarrage » page 59. Procédez comme suit :

1. *Sous Mac OS 9* : Cliquez sur le menu **Pomme**, pointez sur **Tableaux de bord**, **Utilitaires VPN Booster**, puis cliquez sur **Assistant de mise à jour**.

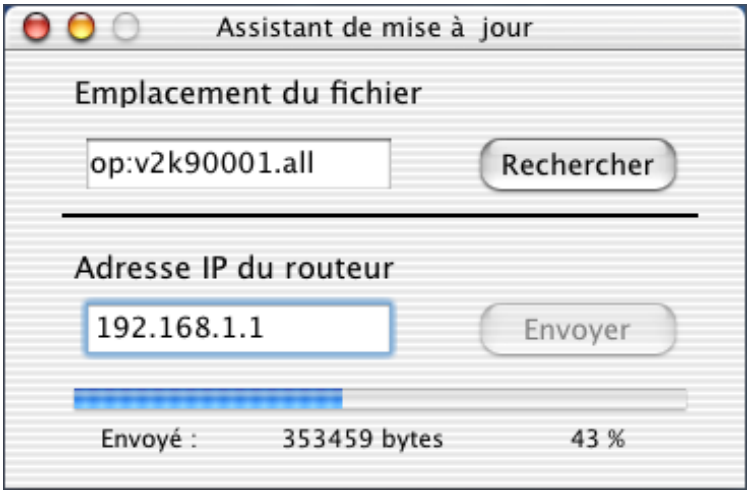
   Sous Mac OS X : Effectuez un double-clic sur le fichier **Utilitaires VPN Booster.dmg**. Un disque virtuel **Utilitaires VPN Booster** est créé sur le bureau de votre Macintosh. Effectuez un double clic sur ce disque. Lancez ensuite l'Assistant de mise à jour.

2. En face de la rubrique **Emplacement du fichier**, cliquez sur le bouton **Rechercher**, puis indiquez le chemin d'accès du fichier de mise à jour.

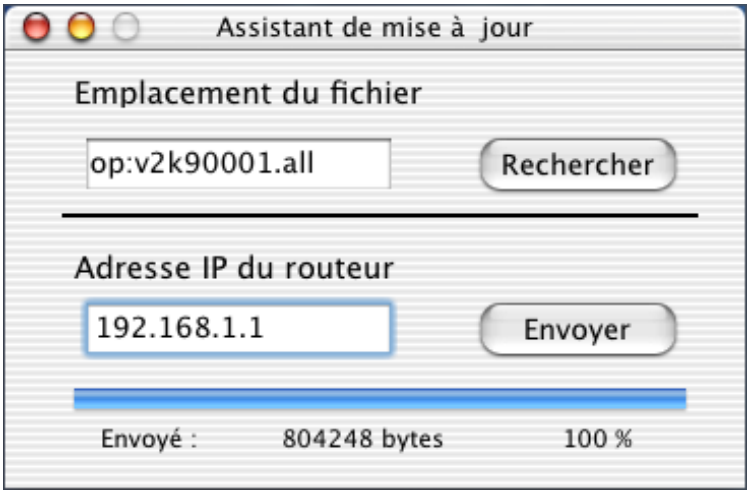
3. Dans la rubrique **Adresse IP du routeur**, indiquez l'adresse IP du VPN Booster.



