DrayTek

Routeurs ADSL2/2+ série Vigor2800V

Guide d'Utilisateur

Version 1.0
Date : 2006/1/12

Copyright

À propos de ce guide de l'utilisateur

Ce guide a pour but de vous familiariser avec l'utilisation de l'un des routeurs ADSL2/2+ de la série Vigor2800. Les informations contenues dans ce document ont été vérifiées avec soin, néanmoins aucune garantie n'est donnée quant à leur exactitude. Les informations contenues dans ce document sont susceptibles d'être modifiées sans préavis. N'hésitez pas à contacter notre support technique par courriel, par télécopie ou par téléphone. Pour connaître les informations les plus récentes sur nos produits, visitez notre site **www.draytek.fr**.

Nous utilisons pour attirer votre attention sur certains points particuliers. Si vous avez des questions ou des suggestions, n'hésitez pas à contacter votre revendeur local ou DrayTek : **support@draytek.com** ou **info@draytek.com** !

Garantie limitée de DrayTek

Ce routeur est garanti à l'utilisateur originel (c'est-à-dire à l'acheteur) contre tout vice de fabrication ou défaut de matière pendant une période de trois (3) ans à compter de la date d'achat au revendeur. Conservez votre justificatif d'achat en lieu sûr.

Pendant la période de garantie et sur présentation du justificatif d'achat, si le produit présente des dysfonctionnements dus à un vice de fabrication ou à défaut de matière, nous nous engageons à réparer ou à remplacer gratuitement les produits ou composants défectueux, pièces ou main-d'œuvre, dans la mesure que nous jugeons nécessaires pour remettre le produit en état. Tout remplacement consistera en un produit neuf ou remis en état, fonctionnellement équivalent et d'égale valeur, et sera proposé à notre seule discrétion. Cette garantie ne s'applique pas si le produit est modifié, mal utilisé, maltraité, endommagé par une catastrophe naturelle ou soumis à des conditions de fonctionnement anormales.

La garantie ne couvre pas les logiciels d'autres sources. Les défauts qui ne modifient pas sensiblement la valeur d'usage du produit ne sont pas couverts par la garantie.

Nous nous réservons le droit de réviser le manuel et la documentation en ligne et de leur apporter des modifications sans préavis.

Enregistrez votre routeur

Il est préférable d'enregistrer votre routeur via l'internet **www.draytek.fr**. Vous pouvez également remplir la carte d'enregistrement et l'envoyer à l'adresse qui figure au verso. Les utilisateurs enregistrés seront informés de l'évolution des produits.

Consignes de sécurité

- Veuillez lire attentivement le guide d'installation avant d'installer le routeur.
- Le routeur est un équipement électronique compliqué qui ne peut être réparé que par des personnes autorisées et qualifiées. Ne tentez pas d'ouvrir ou de réparer le routeur vous-même.
- Ne placez pas le routeur dans un endroit humide, par exemple dans une salle de bain.
- Le routeur doit être utilisé dans un endroit abrité où la température est comprise entre +5 et +40℃.
- N'exposez pas le routeur au soleil ou a une autre source de chaleur. Le boîtier et les composants électroniques peuvent être endommagés par les rayons de soleil ou les sources de chaleur.
- N'installez pas le câble Ethernet raccordé au port LAN à l'extérieur pour éviter les risques d'électrocution.
- Tenez l'emballage hors de la portée des enfants.
- Pour l'élimination du routeur, respectez la réglementation locale sur la préservation de l'environnement.

Déclarations CE

Fabricant : DrayTek Corp.
Adresse : No. 26, Fu Shing Road, HuKou County, HsinChu Industrial Park, Hsin-Chu, Taiwan 303

Produit : Routeurs ADSL2/2+ série Vigor2800V

DrayTek Corp. déclare que les routeurs série Vigor2800 sont conformes aux exigences essentielles suivantes et autres dispositions de la directive 1999/5/CE concernant les équipements hertziens et les équipements terminaux de télécommunication.

Le produit est conforme aux exigences de la directive 89/336/CE concernant la compatibilité électromagnétique (CEM) ainsi qu'aux normes techniques EN 55022/Classe B et EN 55024/Classe B.

Le produit est conforme aux exigences de la directive basse tension (DBT) 73/23/CE et à la norme technique EN 60950.

Les routeurs Vigor2800VG/VGi/G/Gi sont conçus pour le réseau WLAN à 2,4 GHz dans toute l'Union européenne, en Suisse, et tiennent compte des restrictions propres à la France.

Réglementation

Avertissement de la Federal Communication Commission (FCC)

Cet équipement a été testé et trouvé conforme aux limites d'un équipement numérique de classe B selon la Part 15 des règles de la FCC. Ces limites prémunissent raisonnablement contre les perturbations nuisibles dans une installation résidentielle. Cet équipement produit, utilise et peut rayonner de l'énergie radiofréquence et, s'il n'est pas installé ou utilisé conformément aux instructions, peut perturber les communications radio. Toutefois, il n'y a aucune garantie que des perturbations ne peuvent pas se produire dans une installation particulière. Si cet équipement perturbe la réception de radio ou de télévision, ce que l'on peut déterminer en éteignant puis en rallumant l'équipement, l'utilisateur est invité à y remédier en prenant l'une ou l'autre des mesures suivantes :

- Réorienter l'antenne de réception ou la changer de place.
- Augmenter la distance séparant l'équipement du récepteur.
- Branchez l'équipement sur une prise de courant appartenant à un circuit différent de celui sur laquelle le récepteur est branché.
- Consultez le revendeur ou un radioélectricien expérimenté.

Cet équipement est conforme à la Part 15 des règles de la FCC. Son utilisation est soumis aux deux conditions suivantes :

(1) Cet appareil ne peut pas causer de perturbations nuisibles, et

(2) Cet appareil peut accepter des perturbations, y compris des perturbations susceptibles d'entraîner des dysfonctionnements.

Support client

Lorsque vous contactez le support client, préparez les informations suivantes :

- Modèle et numéro de série.
- Conditions de garantie.
- Date de réception de votre routeur.
- Description succincte du problème.
- Opérations que vous effectuées pour le résoudre et messages SysLog associés.

Vous pouvez contacter le support client et les représentants commerciaux respectivement aux adresses support@draytek.com et sales@draytek.com.

Table des matières

Présentation du routeur ADSL2/2+ série Vigor2800

Caractéristiques marquantes

- **Partagez facilement votre accès internet à haut débit**
- **Un pare-feu robuste protège votre réseau des attaques extérieures**
- **Des fonctionnalités complètes de réseau privé virtuel (VPN) permettent de relier différents sites et des télétravailleurs**

Pour les modèles V :

- **Téléphonez sur votre connexion à haut débit simplement en branchant votre téléphone.**
- **La téléphonie sur IP (VoIP) avec garantie de qualité de service.**

Pour les modèles G :

- **Accès LAN sans fil 802.11g avec fonctions de sécurité.**
- **LAN sans fil Super G™ jusqu'à 108 Mbit/s**

Description succincte

Tableau de comparaison des modèles :

	Routeur ADSL2/2+	VoIP	AP sans fil	RNIS
Vigor2800VGi	*	*	*	*
Vigor2800VG	*	*	*	-
Vigor2800Vi	*	*	-	*
Vigor2800V	*	*	-	-
Vigor2800Gi	*	-	*	*
Vigor2800G	*	-	*	-
Vigor2800i	*	-	-	*
Vigor2800	*	-	-	-

Destinés à répondre aux besoins des utilisateurs résidentiels, des travailleurs indépendants et des professions libérales (SOHO) et des entreprises, les routeurs de la série Vigor2800 sont des équipements d'accès intégré (IAD) compatibles ADSL 2/2+. Avec une vitesse descendante pouvant atteindre 12 Mbit/s (ADSL2) ou 24 Mbit/s (ADSL2+), les routeurs Vigor2800 fournissent une bande passante exceptionnelle* pour l'accès à l'internet. (*Nota : la bande passante disponible dépend également du fournisseur d'accès internet).

Dotés de fonctions de pare-feu VPN sophistiquées, les routeurs Vigor2800 permettent de créer 32 réseaux privés virtuels dédiés sur l'internet public. Avec le moteur DES/3DES matériel, toutes les informations transmises sont bien cryptées. Ainsi, les routeurs Vigor2800 sont à l'abri de tout espionnage lorsque la fonctionnalité VPN est activée.

Équipés de deux ports FX à connectivité téléphonique, les modèles Vigor2800 V permettent d'utiliser le service de téléphonie sur IP (VoIP), ce qui réduit sensiblement les frais de téléphone. Pour améliorer la qualité vocale, les Vigor2800 V mettent en œuvre un codec vocal polyvalent et un mécanisme de file d'attente sophistiqué pour améliorer la qualité de service (QoS).

Les modèles Vigor2800 G comportent un module sans fil compatible 802.11g pour l'accès avec LAN sans fil avec un débit pouvant atteindre 54 Mbit/s. Ils intègrent le WPA2(802.11i), l'isolement du LAN sans fil, le système de distribution sans fil (WDS) et l'Universal VLAN™. Les modèles Vigor2800 i offrent le secours RNIS, qui maintient votre accès à l'internet en cas de défaillance de l'accès ADSL.

Branchements

Avant de procéder à la configuration du routeur, vous devez brancher vos appareils correctement.

1. Relier la prise DSL au coupleur ADSL externe avec un câble ADSL.
2. Relier l'un des ports du commutateur 4 ports à votre ordinateur avec un câble RJ-45.
3. Dans le cas des modèles V, relier le port Phone à un téléphone analogique classique avec ou sans fil (DECT) à l'aide d'un câble RJ-11.
4. Dans le cas des modèles G, fixer les antennes amovibles sur le routeur.
5. Brancher l'adaptateur secteur sur la prise PWR.Vérifier l'état des voyants ACT, WAN, LAN.

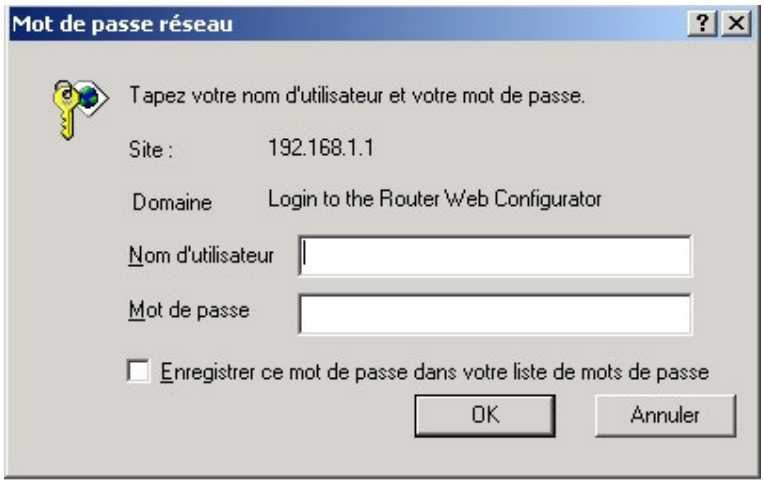
Chapitre 1
Assistant de démarrage rapide

1.1 Introduction

L'assistant de démarrage rapide est conçu pour que vous puissiez facilement configurer votre accès internet à haut débit.

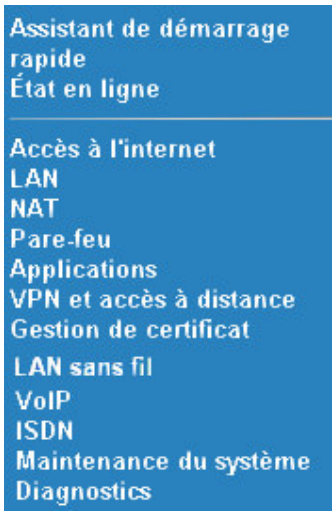
1.2 Configuration de votre routeur à l'aide de l'assistant de démarrage rapide

Étape 1. Ouvrez le navigateur internet sur un PC relié au routeur, puis connectez-vous à l'adresse IP du routeur (l'adresse par défaut est **192.168.1.1**). Une fois la connexion établie (**http://192.168.1.1**), une fenêtre s'ouvre pour vous demander votre nom d'utilisateur et votre mot de passe. Laissez les deux champs vides et appuyez sur **OK** pour continuer.

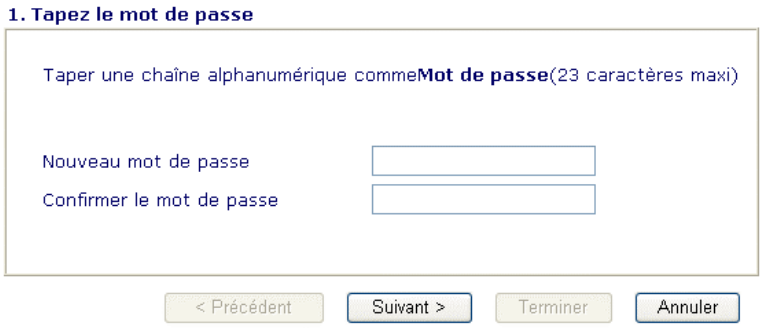


Si vous n'arrivez pas à accéder au configurateur web, reportez-vous à « Dépannage » sur le CD-ROM.

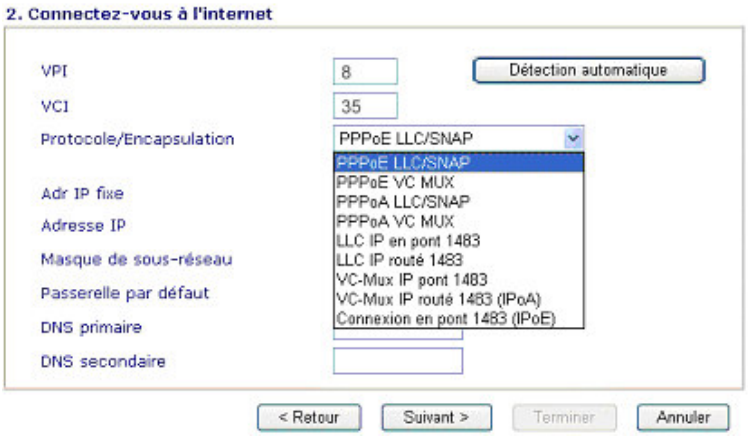
Étape 2. Le **Menu principal** apparaît.



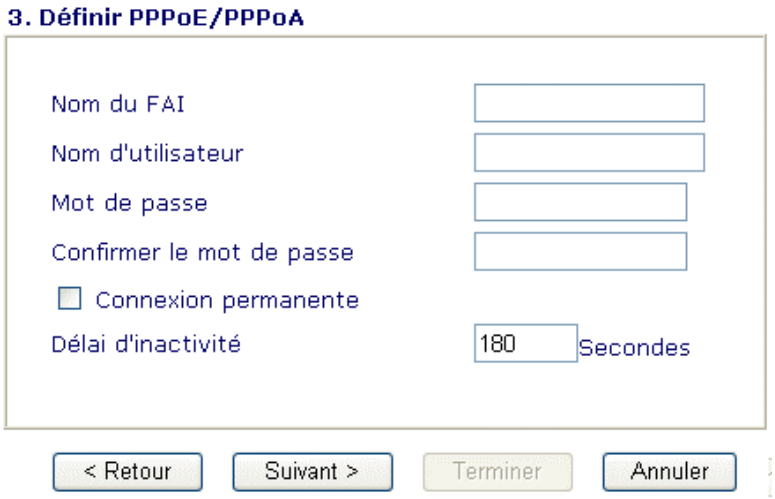
Étape 3. L'assistant de démarrage rapide est maintenant actif. Tapez un mot de passe. Puis cliquez sur **Suivant** pour continuer.



Étape 4 Configurez les paramètres DSL appropriés selon les informations qui vous ont été fournies par votre fournisseur d'accès internet (FAI). La fonction « Détection automatique » peut fournir automatiquement certains des paramètres DSL. Pour plus de détails, voir **Chapitre 3**. Cliquez sur **Suivant** pour continuer.



Étape 5 Si vous sélectionnez PPPoE/PPPoA, entrez le nom d'utilisateur et le mot de passe qui vous ont été fournis par votre FAI. Si vous cliquez sur **Connexion permanente**, la connexion internet reste active, que vous utilisiez ou non l'internet.



É*tape 6* Vérifiez vos paramètres.

En bas de la fenêtre du configurateur web, le système affiche des messages à votre intention.

- « **Prêt** » indique que le système est prêt et que vous pouvez définir vos paramètres.
- « **Paramètre enregistrés** » indique que vos paramètres seront enregistrés quand vous aurez cliqué sur le bouton « Terminer » ou « OK ».

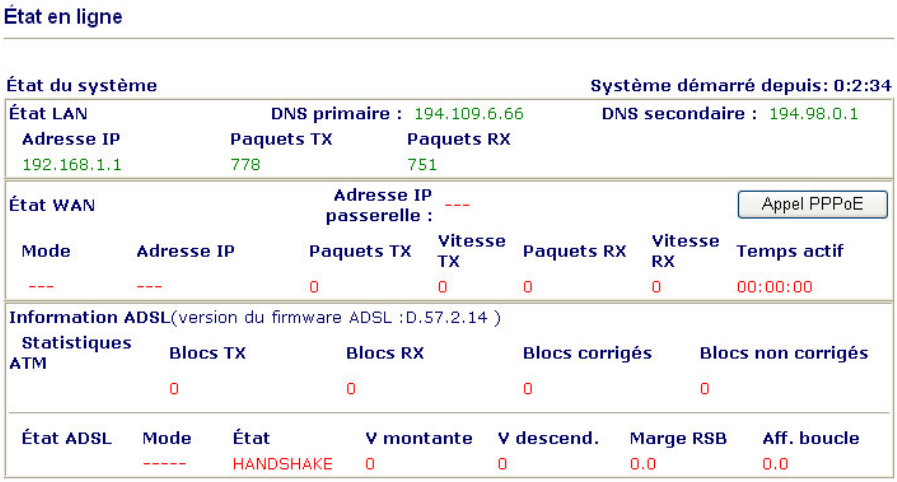
Chapitre 2 État en ligne

2.1 Introduction

L'**État en ligne** fournit quelques informations utiles sur le routeur VIgor, sur le LAN et sur l'interface WAN. Vous pouvez également utiliser la page d'état pour voir quel est l'état de l'accès à l'internet.

2.2 Paramètres

Cliquez sur État en ligne pour ouvrir la page État en ligne.



2.2.1 État du système

Système démarré depuis : Il s'agit du temps de fonctionnement du routeur depuis son démarrage. Le format est HH:MM:SS, où HH, MM, et SS sont respectivement les heures, les minutes et les secondes.

2.2.2 État LAN

Adresse IP	Adresse IP de l'interface LAN.
Paquets TX	Nombre total de paquets IP émis depuis

	l'allumage du routeur.
Paquets RX	Nombre total de paquets IP reçus depuis l'allumage du routeur.
DNS primaire	Vous devez spécifier l'adresse IP du serveur DNS primaire si votre FAI vous l'a communiquée. Si vous ne la spécifiez pas, le routeur applique automatiquement l'adresse IP de serveur DNS par défaut : 194.109.6.66.
DNS secondaire	Vous devez spécifier l'adresse IP du serveur DNS secondaire si votre FAI vous l'a communiquée. Si vous ne la spécifiez pas, le routeur applique automatiquement l'adresse IP de serveur DNS secondaire par défaut : 194.98.0.1.

2.2.3 État WAN

Mode	Indique que le mode d'accès à haut débit est actif. Selon le mode d'accès, on a **PPPoE, PPTP, PPPoA, Adresse IP statique ou DHCP.**
Adresse IP passerelle	Adresse IP de la passerelle.
Adresse IP	Adresse IP de l'interface WAN.
Paquets TX	Nombre total de paquets IP émis au cours de la présente session.
Vitesse TX	Vitesse d'émission en caractères par seconde (cps) pour les données sortantes.
Paquets RX	Nombre total de paquets IP reçus pendant la présente session.
Vitesse RX	Vitesse de réception en caractères par seconde (cps) pour les données entrantes.
Temps actif	Temps de connexion. Le format est HH:MM:SS, où HH, MM, et SS, sont respectivement les heures, les minutes et les secondes.
Abandon/Appel PPPoE ou PPTP	Cliquez sur le lien pour établir ou libérer la connexion PPPoE ou PPTP.

2.2.4 Informations ADSL

Version du logiciel ADSL : Indique la version du logiciel ADSL (le logiciel ADSL est différent du logiciel du routeur).

Statistiques ATM

Blocs TX	Nombre total de blocs ATM émis.
Blocs RX	Nombre total de blocs ATM reçus.
Blocs corrigés	Nombre total de blocs ATM reçus altérés mais corrigés.
Blocs non corrigés	Nombre total de blocs ATM reçus altérés et non corrigés.

État ADSL

Mode	Mode de modulation utilisé : G.DMT, G.Lite ou T1.413.
État	Indique l'état de la ligne DSL.
V. montante	Indique la vitesse montante (bit/s).
V. descend.	Indique la vitesse descendante (bit/s).
Marge RSB	Indique la marge de rapport signal/bruit (dB). Plus la valeur est élevée, meilleure est la qualité des signaux.
Aff. boucle	Indique l'affaiblissement de la boucle d'abonné.

2.2.5 État RNIS (pour les modèles i)

Connexion active	Nom du FAI, de l'utilisateur RNIS distant actif ou de l'interconnexion de LAN ainsi que l'adresse IP de chaque canal B.
Paquets TX	Nombre total de paquets IP émis au cours de la présente session.
Vitesse TX	Vitesse d'émission en caractère par seconde (cps).
Paquets RX	Nombre total de paquets IP reçus pendant la présente session.
Vitesse RX	Vitesse de réception en caractère par seconde (cps).
Temps actif	Temps de connexion. Le format est HH:MM:SS, où HH représente les heures, MM les minutes et SS les secondes.
Abandon de B1	Cliquez pour déconnecter le canal B1.
Abandon de B2	Cliquez pour déconnecter le canal B2.

Chapitre 3
Accès à l'internet

3.1 Introduction

Principes de base d'un réseau à protocole internet (IP)

IP signifie protocole internet. Toutes les machines d'un réseau basé sur le protocole internet (ou réseau IP), notamment les routeurs, le serveur d'impression et certains PC ont besoin d'une adresse IP. Pour éviter les conflits d'adresses, les adresses IP sont enregistrées publiquement auprès d'un organisme appelé Network Information Centre (NIC). Avoir une adresse IP unique est impératif pour les machines qui ont accès au réseau public mais non pour celles des réseaux locaux (LAN) TCP/IP privés, telles que les PC gérés par un routeur, car ils ne sont pas censés être accessibles au public. Le NIC a réservé certaines adresses qui ne seront jamais enregistrées publiquement. Ces adresses dites adresses IP privées appartiennent aux plages suivantes :

De 10.0.0.0 à 10.255.255.255
De 172.16.0.0 à 172.31.255.255
De 192.168.0.0 à 192.168.255.255

Adresse IP publique et adresse IP privée

Comme le routeur Vigor a pour rôle de gérer et de protéger son LAN, il relie entre eux des groupes de PC hôtes qui ont chacun une adresse IP privée attribuée par le serveur DHCP intégré au routeur Vigor. Le routeur lui-même utilise également l'adresse IP par défaut 192.168.1.1 pour communiquer avec les hôtes locaux. Le routeur Vigor communique avec d'autres équipements de réseau à l'aide d'une adresse IP publique. À l'arrivée de données, la fonction de traduction d'adresse réseau (NAT) du routeur Vigor traduit les adresses IP publiques en adresses IP privées et les paquets sont acheminés jusqu'aux PC hôtes appropriés du réseau local. Ainsi, tous les PC hôtes peuvent partager une connexion internet commune.

Comment obtenir une adresse IP publique de votre FAI

Pour obtenir une adresse IP publique de votre FAI pour le routeur Vigor

en tant qu'équipement d'installation d'usager (CPE), il existe trois protocoles courants : le protocole point à point sur Ethernet **(PPPoE),** le protocole point à point sur couche d'adaptation à l'ATM 5 **(PPPoA)** et le multiprotocole sur ATM **(MpoA)**. Le protocole **multi-PVC** est fourni pour une configuration plus évoluée.

En ADSL, une authentification et une autorisation par protocole point à point (PPP) sont nécessaires pour mettre en relation les équipements d'installation d'usager (CPE). Le protocole point à point sur Ethernet (PPPoE) connecte un réseau de machines hôtes par l'intermédiaire d'un équipement d'accès, comme le routeur DSL Vigor Pro, à l'aide d'un circuit virtuel permanent ATM à un concentrateur d'accès à distance ou d'un concentrateur d'agrégation. Cette implémentation donne à l'utilisateur final une grande facilité d'utilisation et ne nécessite pratiquement aucune connaissance autre que celle de la mise en œuvre d'un accès commuté à l'internet. En même temps, elle permet le contrôle d'accès, la facturation et la définition d'un type de service par utilisateur.

Lorsque le routeur Vigor se connecte à votre FAI, un processus de découverte se déroule afin de demander une connexion, puis une session est créée. Votre nom d'utilisateur et votre mot de passe sont authentifiés par PAP ou CHAP à l'aide du système d'authentification RADIUS. Votre adresse IP, votre serveur DNS et autres informations sont généralement fournies par votre FAI.

Le protocole PPPoA, inclus dans RFC 1483, peut être mis en œuvre en mode encapsulation LLC-SNAP (commande logique de liaison – protocole d'accès à un sous-réseau) ou en mode multiplexage par circuits virtuels. En tant qu'équipement d'installation d'usager (CPE), le routeur Vigor encapsule la session PPP pour son transport sur la boucle ADSL jusqu'au multiplexeur d'accès DSL (DSLAM) de votre FAI.

Le protocole MPoA permet d'intégrer les services ATM aux LAN existants utilisant le protocole Ethernet, Token Ring ou TCP/IP. Le but de MPoA est de permettre à des LAN différents d'échanger des paquets par l'intermédiaire d'une dorsale ATM.

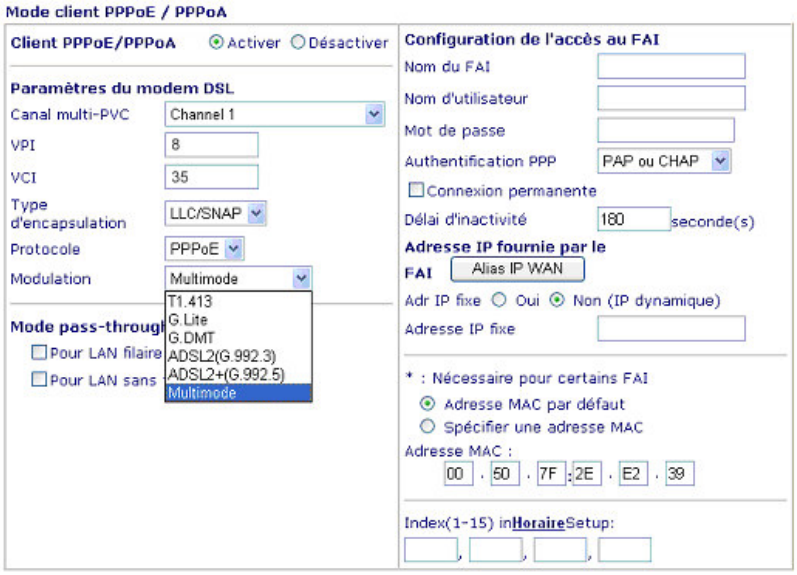
Si vous avez déjà accès à l'internet (vous avez configuré votre routeur comme indiqué au « Chapitre 1 Assistant de démarrage rapide »), il est inutile de reparamétrer votre connexion internet sauf si vous voulez faire des modifications.

3.2 Paramètres

Cliquez sur **Accès à l'internet** pour ouvrir la page Accès à l'internet.

3.2.1 PPPoE/PPPoA

Cliquez sur **Activer** pour activer cette fonction.



Paramètres du modem DSL

Configurez les paramètres DSL selon les informations fournies par votre FAI. Ils sont essentiels pour établir la connexion DSL à votre FAI.

Mode pass-through PPPoE

Le routeur Vigor offre une connexion commutée PPPoE. En outre, vous pouvez établir la connexion PPPoE directement entre des clients locaux et votre FAI par l'intermédiaire du routeur Vigor.

Configuration du secours RNIS (pour le modèle i seulement)

Néant	Désactiver cette fonction
Déclenchement par paquet	Activer cette fonction à la réception d'un paquet
Connexion permanente	Fonction toujours activée

Configuration de l'accès au FAI

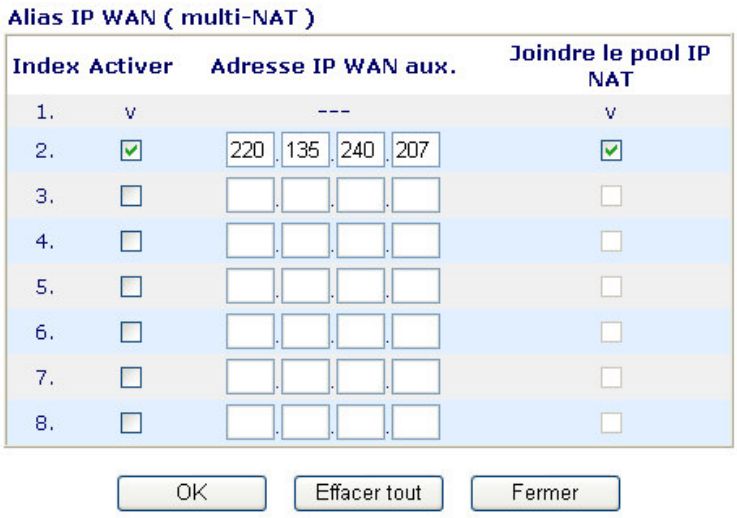
Entrez le nom d'utilisateur, le mot de passe et les paramètres d'authentification qui vous ont été fournis par votre FAI. Si vous voulez rester connecté à l'internet en permanence, vous pouvez cocher « Connexion permanente ».

IP fixe :

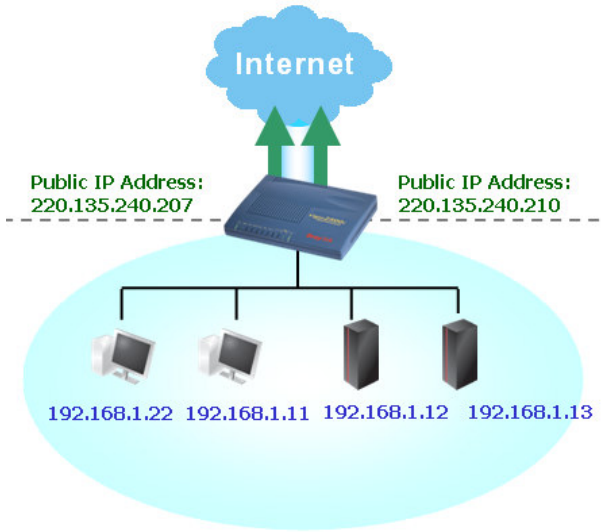
D'une manière générale, le FAI vous attribue dynamiquement une adresse IP chaque fois que vous vous connectez et que vous demandez une adresse IP. Dans certains cas, votre FAI vous attribue toujours la même adresse IP chaque fois que vous en demandez une. Dans ce cas, vous pouvez taper cette adresse IP dans le champ Adresse IP fixe. Contactez votre FAI avant d'utiliser cette fonction.

Alias IP WAN :

Si vous avez plusieurs adresses IP publiques et que vous voulez les utiliser sur l'interface WAN, vous pouvez utiliser la fonction **Alias IP WAN**. Vous pouvez programmer jusqu'à 8 adresses IP publiques autres que celles que vous utilisez actuellement.

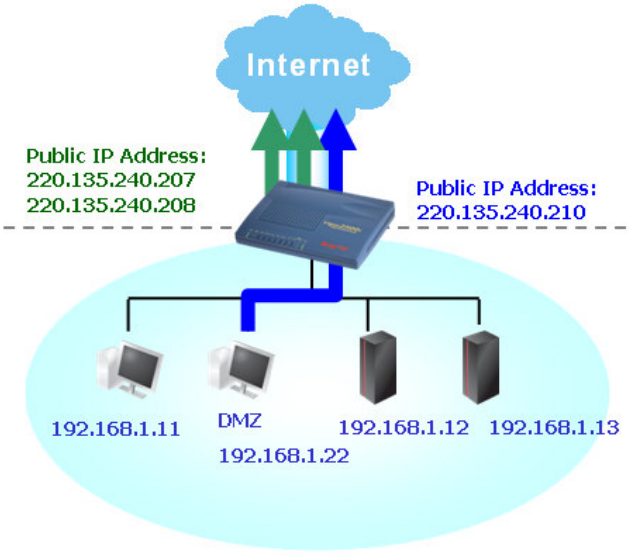


Si vous cochez **Joindre le pool IP NAT**, les données provenant des hôtes NAT sont transmises cycliquement session par session.



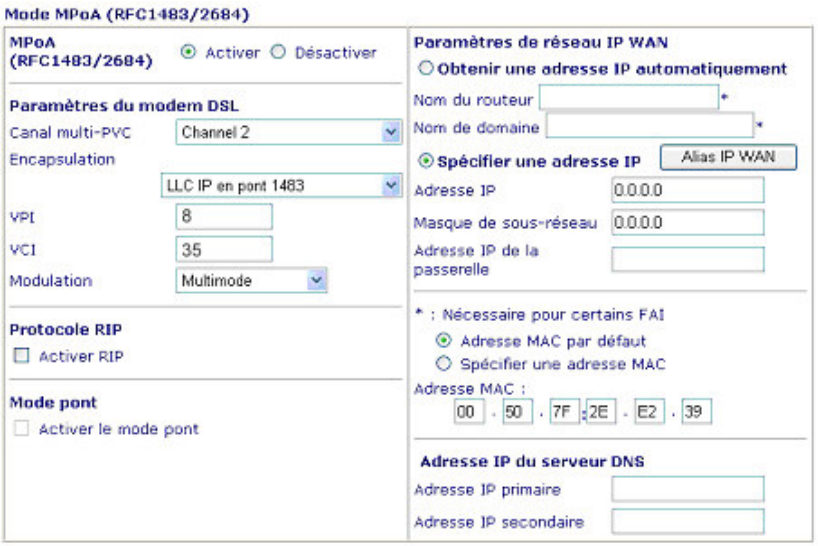
Public IP Address | *Adresse IP publique*
Public IP Address | *Adresse IP publique*

Si vous ne cochez pas **Joindre le pool IP NAT**, vous pouvez néanmoins utiliser ces adresses IP publiques à d'autres fins : hôte DMZ, ouverture de ports. Reportez-vous au Chapitre 5 NAT pour plus de détails.



Public IP Address	*Adresse IP publique*
Public IP Address	*Adresse IP publique*

3.2.2 MPoA



Paramètres du modem DSL

Configurez les paramètres DSL selon les informations fournies par votre FAI.

Configuration du secours RNIS (pour le modèle i seulement)

Néant	Désactiver cette fonction
Déclenchement par paquet	Activer cette fonction à la réception d'un paquet
Connexion permanente	Fonction toujours activée

Protocole RIP

Le protocole d'information de routage ou RIP (RFC1058) définit comment les routeurs échangent les informations des tables de routage.

Activer RIP :

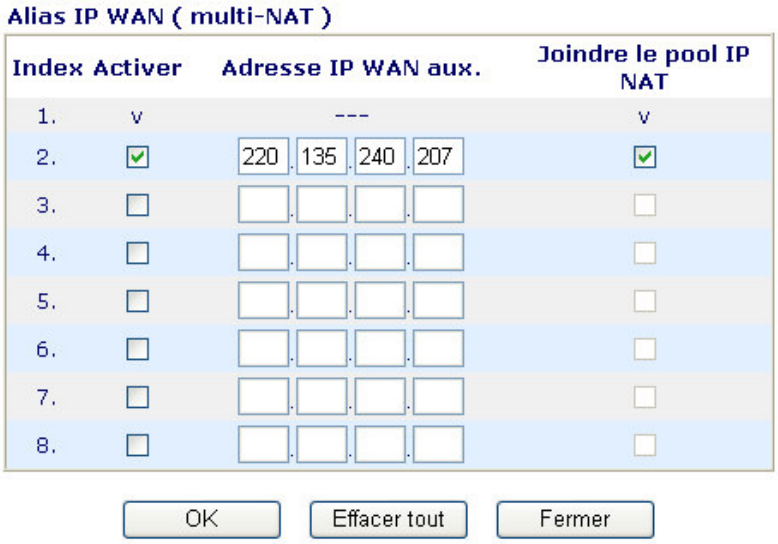
Cochez cette case. Le routeur échange périodiquement les tables de routage.

Paramètres de réseau IP WAN

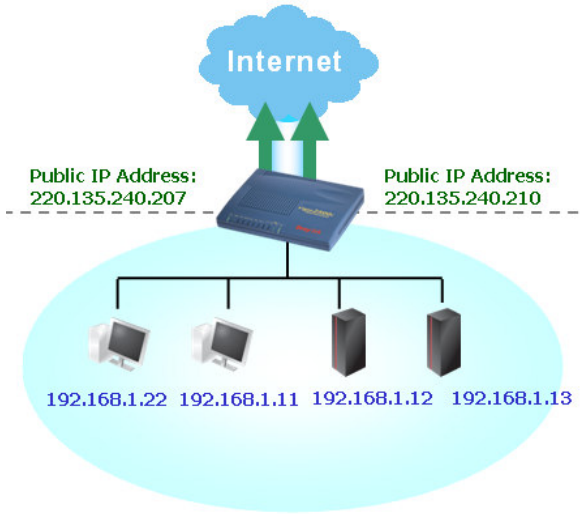
Vous pouvez obtenir une adresse IP automatiquement en indiquant le nom de routeur et le nom de domaine ou simplement en spécifiant une adresse IP.

Alias IP WAN :

Si vous avez plusieurs adresses IP publiques et que vous voulez les utiliser sur l'interface WAN, vous pouvez utiliser la fonction **Alias IP WAN**. Vous pouvez programmer jusqu'à 8 adresses IP publiques autres que celles que vous utilisez actuellement.

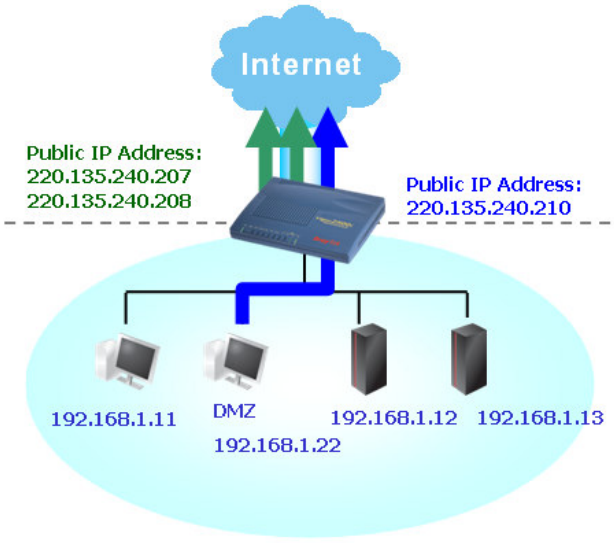


Si vous cochez J**oindre le pool IP NAT**, les données provenant des hôtes NAT sont transmises cycliquement session par session.



Public IP Address | *Adresse IP publique*
Public IP Address | *Adresse IP publique*

Si vous ne cochez pas **Joindre le pool IP NAT**, vous pouvez néanmoins utiliser ces adresses IP publiques à d'autres fins : hôte DMZ, ouverture de ports. Reportez-vous au Chapitre 5 NAT pour plus de détails.



Public IP Address	*Adresse IP publique*
Public IP Address	*Adresse IP publique*

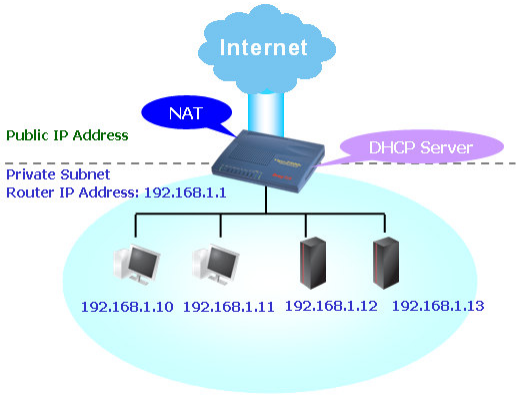
Chapitre 4
Configuration du LAN

4.1 Introduction

Un réseau local (LAN) est un groupe de sous-réseaux gérés par le routeur. La structure du réseau dépend du type d'adresses IP publiques que votre FAI propose.

Principes de création de votre LAN

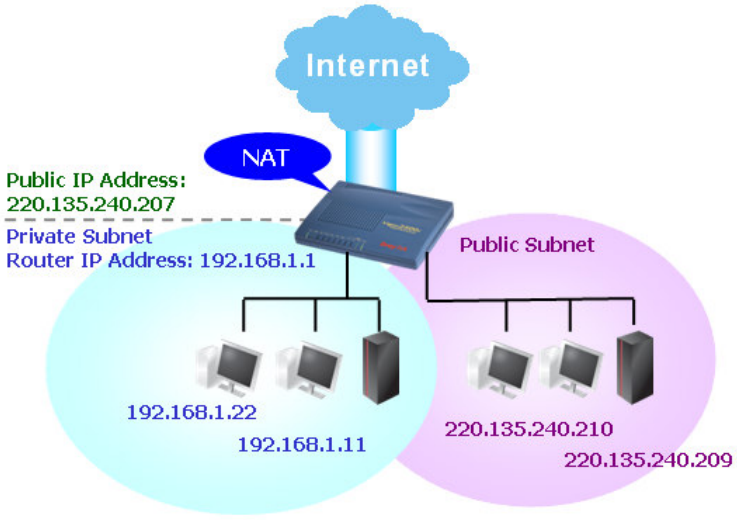
La fonction la plus générique du routeur Vigor est la fonction NAT, qui crée un sous-réseau privé qui vous est propre. Comme indiqué au paragraphe 3.1, le routeur communique avec les autres hôtes publics sur l'internet à l'aide d'une adresse IP publique et avec les hôtes locaux à l'aide de leur adresse IP privée. Le traducteur d'adresse réseau (NAT) traduit une adresse IP publique en une adresse IP privée afin que les paquets soient acheminés jusqu'à l'hôte à qui ils sont destinés, et vice-versa. En outre, le routeur Vigor comporte un serveur DHCP intégré qui attribue une adresse IP privée à chaque hôte local. Il est donc extrêmement facile de créer une structure de LAN tel que celle illustrée ci-dessous :



Public IP Address	*Adresse IP publique*
DHCP Server	*Serveur DHCP*
Private Subnet	*Sous-réseau privé*
Router IP Address	*Adresse IP de routeur*

Création d'un LAN plus complexe

Dans certains cas, votre FAI peut vous avoir attribué un sous-réseau IP public, par exemple, 220.135.240.0/24. Vous pouvez alors configurer un sous-réseau public, ou 2e sous-réseau, dont chaque hôte possède une adresse IP publique. Dans le cadre du sous-réseau public, le routeur Vigor assure le routage IP afin d'aider les hôtes du sous-réseau public à communiquer avec d'autres hôtes ou serveurs publics extérieurs. Dans ce cas, le routeur doit être configuré en passerelle pour les hôtes publics.



Public IP Address	*Adresse IP publique*
Public Subnet	*Sous-réseau public*
Private Subnet	*Sous-réseau privé*
Router IP Address	*Adresse IP de routeur*

Protocole d'information de routage (RIP)

Pour échanger des informations de routage avec les routeurs voisins, le routeur Vigor utilise le protocole d'information de routage (RIP). Cela permet aux utilisateurs de modifier à leur gré les informations du routeur, par exemple, l'adresse IP, les routeurs s'informant mutuellement et automatiquement des modifications faites.

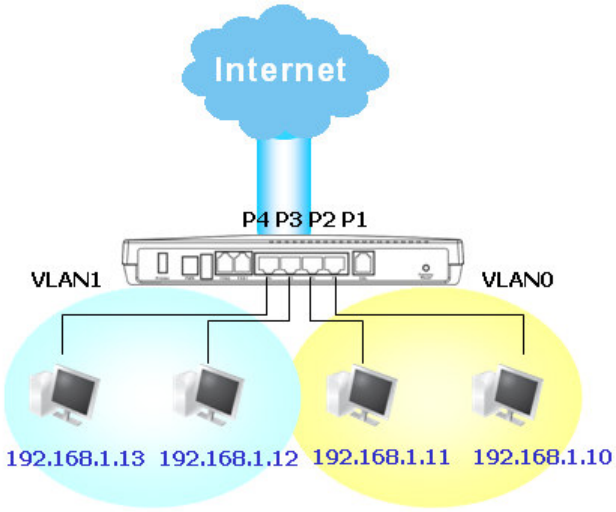
Routes statiques

Lorsque vous avez plusieurs sous-réseaux dans votre LAN, il est quelquefois plus efficace et plus rapide d'utiliser la fonction **Routes statiques**. Avec cette fonction, il vous suffit de définir des règles de transfert des données d'un sous-réseau spécifié à un autre

sous-réseau spécifié sans utiliser le RIP.

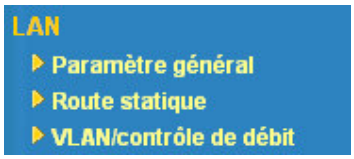
LAN virtuels et contrôle de débit

Vous pouvez grouper les hôtes locaux par port physique et créer jusqu'à 4 LAN virtuels. Pour gérer les communications entre les différents groupes, vous pouvez définir des règles dans la fonction LAN virtuel (VLAN) et un débit pour chaque.



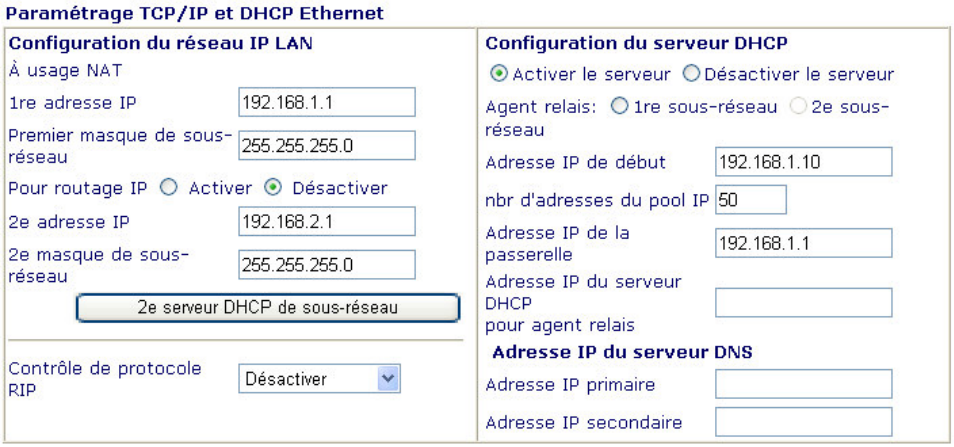
4.2 Paramètres

Cliquez sur **LAN** pour ouvrir la page de configuration du LAN.



4.2.1 Paramètres TCP/IP et DHCP du LAN

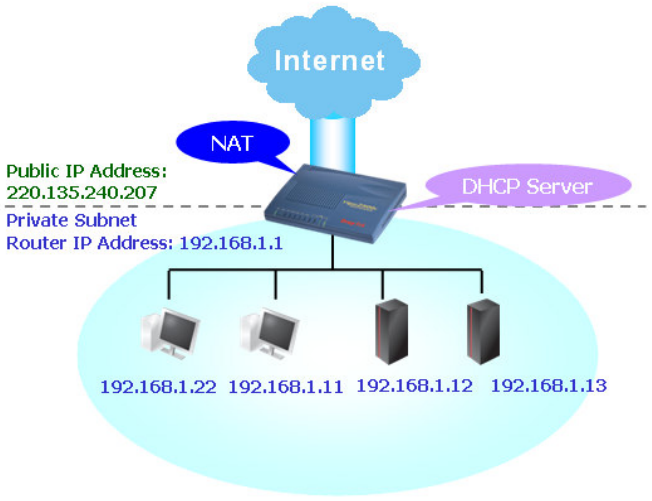
Cliquez sur **LAN TCP/IP et DHCP** ; l'écran suivant apparaît.



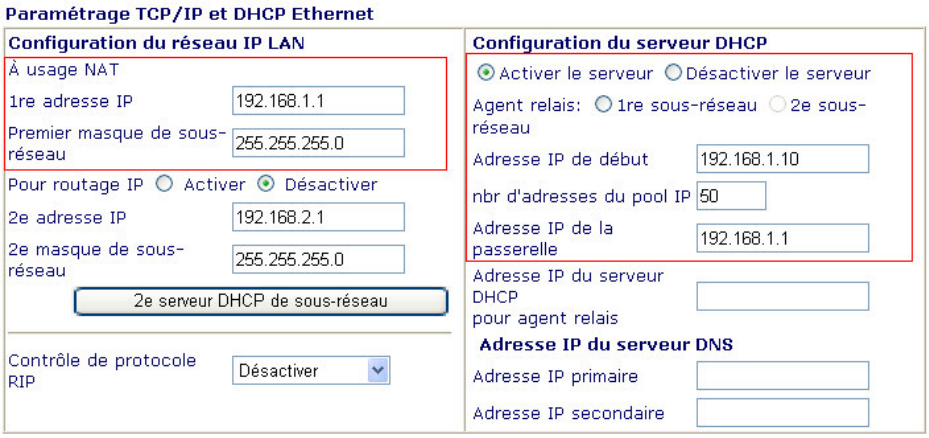
Nous allons examiner deux scénarios courants avec une explication détaillée de chaque champ.

Paramètres du 1er sous-réseau – Sous-réseau créé à l'aide du NAT

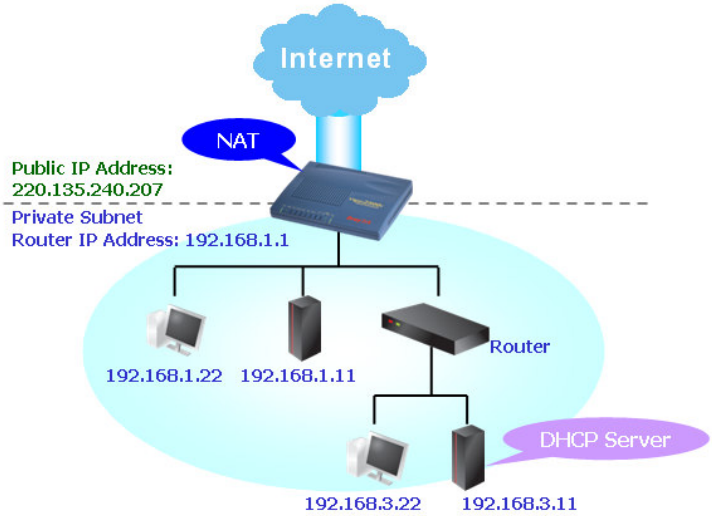
Un exemple de paramétrage par défaut avec la topologie correspondante est donné ci-dessous. Par défaut, le routeur Vigor a pour adresse IP privée 192.168.1.1 et comme masque de sous-réseau 255.255.255.0. Le serveur DHCP intégré est activé et attribue à chaque hôte NAT local une adresse IP 192.168.1.x à partir de 192.168.1.10.



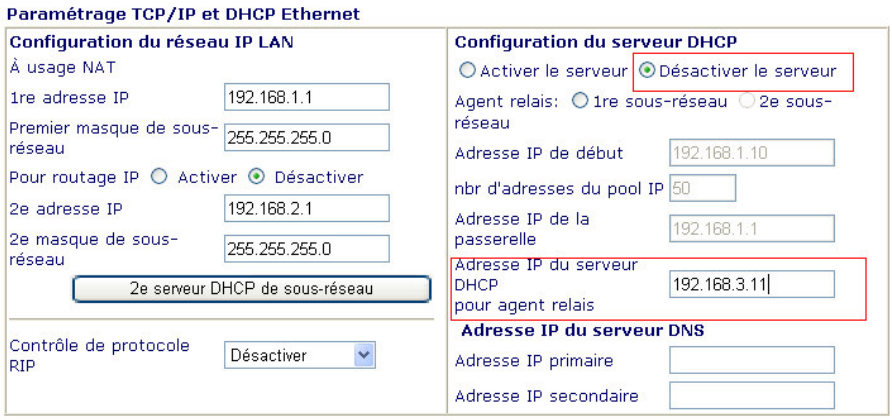
Public IP Address	*Adresse IP publique*
DHCP Server	*Serveur DHCP*
Private Subnet	*Sous-réseau privé*
Router IP Address	*Adresse IP de routeur*



Pour utiliser un autre serveur DHCP du réseau au lieu du routeur Vigor, il vous faudra sans doute modifier les paramètres comme indiqué ci-dessous.