4. Cliquez sur **Envoyer**. Le fichier de mise à jour est alors en cours de chargement dans la mémoire du VPN Booster.

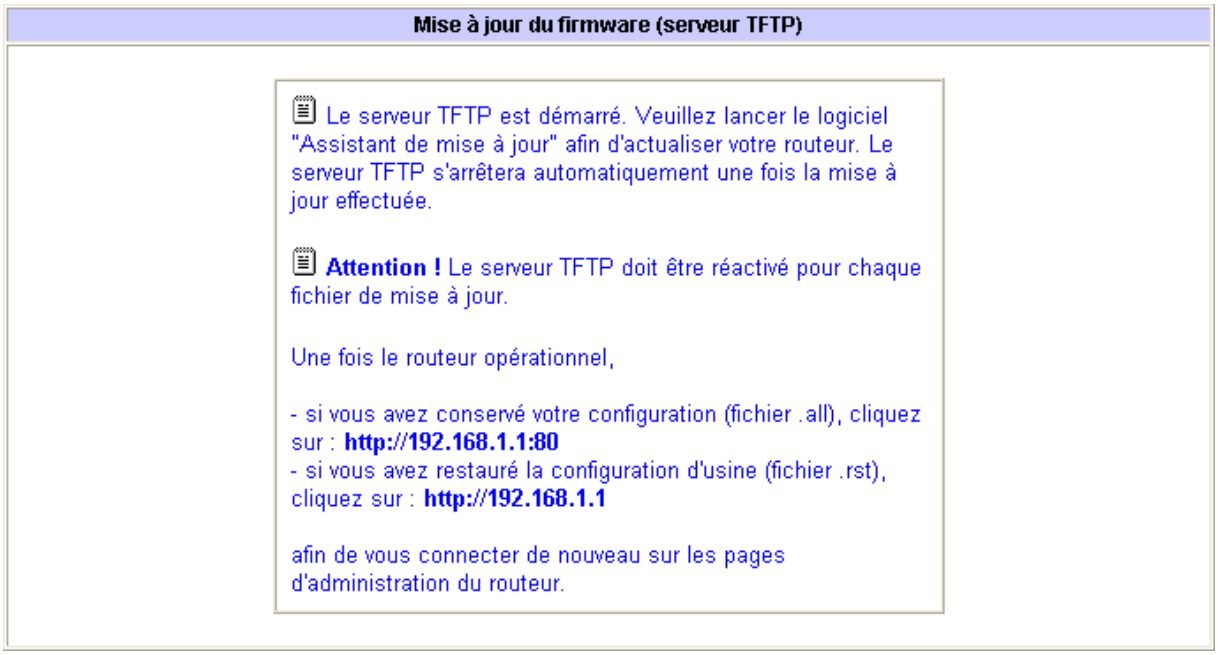


5. Lorsque vous êtes à 100% du transfert, la mise à jour est effectuée.



Redémarrage du VPN Booster

Le VPN Booster redémarre ensuite automatiquement afin que la mise à jour soit prise en compte. Selon le fichier de mise à jour utilisé (.ALL ou .RST), cliquez sur l'adresse http correspondante sur l'interface Web pour revenir sur la page d'accueil.



Attention :

- *Le redémarrage du VPN Booster interrompt les éventuelles connexions en cours.*
- *N'éteignez en aucun cas le VPN Booster pendant cette phase de redémarrage, vous risqueriez d'endommager sa mémoire et de le rendre inutilisable (dommage non couvert par la garantie).*

La mise à jour du VPN Booster est maintenant terminée. Vous pouvez fermer l'Assistant de mise à jour.

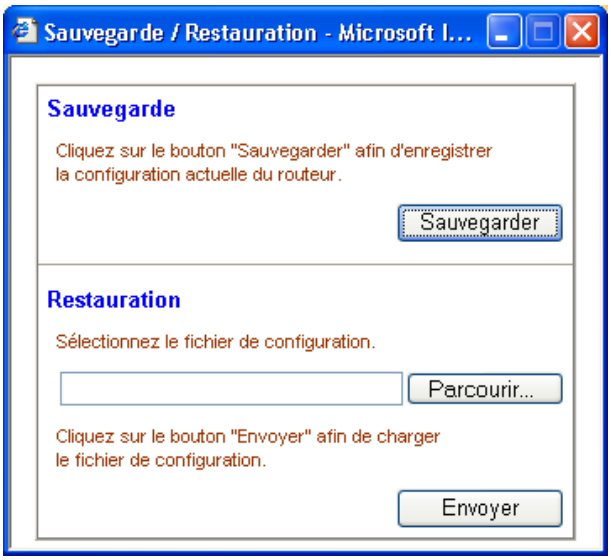
Sauvegarde / Restauration de configuration

Vous avez la possibilité de sauvegarder votre configuration complète (via la création d'un fichier .CFG). Votre configuration entière est ainsi disponible à tout moment en cas de problème sur votre routeur ou pour une utilisation ultérieure.