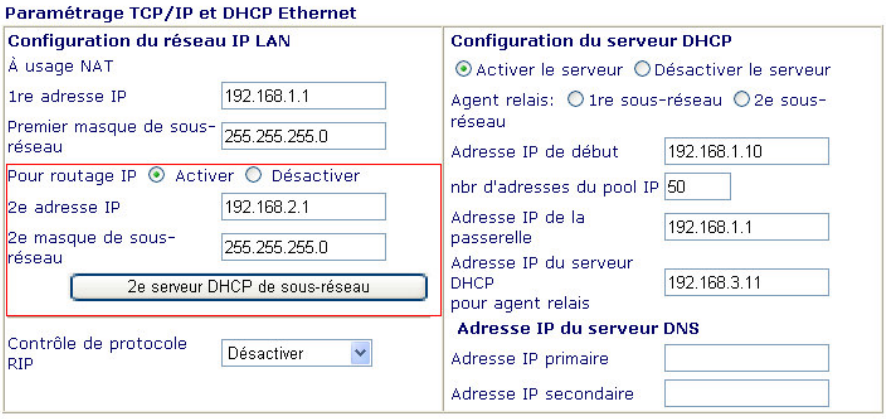


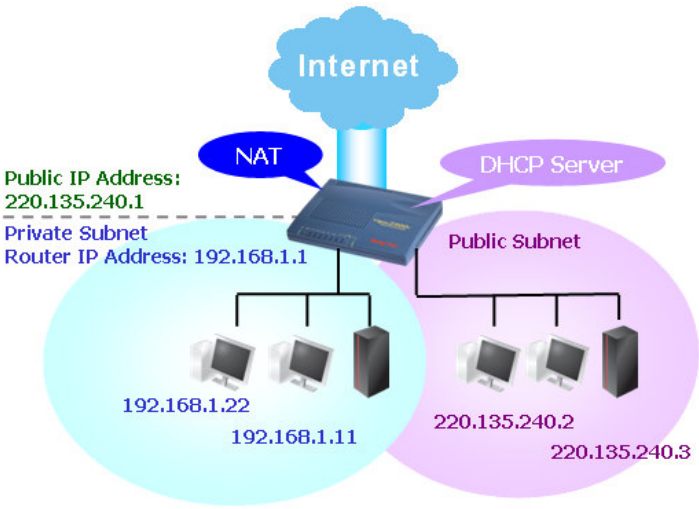
Public IP Address	*Adresse IP publique*
DHCP Server	*Serveur DHCP*
Private Subnet	*Sous-réseau privé*
Router IP Address	*Adresse IP de routeur*



Paramètres du 2e sous-réseau – Sous-réseau public

Un exemple de configuration du routeur Vigor pour le routage IP d'un sous-réseau public avec la topologie correspondante est donné ci-dessous.





Public IP Address	*Adresse IP publique*
DHCP Server	*Serveur DHCP*
Private Subnet	*Sous-réseau privé*
Router IP Address	*Adresse IP de routeur*
Public Subnet	*Sous-réseau public*

Configuration du réseau IP LAN

L'explication de chaque champ est donnée ci-dessous.

À usage NAT :

1re adresse IP	Adresse IP privée permettant de se connecter à un réseau local (valeur par défaut : 192.168.1.1).
1er masque de sous-réseau	Code d'adresse qui détermine la taille du réseau. (Valeur par défaut : 255.255.255.0/ 24)

Pour routage IP : (par défaut : Désactiver)

2e adresse IP	Adresse IP secondaire permettant de se connecter à un sous-réseau (par défaut : 192.168.2.1/ 24)
2e masque de sous-réseau	Code d'adresse qui détermine la taille du réseau. (Valeur par défaut : 255.255.255.0/ 24)

2e serveur DHCP	Vous pouvez configurer le routeur pour qu'il serve de serveur DHCP pour le deuxième sous-réseau. **Adresse IP de début :** Tapez une valeur du pool d'adresses IP pour définir le début de la plage d'adresses IP qu'attribuera le serveur DHCP. Si la 2e adresse IP de votre routeur est 220.135.240.1, l'adresse IP de début doit être égale ou supérieure à 220.135.240.2 mais inférieure à 220.135.240.254. **Nbr d'adresses du pool IP :** Tapez le nombre d'adresses IP du pool (10 maximum). Par exemple, si vous tapez 3 et que la 2e adresse IP de votre routeur est 220.135.240.1, la plage d'adresses IP fournie par le serveur DHCP ira de 220.135.240.2 à 220.135.240.11. **Adresse MAC :** Tapez l'adresse MAC des hôtes pour créer une liste d'hôtes auxquelles sont attribuées des adresses IP du pool.

La création d'une telle liste pour le 2e serveur DHCP aidera le routeur à attribuer l'adresse IP correcte du sous-réseau correct à l'hôte correct. Ainsi, les hôtes du 2e sous-réseau n'obtiendront pas une adresse IP appartenant au 1er sous-réseau.

Contrôle du protocole RIP

Désactiver	Désactiver le protocole RIP. Cela a pour effet d'arrêter l'échange d'informations de routage entre les routeurs. (Par défaut, le protocole RIP est désactivé).
1er sous-réseau	Sélection du routeur pour modifier les informations RIP du 1er sous-réseau avec information des routeurs voisins.
2e sous-réseau	Sélection du routeur pour modifier les informations RIP du 2e sous-réseau avec information des routeurs voisins.

Configuration du serveur DHCP

Le sigle DHCP signifie Dynamic Host Configuration Protocol (protocole de configuration dynamique de machine hôte). Par défaut, le routeur joue le rôle de serveur DHCP pour votre réseau. Il transmet automatiquement les paramètres IP à tout utilisateur local configuré en client DHCP. Il est vivement recommandé de laisser le routeur configuré en serveur DHCP en l'absence de serveur DHCP dans votre réseau.

Si vous voulez utiliser un autre serveur DHCP du réseau au lieu de celui du routeur Vigor, vous pouvez laisser l'agent relais vous aider à rediriger la requête DHCP.

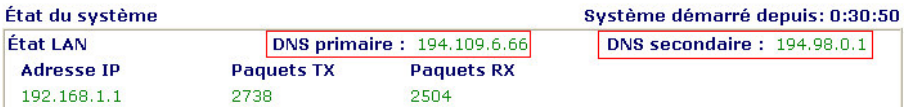
Activer le serveur	Le routeur attribue automatiquement une adresse IP à tous les hôtes du réseau local.
Désactiver le serveur	Vous attribuez manuellement une adresse IP à tous les hôtes du réseau local.
Agent relais **1er sous-réseau/2e sous-réseau**	Spécifiez le sous-réseau où se trouve le serveur DHCP vers lequel l'agent relais doit rediriger la requête DHCP.
Adresse IP de début	Tapez une valeur du pool d'adresses IP pour définir le début de la plage d'adresses IP qu'attribuera le serveur DHCP. Si la 1e adresse de votre routeur est 192.168.1.1, l'adresse IP de début doit être égale ou supérieure à 192.168.1.2 mais inférieure à 192.168.1.254.
Nombre d'adresses du pool IP	Tapez le nombre maximum de PC auquel le serveur DHCP doit attribuer une adresse IP. La valeur par défaut est 50 et la valeur maximale est 253.
Adresse IP de la passerelle	Tapez l'adresse IP de passerelle pour le serveur DHCP. Cette adresse est généralement la même que la 1re adresse IP du routeur, ce qui veut dire que le routeur est la passerelle par défaut.
Adresse IP du serveur DHCP pour l'agent relais	Spécifiez l'adresse IP du serveur DHCP que vous allez utiliser pour que l'agent relais aide à transmettre la requête DHCP au serveur DHCP.

Configuration du serveur DNS

Le sigle DNS signifie Domain Name System (système d'adressage par domaines). Sur l'internet, chaque machine hôte doit avoir une adresse IP unique et peut aussi avoir un nom reconnaissable et facile à mémoriser, comme www.yahoo.com. Le serveur DNS convertit ce nom en l'adresse IP correspondante.

Adresse IP primaire	Vous devez spécifier ici une adresse IP de serveur DNS car votre FAI vous en fournira généralement plusieurs. Si votre FAI n'en fournit pas, le routeur applique automatiquement l'adresse IP de serveur DNS par défaut : 194.109.6.66.
Adresse IP secondaire	Vous pouvez spécifier ici une adresse IP de serveur secondaire car votre FAI vous en fournira plusieurs. Si votre FAI ne vous en fournit pas, le routeur applique automatiquement l'adresse IP de serveur DNS secondaire par défaut : 194.98.0.1.

Vous pouvez utilisez la fonction Aide en ligne pour connaître l'adresse IP de serveur DNS par défaut :



Si les deux champs d'adresse IP primaire et secondaire sont laissés vides, le routeur attribue sa propre adresse IP aux utilisateur locaux en tant que serveur proxy DNS et gère un cache DNS.

Si l'adresse IP d'un nom de domaine se trouve déjà dans le cache DNS, le routeur « résoud » immédiatement le nom de domaine. Autrement, le routeur transmet le paquet d'interrogation DNS au serveur DNS externe en établissant une connexion WAN (DSL ou câble).

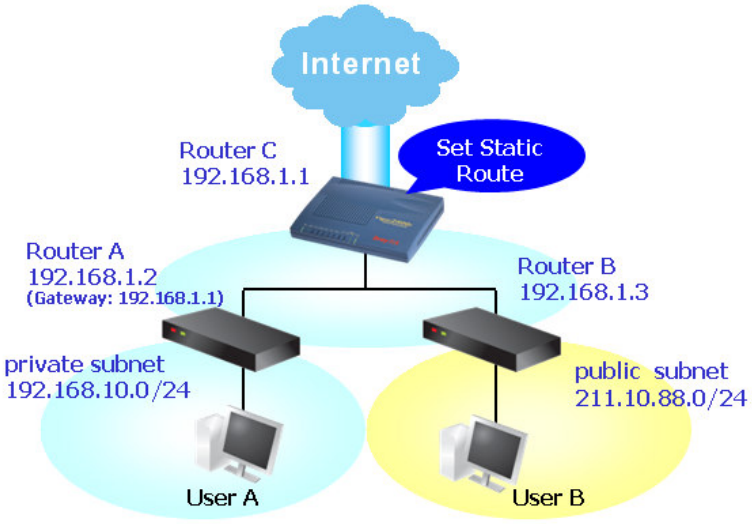
4.2.2 Route statique

Ajout de routeurs statiques à des réseaux privés publics

Voici un exemple de configuration d'une route statique dans le routeur principal afin que les utilisateurs A et B se trouvant dans des sous-réseaux différents puissent communiquer par l'intermédiaire du routeur Vigor. On suppose que l'accès à l'internet a été configuré et que le routeur fonctionne correctement :

- Vous utilisez le routeur principal pour naviguer sur l'internet.
- Vous créez un sous-réseau privé 192.168.10.0 à l'aide d'un routeur interne A (192.168.1.2)
- Vous créez un sous-réseau public 211.100.88.0 à l'aide d'un routeur interne B (192.168.1.3).
- Vous avez configuré le routeur principal 192.168.1.1 comme passerelle par défaut pour le routeur A 192.168.1.2.

Tant qu'une route statique n'a pas été configurée, l'utilisateur A ne peut pas communiquer avec l'utilisateur B car le routeur A ne peut transmettre des paquets reconnus qu'à sa passerelle par défaut, à savoir le routeur principal.

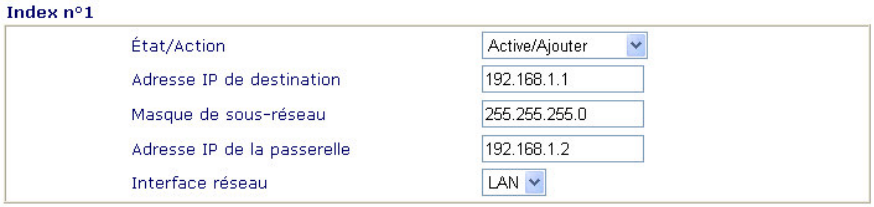


Router A	*Routeur A*
Router B	*Routeur B*
Router C	*Routeur C*
Private subnet	*Sous-réseau privé*
Public subnet	*Sous-réseau public*
Set Static route	*Configurer une route statique*
User A	*Utilisateur A*
User B	*Utilisateur B*

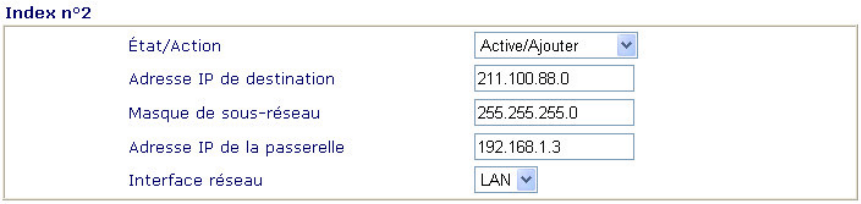
1. Cliquez sur **Paramètres TCP/IP et DHCP du LAN**, sélectionnez **Contrôle de protocole RIP** pour le 1er sous-réseau, puis cliquez sur le bouton **OK**.

Nous appliquons le contrôle de protocole RIP au 1er sous-réseau pour deux raisons. La première est que l'interface LAN peut échanger des paquets RIP avec les routeurs voisins via le 1er sous-réseau (192.168.1.0/24). La deuxième est que les hôtes des sous-réseaux privés internes (par exemple, 192.168.10.0/24) peuvent accéder à l'internet via le routeur et échanger en permanence des informations de routage IP avec différents sous-réseaux.

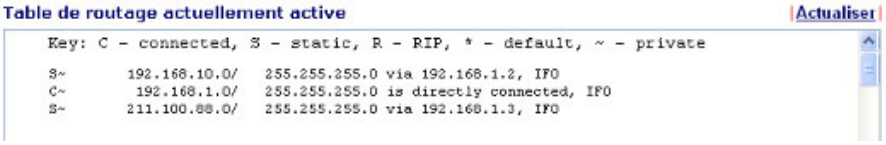
2. Cliquez sur **Configuration de route statique** et sur **Index n°.** Cela a pour effet d'ajouter une route statique comme indiqué ci-dessous ; tous les paquets destinés à 192.168.10.0 seront transmis à 192.168.1.2.



3. Cliquez sur un autre **Index n°** pour ajouter une autre route statique comme indiqué ci-dessous ; tous les paquets destinés à 211.100.88.0 seront transmis à 192.168.1.2.



4. Cliquez sur **Diagnostics >>Table de routage** pour vérifier la table de routage actuelle.



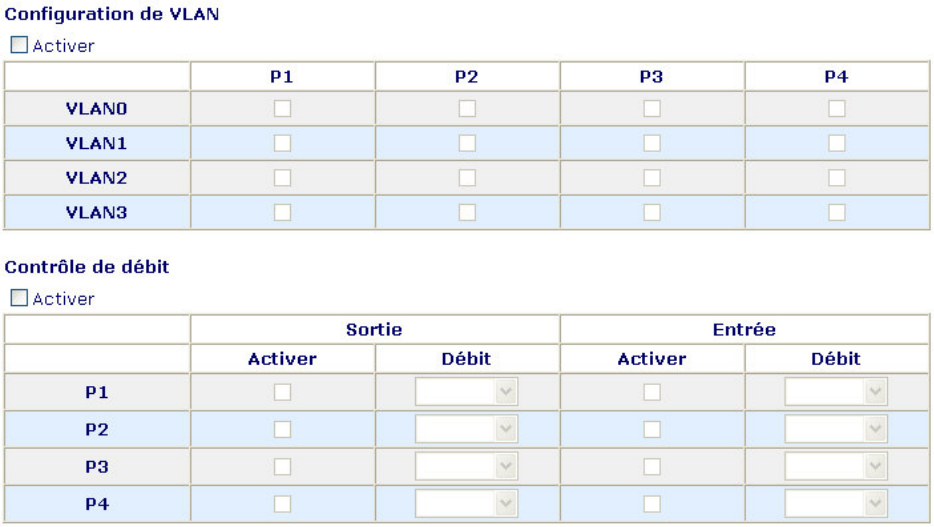
Suppression ou désactivation de route statique

1. Cliquez sur **Configuration de route statique** et sélectionnez le numéro d'index que vous voulez supprimer.
2. Sélectionnez l'option **Vider/Effacer** du menu déroulant, puis cliquez sur le bouton **OK** pour supprimer la route.

4.2.3 VLAN/Contrôle de débit

La fonction LAN virtuel vous permet de gérer commodément les hôtes en les groupant dans le port physique. Vous pouvez également gérer le débit d'entrée/sortie de chaque port.

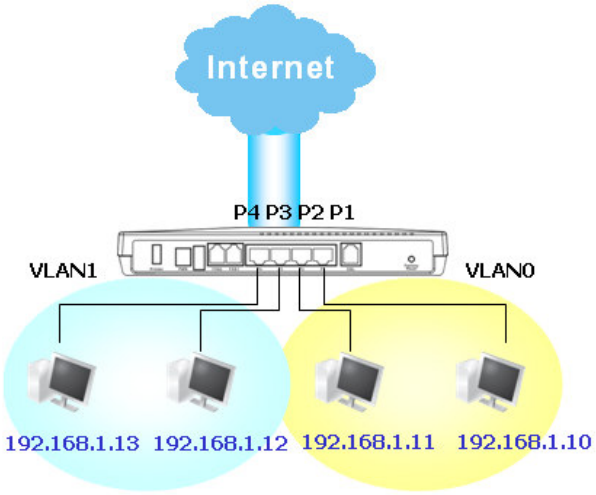
Cliquez sur **VLAN/contrôle de débit**. L'écran ci-dessous apparaît.



Ajouter/Supprimer des VLAN

Voici un exemple de paramétrage de VLAN.

- Le VLAN 0 se compose d'hôtes reliés à P1 et à P2
- Le VLAN 1 se compose d'hôtes reliés à P3 et à P4



Cochez la case Activer pour activer la fonction VLAN. Après avoir coché la case pour activer la fonction VLAN, cochez les cases appropriées du tableau ci-dessous.

Configuration de VLAN

☑ Activer

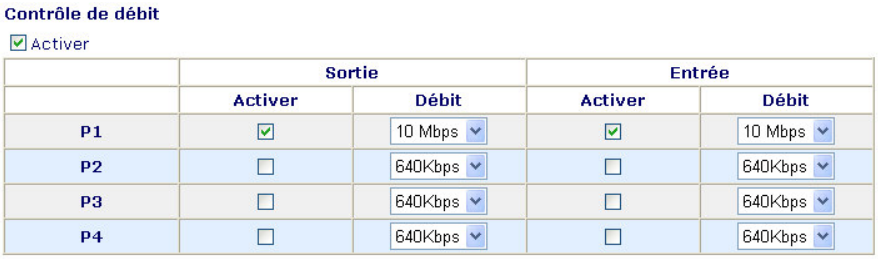
	P1	P2	P3	P4
VLAN0	☑	☑	☐	☐
VLAN1	☐	☐	☑	☑
VLAN2	☐	☐	☐	☐
VLAN3	☐	☐	☐	☐

Pour désactiver la fonction VLAN, décochez la case Activer et cliquez sur OK pour sauvegarder.

Contrôle de débit

Vous pouvez gérer le débit d'entrée et de sortie d'un port physique. Quatre débits sont possibles : 650 kbit/s, 1,5 Mbit/s, 3 Mbit/s, 5,5 Mbit/s et 10 Mbit/s.

Pour régler le débit d'entrée et de sortie de P1 à 10 Mbit/s :



Chapitre 5
Paramétrage du NAT

5.1 Introduction

Dans la plupart des cas, le routeur Vigor se comporte comme un routeur traducteur d'adresse réseau (NAT). Le traducteur d'adresse réseau (NAT) convertit une ou plusieurs adresses IP en une seule adresse IP publique. L'adresse IP publique est généralement attribuée par votre FAI qui peut vous la facturer. Les adresses IP privées ne sont reconnues que par les hôtes internes.

Lorsque des paquets sortants à destination d'un serveur public sur l'internet parviennent au routeur NAT, celui-ci traduit l'adresse d'origine en l'adresse IP publique qui lui a été attribuée, sélectionne le port public disponible, puis transmet les paquets. En même temps, le routeur consigne la correspondance adresse-port dans une table. Lorsque le serveur public répond, c'est à l'adresse publique du routeur qu'arrive le trafic entrant et le routeur effectue la traduction inverse. Ainsi, l'hôte interne peut communiquer avec l'hôte externe d'une manière transparente.

La traduction d'adresse réseau présente plusieurs avantages, dont les suivants :

- **Un avantage économique par l'utilisation efficace de l'adresse IP.** Le NAT permet de traduire les adresses IP internes des hôtes locaux en une seule adresse IP publique. Il suffit donc d'avoir une seule adresse IP publique pour tous les hôtes internes.
- **Elle renforce la sécurité du réseau interne en cachant les adresses IP privées.** De nombreuses attaques utilisent l'adresse IP. Comme l'attaquant ne peut connaître aucune des adresses IP privées, la fonction NAT peut protéger le réseau interne.

5.2 Paramètres

Cliquez sur **Paramétrage du NAT**.

Dans la page qui s'ouvre est affichée l'adresse IP privée définie par le RFC 1918. Nous utilisons généralement le sous-réseau 192.168.1.0/24 pour le routeur. Comme il a été dit plus haut, la fonctionnalité NAT peut transposer une ou plusieurs adresses IP, un ou plusieurs ports de service en différents services. En d'autres termes, la fonctionnalité NAT peut être mise en œuvre en utilisant le mappage de ports.

Les routeurs Vigor autorisent 3 méthodes de mappage de ports :

Redirection de ports, **Ouverture de ports** et **Hôte DMZ**

Redirection de ports	Le routeur transmet les paquets adressés à un port public spécifique à partir du réseau externe à un port privé spécifique d'un hôte local spécifique.
Ouverture de ports	Cette fonction, semblable à la fonction de redirection de ports, permet aux utilisateurs de définir une plage de ports à ouvrir et de transmettre le trafic à un même port des hôtes internes.
Hôte DMZ	Cette fonction permet d'exposer complètement sur l'internet un hôte local en ouvrant tous ses ports pour certains services particuliers. Tous les paquets entrants sont transmis au PC désigné.

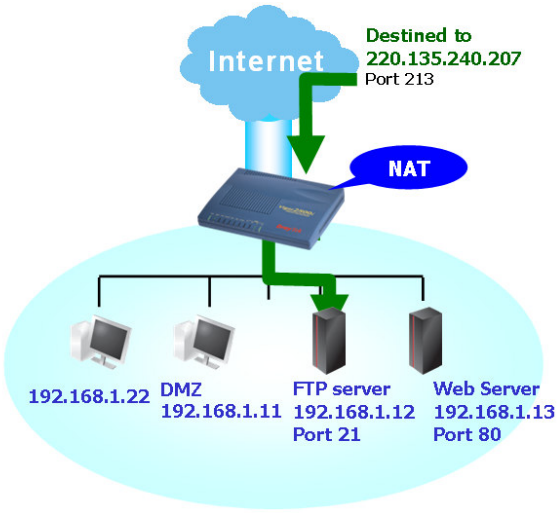
À noter que si vous activez simultanément ces options, un ordre de priorité permet d'éviter les conflits possibles. L'ordre de priorité est le suivant : **Redirection de ports > Ouverture de ports > Hôte DMZ**

Vérification de l'état

Cliquez sur **Diagnostics** pour vérifier la table de correspondance adresses-ports du routeur.

5.2.1 Table de redirection de ports

La redirection de ports sert généralement pour la mise en œuvre de services au sein du réseau local (LAN) : serveurs web, serveurs FTP, serveurs de messagerie, etc. Dans la plupart des cas, il vous faut une adresse IP publique pour chaque serveur et la combinaison adresse IP publique/nom de domaine est reconnue par tous les utilisateurs. Comme le serveur est situé à l'intérieur du LAN et que le réseau est bien protégé par le NAT du routeur identifié par son adresse/port IP privés, la fonction de redirection de ports transmet toutes les demandes d'accès provenant d'utilisateurs externes au mécanisme de mappage de ports du serveur.



Destined to	*Trafic à destination de*
FTP Server	*Serveur FTP*
Web Server	*Serveur web*

La redirection de ports ne s'applique qu'au trafic entrant. Les utilisateurs du serveur au sein du LAN ne peuvent pas accéder à l'adresse IP publique du serveur. Vous accédez au serveur à l'aide de l'adresse IP privée locale de celui-ci ou bien vous devez définir un alias dans un fichier d'hôtes Windows. Redirigez uniquement les ports qui doivent l'être et non tous les ports. Autrement, vous compromettrez la sécurité de type pare-feu mise en place initialement par la fonction NAT.

La **table de redirection de ports** permet de définir 10 redirections pour les machines hôte internes.

Table de redirection de ports

Index	Nom du service	Protocole	Port public	Adr IP privé	Port privé	Actif
1	FTP du service	TCP	213	192.168.1.12	21	☑
2	Web du service	TCP	80	192.168.1.13	80	☑
3		---	0		0	☐
4		---	0		0	☐
5		---	0		0	☐
6		---	0		0	☐
7		---	0		0	☐
8		---	0		0	☐
9		---	0		0	☐
10		---	0		0	☐

Nom du service	Tapez la désignation du service de réseau.
Protocole	Sélectionnez le protocole de transport (TCP ou UDP).
Port public	Spécifiez quel port doit être redirigé vers **l'adresse IP privée et le port privé** spécifiés.
Adresse IP privée	Spécifiez l'adresse IP privée de la machine hôte interne offrant le service.
Port privé	Spécifiez le numéro de port privé du service offert par la machine hôte interne.
Actif	Cochez cette case pour activer la redirection.

À noter que le routeur a ses propres services intégrés (serveurs), comme Telnet, HTTP, FTP, etc. Comme ces services (serveurs) ont le même numéro de port, il peut être nécessaire de réinitialiser le compteur afin d'éviter les conflits.

Par exemple, le configurateur web du routeur a comme port par défaut le port 80, il peut y avoir conflit avec le serveur web du réseau local, http://92.168.1.13:80. Par conséquent, il vous faut **définir comme port http du routeur un port autre que le port par défaut 80** pour éviter un conflit. À partir du menu **Maintenance du système >>Paramètres de gestion**, accédez à l'écran d'administration en faisant suivre l'adresse IP de 8080, par exemple : http://192.168.1.1:8080.