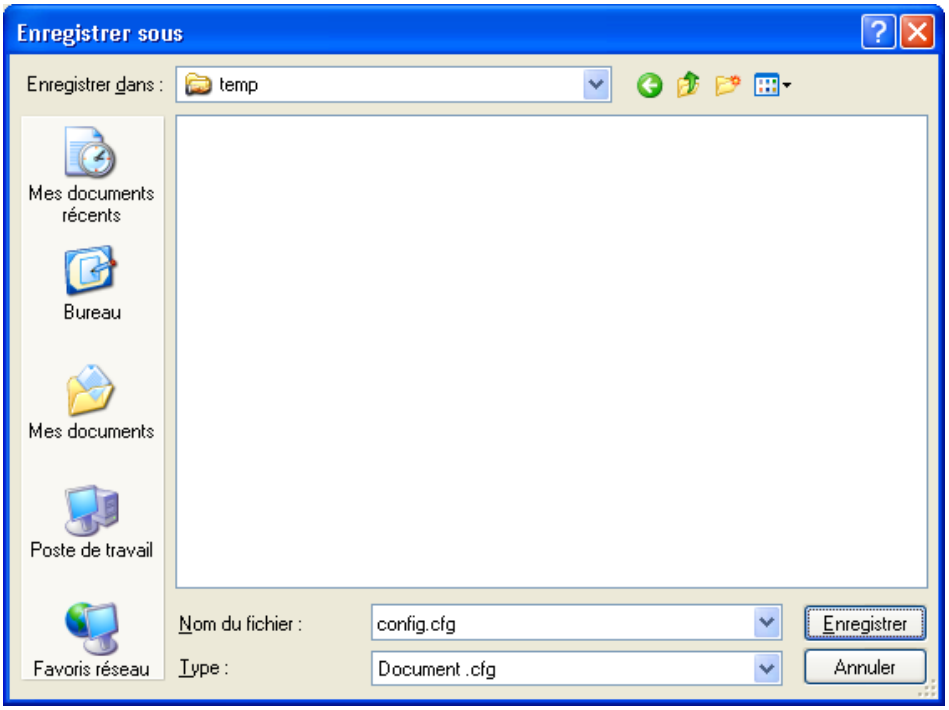
Sauvegarde d'une configuration

Procédez comme suit :

1. Dans le menu **Administration Système**, sélectionnez **Sauvegarde / Restauration de configuration**.
2. Une fenêtre apparaît. Dans la partie **Sauvegarde**, cliquez alors sur le bouton **Sauvegarder**.



3. Vous devez désormais enregistrer votre fichier de sauvegarde sur votre disque. Indiquez l'emplacement du fichier .CFG que vous souhaitez sauvegarder, renommez-le si nécessaire, puis cliquez sur **Enregistrer**.