Paramètres de gestion

Contrôle d'accès pour la gestion

☐ Activer la mise à jour à distance du firmware (FTP)
☐ Autoriser la gestion à partir de l'internet
☑ Désactiver le PING en provenance de l'internet

Liste des accès

Liste IP | Masque de sous-réseau
1

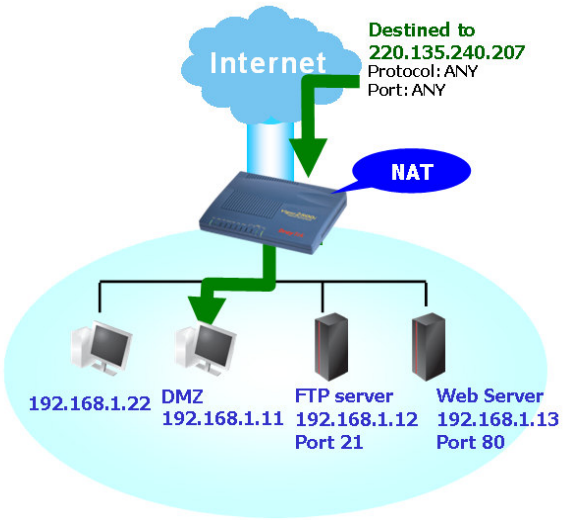
Paramétrage du port de gestion

○ Ports par défaut (Telnet: 23, HTTP: 80, HTTPS: 443, FTP: 21)
◉ Ports définis par l'utilisateur

Port Telnet 23
Port HTTP 8080
Port HTTPS 443
Port FTP 21

5.2.2 Configuration de l'hôte DMZ

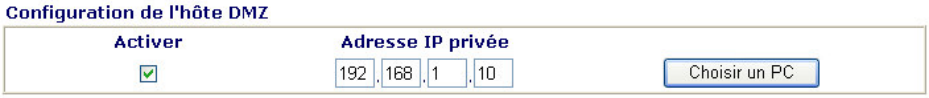
Comme indiqué plus haut, la **redirection de ports** peut rediriger les paquets TCP/UDP entrants ou autre trafic arrivant sur des ports particuliers vers l'adresse IP privée et le port privé d'un hôte du LAN. Toutefois, d'autres protocoles IP, comme les protocoles 50 (ESP) et 51 (AH) n'ont pas un port fixe. Le routeur Vigor a une fonction « **hôte DMZ** » qui vous permet de faire en sorte que TOUTES les données non sollicitées soient transmises, quel que soit le protocole, vers un hôte déterminé du LAN. La navigation normale sur l'internet et autres activités de ce genre des autres clients peuvent se poursuivre sans interruption intempestive. **L'hôte DMZ** permet d'exposer un utilisateur interne déterminé sur l'internet afin d'utiliser certaines applications spéciales, comme Netmeeting, des jeux internet, etc.



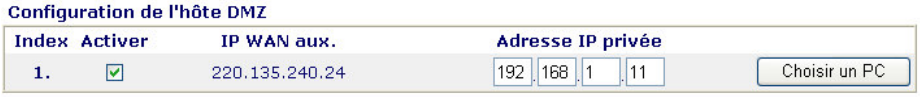
Destined to	*Trafic à destination de*
FTP Server	*Serveur FTP*
Web Server	*Serveur web*

Si vous configurer un hôte DMZ, vous compromettez dans une certaine mesure les propriétés de sécurité inhérentes au NAT. Vous pouvez envisager d'ajouter des règles de filtrage supplémentaires ou un pare-feu secondaire.

Cliquez sur **Configuration de l'hôte DMZ** pour ouvrir la page de paramétrage.



Si vous avez défini précédemment une série **d'alias WAN** dans **Accès à l'internet >>PPPoE/PPPoA** ou **Accès à l'internet >>MPoA,** vous les trouverez dans la **liste IP WAN aux**.

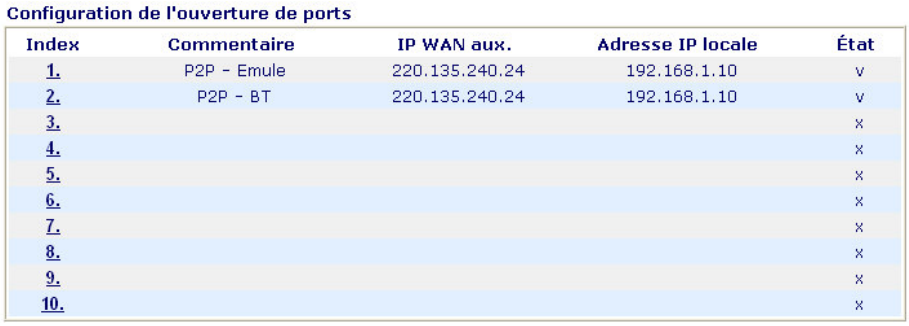


Activer	Cochez cette case pour activer la fonction Hôte DMZ.
Adresse IP privée	Entrez l'adresse IP privée de l'hôte DMZ.
Choisir un PC	Cliquez sur ce bouton pour faire apparaître une fenêtre affichant une liste des adresses IP privées de tous les hôtes de votre réseau local. Sélectionnez-en une comme adresse de l'hôte DMZ.

5.2.3 Ouverture de ports

La fonction d'**ouverture de ports** vous permet d'ouvrir une plage de ports pour des applications spéciales dont les plus courantes sont les applications de partage de fichiers entre homologues dites P2P (BT, KaZaA, Gnutella, WinMX, eMule et autres), les caméras internet, etc. Veillez à tenir à jour les applications pour éviter d'être victime de l'exploitation éventuelle de failles de sécurité.

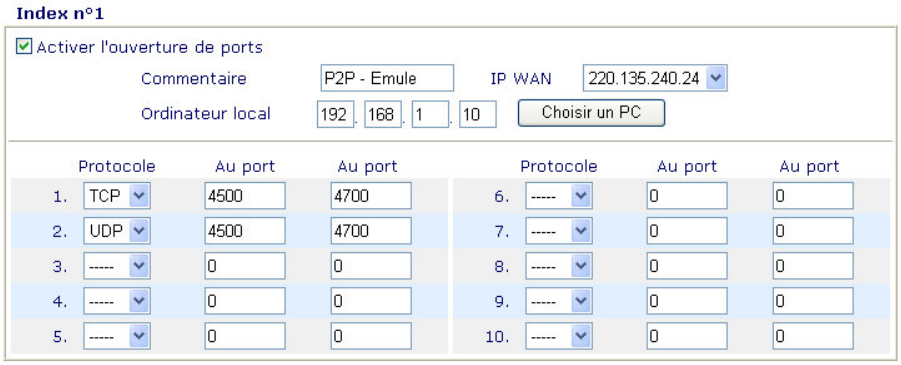
Dans le routeur Vigor, la fonction **d'ouverture de ports** permet de définir 10 redirections pour les hôtes internes.



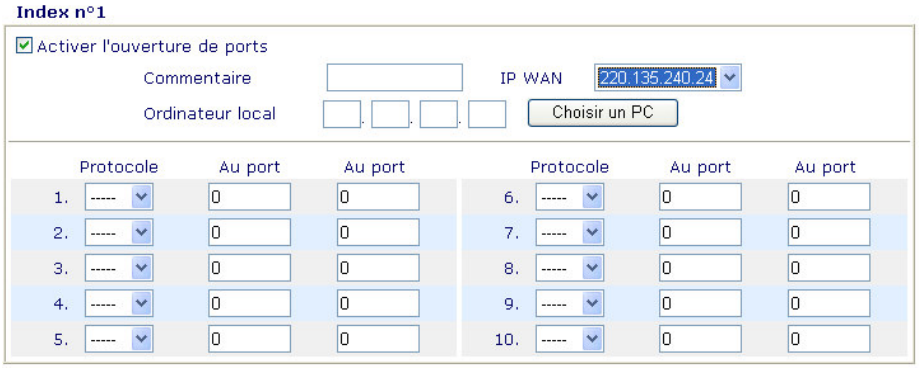
Index	Numéro d'ordre de la redirection de port à définir. Cliquez sur le numéro approprié pour modifier ou effacer la redirection correspondante.
Commentaires	Spécifiez le nom du service réseau.
Adresse IP locale	Adresse IP privée de l'hôte local pour un service.

État	État de la redirection correspondante. X = redirection inactive, V = redirection active.

Cliquez sur un index. La page de paramétrage correspondante apparaît. Pour chaque index, vous pouvez spécifier 10 plages de ports pour divers services.



Si vous avez défini précédemment une série **d'alias WAN** dans **Accès à l'internet >>PPPoE/PPPoA** ou **Accès à l'internet >>MPoA,** vous les trouverez dans la **liste IP WAN aux**.



Activer l'ouverture de ports	Cochez cette case pour activer cet index.
Commentaires	Tapez la désignation de l'application ou du service de réseau.
Ordinateur local	Entrez l'adresse IP privée de la machine locale.
Choisir un PC	Cliquez sur ce bouton pour faire apparaître une fenêtre affichant la liste des adresses IP privées des hôtes locaux. Sélectionnez une adresse IP appropriée dans la liste.
Protocole	Spécifiez le protocole de couche transport : TCP, UDP ou ----- (NÉANT).

Du port	Spécifiez le numéro du premier port de la plage de ports.
Au port	Spécifiez le numéro du dernier port de la plage de ports.

Chapitre 6 VoIP

6.1 Introduction

La téléphonie sur IP (VoIP) vous permet d'utilise votre connexion à internet à haut débit pour téléphoner via l'internet.

Il existe de nombreux protocole de signalisation d'appel qui permettent à des équipements VoIP de converser. Les protocoles les plus répandus sont SIP, MGCP, Megaco et H.323. Ces protocoles ne sont pas tous compatibles entre eux (sauf si un serveur d'appels est utilisé).

Les modèles Vigor V prennent en charge le protocole SIP car c'est un protocole idéal pour le fournisseur de service téléphonique sur internet (ITSP) et pour les logiciels de téléphonie (« softphones ») et qu'il est très répandu. Le protocole SIP est un protocole de signalisation de bout en bout qui établit la présence et la mobilité des utilisateurs dans une structure VoIP. Pour converser, on utilise un identificateur uniforme de ressource (URI) (« adresse SIP »). Le format normalisé de l'URI SIP est

sip: user:password @ host: port

Certains champs peuvent être facultatifs selon l'utilisation. En général, « host » fait référence à un domaine. « userinfo » comprend le champ utilisateur, le champ mot de passe et le signe @. L'URI est très semblable à une adresse universelle (URL). C'est pourquoi certains l'appellent « URL SIP ». Le SIP permet l'appel direct d'homologue à homologue ainsi que l'appel via un serveur mandataire (proxy) SIP (qui joue un rôle semblable au portier des réseaux H.323), alors que le protocole MGCP utilise une architecture client-serveur, le scénario d'appel étant très semblable à celui du RTCP actuel.

Après l'établissement d'un appel, les flux téléphoniques sont transmis via le protocole de transport en temps réel (RTP). Différents codecs (qui compriment et codent la voix) peuvent être intégrés aux paquets RTP. Les modèles Vigor V fournissent différents codecs, G.711 loi A/µ, G.723, G.726 et G.729 A & B. Chaque codec a une bande passante différente et donc donne une qualité vocale différente. Plus la bande passante d'un codec est large, meilleure est la qualité vocale. Toutefois, le codec utilisé doit être approprié à votre débit internet.

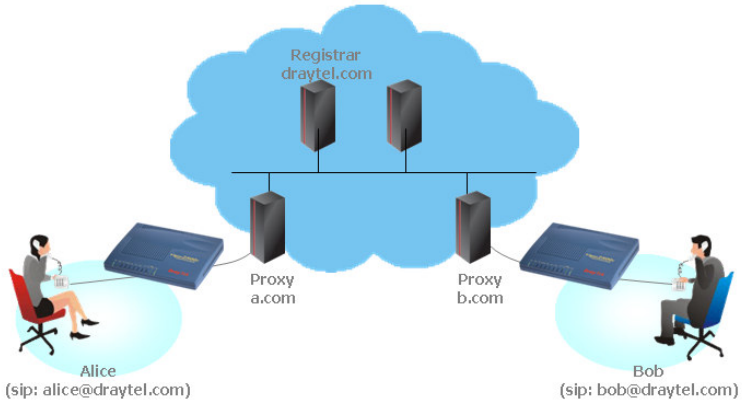
6.2 Paramètres

Il y a normalement deux scénarios d'appel possible :

- **Appel via des serveurs SIP**

  Tout d'abord, vos Vigor V doivent s'inscrire sur un serveur registre SIP en envoyant des messages d'inscription. Puis les serveurs mandataires SIP des deux correspondants transmettent la suite de message à l'appelant pour établir la session.

  Si les deux correspondants s'inscrivent sur le même serveur registre SIP les choses se passent comme ci-dessous :



  Le principal avantage de ce scénario est que vous n'avez pas à mémoriser l'adresse IP de votre correspondant, qui peut changer très fréquemment si elle est dynamique. Au lieu de cela, il vous suffit d'utiliser le **plan de numérotation** ou d'appeler directement le **nom de compte** de votre correspondant si vous êtes inscrit sur le même serveur registre SIP. Reportez-vous aux **exemples 1 et 2** du **scénario d'appel.**

- **Communication d'homologue à homologue (P2P)**

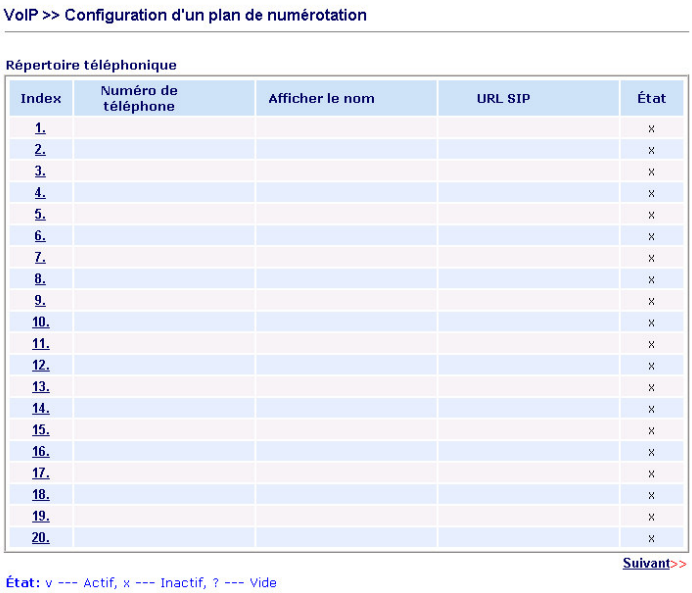
  Pour appeler, vous devez connaître l'adresse IP de votre correspondant. Les routeurs VoIP Vigor établissent la connexion. Reportez-vous à l'**exemple 3 du scénario d'appel.**

Nos modèles Vigor V mettent d'abord en œuvre des codecs efficaces conçus pour utiliser au mieux la bande passante disponible. Ils sont également dotés d'une fonction d'assurance automatique de la qualité de service. L'assurance de la qualité de service permet de donner la priorité au trafic téléphonique. Votre bande passante d'arrivée et de départ donne la priorité au trafic téléphonique mais vos données subissent un léger retard, tolérable pour le trafic de données.

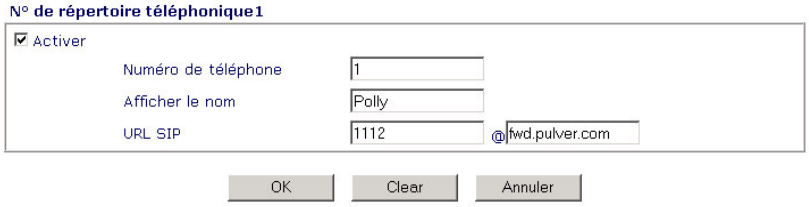
Les différentes options du menu VoIP sont décrites ci-après.

6.2.1 DialPlan (plan de numérotation)

Vous pouvez mettre vos contacts VoIP dans le « répertoire téléphonique » appelé DialPlan. Cela vous permettra d'appeler rapidement et facilement en utilisant la **numérotation abrégée**. Dans le DialPlan, vous pouvez enregistrer jusqu'à 60 adresses IP d'amis ou de parents.



Cliquez sur un index pour afficher la page de configuration d'un plan de numérotation.

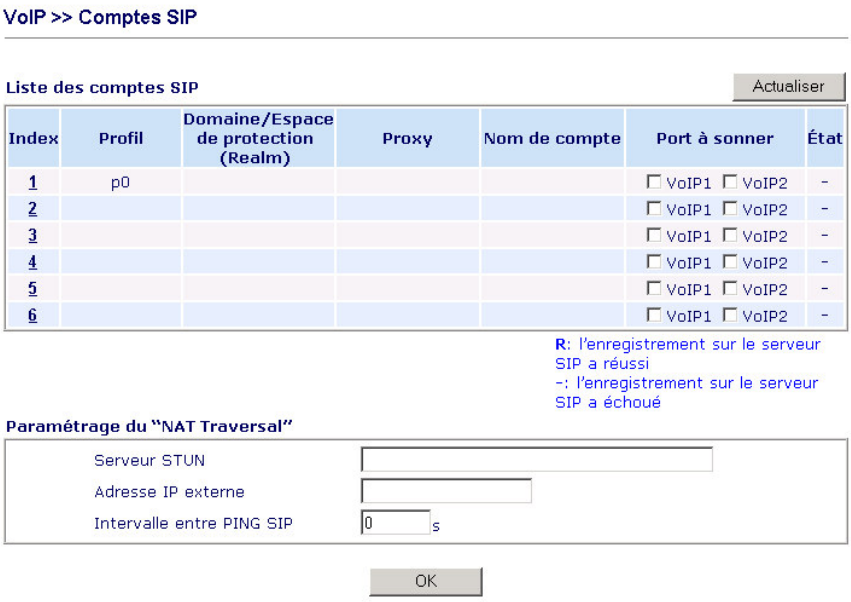


Activer	Cochez la case pour activer cette entrée.
Numéro de téléphone	Numéro abrégé. N'importe quelle combinaison des chiffres 0 à 9 et de *.
Afficher le nom	Identifiant d'appelant qui s'affichera sur l'écran de votre contact, ce qui lui permettra de savoir d'emblée qui appelle sans avoir à mémoriser une multitude d'URL SIP.
URL SIP	Tapez l'adresse SIP de votre contact.

6.2.2 Comptes SIP

Définissez ici vos propres paramètres SIP. Lorsque vous demandez un compte, votre fournisseur de service SIP vous alloue un **nom de compte** ou nom d'utilisateur, un serveur **registre SIP,** un serveur **proxy SIP** et un **nom de domaine**. (Dans certains cas, il se peut que les trois derniers soient identiques). Vous pourrez alors donner à vos contacts votre adresse SIP. **Nom de compte@ Nom de domaine.**

Lorsque vous allumez le routeur VoIP Vigor, il s'inscrit d'abord sur le serveur registre avec Nom d'utilisateur autorisé@Domaine/Espace de protection (Realm). Puis votre appel est acheminé à destination par le serveur proxy SIP avec Nom de compte@Domaine/Espace de protection comme identifiant.



Index Cliquez sur un index pour accéder à la page de configuration d'un compte SIP.

Profil Nom de profil du compte.

Domaine/Espace de protection (Realm) Nom de domaine ou adresse IP du serveur registre SIP

Proxy Nom de domaine ou adresse IP du serveur proxy SIP.

Nom de compte Nom de compte de votre adresse SIP avant @.

Port à sonner Spécifiez le port qui sonnera à la réception d'un appel téléphonique.

Serveur STUN Tapez l'adresse IP du serveur STUN.

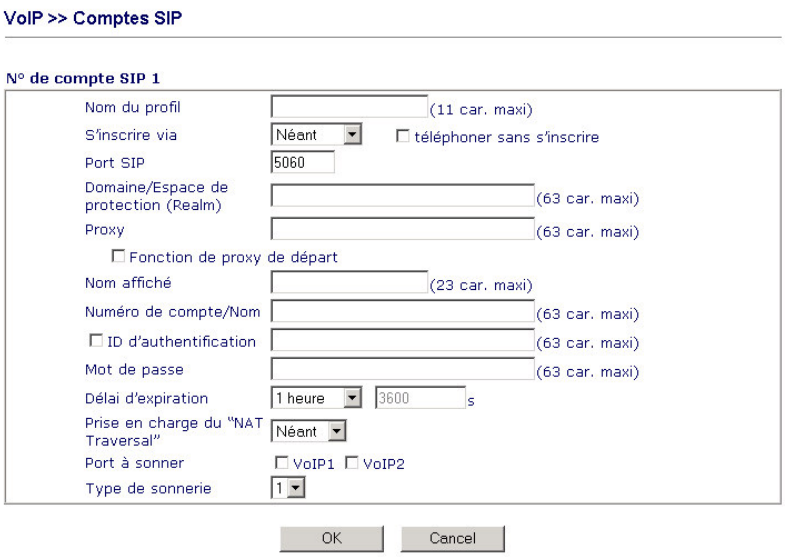
Adresse IP externe Tapez l'adresse IP de passerelle.

Intervalle entre la PING SIP La valeur par défaut est 150s. Ce paramètre est utile pour prise en charge du mécanisme « NAT Traversal » d'un serveur Nortel.

État Affiche l'état du compte SIP correspondant.

R signifie que le compte est bien est enregistré sur le serveur SIP.

– signifie que l'enregistrement du compte sur le serveur SIP a échoué.



Nom du profil

Donnez un nom à ce profil. Vous pouvez taper un nom semblable au nom de domaine. Par exemple, si le nom de domaine est *draytel.org*, vous pouvez tapez *draytel-1*dans ce champ.

S'inscrire via

Si vous voulez faire un appel VoIP sans vous inscrire, choisissez **Néant**. Certains serveurs SIP permettent d'utiliser la fonction VoIP sans s'inscrire. Avec un tel serveur, cochez la case **téléphoner sans s'inscrire**. Il est recommander de choisir **Auto**. Le système se chargera d'acheminer votre appel VoIP.

Port SIP

Spécifiez le numéro de port pour l'envoi et la réception du message SIP d'ouverture de session. La valeur par défaut est **5060.** Votre homologue doit spécifier la même valeur dans son Registre.

Domaine/Espace de protection (Realm)

Tapez le nom de domaine ou l'adresse IP du serveur registre SIP.

Proxy

Spécifiez le nom de domaine ou l'adresse IP du serveur proxy SIP. Vous pouvez maintenant faire suivre le nom de domaine du numéro de **port** de destination des données (par exemple, nat.draytel.org**:5065**)

Fonction de proxy de départ

Cochez cette case pour que le serveur mandataire serve de mandataire de départ.

Nom affiché

Identifiant d'appelant qui s'affichera sur l'écran de votre correspondant.

votre correspondant.

Numéro/nom de compte

Tapez le nom de compte de votre adresse SIP, c'est-à-dire tout ce qui précède @.

ID d'authentification

Cochez la case pour activer la fonction d'authentification et tapez le nom ou le numéro pour l'authentification SIP sur le serveur registre SIP. S'il s'agit du numéro de compte, il n'est pas nécessaire de cocher la case ni de taper quoi que ce soit dans ce champ.

Mot de passe

Le mot de passe qui vous a été fourni lorsque vous vous êtes inscrit pour un service SIP.

Délai d'expiration

Période de temps pendant laquelle votre serveur registre SIP conserve votre inscription. Avant l'expiration du délai, le routeur enverra une autre demande d'inscription au serveur registre SIP.

Prise en charge du « NAT Traversal »

Si le routeur que vous utilisez (par exemple**,** un routeur à large bande) se connecte à l'internet pour un autre équipement, vous devez sélectionner l'option désirée.

Néant – Désactiver cette fonction.
STUN – Choisissez cette option s'il y a un serveur STUN pour votre routeur.
Manuel – Choisissez cette option si vous voulez spécifier une adresse IP externe pour le « NAT Transversal ».
Nortel – Si le serveur d'appels que vous utilisez prend en charge la solution Nortel, vous pouvez choisir cette option.

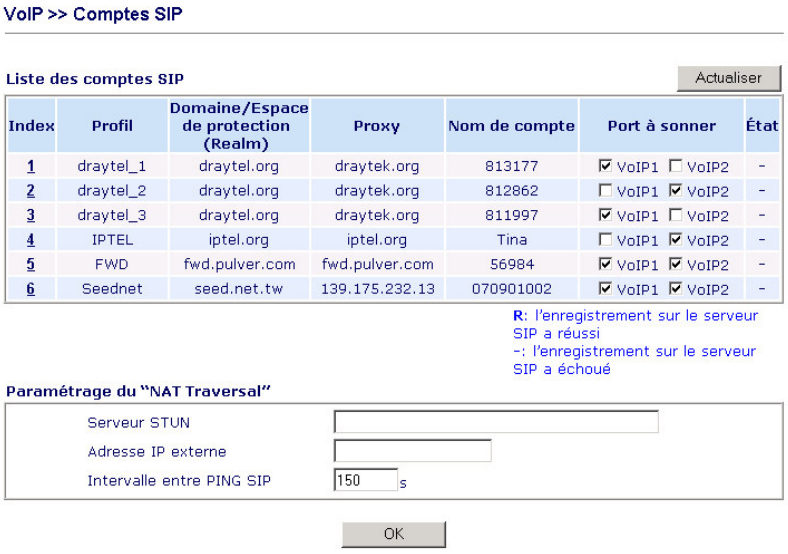
Port à sonner

Choisissez VoIP 1 ou VoIP 2 comme port à sonner par défaut.

Type de sonnerie

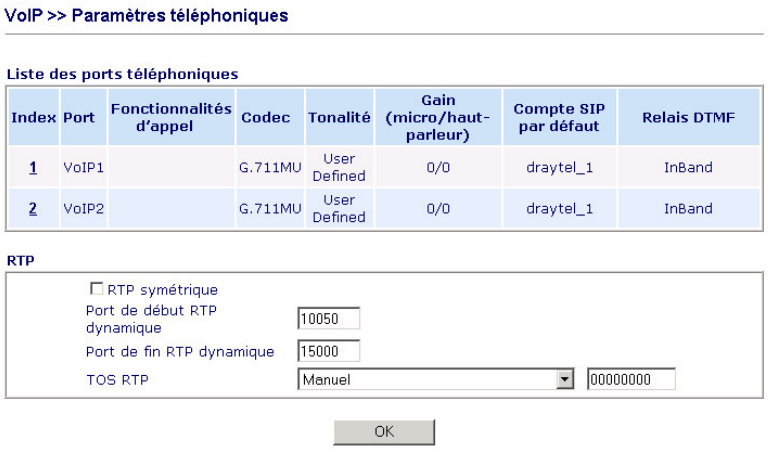
Choisissez un type de sonnerie pour l'appel VoIP.

Le tableau ci-dessous donne des exemples de comptes SIP.



6.2.3 Paramètres téléphoniques

Cette page permet de définir les paramètres téléphoniques de VoIP 1 et VoIP 2.



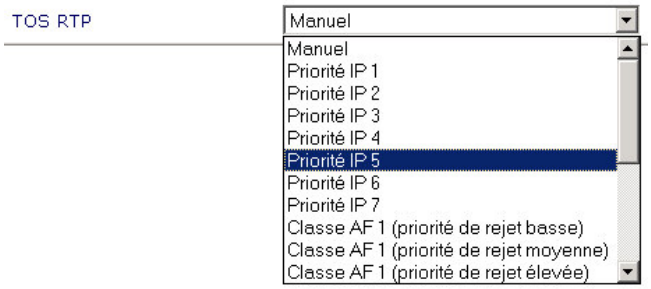
RTP

RTP symétrique – Cochez cette case pour éviter des anomalies de transmission de données au niveau du routeur local et du routeur distant du fait de la perte de paquets IP (par exemple, envoi de données de l'adresse IP publique du routeur distant à l'adresse IP privée du routeur local).

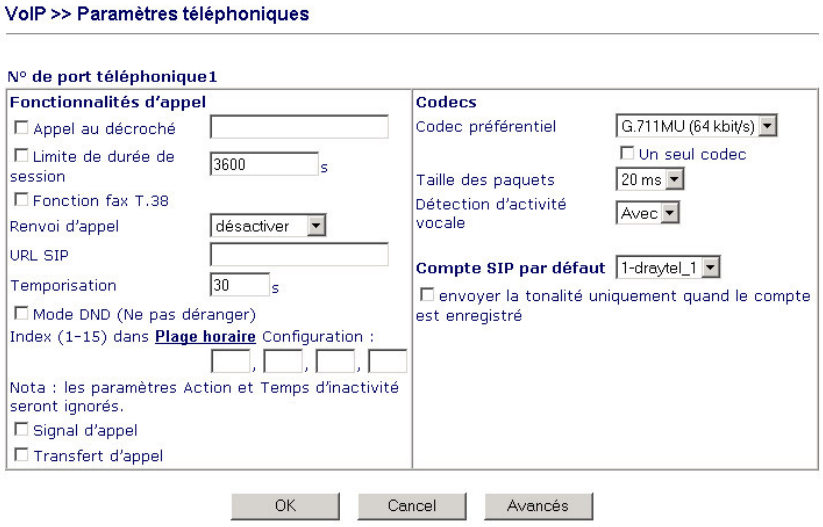
Port de début RTP dynamique – Port de début du flux RTP. La valeur par défaut est 10050.

Port de fin RTP dynamique – Port de fin du flux RTP. La valeur par défaut est 15000.

TOS RTP– Détermine le niveau de service VoIP. Utilisez la liste déroulante pour choisir l'un d'entre eux.



Cliquez sur **1** ou **2** dans la colonne Index pour accéder aux pages de configuration des paramètres téléphoniques.



Appel au décroché – Cochez la case pour activer l'appel au décroché. Tapez dans le champ l'URL SIP à appeler automatiquement lorsque vous décrochez le téléphone.

Limite de durée de session – Cochez la case pour activer pour activer la fonction. En l'absence d'activité pendant la période spécifiée dans ce champ, la communication est coupée automatiquement.

Fonction fax T.38 – Si l'extrémité distante a également la fonction FAX, vous pouvez cocher cette case pour activer cette fonction.

Renvoi d'appel

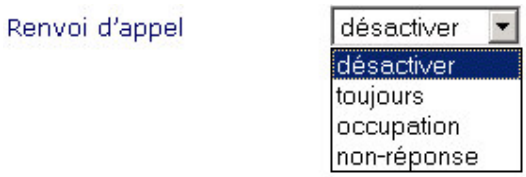
Il y a quatre options.

Désactiver : désactive la fonction de renvoi d'appel.

Toujours : tous les appels entrants sont renvoyés vers l'URL SIP.

Occupation : les appels entrants sont renvoyés vers l'URL SIP uniquement lorsque le système local est occupé.

Non-réponse : en l'absence de réponse, les appels entrants sont renvoyés vers l'URL SIP à l'expiration de la temporisation.



URL SIP – Tapez l'URL SIP (par exemple, aaa@draytel.org ou abc@iptel.org) vers laquelle les appels seront renvoyés.
Temporisation – Définissez la temporisation de renvoi d'appel. La valeur par défaut est 30 s.

Mode DND (ne pas déranger)

Permet de définir une période de repos téléphonique durant laquelle l'appelant entend la tonalité d'occupation. L'utilisateur local n'est pas sonné.

Plage horaire – Entrez des numéros de plage horaire pour activer le mode DND selon les plages horaires préconfigurées. Voir **Plages horaires**.

Signal d'appel

Cochez la case pour activer cette fonction. Un signal est émis pour prévenir l'utilisateur de l'arrivée d'un nouvel appel. Utilisez la fonction « R » (flash) pour prendre l'appel en attente.

Transfert d'appel

Cochez la case pour activer cette fonction. Utilisez la fonction « R » (flash) pour appeler un autre interlocuteur. Lorsque la communication est établie, raccrochez. Les deux autres interlocuteurs sont en communication.

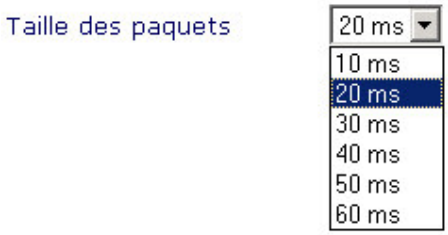
Codec préférentiel

Sélectionnez l'un des cinq codecs pour vos appels VoIP. Le codec utilisé pour chaque appel sera négocié avec l'homologue avant chaque session et peut donc ne pas être celui choisi par défaut. Le codec par défaut est G.729A/B ; il occupe peu de bande passante tout en maintenant une bonne qualité vocale.

Si votre vitesse montante ne dépasse pas 64 kbit/s, n'utilisez pas le codec G.711. Pour utiliser celui-ci, il vaut mieux avoir au moins 256 kbit/s dans le sens montant.

Un seul codec – Si la case est cochée, seul le codec sélectionné sera utilisé.

Taille des paquets - La valeur par défaut est 20 ms, ce qui signifie que le paquet de données contient 20 ms d'informations vocale.

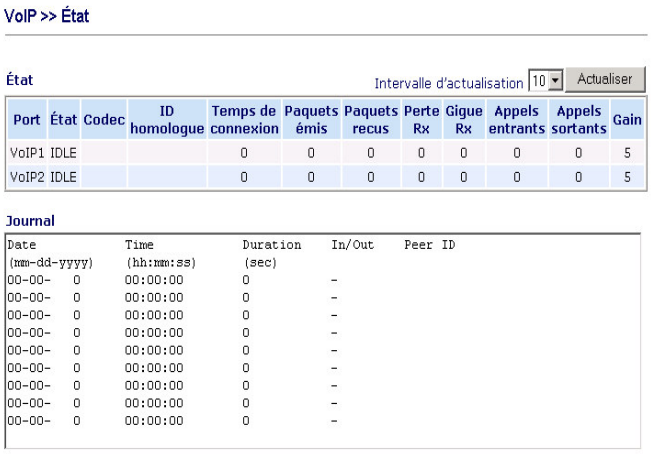


Détection d'activité vocale - Cette fonction détecte s'il y a une activité vocale des deux côtés. En l'absence d'activité vocale, le routeur fera en sorte d'affecter la bande passante à un autre usage. Cliquez sur Avec pour activer cette fonction ; cliquez sur Sans pour désactiver la fonction.

Compte SIP par défaut	Vous pouvez paramétrer six groupes de comptes SIP. Utilisez la liste déroulante pour choisir le nom de profil du compte par défaut.
Envoyer la tonalité uniquement quand le compte est enregistré	Cochez la case pour activer cette fonction.

6.2.4 État

La fonction État de l'appel téléphonique vous permet de visualiser des informations d'état relatives notamment au codec et à la connexion pour les ports VoIP 1 et VoIP 2 .



Intervalle d'actualisation Spécifiez l'intervalle d'actualisation. Les informations sont mises à jour immédiatement lorsque vous cliquez sur le bouton **Actualiser.**

Port VoIP 1 et VoIP 2

État Pour visualiser l'état de la connexion VoIP

IDLE - Indique que la fonction VoIP est active.

HANG_UP - Indique que la connexion n'est pas établie (tonalité d'occupation).

CONNECTING - Indique que l'utilisateur appelle.

WAIT_ANS - Indique qu'une connexion est établie et qu'une réponse de l'utilisateur distant est attendue.

ALERTING - Indique qu'un appel arrive.

ACTIVE - Indique que la connexion VoIP est activée.

Codec Indique que le codec vocal utilisé par le canal actuel.

ID homologue L'ID homologue entrant ou sortant (le format peut être IP ou Domaine).

Temps de connexion Le temps est exprimé en secondes.

Paquets émis Nombre total de paquets téléphoniques émis pendant la communication.

Paquets reçus Nombre total de paquets reçus pendant la communication téléphonique.

Perte Rx Nombre total de paquet perdus pendant la communication.

Gigue Rx Gigue des paquets téléphoniques reçus.

Appels entrants Durée cumulée des appels entrants.

Appels Sortants Durée cumulée des appels sortants.

Gain Volume de l'appel actuel.

Journal Journal des communications VoIP.

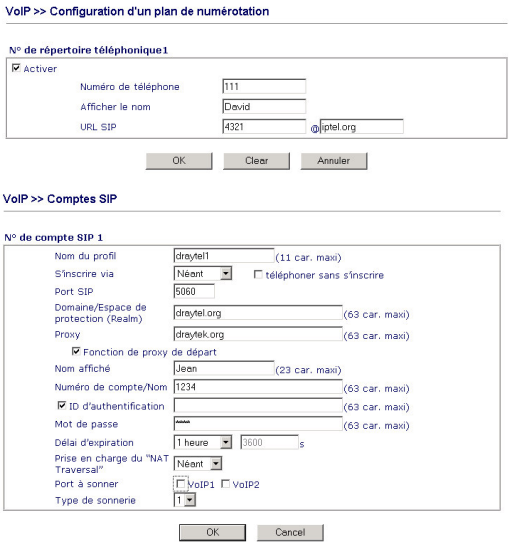
6.3 Scénario d'appel pour la fonction VoIP

6.3.1 Appel via le serveur SIP

Exemple 1 : Jean et David ont une adresse IP provenant de fournisseurs de service **différents**.

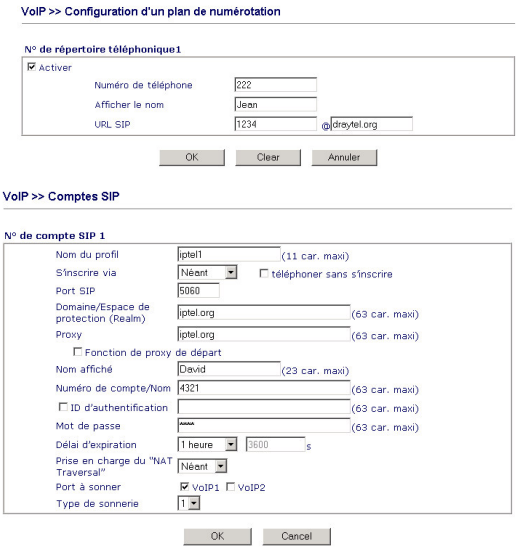
URL SIP de Jean : 1234@draytel.org, URL SIP de David : 4321@iptel.org

Paramètres de Jean
DialPlan index 1
Numéro de téléphone : 1111
Nom affiché : David
URL SIP: 4321@iptel.org
Paramètres des comptes SIP ---
Nom du profil : draytel1
S'inscrire via : Auto
Port SIP : 5060 (valeur par défaut)
Domaine/Espace de protection (Realm) : draytel.org
Proxy: draytel.org
Fonction de proxy de départ : non coché
Nom affiché : Jean
Numéro/nom de compte : 1234
ID authentification : non coché Mot de passe : ****
Délai d'expiration : (utiliser la valeur par défaut)
CODEC/RTP/DTMF ---
(Utiliser la valeur par défaut)



Jean appelle David ---
Il décroche le téléphone et compose **1111#**.
(Numéro abrégé de David)

Paramètres de David
DialPlan index 1
Numéro de téléphone :2222
Nom affiché : Jean
URL SIP :1234@draytel.org
Paramètres des comptes SIP ---
Nom du profil : iptel 1
S'inscrire via : Auto
Port SIP : 5060(valeur par défaut)
Domaine/Espace de protection (Realm) : iptel.org
Proxy : iptel.org
Fonction de proxy de départ : non coché
Nom affiché : David
Nom de compte : 4321
ID authentification : non coché Mot de passe : ****
Délai d'expiration : (utiliser la valeur par défaut)
CODEC/RTP/DTMF ---
(Utiliser la valeur par défaut)



David appelle Jean ---
Il décroche le téléphone et compose 2222#
(Numéro abrégé de Jean)

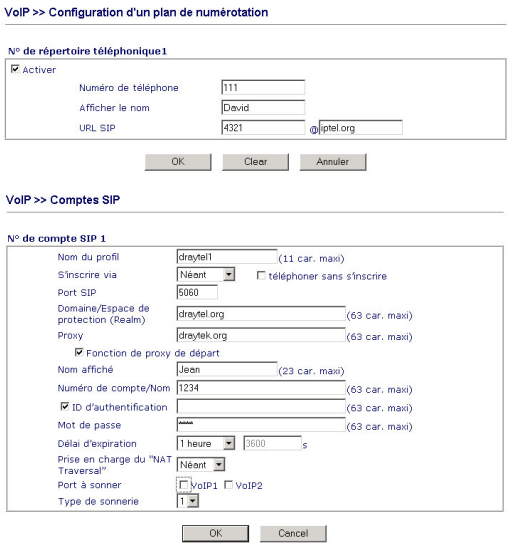
Exemple 2 : Jean et David ont une adresse IP provenant **du même** fournisseur de service.

URL SIP de Jean : 1234@draytel.org, URL SIP de David : 4321@draytel.org

Paramètres de Jean
DialPlan index 1
Numéro de téléphone : 1111
Nom affiché : David
URL SIP: 4321@iptel.org
Paramètres des comptes SIP ---
Nom du profil : draytel1
S'inscrire via : Auto
Port SIP : 5060 (valeur par défaut)
Domaine/Espace de protection (Realm) : draytel.org
Proxy : draytel.org

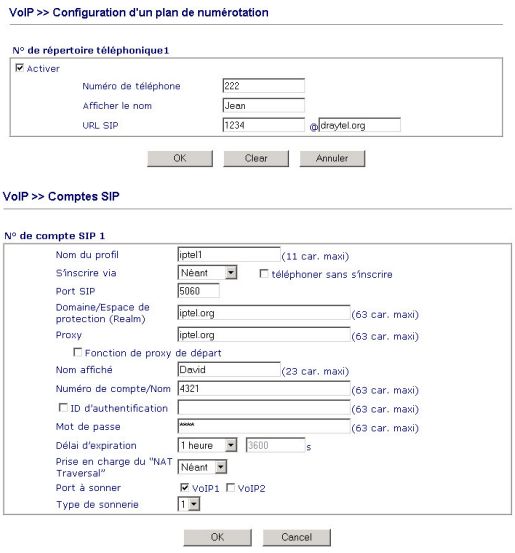
Fonction de proxy de départ : non coché

Nom affiché : Jean
Numéro/nom de compte : 1234
ID authentification : non coché Mot de passe : ****
Délai d'expiration : (utiliser la valeur par défaut)
CODEC/RTP/DTMF ---
(Utiliser la valeur par défaut)



Jean appelle David
Il décroche le téléphone et compose **1111#**. (Numéro abrégé de David) Ou,
Il décroche le téléphone et compose **4321#**. (Nom de compte de David)

Paramètres de David
DialPlan index 1
Numéro de téléphone :2222
Nom affiché : Jean
URL SIP :1234@draytel.org
Paramètres des comptes SIP ---
Nom du profil : iptel 1
S'inscrire via : Auto
Port SIP : 5060(valeur par défaut)
Domaine/Espace de protection (Realm) : draytel.org
Proxy : iptel.org
Fonction de proxy de départ : non coché
Nom affiché : David
Nom de compte : 4321
ID authentification : non coché Mot de passe : ****
Délai d'expiration : (utiliser la valeur par défaut)
CODEC/RTP/DTMF---
(Utiliser la valeur par défaut)



David appelle Jean
Il décroche le téléphone et compose 2222# (Numéro abrégé de Jean) Ou, Il décroche le téléphone et compose 1234# (Nom de compte de Jean)

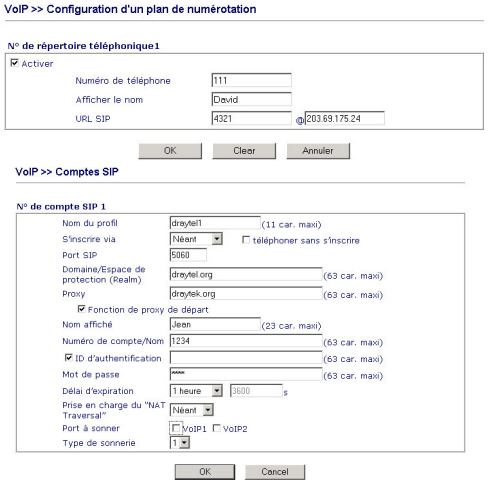
6.3.2 Communication d'homologue à homologue (P2P)

Exemple 3 : Jean et David ont chacun un routeur Vigor. Ils peuvent communiquer entre eux sans passer par un serveur registre SIP. Ils se communiquent au préalable leurs adresses IP respectives et attribuent un nom de compte au port qui sert à appeler.

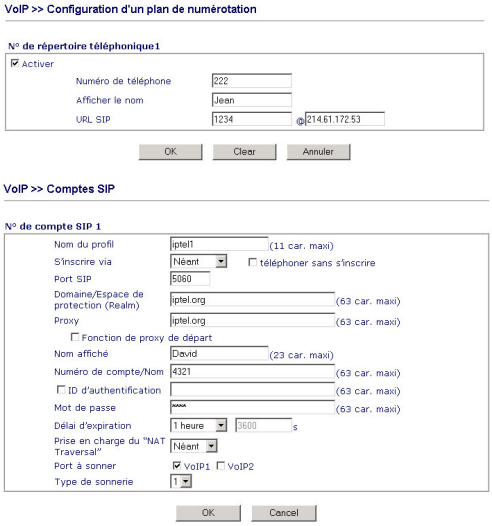
URL SIP de Jean : 1234@214.61.172.53 URL SIP de David : 4321@ 203.69.175.24

Paramètres de Jean
DialPlan index 1
Numéro de téléphone : 1111
Nom affiché : David
URL SIP: 4321@ 203.69.175.24
Paramètres des comptes SIP ---
Nom du profil : David
S'inscrire via : Néant
Port SIP : 5060(valeur par défaut)
Domaine/Espace de protection (Realm) : (vide)
Proxy: (vide)
Fonction de proxy de départ : non coché
Nom affiché : Jean
Nom de compte : 1234
ID authentification : non coché
Mot de passe : (vide)
Délai d'expiration : (utiliser la valeur par défaut)
CODEC/RTP/DTMF---
(Utiliser la valeur par défaut)

Paramètres de David
DialPlan index 1
Numéro de téléphone :2222
Nom affiché : Jean
URL SIP: 1234@214.61.172.53
Paramètres des comptes SIP ---
Nom du profil : Jean
S'inscrire via : Néant
Port SIP : 5060(valeur par défaut)
Domaine/Espace de protection (Realm) : (vide)
Proxy: (vide)
Fonction de proxy de départ : non coché
Nom affiché : David
Nom de compte : 4321
ID authentification : non coché
Mot de passe : (vide)
Délai d'expiration : (utiliser la valeur par défaut)
CODEC/RTP/DTMF---
(Utiliser la valeur par défaut)



Jean appelle David
Il décroche le téléphone et compose **1111#** (Numéro abrégé de David)



David appelle Jean
Il décroche le téléphone et compose 2222# (Numéro abrégé de Jean)

Chapitre 7
Paramétrage du pare-feu

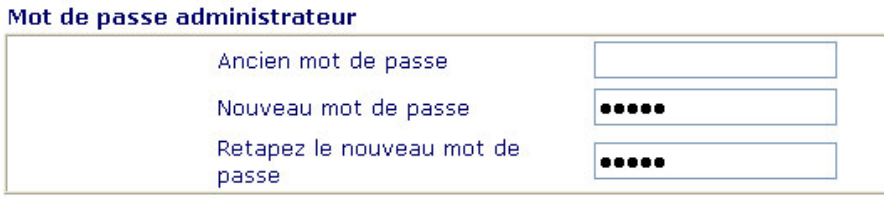
7.1 Introduction

À l'heure où les utilisateurs d'accès à haut débit demandent plus de bande passante pour le multimédia, les applications interactives ou le téléenseignement, la sécurité devient la priorité des priorités. Le pare-feu du routeur Vigor contribue à protéger votre réseau local contre les attaques extérieures. Il permet également de restreindre l'accès des utilisateurs locaux à l'internet. En outre, il permet d'identifier des paquets spécifiques à la réception desquels le routeur va établir une connexion de départ.

Avant de commencer

Avant tout, nous vous recommandons vivement de définir un nom d'utilisateur et un mot de passe lors de l'installation de votre routeur. En définissant un nom d'utilisateur et un mot de passe administrateur, vous empêcherez l'accès non autorisé aux menus de configuration du routeur à partir de votre routeur.

Si vous n'avez pas défini de mot de passe lors de l'installation, passez en mode **Maintenance du système**.



Fonctionnalités de pare-feu

Les utilisateurs en réseau sont protégés par les fonctions de pare-feu suivantes :

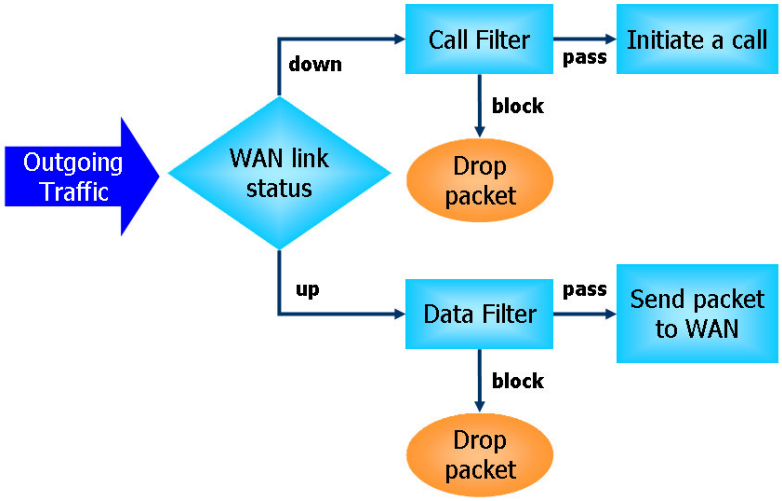
- Filtre de paquets configurable par l'utilisateur (filtre d'appel/filtre de données).
- Inspection des paquets en fonction de l'état de la connexion (filtrage adaptatif) : refus des données entrantes non sollicitées
- Protection anti-DoS/DdoS.
- Filtre de contenu d'URL.

Filtres IP

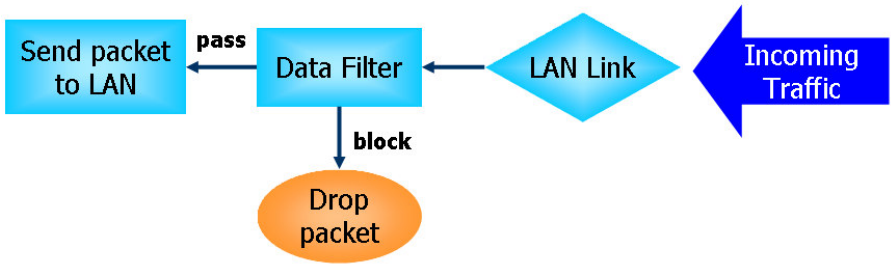
Selon qu'une connexion internet est active ou non ou, en d'autres termes, selon que « la connexion WAN est établie ou non », l'architecture des filtres IP met en œuvre deux types de filtres : le **filtre d'appel** et le **filtre de données**.

- En l'absence de connexion internet active, le **filtre d'appel** est appliqué à tout le trafic, lequel, en l'occurrence, est du trafic de départ. Il vérifie chaque paquet selon les règles de filtrage et laisse passer le paquet s'il est licite. Le routeur déclenche alors un **appel** pour établir la connexion internet et transmettre le paquet.
- Si une connexion internet est active, le **filtre de données** est appliqué au trafic d'arrivée et de départ. Il vérifie les paquets selon les règles de filtrage et les transmet au routeur s'ils sont licites.

Le processus de filtrage du trafic entrant et du trafic sortant est représenté schématiquement ci-après.



down	*inactif*
Call Filter	*Filtre d'appel*
pass	*laisse passer*
Initiale a call	*Déclenchement d'un appel*
block	*bloque*
Outgoing Traffic	*Trafic sortant*
WAN link status	*État de la connexion WAN*
Drop packet	*Rejet du paquet*
up	*actif*
Data Filter	*Filtre de données*
pass	*laisse passer*
block	*bloque*
Send packet to WAN	*Envoi du paquet sur le WAN*
Drop packet	*Rejet du paquet*



Send packet to WAN	*Envoi du paquet sur le WAN*
pass	*laisse passer*
Data Filter	*Filtre de données*
block	*bloque*
Drop packet	*Rejet du paquet*
LAN Link	*Connexion LAN*
Incoming Traffic	*Trafic entrant*

Filtrage adaptatif (SPI)

L'inspection des paquets en fonction de l'état de la connexion ou filtrage adaptatif est une architecture de pare-feu qui fonctionne au niveau de la couche réseau. À la différence du filtrage statique des paquets qui examine un paquet sur la base des informations de son en-tête, le

filtrage adaptatif crée une machine à états qui contrôle la connexion via toutes les interfaces du pare-feu. Le pare-feu adaptatif du routeur Vigor ne se contente pas d'examiner l'en-tête ; il contrôle également l'état de la connexion.

Blocage des applications de messagerie instantanée (IM) et de partage de fichiers (P2P)

Avec la popularité croissante des applications de messagerie instantanée, les communications peuvent devenir beaucoup plus faciles. Néanmoins, si certaines industries peuvent mettre à profit cet outil pour communiquer avec leurs clients, d'autres peuvent adopter une attitude plus réservée afin de réduire son utilisation abusive par les employés pendant les heures de travail ou pour éviter les failles de sécurité inconnues. Il en va de même pour les applications « peer to peer » car les partages de fichiers, s'ils peuvent être commodes, peuvent aussi poser des problèmes de sécurité. C'est pourquoi le routeur Vigor comporte une fonction de blocage d'IM et de P2P.