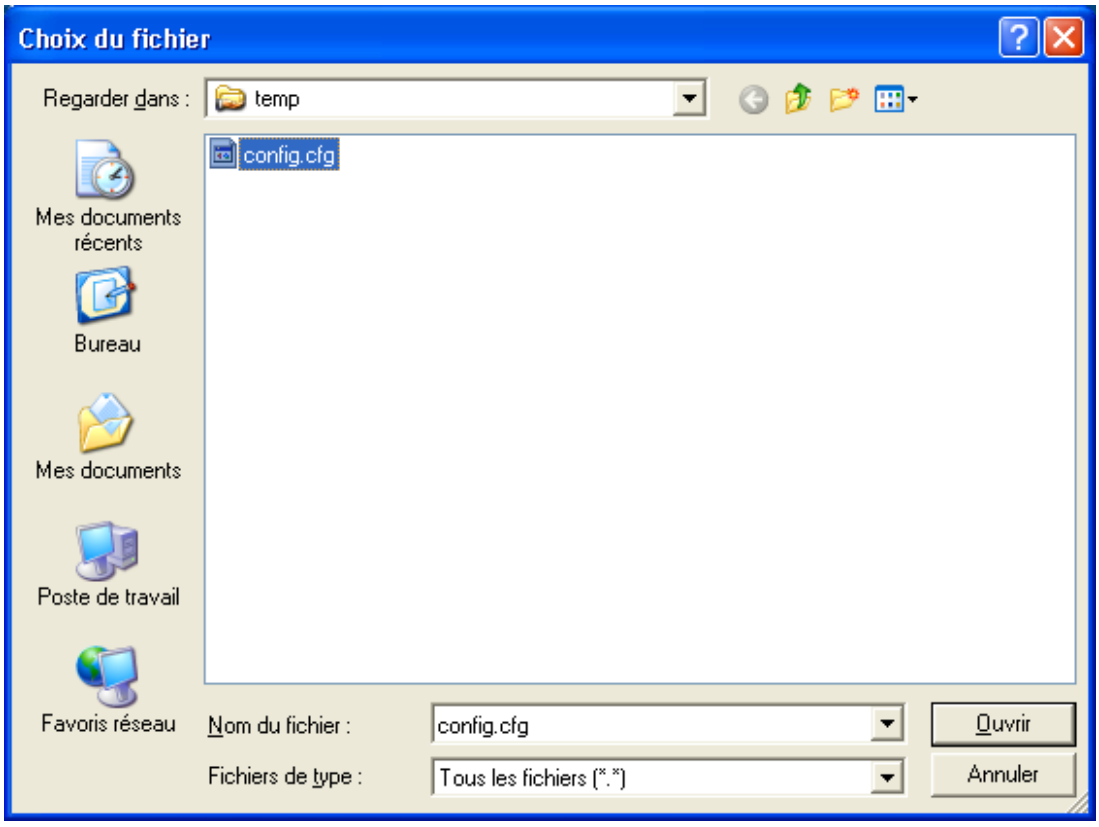


4. Le fichier est désormais sauvegardé. Fermez la fenêtre **Sauvegarde / Restauration**.

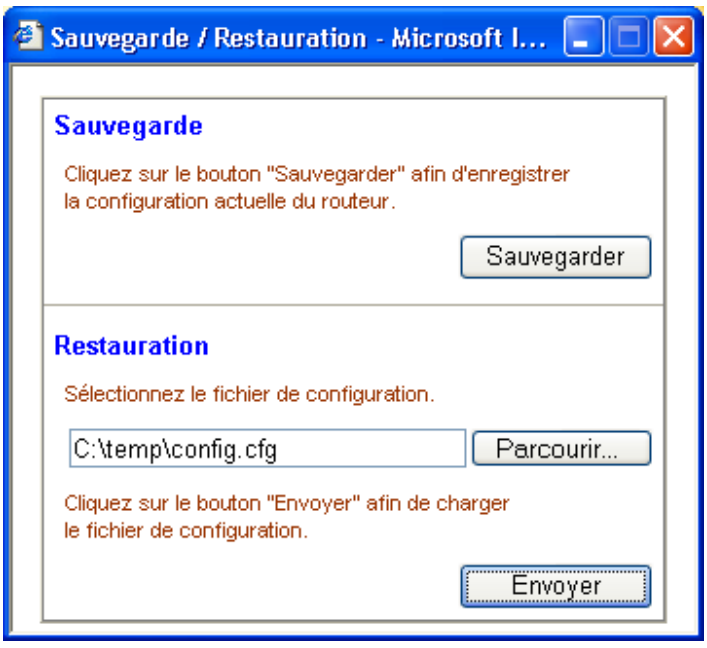
Restauration d'une configuration

Si vous souhaitez remettre à jour votre routeur via un fichier .CFG, dans une configuration que vous avez préalablement sauvegardée (reportez-vous à la section précédente), procédez comme suit :

1. Dans le menu **Administration Système**, sélectionnez **Sauvegarde / Restauration de configuration**.
2. Une fenêtre apparaît. Dans la partie **Restauration**, indiquez le chemin d'accès du fichier .CFG de mise à jour. Cliquez pour cela sur le bouton **Parcourir…**.
3. Une fois le fichier sélectionné, cliquez sur **Ouvrir**.