Protection contre les attaques de type « déni de service » (DoS)

La **protection anti-DoS** vous aide à détecter les attaques de type « déni de service » (DoS) et à en atténuer les effets. Les attaques sont généralement de deux types : les attaques de type inondation et les attaques qui exploitent des failles de sécurité. Les attaques par inondation visent à saturer votre système, tandis que les attaques de vulnérabilité tentent de paralyser le système en exploitant les failles du protocole ou du système d'exploitation.

La fonction de protection **anti-DoS** permet au routeur Vigor de confronter chaque paquet entrant avec la base de données de signatures d'attaque. Tout paquet susceptible de se dupliquer pour paralyser la machine hôte au sein du LAN sécurisé est bloqué et un message SysLog est envoyé, si toutefois vous avez configuré le serveur SysLog.

Le routeur Vigor surveille également le trafic. Tout trafic anormal violant un paramètre préétabli, comme le nombre de seuils, est identifié comme une attaque et le routeur Vigor active son mécanisme de protection en temps réel.

La fonction de protection anti-DoS/DDoS peut détecter et contrer les attaques suivantes :

1. attaque par inondation SYN
2. attaque par inondation UDP
3. attaque par inondation ICMP
4. scrutation de flag TCP
5. « trace route »
6. options IP
7. protocole inconnu
8. attaque « land »
9. attaque « smurf » (attaque par surcharge
10. fragments SYN
11. fragments ICMP
12. attaque « tear drop »
13. attaque « fraggle »
14. attaque « ping of death »
15. scrutation de port TCP/UDP

Filtrage de contenu

Pour fournir aux utilisateurs un cyberespace approprié, le routeur Vigor est doté d'un outil de **filtrage de contenu d'URL** qui non seulement limite le trafic illégal en provenance ou à destination de certains sites web mais également interdit d'autres fonctionnalités web susceptibles de comporter du code malveillant.

Lorsqu'un utilisateur tape des mots-clés douteux ou clique sur une adresse universelle (URL) comportant des mots-clés douteux, la fonction de blocage par mots-clés refuse la demande HTTP d'accès à la page web concernée et peut donc limiter l'accès de l'utilisateur au site. Le **filtrage de contenu d'URL** peut être assimilé au comportement du commerçant qui refuse de vendre des magazines pour adultes à des adolescents. Au bureau, le **filtrage de contenu d'URL** peut également être utilisé pour augmenter le rendement des employés en les empêchant d'accéder à des ressources internet qui n'ont pas de rapport avec leur travail. Comment le filtrage de contenu d'URL peut-il être plus efficace qu'un pare-feu traditionnel ? Parce qu'il vérifie les chaînes d'URL ou certaines données HTTP cachées dans la charge utile des paquets TCP, tandis que le pare-feu traditionnel se contente d'analyser les champs des en-têtes TCP/IP.

D'autre part, le routeur Vigor peut empêcher un utilisateur de télécharger accidentellement du code malveillant à partir de pages web. Il est très courant que du code malveillant se cache dans les objets exécutables, comme les contrôles ActiveX, les applets Java, les fichiers comprimés et autres fichiers exécutables. Le téléchargement de ces types de fichiers à partir de sites web peut faire courir des risques à votre système. Par exemple, un contrôle ActiveX est généralement utilisé pour fournir une fonction web interactive. Si du code malveillant s'y cache, il peut se retrouver dans le système de l'utilisateur.

Filtrage web

Nous savons tous que le contenu de l'internet, comme celui d'autres types de média, peut quelquefois être inconvenant. En tant que parent ou employeur responsable, vous devez protéger ceux dont vous avez la charge contre les dangers éventuels. Avec le service de filtrage web du routeur Vigor, vous pouvez protéger votre entreprise contre les menaces courantes, notamment contre les menaces pour la productivité, la responsabilité civile, le réseau et la sécurité. En tant que parent, vous pouvez empêcher vos enfants d'accéder à des sites pour adultes ou à des sites de messagerie en temps réel (« cybersalons » ou « chat rooms »).

Une fois que vous avez activé le service de filtrage web du routeur Vigor et choisi les catégories de sites que vous voulez rendre inaccessibles, chaque adresse URL demandée (par exemple, www.bbc.co.uk) sera vérifiée par rapport à notre base de données sous le contrôle de SurfControl. La base de données, qui couvre plus de 70 langues et 200 pays, contient plus de 1 milliards de pages web classées en 40 catégories explicites. Cette base de données est mise à jour quotidiennement par une équipe mondiale de chercheurs internet. Le serveur examine l'URL et informe votre routeur de la catégorie à laquelle elle appartient. Votre routeur Vigor décide alors d'autoriser ou non l'accès à ce site selon les catégories que vous avez sélectionnées. À noter que cette opération ne ralentit en rien votre navigation sur l'internet car chacun des multiples serveurs de base de données à équilibre de charge peut traiter des millions de requêtes.

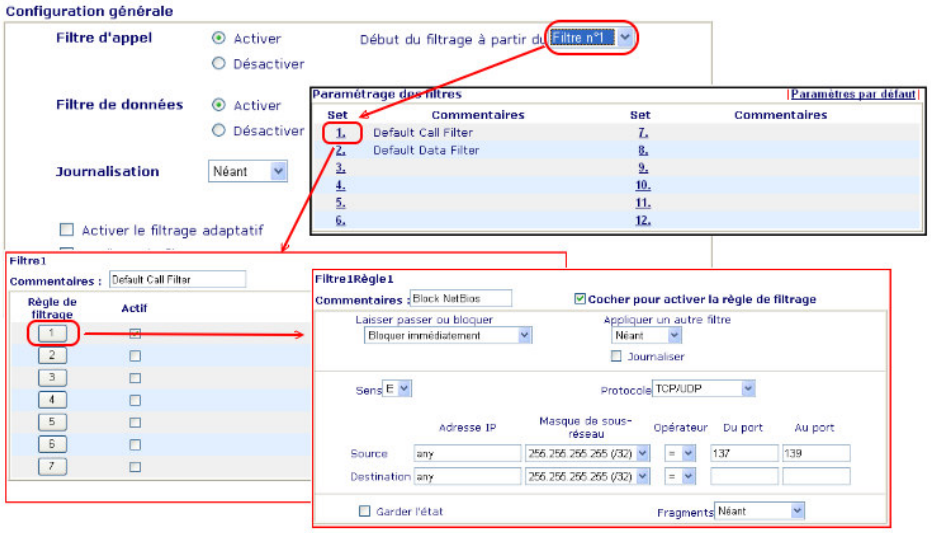
7.2 Paramétrage

Cliquez sur **Paramétrage du pare-feu** pour ouvrir la page de paramétrage.

Configuration générale	Paramètres généraux des filtres IP et options communes.
Paramétrage du filtre	Vous avez la possibilité de configurer 12 filtres IP.
Blocage d'IM	Fonction de blocage des applications de messagerie instantanée courantes. Il faut spécifier une plage horaire.
Blocage de P2P	Fonction de blocage des applications de partage de fichiers « peer to peer » courantes. Il faut spécifier une plage horaire.
Protection anti-DoS	Paramétrage de la protection anti-DoS afin de détecter les attaques de type DoS et d'en atténuer les effets.
Filtre de contenu d'URL	Paramétrage d'un filtre pour bloquer les URL indésirables afin de protéger les enfants à la maison ou d'empêcher les abus des employés. Blocage de fonctions web susceptibles de transporter du code malveillant.
Filtre web CPA	Paramétrage d'un filtre web pour interdire l'accès à des sites inconvenants.

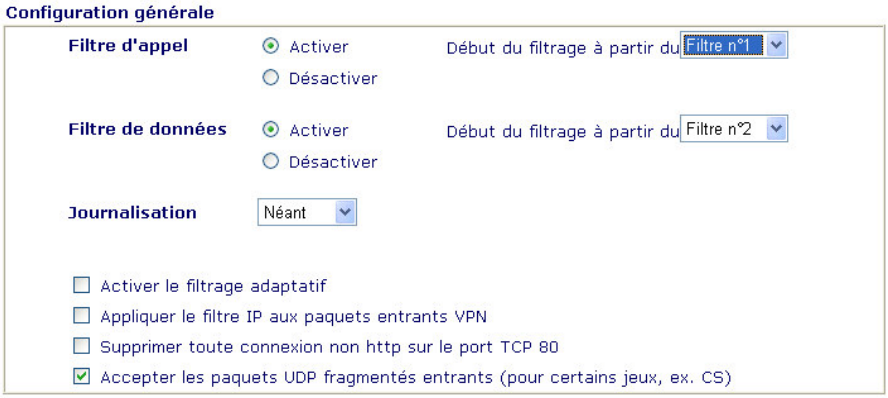
Les paragraphes qui suivent décrivent la **configuration générale** et le **paramétrage des filtres**.

Comme indiqué plus haut, il existe deux types de filtres IP : le filtre d'appel et le filtre de données. Vous pouvez configurer 12 filtres d'appel ou de données dans **Paramétrage des filtres** et les enchaîner. Pour chaque filtre, vous pouvez définir 7 règles de filtrage. Puis, dans **Configuration générale**, vous pouvez spécifier un filtre d'appel de début et un filtre de données de début.



7.2.1 Configuration générale

Vous pouvez activer ou désactiver le **filtre d'appel** ou le **filtre de données**. Dans certaines circonstances, vous pouvez enchaîner les filtres. Ici, vous activez uniquement le **filtre de début**. Vous pouvez également configurer la journalisation, activer le filtrage adaptatif, appliquer le filtre IP aux paquets entrants VPN, supprimer les connexions non http sur le port TCP 80 et accepter les paquets UDP fragmentés entrants (pour certains jeux, comme CS).



Certains jeux en ligne (par exemple, Half Life) utilisent un grand nombre de paquets UDP fragmentés pour le transfert des données de jeu. Instinctivement, en tant que pare-feu sécurisé, le routeur Vigor rejette ces paquets fragmentés pour éviter les attaques, sauf si vous cochez la case « Accepter les paquets UDP fragmentés entrants ». En cochant cette case, vous pouvez participer à ce type de jeu en ligne. Si la sécurité est votre souci principal, ne cochez pas la case « Accepter les paquets UDP fragmentés entrants ».

Filtre d'appel

Cochez **Activer** pour activer la fonction Filtre d'appel et spécifiez un filtre de début.

Filtre de données

Cochez **Activer** pour activer la fonction Filtre de données et spécifiez un filtre de début.

Journalisation

Vous pouvez définir ici les conditions de journalisation.

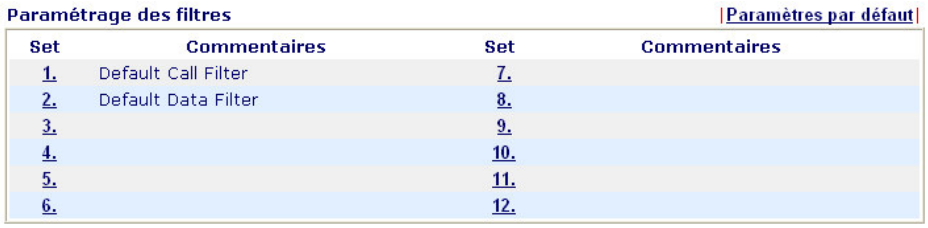
Néant	La fonction de journalisation n'est pas activée.
Bloquer	Les paquets bloqués seront journalisés.
Laisser passer	Les paquets passés seront journalisés.
Pas de correspondance	La fonction de journalisation enregistrera tous les paquets qui ne correspondent pas aux règles de filtrage.

Le fichier de journalisation sera affiché sur le terminal Telnet lorsque vous taperez la commande « log –f ».

7.2.2 Paramétrage des filtres

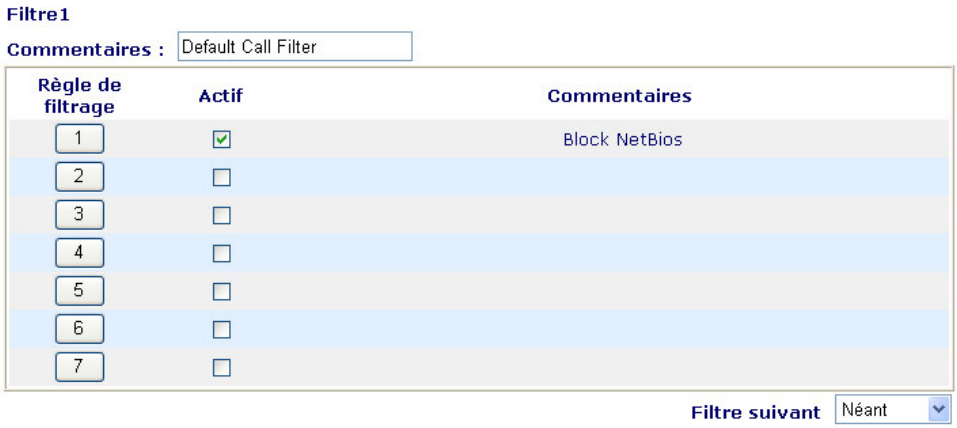
Récapitulatif des filtres

Lorsque vous cliquez sur Paramétrage des filtres, vous obtenez d'abord le tableau récapitulatif des filtres avec la liste de tous les filtres, dont deux filtres par défaut. Cliquez sur le numéro de filtre pour le modifier.



Édition/modification des filtres

Chaque filtre comporte jusqu'à 7 règles. Cliquez sur le numéro de règle pour la modifier. Cliquez sur Active pour activer la règle.



Règles de filtrage

Cliquez sur l'un des boutons **1 à 7** pour éditer/modifier la règle de filtrage.

Actif

Active ou désactive la règle de filtrage.

Commentaires

Tapez des commentaires ou une description du filtre (longueur maximale : 23 caractères).

Filtre suivant

Spécifie le filtre qui doit suivre le filtre actuel. Les filtres ne peuvent pas être appliqués en boucle.

Éditer/modifier les règles de filtrage

Cliquez sur le numéro de règle de filtrage pour afficher la page de configuration des règles de filtrage.

Commentaires

Tapez des commentaires ou une description de la règle de filtrage (longueur maximale : 14 caractères).

Cocher pour activer la règle de filtrage

Active la règle de filtrage.

Laisser passer ou bloquer

Spécifiez l'action que doit avoir la règle sur les paquets.

Bloquer immédiatement	Les paquets correspondants à la règle sont rejetés immédiatement.
Laisser passer immédiatement	Les paquets correspondants à la règle sont passés immédiatement.
Bloquer si plus de corresp.	Un paquet qui correspond à la règle mais qui ne correspond pas aux règles suivantes est rejeté.
Laisser passer si plus de corresp.	Un paquet qui correspond à la règle mais qui ne correspond pas aux règles suivantes est passé.

Appliquer un autre filtre

Si le paquet correspond à la règle de filtrage, la règle de filtrage suivante fait passer au filtre spécifié.

Journal

Cochez cette case pour activer la fonction de journalisation. Pour visualiser les journaux, utilisez la commande Telnet **log-f**.

Sens (filtre de données seulement)

Définit la direction des paquets.

Pour le filtre d'appel, ce paramètre n'est pas disponible puisque le filtre d'appel est appliqué au trafic sortant.

Protocole

Spécifie le ou les protocoles auxquels s'applique cette règle de filtrage.

Adresse IP

Spécifiez une adresse IP d'origine et une adresse IP de destination auxquelles s'applique cette règle de filtrage. Le symbole **!** devant une adresse IP particulière empêche l'application de la règle à cette adresse IP. Il est équivalent à l'opérateur logique NON. Pour appliquer la règle à toutes les adresses IP, tapez « n'importe laquelle » ou laissez le champ vide.

Masque de sous-réseau

Spécifiez le masque de sous-réseau correspondant aux adresses IP.

Opérateur, Du Port et Au Port

La colonne opérateur précise les ports concernés. Si le champ **Du port** est vide, les colonnes **Du port** et **Au port** sont ignorées. La règle de filtrage s'applique à tous les ports.

=	Si le champ Au port est vide, la règle de filtrage s'applique au seul port dont le numéro figure dans le champ Du port. Sinon, la règle de filtrage s'applique à la plage de ports définie par les champs Du port et Au port.
!=	Si le champ Au port est vide, la règle de filtrage s'applique à tous les ports à l'exception de celui dont le numéro figure dans le champ Du port. Sinon, elle s'applique à tous les ports à l'exception de la plage de ports définie par les champs Du port et Au port.
>	La règle de filtrage s'applique au port dont le numéro figure dans le champ Du port et à tous les ports supérieurs.
<	La règle de filtrage s'applique au port dont le numéro figure dans le champ Du port et à tous les ports inférieurs.

Garder l'état (filtre de données seulement)

Cette fonction utilise les paramètres **Sens, Protocole, Adresse IP, Masque de sous-réseau, Opérateur, Port de début et Port de fin**.

La fonction Garder l'état est du même ordre que la fonction de filtrage adaptatif. Elle contrôle les paquets et accepte ceux qui ont des caractéristiques appropriées l'identifiant comme licite selon le protocole. Elle rejette les données entrantes non sollicitées. Vous pouvez choisir les protocoles suivants : **any (n'importe lequel), TCP, UDP, TCP/UDP, ICMP** et **IGMP**.

Fragments (filtre de données seulement)

Spécifiez une action sur les paquets fragmentés.

Néant	Aucune action sur les paquets fragmentés.
Non fragmenté	Applique la règle aux paquets non fragmentés.
Fragmenté	Applique la règle aux paquets fragmentés
Trop court	Applique la règle uniquement aux paquets qui sont trop courts pour avoir un en-tête complet.

Exemple

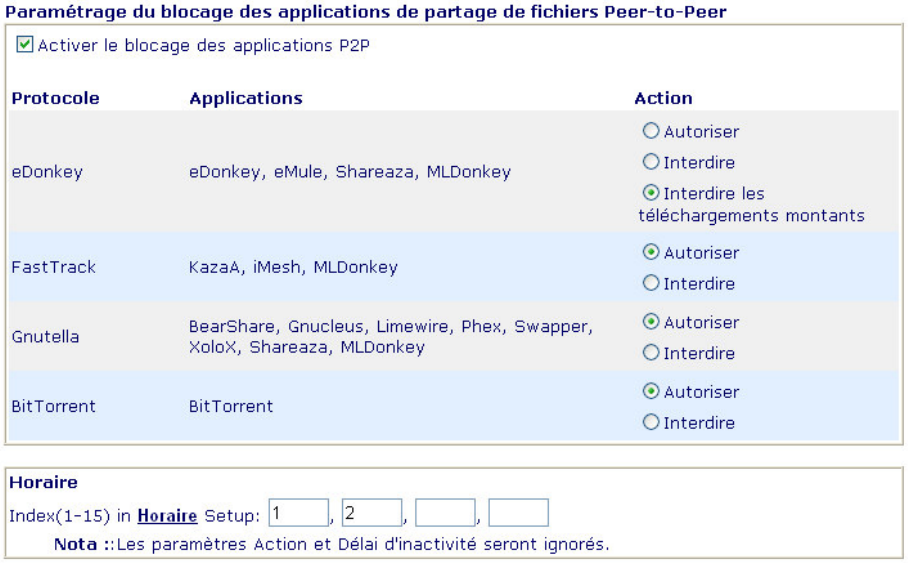
L'exemple qui suit montre comment empêcher tout accès d'un utilisateur aux services WWW. L'adresse IP de l'utilisateur est 192.168.1.10. Dans le filtre 2 – Filtre de données, vous pouvez créer une règle telle que celle ci-dessous. Le port 80 correspond au port http.

7.2.3 Blocage des applications de messagerie instantanée (IM)

Cliquez sur **Blocage d'IM** pour afficher la fenêtre de configuration. Celle-ci contient une liste des applications de messagerie instantanée courantes. Cochez la case correspondant à celle(s) que vous voulez bloquer. Pour bloquer les applications de messagerie instantanée sélectionnées pendant des périodes spécifiques, tapez le numéro de plage horaires défini dans **Applications>>Plages horaires**.

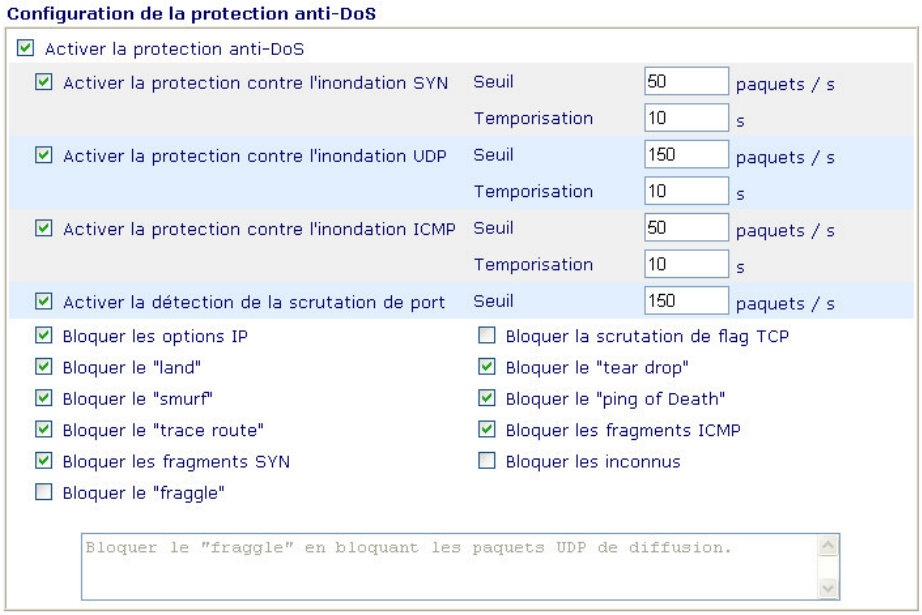
7.2.4 Blocage des applications de partage de fichiers entre homologues (P2P)

Cliquez sur **Blocage de P2P** pour afficher la fenêtre de paramétrage. Cette fenêtre contient une liste des applications P2P courantes. Sélectionnez celle(s) à bloquer. Pour bloquer les applications P2P sélectionnées pendant des périodes déterminées, tapez le numéro de plage horaire défini dans **Applications>>Plages horaires**.



7.2.5 Protection anti-DoS (déni de service)

Il y a quinze sortes de protection au total. Par défaut, la fonctionnalité de protection anti-DoS est désactivée.



Activer la protection anti-DoS

Cliquez sur la case à cocher pour activer la protection anti-DoS.

Activer la protection contre l'inondation SYN

Cochez la case pour activer la **protection contre l'inondation SYN**.

Si le nombre de paquets SYN TCP provenant de l'internet dépasse le seuil défini, le routeur Vigor rejette les paquets SYN TCP qui suivent pendant le temps défini par le paramètre **Temporisation**. Le but est d'empêcher la saturation du routeur Vigor par les paquets SYN TCP. Par défaut, le seuil et la temporisation ont respectivement pour valeur 50 paquets par seconde et 10 secondes.

Activer la protection contre l'inondation UDP

Cochez la case pour activer la **protection contre l'inondation UDP**. Si le nombre de paquets UDP provenant de l'internet dépasse le seuil défini, le routeur Vigor rejette les paquets UDP qui suivent pendant le temps défini par le paramètre **Temporisation**. Le but est d'empêcher la saturation du routeur Vigor par les paquets UDP. Par défaut, le seuil et la temporisation ont respectivement pour valeur 50 paquets par seconde et 10 secondes.

Activer la protection contre l'inondation ICMP

Cochez la case pour activer la fonction de **protection contre l'inondation ICMP**. Lorsque le nombre de paquets ICMP provenant de l'internet dépasse le seuil défini, le routeur rejette toutes les requêtes d'écho ICMP qui suivent pendant le temps défini par le paramètre **Temporisation**. Le seuil et la temporisation ont respectivement pour valeur par défaut 50 paquets par seconde et 10 secondes.

Activer la détection de la scrutation de port

Une attaque par scrutation de port consiste à envoyer un grand nombre de paquets à de nombreux ports pour tenter de déterminer à quels services un port répond. Pour activer la fonction de **détection de scrutation de port**, cochez la case. S'il détecte une telle tentative (dépassement du seuil), le routeur Vigor émet un message d'avertissement. Le seuil par défaut est de 150 paquets par seconde.

Bloquer les options IP

Cochez la case pour activer la fonction de blocage des options IP. Le routeur Vigor ignorera tous les paquets IP dans l'en-tête desquels figurent des options IP. Les options IP constituent une vulnérabilité du LAN car elles véhiculent des informations importantes, telles que des paramètres de sécurité, de compartimentage, TCC (groupe fermé d'utilisateurs), une série d'adresses internet, des messages de routage, etc. Un attaquant potentiel peut obtenir des renseignements sur vos réseaux privés.

Bloquer le « land »

Cochez la case pour activer la protection contre les attaques de type

« land ». L'attaque de type « land » combine l'attaque SYN avec l'usurpation d'adresse IP. Une attaque de type « land » consiste à envoyer des paquets SYN usurpés dont les adresses d'origine et de destination ainsi que les numéros de port sont identiques à ceux de la victime.

Bloquer le « smurf »

Cochez la case pour activer la fonction de blocage de « smurf ». Le routeur Vigor rejettera toute requête d'écho ICMP.

Bloquer le « trace route »

Cochez la case pour que le routeur Vigor ne laisse pas passer les paquets « trace route ».

Bloquer les fragments SYN

Cochez la case pour activer la fonction de blocage des fragments SYN. Le routeur Vigor rejettera tous les paquets dont l'indicateur SYN et le bit MF (more fragments) sont à 1.

Bloquer le « fraggle »

Cochez la case pour activer la fonction de blocage de « fraggle ». Tous les paquets UDP de diffusion provenant de l'internet sont bloqués.

Il se peut que la protection anti-DoS/DDoS bloque certains paquets licites. Par exemple, lorsque vous activez la protection contre le « fraggle », tous les paquets UDP de diffusion provenant de l'internet sont bloqués. Par conséquent, il se peut que les paquets RIP soient bloqués.

Bloquer la scrutation de flag TCP

Cliquez sur la case à cocher pour activer la fonction de blocage de la scrutation de flag TCP. Tout paquet TCP présentant une anomalie au niveau des indicateurs (« flags » est rejeté. Les anomalies sont, entre autres : **absence d'indicateurs, *FIN sans ACK***, ***SYN FIN ensemble***, ***Xmas (indicateurs FIN URG et PSH à 1)*** et ***full Xmas (tous les indicateurs à 1)***.

Bloquer le « tear drop »

Cliquez sur la case à cocher pour activer la fonction de blocage de « tear drop ». De nombreuses machines peuvent se bloquer à la réception de datagrammes (paquets) ICMP qui dépassent la longueur maximale. Pour éviter ce type d'attaque, le routeur Vigor est

capable de rejeter les paquets ICMP fragmentés dont la longueur dépasse 1024 octets.

Bloquer le « ping of death »

Cliquez sur la case à cocher pour activer la fonction de blocage du « ping of death ». Dans ce type d'attaque, l'attaquant envoie des paquets qui se chevauchent aux machines hôtes cibles, lesquelles se bloquent lorsqu'elles reconstituent les paquets. Les paquets de ce type sont bloqués par le routeur Vigor.

Bloquer les fragments ICMP

Cliquez sur la case à cocher pour activer la fonction de blocage des fragments ICMP. Les paquets ICMP dont le bit MF (« more fragments ») est à 1 sont rejeté.

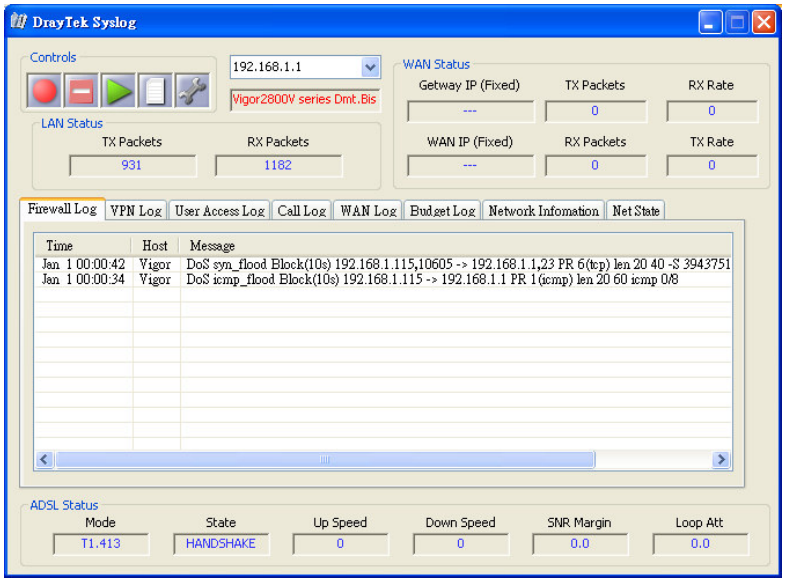
Bloquer les protocoles inconnus

Cliquez sur la case à cocher pour activer la fonction de blocage des protocoles inconnus. Dans l'en-tête de chaque paquet IP, il y a un champ qui indique le type de protocole de couche supérieure. Toutefois, les types de protocole supérieurs à 100 sont réservés et non définis pour l'instant. Par conséquent, le routeur doit pouvoir détecter et rejeter ce genre de paquet.

Messages d'avertissement

La fonction SysLog permet à l'utilisateur de visualiser les messages du routeur Vigor. L'utilisateur, en tant que serveur SysLog, reçoit les rapports émis par le routeur Vigor qui est un client SysLog. (Reportez-vous au Chapitre 12 Maintenance du système pour plus de détails).

Tous les messages d'avertissement liés à la **protection anti-DoS** sont envoyés à l'utilisateur qui peut les visualiser à l'aide du démon SysLog. Ces messages ont comme préfixe le mot-clé « DoS », suivi d'un nom qui indique le type d'attaque détecté.



7.2.6 Filtre de contenu d'URL

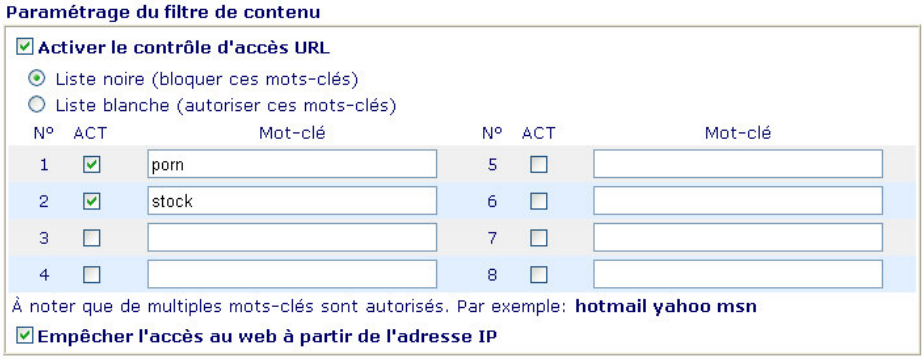
La fonction de **filtrage de contenu d'URL** du routeur Vigor inspecte chaque chaîne d'URL de la requête HTTP entrante par rapport à la liste de mots-clés. Si tout ou partie de l'URL correspond à un mot-clé, le routeur Vigor la bloque.

Par exemple, si vous ajoutez le mot-clé « sexe », le routeur Vigor interdit l'accès à des sites ou pages web, tels que « www.sex.com », « www.backdoor.net/images/sex/p_386.html ». Vous pouvez simplement spécifier l'URL complète ou partielle, comme « www.sex.com » ou « sex.com ».

Par ailleurs, le routeur Vigor rejette toute requête qui tente de récupérer du code malveillant.

Activer le contrôle d'accès URL

Pour activer le **contrôle d'accès URL**, cochez la case.



Mot-clé	Le routeur Vigor permet de définir des mots-clés dans 8 trames, chacune pouvant en contenir plusieurs. Le mot-clé peut être un nom, une partie de nom ou une URL complète. Dans une trame, les mots-clés sont séparés par un espace, une virgule ou un point-virgule. De plus, la longueur maximale de chaque trame est de 32 caractères. Une fois les mots-clés spécifiés, le routeur Vigor interdit l'accès à tout site dont tout ou partie de l'URL correspond à un mot-clé défini par l'utilisateur. À noter que plus la liste des mots-clés de blocage est simple, plus le routeur Vigor sera efficace.
Empêcher l'accès au web à partir de l'adresse IP	Cochez cette case pour interdire l'accès au web à l'aide d'une adresse IP, comme http://202.6.3.2. Il s'agit d'empêcher que quelqu'un esquive le contrôle d'accès URL.

Vous devez effacer le cache de votre navigateur pour que le filtrage de contenu d'URL fonctionne correctement sur une page web que vous avez déjà visitée.

Activer la fonction de restriction web

Java	Cochez la case pour activer la fonction de blocage d'objet Java. Le routeur Vigor rejettera les objets Java provenant de l'internet.
ActiveX	Cliquez sur la case à cocher pour activer la fonction de blocage des objets ActiveX. Tout objet ActiveX provenant de l'internet sera refusé.
Fichiers compressés	Cochez la case pour activer la fonction de blocage des fichiers compressés et donc empêcher le téléchargement de fichiers compressés. Le routeur Vigor peut bloquer les types de fichiers compressés suivants : **.zip, .rar,.arj,.ace,.cab,.sit**
Fichiers exécutables	Cochez la case pour empêcher le téléchargement de fichiers exécutables à partir de l'internet. **.exe,.com,.scr,.pif,.bas,.bat,inf,.reg**

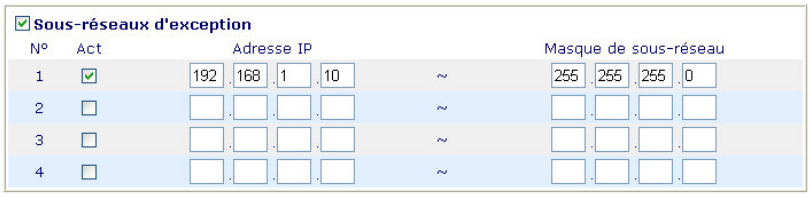
Une fonction *cookie* introduite par Netscape vous permet de surveiller étroitement les demandes et réponses http de sessions individuelles. De nombreux sites utilisent les cookies pour suivre les internautes à la trace, portant atteinte à leur vie privée. Le routeur Vigor comporte une *fonction de filtrage de cookies* qui vous permet de filtrer l'envoi d'informations vers l'extérieur via les cookies. En outre, le routeur Vigor permet également de bloquer toute transmission liée à un proxy afin de renforcer la sécurité.

Cookie	Cochez la case pour bloquer la transmission d'informations vers l'extérieur via les cookies afin de protéger votre vie privée.
Proxy	Cochez la case pour rejeter toute transmission via un proxy. Pour maîtriser l'utilisation de la bande passante, il peut être très intéressant de bloquer le téléchargement de fichiers multimédias à partir de

	pages web. Les fichiers ayant les extensions suivantes seront bloqués par le routeur Vigor : **.mov .mp3 .rm .ra .au .wmv** **.wav .asf .mpg .mpeg .avi .ram**

Sous-réseaux d'exception

Vous pouvez spécifier jusqu'à 4 adresses IP ou sous-réseaux pour les exempter du *contrôle d'accès URL.* Pour activer une entrée, cochez la case « **ACT** » correspondante.



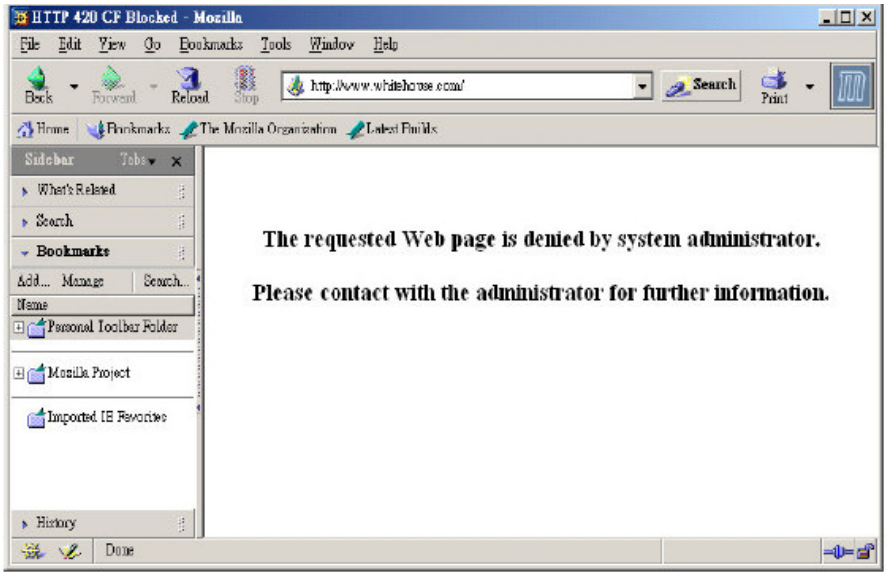
Horaire

Spécifiez l'horaire de mise en œuvre de la fonction de filtrage de contenu d'URL.

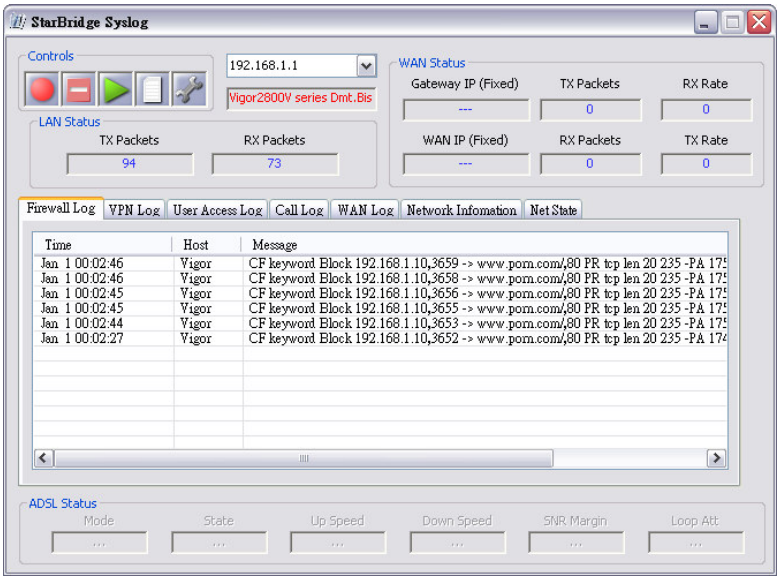
Toujours bloquer	Le filtrage de contenu d'URL est permanent.
Bloquer à partir de H1:M1 à H2:M2	Spécifiez une plage journalière de H1:M1 à H2:M2. H1 et H2 sont les heures. M1 et M2 sont les minutes.
Jours de la semaine	Spécifiez quels jours de la semaine le filtrage de contenu d'URL doit être mis en œuvre. Le routeur Vigor offre deux options exclusives : tous les jours ou certains jours. Si vous voulez que le filtrage de contenu d'URL soit actif toute la semaine, cliquez sur la case « Tous les jours ». Sinon, indiquez les jours de la semaine. Par exemple, si vous voulez que le filtrage de contenu d'URL fonctionne du lundi au mercredi, cliquez sur les cases appropriées (lundi, mardi et mercredi). Les autres jours, le filtrage de contenu d'URL sera inactif.

Messages d'avertissement

Lorsqu'une requête http est rejetée, une page d'avertissement apparaît dans votre navigateur, comme le montre la figure suivante.



Par ailleurs, le message d'avertissement est envoyé automatiquement au client SysLog, si la fonction SysLog est activée. L'administrateur peut configurer le client SysLog dans **Paramétrage de SysLog** à l'aide du configurateur web. L'administrateur peut visualiser les messages d'avertissement provenant de la fonctionnalité **Filtrage de contenu d'URL** à l'aide du démon SysLog DrayTek. Ce type de message d'avertissement a une structure semblable à ceux de **Filtre IP/Pare-feu**, à cette différence près qu'il est préfixé par le mot clé « **CF** », suivi d'un nom indiquant le type de requête HTTP bloqué.



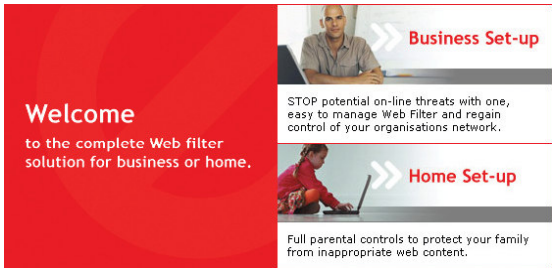
7.2.7 Filtre web

Activez votre essai gratuit

Le logiciel de votre routeur vous permet d'utiliser gratuitement le service de filtrage web pendant 30 jours.

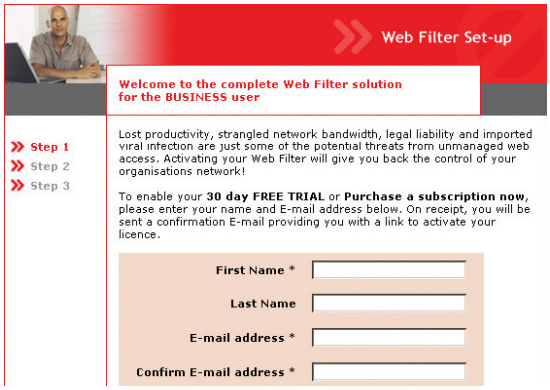
1. Cliquez sur « Activer un essai gratuit et acheter un abonnement »

2. Choisissez entre paramétrage professionnel ou résidentiel

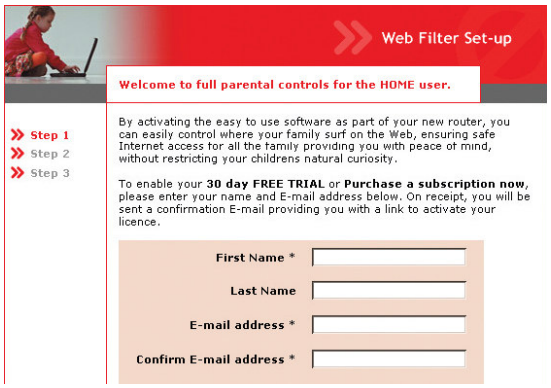


3. Tapez vos coordonnées

Remplissez les champs Name et E-mail address. Cochez « I have read and accepted the Terms and Conditions below ». Cliquez sur « Activate Free Trial ».



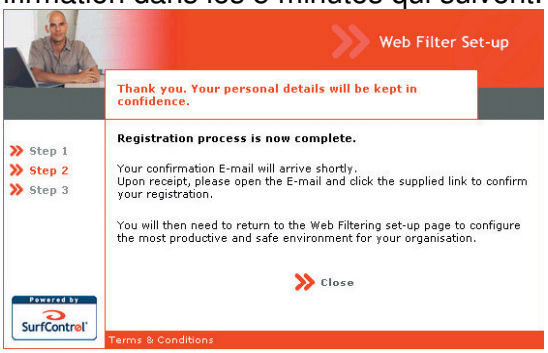
Utilisateur résidentiel



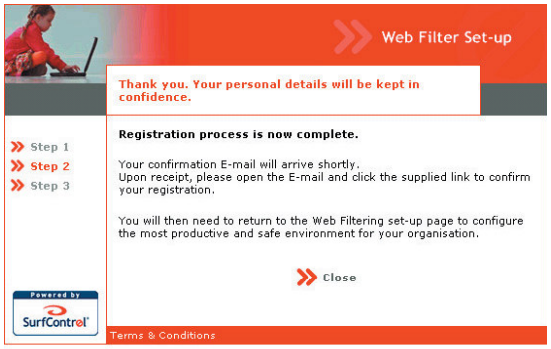
Utilisateur professionnel

4. Inscription complète.

Si vous déjà activé l'essai gratuit de ce routeur un message d'erreur est affiché. Si l'inscription a réussi, vous recevrez un message de confirmation dans les 5 minutes qui suivent. Fermez la fenêtre.



Utilisateur professionnel



Utilisateur résidentiel

5. Confirmez votre inscription

Vérifiez vos e-mails pour voir si vous avez reçu un message de confirmation de PowerNetIX Ltd. Cliquez sur le lien du message pour confirmer votre inscription. En cas de succès, vous bénéficiez d'un essai gratuit de 30 jours.

Dear Sir/Madam,

Thank you for registering for your 30 day FREE TRIAL. By activating Parental Controls as part of your set up, you can easily control where your children surf, ensuring safe and worry free access to the wonders of the Internet.

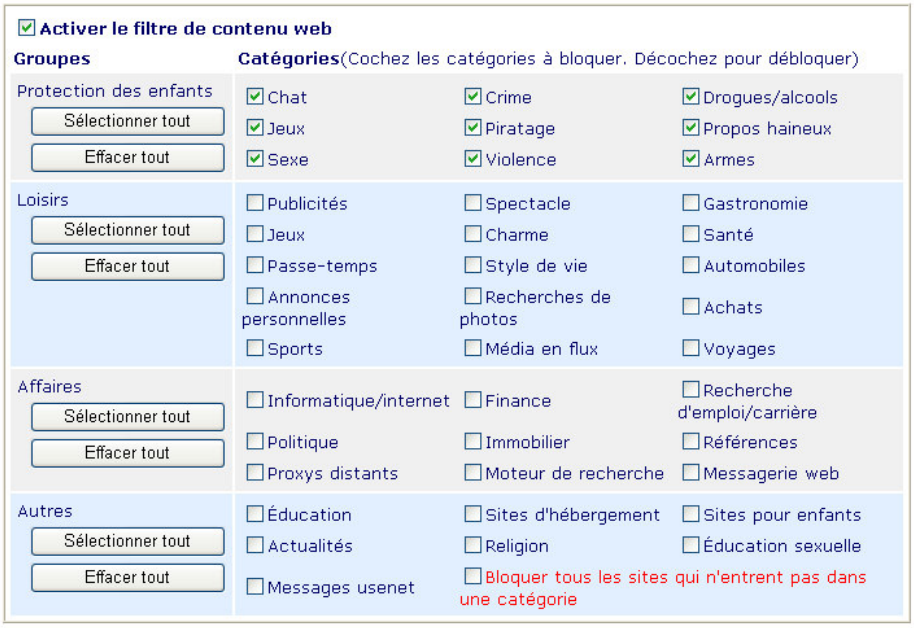
Please click on the link below to confirm your registration.
http://surfcontrol.powernetix.com/sc2/others/trialconfirm.php?key=d81935e8122f27b43b9ab65741e62927
<http://surfcontrol.powernetix.com/sc2/others/trialconfirm.php?key=d81935e8122f27b43b9ab65741e62927&type=home_thankyou> &type=home_thankyou
You will need to return to the Parental Controls set-up page and decide which categories you wish to block.

Please contact us if you have any further questions:
Office hours: 24 hours
E-mail: noc@powernethk.com
Tel (USA): 714-418-4100
Tel (Hong Kong): (852) 2189-7222

Sincerely,
Subscriptions Manager
PowerNetIX Ltd.

Configuration des catégories de filtrage

Pour que le service de filtrage web fonctionne correctement, vous devez sélectionner les catégories de sites que vous voulez interdire. Pour le contenu de chaque catégorie, voir plus loin. Une fois que vous avez sélectionné vos catégories, vous devez enregistrer la configuration pour que l'interdiction d'accès aux sites des catégories choisies soit effective.



Étape 1 Vérifiez que la requête d'accès à l'internet/DNS du routeur fonctionne correctement. Assurez-vous de l'absence entre le routeur et l'internet d'un pare-feu qui bloque le port UDP 9020.

Étape 2 Choisissez un serveur CPA proche de vous (Asie, Europe, États-Unis)

Étape 3 Cochez la case « Activer le filtre de contenu web ». Cochez les catégories que vous voulez bloquer. Pour une description détaillée des catégories, reportez-vous à l'Annexe A de ce chapitre.

Étape 4 Pour mettre en œuvre le filtrage de contenu web pendant une période déterminée, remplissez les champs de plage horaire, la plage horaire ayant été définie dans **Plages horaires**.

Étape 5 Lancez un navigateur et essayez de vous connecter à un site que vous avez interdit d'accès. Une page d'avertissement doit s'afficher à la place du site.

1. Vous pouvez également configurer la fonction SysLog pour recevoir les résultats du filtrage de contenu web.

2. La page de gestion web du routeur lui-même n'est jamais bloquée.

3. Vous pouvez cliquer sur « Tester un site pour voir s'il entre dans une catégorie ». Tous les sites qui ne figurent pas dans la base de données SurfControl sont classés comme n'entrant pas dans une catégorie.

4. Le filtre de contenu web ne peut pas jouer son rôle via un serveur Proxy ou Socks.

5. Si l'essai gratuit n'est pas activé, a expiré ou en cas d'échec d'accès au serveur CPA, le routeur ne bloque l'accès à aucun site.

Abonnement et renouvellement

À l'expiration de votre essai gratuit de 30 jours, vous pouvez décider de renouveler l'abonnement. Vous pouvez payer en ligne à l'aide du service de paiement en ligne  (www.worldpay.com) ou  (www.paypal.com). Ces services sont rapides, faciles à utiliser et totalement sécurisés.

1. - 3. Répétez la procédure d'activation de l'essai gratuit

Puis cliquez sur **Purchase a subscription**. Vous serez redirigé(e) vers la page de paiement.

4. Entrez les détails de paiement

Après avoir choisi votre mode de paiement, tapez les informations de votre carte. Assurez-vous que votre adresse e-mail est la même que l'adresse e-mail que vous avez utilisée pour votre abonnement gratuit de 30 jours.

5. Confirmation de la transaction

Si vous utilisez WorldPay, vous recevrez un e-mail de WorldPay. Vous pouvez conserver cet e-mail.

6. Votre abonnement est enregistré

Vous recevrez un e-mail de  pour confirmer votre abonnement.

Informations sur les catégories

Adultes/actes sexuels explicites
• Produits pour adultes, notamment gadgets sexuels, CD-ROM et vidéos
• Services pour adultes, notamment visioconférence, services d'escorte et clubs de striptease
• Histoires érotiques et description textuelle d'actes sexuels
• Dessins animés explicites
• Groupes en ligne, notamment forums sexuellement explicites
• Nudité complète ou partielle à connotation sexuelle ou érotique
• Description ou images d'actes sexuels, notamment animaux ou objets inanimés utilisés d'une manière sexuelle
• Textes ou graphiques à connotation sexuelle
• Bondage, fétichisme, piercing des parties génitales
• Sites de nudisme mettant en évidence la nudité
• Photographies érotiques ou fétichistes représentant la nudité

NOTA : Nous n'incluons pas les sites concernant l'hygiène sexuelle, le cancer du sein ou les maladies sexuellement transmissibles (sauf sous la forme d'exemples graphiques).

Publicités
• Serveurs de bandeaux publicitaires

Arts et divertissements
• Guides de programmes de télévision, de cinéma, de musique et de vidéo
• Films, vidéos ou clips sonores téléchargeables (non en continu)
• Forums de discussion sur la télévision, les films, la musique et les vidéos
• Magazines et revues en ligne sur le show-business
• Sites de fans de célébrités
• Horoscopes
• Cartes de vœux en ligne
• Blagues, bandes dessinées, comiques ou tout site humoristique ou satirique
• Cirques, théâtres, magazines de variétés et radio
• Sociétés et technologies de diffusion (satellite, câble, etc.)
• Critiques et promotions de livres, éditeurs et poésie
• Musées, galeries, sites artistiques (notamment sculpture, photographie, etc.)

Chat/messagerie en temps réel
• Chat sur internet, cybersalons

Informatique & internet
• Revues, informations, guides d'achat d'ordinateurs, de composants et d'accessoires d'ordinateur et de logiciels
• Sociétés informatiques/SSII/sociétés internet, actualités et magazines de l'industrie
• Enregistrements ou sauvegardes personnelle
• Sites payants
• Téléchargement de logiciels gratuits, de logiciels à contribution et de logiciels en général
• Pages d'objets graphiques (« clipart »), de polices et d'images gif animées
• Jeux, thèmes, graphiques et sonneries de téléphone mobile/PDA téléchargeables
• Échange d'albums de photos/photos numériques en ligne

Pratiques illégales
• Encouragements, instructions ou conseils pour l'accomplissement d'actes illégaux, tels que détournement de services, fraude fiscale, crochetage de serrures, cambriolage
• Plagiats/escroqueries, notamment la vente de thèses, etc.

Drogues, alcools et tabacs

• Recettes, instructions ou kits pour la fabrication ou la culture de substances illicites, notamment l'alcool, à des fins autres qu'industrielles
• Valorisation, encouragement ou instructions concernant l'usage ou le camouflage de l'usage d'alcool, de tabac, de drogues illicites ou autres substances illégales pour les mineurs
• Promotion de l'alcool et du tabac
• Informations sur le sniffage de colle, le détournement de médicaments ou l'abus d'autres substances légales
• Distribution gratuite ou onéreuse d'alcool, de drogue ou de tabac
• Affichage et vente d'attirail de toxicomane et mode d'emploi

NOTA : Nous n'incluons pas les sites qui traitent de l'usage des médicaments, de l'usage industriel du chanvre ou du problème de la légalisation de certaines drogues. Nous n'incluons pas non plus les sites parrainés par un organisme public ou privé fournissant des informations éducatives sur l'usage des médicaments.