4. Cliquez ensuite sur **Envoyer**. Le fichier de restauration est envoyé au VPN Booster.



5. Un message apparaît alors, vous indiquant que le fichier de restauration a bien été chargé dans le VPN Booster. Cliquez sur le bouton **Redémarrer** afin que la mise à jour soit prise en compte.

Attention :

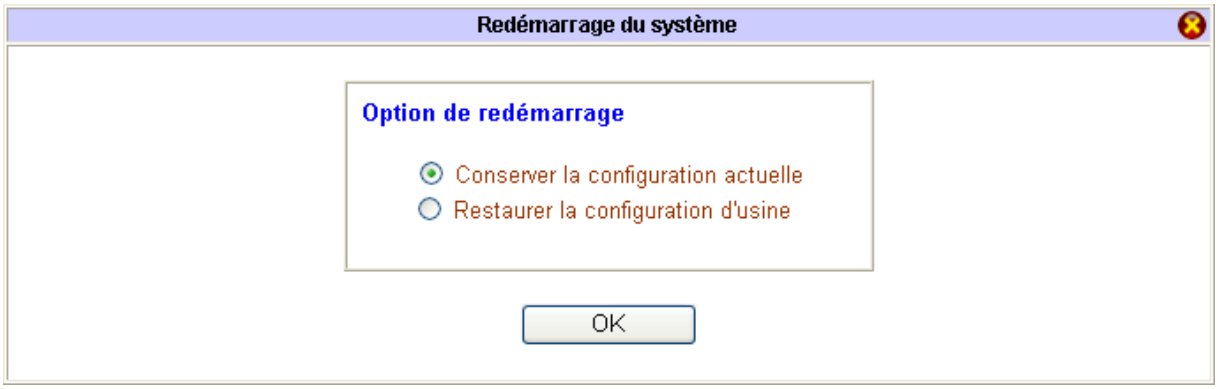
- *Le redémarrage du VPN Booster interrompt les éventuelles connexions en cours.*
- *N'éteignez en aucun cas le VPN Booster pendant cette phase de redémarrage, vous risqueriez d'endommager sa mémoire et de le rendre inutilisable (dommage non couvert par la garantie).*

La mise à jour du VPN Booster via le fichier de sauvegarde est maintenant terminée.

Redémarrage du routeur

Pour redémarrer le VPN Booster à partir de son configurateur HTML, procédez comme suit :

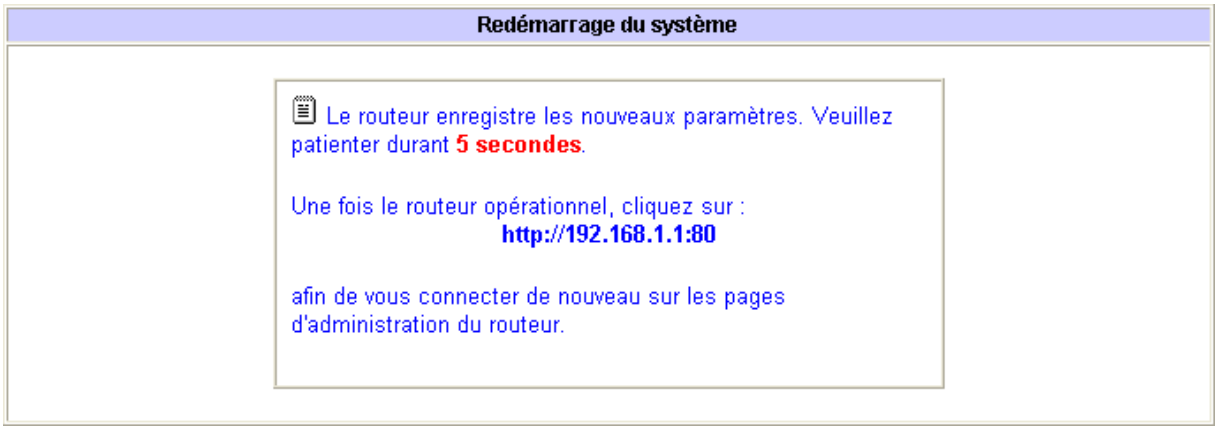
1. Dans le menu **Administration Système**, sélectionnez **Redémarrage du système**.
2. Vous avez deux options possibles de redémarrage :
   - **Conserver la configuration actuelle** : sélectionnez cette option si vous souhaitez que le VPN Booster utilise vos paramètres et les dernières modifications effectuées lors du redémarrage.
   - **Restaurer la configuration d'usine** : sélectionnez cette option si vous souhaitez que le VPN Booster redémarre dans sa configuration d'usine.



   Cliquez sur **OK**.
3. Attendez ensuite environ 5 secondes afin que le redémarrage du routeur soit terminé et que celui-ci soit à nouveau opérationnel.

   Attention :

   - *Le redémarrage du VPN Booster interrompt les éventuelles connexions en cours.*
   - *N'éteignez en aucun cas le VPN Booster pendant cette phase de redémarrage, vous risqueriez d'endommager sa mémoire et de le rendre inutilisable (dommage non couvert par la garantie).*



4. Cliquez sur l'adresse http qui correspond à la première adresse de sous-réseau de votre routeur. Vous revenez alors sur le menu du configurateur.

DECLARATION DE CONFORMITE

Equipement terminal de télécommunications

Nom du constructeur : BeWAN systems

Siège social : BeWAN systems — Téléphone : 01 43 34 69 20

Adresse : 16, rue du Moulin des Bruyères — Télécopie : 01 46 91 03 71

Code postal : 92400

Localité : Courbevoie - France

Identification du produit :

Noms : VPN Booster 8, VPN Booster 32, VPN Booster 32 i et VPN Booster 32 V

Type : Routeurs 10/100 BaseTx

Références : VPNB8, VPNB32, VPNB32i et VPNB32V

Déclare sous son entière responsabilité que les produits décrits ci-dessus sont en conformité avec les exigences essentielles applicables et en particulier celles de la Directive R&TTE 1999/5/CE.

Les produits sont conformes aux exigences définies par la Directive 89/336/CEE concernant la compatibilité électromagnétique, et la Directive 73/23/CEE sur les basses tensions, la protection de la santé et la sécurité de l'utilisateur.

Les produits sont en conformité avec les normes suivantes :

EN55022 Classe B
EN55024 Classe B
EN60950

Information supplémentaire : le produit a été testé dans une configuration standard.

Date : juillet 2004

Eric TEISSANDIER
Président du Conseil d'Administration

DECLARATION DE CONFORMITE

Equipement terminal de télécommunications

Nom du constructeur : BeWAN systems

Siège social : BeWAN systems — Téléphone : 01 43 34 69 20

Adresse : 16, rue du Moulin des Bruyères — Télécopie : 01 46 91 03 71

Code postal : 92400

Localité : Courbevoie - France

Identification du produit :

Noms : VPN Booster 32 g et VPN Booster 32 Vg

Type : Routeurs 10/100 BaseTx avec Point d'Accès Wi-Fi (IEEE 802.11g)

Références : VPNB32G et VPNB32VG

Déclare sous son entière responsabilité que les produits décrits ci-dessus sont en conformité avec les exigences essentielles applicables et en particulier celles de la Directive R&TTE 1999/5/CE.

Les produits sont conformes aux exigences définies par la Directive 89/336/CEE concernant la compatibilité électromagnétique, et la Directive 73/23/CEE sur les basses tensions, la protection de la santé et la sécurité de l'utilisateur. Ils sont conçus pour les réseaux WLAN fonctionnant dans la bande des 2.4 Ghz.

Les produits sont en conformité avec les normes suivantes :

EN55022 Classe B
EN55024 Classe B
EN60950

Information supplémentaire : le produit a été testé dans une configuration standard.

Date : juillet 2004

Eric TEISSANDIER
Président du Conseil d'Administration