Éducation

• Établissements d'enseignement, notamment écoles primaires, élémentaires, secondaires et supérieures ; universités
• Sites d'enseignement : primaire, élémentaire, secondaire et supérieur ; universités
• Téléenseignement et écoles de commerce, notamment formations en ligne
• Ressources d'enseignement en ligne (plans de leçons, etc.)

Finance & investissements

• Cours des actions, renseignements boursiers et taux de rendement
• Opérations de bourse en ligne
• Services de banque et de paiement en ligne
• Conseils en investissement ou contacts pour les opérations sur valeurs mobilières
• Services ou sociétés de gestion financière ou d'investissement
• Finances générales et sociétés de conseils
• Comptables, actuaires, banques, sociétés de crédit hypothécaire et compagnies d'assurances générales

Aliments et boissons

• Recettes, instructions et conseils pour la cuisine, produits alimentaires et conseillers en vins
• Restaurants, cafés et bars
• Revues et critiques gastronomiques

Jeux d'argent

• Sites de jeux d'argent ou de loterie en ligne invitant à l'utilisation d'argent réel ou virtuel
• Informations ou conseils pour le placement des salaires, la participation à des loteries ou à des jeux d'argent
• Casinos virtuels et jeux d'argent extraterritoriaux
• Ligues sportives virtuelles et paris sportifs

NOTA : Les sites de casinos/hôtels/stations qui ne proposent pas des jeux d'argent en ligne ou qui ne donnent pas de conseils de tels jeux sont classés dans la catégorie Voyages.

Jeux

• Téléchargement de jeux ou participation à des jeux ; hébergement de jeux ou de concours
• Tuyaux et conseils sur les jeux ou sur l'obtention de codes frauduleux (« cheatz »)
• Revues et magazines dédiés aux jeux

Charme & lingerie intime

• Présentation de lingerie, de déshabillés ou de maillots de bain
• Pages de fans de mannequins ; modèles de « fitness »/célébrités sportives
• Magazines de mode ou de charme en ligne

• Beauté et cosmétiques
• Informations sur les mannequins et agences de mannequins

Gouvernement et politique

• Services gouvernementaux : impôts, forces armées, douanes, services d'urgence
• Sites de collectivités locales
• Débats politiques, campagnes, informations et résultats d'élections
• Sites politiques locaux, nationaux et internationaux

Piratage

• Promotion, instructions ou conseils sur l'usage discutable ou illicite d'équipements. Logiciels pour le piratage de mots de passe, la création de virus, l'accès à d'autres ordinateurs et/ou systèmes de communication informatisés
• Sites contenant des exécutables malveillants ou des virus
• Sites donnant des instructions pour faire échec au logiciel de filtrage de SurfControl
• Sites de logiciels piratés
• Sites de téléchargement de logiciels et de fichiers multimédias piratés
• Sites fournissant ou promouvant des parasites, tels que logiciels espions, logiciels publicitaires et autres logiciels commerciaux non sollicités

Haine

• Incitation à la dégradation ou à l'attaque de populations ou d'institutions spécifiques sur la base de critères tel que la religion, la race, la nationalité, le sexe, l'âge, l'infirmité ou l'orientation sexuelle
• Promotion d'idées politiques ou sociales de nature suprématiste, excluant autrui sur la base de la race, de la religion, de la nationalité, du sexe, de l'âge, de l'infirmité ou de l'orientation sexuelle
• Sites révisionnistes
• Coercition ou recrutement pour un gang* ou une secte**
• Action militante, extrémisme
• Matériel visiblement indélicat ou injurieux

NOTA : Nous n'incluons pas les actualités, les incidents historiques ou reportages pouvant inclure les critères ci-dessus (sauf dans des exemples graphiques).
* Un gang est défini comme un groupe dont les activités principales sont l'accomplissement d'actes criminels, qui ont une dénomination commune ou un signe ou symbole d'identification et dont les membres s'engagent individuellement ou collectivement dans une activité criminelle au nom du groupe.
** Une secte est définie comme un groupe dont les membres ont été recrutés par tromperie ou par manipulation et maintenus sous influence de telle façon que leur personnalité et leur comportement sont modifiés. La hiérarchie est toute puissante, l'idéologie est totalitaire et la volonté de l'individu est subordonnée au groupe qui se place en dehors de la société.

Santé & médecine

• Santé générale, notamment forme et bien-être
• Informations médicales sur les affections, les pathologies et les médicaments
• Références médicales
• Actes médicaux, notamment opérations chirurgicales non urgentes et chirurgie esthétique
• Traitements alternatifs et complémentaires
• Médicaments vendus sur ordonnance
• Hôpital, assurance médicale
• Dentisterie, optométrie et autres sites médicaux
• Sites de psychiatrie générale et de santé mentale
• Promotion du traitement par soi-même des dépendances, affections et abus physiques et mentaux
• Psychologie, ouvrages et organisations d'entraide

Passe-temps & récréation

• Passe-temps tels que collections, jardinage, maquettes d'avions
• Activités récréatives extérieures, comme la randonnée, le camping, l'escalade

• Conseils axés sur un art, un artisanat ou une technique spécifique
• Publications en ligne sur un passe-temps ou une activité récréative spécifique
• Clubs, associations ou forums en ligne dédiés à un passe-temps
• Jeux traditionnels (échecs, cartes, etc.) et leurs passionnés
• Sites relatifs aux animaux de compagnie, notamment sites propres à une espèce particulière, dressage, spectacles et sociétés protectrices des animaux

Sites d'hébergement

• Sites hébergeant les pages web d'entreprises et d'individus (par exemple, GeoCities, earthlink.net, AOL)

Recherche d'emploi & développement de carrière

• Agences de recrutement, petites annonces, informations sur les carrières
• Recherches de carrière, réseaux

Sites pour enfants

• Sites pour enfants et sites publiés par des enfants

Style de vie & culture

• Vie de famille et sujets liés à la famille, notamment conseils pour les parents, sites pour les homosexuels ou bisexuels (non pornographiques), mariages, naissances et funérailles
• Cultures étrangères, informations socioculturelles

Automobiles et autres véhicules

• Critiques automobiles, conseils d'achat ou de vente de véhicules, catalogues de pièces
• Négoces d'automobiles, photos, discussions concernant les véhicules, notamment les motos, les bateaux, les voitures, les camions et les autocaravanes (camping-cars)
• Revues et magazines sur la modification, la réparation et la personnalisation des véhicules
• Clubs de passionnés de l'automobile en ligne

Actualités

• Journaux en ligne
• Sites de titres de l'actualité, services d'agence de presse et services d'actualités personnalisées
• Sites météorologiques

Annonces personnelles et rencontres

• Listes de célibataires, services matrimoniaux et de rencontres
• Conseils pour les rencontres ou les entrées en relation ; conseils et suggestions pour séduire

Recherches de photos

• Sites fournissant des ressources pour la recherche de photos et d'images

Immobilier

• Listes de maisons individuelles, d'appartements et de terrains
• Services de location ou de déménagement
• Conseils pour l'achat ou la vente d'une maison
• Agents immobiliers
• Sites d'amélioration et d'expertise de l'habitat

Références

• Références personnelles, professionnelles ou éducatives
• Dictionnaires, cartes en ligne et sites de traduction de langues
• Recensement, almanachs et catalogues de bibliothèques
• Moteurs de recherche thématique

Religion
• Églises, synagogues et autres lieux de culte
• Religions et croyances religieuses, notamment les religions non traditionnelles, comme la Wicca et la sorcellerie

Proxys distants
• Proxys distants ou navigation anonyme
• Sites de traduction web qui contournent le filtrage
• Partage de fichiers « peer to peer »

Éducation sexuelle
• Images ou textes consacrés au bon usage des contraceptifs
• Sites consacrés à la discussion de l'utilisation de la pilule, du diaphragme et d'autres types de contraceptifs
• Sites de discussion sur la manière de parler avec votre partenaire des maladies, de la grossesse et du respect des limites

NOTA : Ne sont pas inclus dans la catégorie les sites commerciaux qui vendent des accessoires sexuels. Ces sites sont généralement classés dans la catégorie Adultes.

Moteurs de recherche
• Moteurs de recherche généraux (Yahoo, AltaVista, Google)

Achats
• Enchères en ligne
• Grands magasins, magasins de détail, catalogues et autres sites qui permettent de faire des achats en ligne
• Dépôts de produits téléchargeables en ligne ; spécialités à vendre
• Sites de braderie

Sports
• Sites d'équipes ou de conférence
• Résultats et calendriers nationaux, internationaux, universitaires, professionnels
• Magazines ou bulletins d'information liés au sport

Média en flux
• Événements ou fichiers de média en flux (tout fichier audio ou vidéo archivé ou accessible en direct)
• TV et radio internet
• Sites de webcam personnels (non explicites)
• Sites téléphoniques qui permettent aux utilisateurs d'appeler via l'internet

Voyages
• Compagnies aériennes et agences de réservation de billets
• Informations d'hébergement
• Listes de voyages organisés
• Guides de villes et informations touristiques
• Bureaux météorologiques
• Location de voitures

Messages usenet /forums
• Forums
• Forums d'opinion et de discussion
• Blocs-notes web (« blogs »)

Violence/injures
• Description ou promotion d'agressions physiques contre les êtres humains, les animaux et les institutions
• Description de scènes de torture, de mutilation, d'horreur ou de mort atroce
• Encouragement ou description d'actes contre soi-même ou de suicide, notamment par

l'ingestion de substances nocives ou la dépendance
• Instructions, recettes ou kits pour la fabrication de bombes ou autres dispositifs dangereux ou destructeurs
• Utilisation excessive d'injures ou de gesticulations obscènes
• Sites faisant la promotion du terrorisme
• Sports ou jeux d'une violence excessive
• Propos ou pamphlets injurieux ou violents

NOTA : Nous ne bloquons pas les actualités, les incidents historiques ou les reportages qui peuvent inclure les critères ci-dessus (sauf dans des exemples graphiques).

Armes

• Achats en ligne ou informations pour la commande en ligne, notamment listes de prix et adresses de revendeurs
• Toute page ou tout site contenant majoritairement des liens vers un contenu lié à la vente de fusils, d'armes, de munitions ou de substances toxiques
• Affichage ou mode d'emploi de fusils, d'armes, de munitions ou de substances toxiques
• Clubs proposant un entraînement au maniement de mitraillettes, d'armes automatiques et autres armes d'assaut et/ou un entraînement à la guérilla urbaine

NOTA : Une arme est définie comme étant un objet (gourdin, couteau ou fusil) utilisé pour blesser, réduire à l'impuissance ou détruire.

Messagerie web

• Comptes de messagerie web
• Sites de messagerie

Chapitre 8
Paramétrage des applications

8.1 Introduction

Ce chapitre traite du **DNS dynamique, des plages horaires, des paramètres RADIUS, des paramètres UPnP et des paramètres de qualité de service.**

DNS dynamique

Le FAI vous fournit souvent une adresse IP dynamique au moment où vous vous connectez à l'internet. Cela veut dire que l'adresse IP publique de votre routeur change chaque fois où vous accédez à l'internet. La fonction DNS dynamique vous permet d'affecter un nom de domaine à une adresse IP WAN dynamique. Elle permet au routeur de mettre à jour son adresse IP WAN sur le serveur DNS dynamique spécifié. Une fois le routeur en ligne, vous pourrez utiliser le nom de domaine enregistré pour accéder au routeur ou à des serveurs virtuels internes à partir de l'internet. Cette fonction est particulièrement utile si vous hébergez un serveur web, un serveur ftp ou autre derrière le routeur.

Avant de pouvoir utiliser la fonction DNS dynamique, il faut demander un service DNS dynamique gratuit aux fournisseurs de service DNS dynamique. Le routeur Vigor permet d'ouvrir jusqu'à trois comptes auprès de trois fournisseurs de service DNS dynamique différents. Les routeurs Vigor sont donc compatibles avec les services DNS dynamiques fournis par la plupart des fournisseurs de service DNS dynamique, tels que **www.dyndns.org**, **www.no-ip.com**, **www.dtdns.com**, **www.changeip.com**, **www.dynamic- nameserver.com.** Visitez leur site pour enregistrer votre nom de domaine pour le routeur.

Plages horaires

Le routeur Vigor a une horloge temps réel intégrée qui peut être mise à jour manuellement ou automatiquement à partir d'un serveur de synchronisation internet (NTP). Vous pouvez donc faire en sorte que le routeur se connecte à l'internet à une certaine heure ou bien limiter l'accès à l'internet à certaines heures (par exemple, aux heures ouvrables). La fonction de gestion des plages horaires est également applicable à d'autres fonctions.

RADIUS

Le service d'usager commuté à authentification distante (RADIUS) est un protocole client-serveur d'authentification qui prend en charge l'authentification, l'autorisation et la comptabilité et qui est largement utilisé par les fournisseurs d'accès internet. C'est la méthode la plus courante d'authentification et d'autorisation des utilisateurs à accès commuté ou par tunnel.

Le client RADIUS intégré permet au routeur d'aider l'utilisateur distant ou une station sans fil et le serveur RADIUS à effectuer une authentification mutuelle. Il permet l'authentification centralisée des accès à distance pour la gestion du réseau.

UPnP

Le protocole **UPnP** (Universal Plug and Play) apporte aux périphériques reliés au réseau la faciliter d'installation et de configuration dont bénéficient déjà les périphériques raccordés à un PC avec le système « Plug and Play » Windows existant. Dans le cas des routeurs NAT, la principale fonction du protocole UPnP est le « NAT Traversal ». Elle permet aux applications situées derrière le pare-feu d'ouvrir automatiquement les ports dont elles ont besoin pour passer. C'est plus sûr que de demander à un routeur de déterminer lui-même quels ports ouvrir. De plus, l'utilisateur n'a pas besoin de configurer manuellement des mappages de ports ou un DMZ. Le protocole UPnP est disponible sous Windows XP et le routeur assure la prise en charge de MSN Messenger pour permettre d'exploiter pleinement les fonctionnalités de téléphonie, de vidéo et de messagerie.

Gestion de la qualité de service (QoS)

La gestion de la qualité de service (QoS) pour garantir à toutes les applications les niveaux de service voulus et une bande passante suffisante pour que les objectifs de performance soient remplis constitue l'un des aspects importants des réseaux d'entreprise modernes.

L'une des raisons qui expliquent l'importance de la QoS est que de nombreuses applications TCP augmentent sans cesse leur vitesse de transmission et consomment toute la bande passante disponible. Si les autres applications ne sont pas protégées par la fonction QoS, elles perdent beaucoup en performances dans le réseau encombré. C'est particulièrement essentiel pour les applications qui tolèrent mal les pertes de paquets, les délais de transmission ou la gigue (variations de délai), comme la téléphonie sur IP, la visioconférence, la vidéo et les

données en flux.

Une autre raison est l'encombrement aux intersections de réseau où les vitesses respectives des circuits interconnectés diffèrent et où les trafics s'agrègent. La file d'attente des paquets s'allonge et le trafic peut être ralenti. Si aucun ordre de priorité n'a été défini pour spécifier quels paquets doivent être supprimés d'une file d'attente saturée, ce sont les paquets des applications sensibles mentionnées plus haut qui risquent d'être rejetés. Cela peut affecter les performances de ces applications.

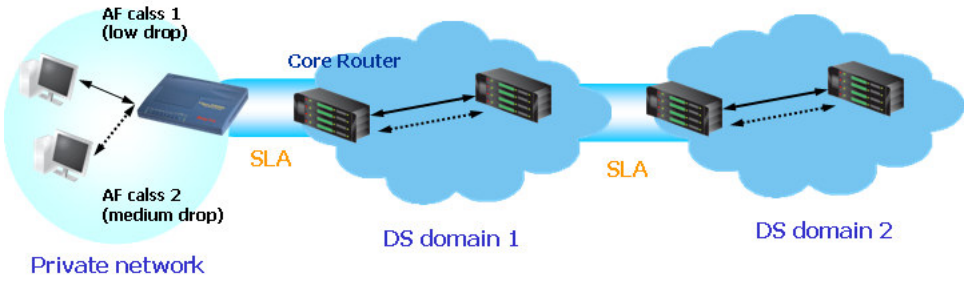
Il existe deux composantes dans la configuration primaire de la QoS :

- Classification : identification des applications à faible latence ou cruciales et marquage de ces applications pour la mise en œuvre d'un niveau de service prioritaire dans tout le réseau.
- Ordonnancement : sur la base de la classification des niveaux de service, affectation des paquets à des files d'attente et à des types de services associés.

Dans les routeurs Vigor, l'implémention de base de la QoS consiste à classer et à ordonnancer les paquets en fonction de l'information de type de service de l'en-tête IP. Par exemple, pour sa connexion avec le siège, un télétravailleur peut appliquer un index de contrôle de QoS pour réserver de la bande passante pour la connexion HTTPS tout en utilisant simultanément un grand nombre d'applications.

Une implémentation de réseau à QoS à plus grande échelle consiste à appliquer un code d’accès services différenciés (DSCP) et la priorité IP au niveau de la couche 3. Par comparaison avec la priorité IP antérieure qui utilise le champ « type de service » (ToS) de l'en-tête IP pour définir 8 classes de service, le DSCP crée 64 classes possibles rétrocompatibles. Dans un réseau à QoS, ou dans le cadre de services différenciés (DiffServ ou DS), un propriétaire de domaine DS signe un contrat de niveau de service (SLA) avec d'autres propriétaires de domaine DS pour définir le niveau de service fourni pour des trafics issus de domaines différents. Chaque nœud DS de ces domaines effectue un traitement différencié. C’est le comportement de commutation de proche en proche (PHB). La définition du PHB comprend la commutation diligentée (EF), l'acheminement assuré (AF) et l'acheminement au mieux (BE). L'acheminement assuré (AF) définit 4 classes d'acheminement avec chacune trois niveaux de priorité de rejet de paquets.

Les routeurs Vigor, en tant que routeurs périphériques de domaine DS, vérifient la valeur du champ DSCP de l'en-tête des paquets IP afin d'allouer une certaine quantité de ressources et d'exécuter les opérations de police, de classification ou d'ordonnancement appropriées. Les routeurs de cœur de réseau effectuent la même vérification avant d'exécuter les traitements afin d'assurer la cohérence du niveau de service dans tout le réseau à QoS.



AF class 1 (low drop)	*AF classe 1 (niveau de rejet bas)*
Core Router	*Routeur de cœur de réseau*
AF class 2 (medium drop)	*AF classe 2 (niveau de rejet moyen)*
DS domain 1	*Domaine DS 1*
DS domain 2	*Domaine DS 2*
Private network	*Réseau privé*

Toutefois, chaque nœud peut se comporter différemment vis-à-vis des paquets marqués comme prioritaires car il peut dépendre des modalités commerciales propres aux différents propriétaires de domaine DS. Il ne dépend pas que du routeur Vigor de garantir un trafic prioritaire à QoS homogène et déterministe dans l'ensemble du réseau.

8.2 Paramètres

Cliquer sur une option du menu **Applications** pour ouvrir la page de paramétrage correspondante.

DNS dynamique	Paramétrage des noms de domaines souscrits auprès d'un maximum de trois fournisseurs de service DNS dynamique.
Plages horaires	Réglage d'une horloge temps réel qui se met à jour automatiquement à partir d'un serveur de synchronisation

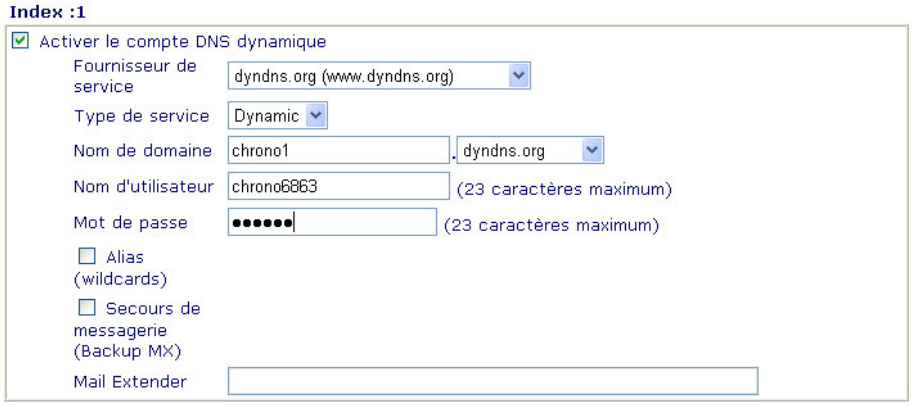
	internet (NTP).
Paramètres RADIUS	Paramétrage du serveur RADIUS
UPnP	Paramétrage du protocole UPnP pour les périphériques raccordés directement à un PC avec le système « Plug and Play » Windows existant.
Qualité de service	Paramétrage des informations de la QoS, telles que l'adresse, le DSCP, le type de service, etc.

8.2.1 DNS dynamique

1. Supposons que vous ayez enregistré un nom de domaine auprès du fournisseur de service DDNS ***hostname.dyndns.org*** et ouvert un compte dont le nom d'utilisateur est ***test*** et dont le mot de passe est ***test***.

2. Dans le menu de paramétrage du DNS dynamique, cochez **Activer le paramétrage du DNS dynamique.**

3. Sélectionnez l'index n°**1** pour ajouter un compte pour le routeur. Cochez **Activer le compte DNS dynamique** et sélectionnez le **fournisseur de service approprié** : **dyndns.org**. Tapez le nom de domaine enregistré : ***hostname*** et le suffixe du nom de domaine : **dyndns.org** dans le champ **Nom de domaine**. Dans les deux champs suivants, tapez votre **nom d'utilisateur** : ***test*** et votre **mot de passe** : ***test***.



4. Cliquez sur le bouton **OK** pour activer les paramètres. Vous pouvez voir que vos paramètres ont été enregistrés.

Les fonctions Alias et Secours de messagerie ne sont pas prises en charge pour tous les fournisseurs de service DNS dynamique. Visitez leur site pour plus de détails.

Désactiver la fonction et effacer tous les comptes DNS dynamique

Dans le menu de paramétrage du DDNS dynamique, décochez **Activer le paramétrage du DNS dynamique** et cliquez sur le bouton **Effacer tout** pour désactiver la fonction et effacer tous les comptes.

Supprimer un compte DNS dynamique

Dans le menu de paramétrage du DNS dynamique, cliquez sur le numéro d'**index** que vous voulez supprimer, puis cliquez sur le bouton **Effacer tout** pour supprimer le compte.

Validation et dépannage

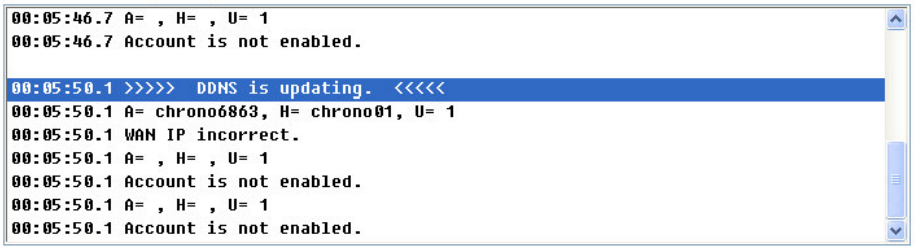
Vérification du nom de domaine enregistré par PING

1. Le routeur étant en ligne, utilisez l'utilitaire PING pour vérifier le fonctionnement de votre nom de domaine enregistré.
2. Utilisez l'option **État en ligne** du menu principal pour vérifier que l'adresse IP envoyée par le serveur DNS dynamique est identique à l'adresse IP WAN du routeur.

Visualisez les journaux DDNS

1. Applications >> Paramétrage du DNS dynamique.
2. Cliquez sur le bouton **Afficher le journal**. Le journal des mises à jour DDNS est affiché :

Journal DDNS dynamique



Avec A : nom d'utilisateur

H : nom de domaine sans suffixe.

Code retour= good 61.230.170.145

Si vous avez un problème de mise à jour DDNS, les journaux sont utiles pour déterminer où le problème se situe.

3. Cliquez sur **État en ligne** pour connaître l'adresse IP WAN actuelle.

Vérifiez si l'adresse IP dans le cercle est identique au code retour des journaux DDNS. Cela indique que la mise à jour a réussi.

8.2.2 Plages horaires

Avant de commencer

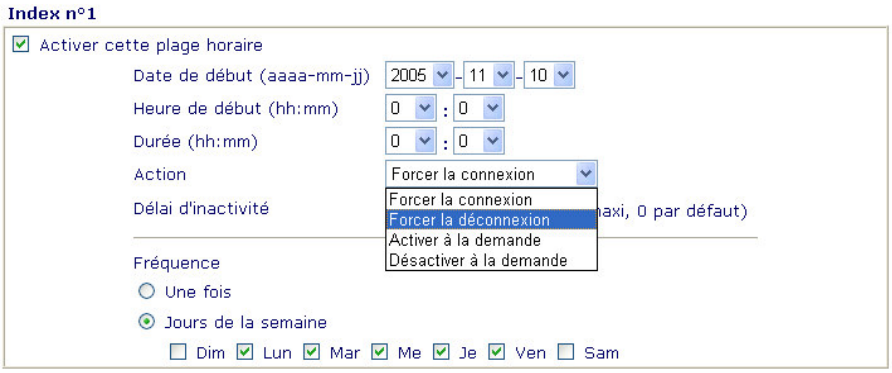
Vous devez vous synchroniser avant de paramétrer une plage horaire. Dans le menu **Maintenance du système>>Réglage de l'heure**, cliquez sur le bouton **Demander l'heure** pour régler l'horloge du routeur Vigor sur l'heure actuelle de votre PC. L'horloge se réinitialise si vous éteignez ou réinitialisez le routeur. Vous pouvez aussi utiliser un serveur NTP sur l'internet pour synchroniser l'horloge du routeur. Pour cela, il faut que la connexion WAN soit établie.

Paramétrage de plages horaires

Vous pouvez paramétrer jusqu'à 15 plages horaires. Ces plages horaires peuvent être appliquées à de nombreuses fonctions.

Ajouter une plage horaire

Cliquez sur un numéro d'index, par exemple 1. Les paramètres de la plage horaire correspondante sont affichés.



Activer cette plage horaire

Cochez la case pour activer la plage horaire.

Date de début (aaaa-mm-jj)

Spécifiez la date de début de la plage horaire.

Heure de début (hh:mm)

Spécifiez l'heure de début de la plage horaire.

Durée (hh:mm)

Spécifiez la durée de la plage horaire.

Action :

Spécifiez quelle action doit être effectuée durant la plage horaire.

Forcer la connexion	Connexion permanente durant la plage horaire.
Forcer la déconnexion	Connexion interdite durant la plage horaire.
Activer à la demande	Connexion établie à la demande avec un **Délai d'inactivité**.
Désactiver à la demande	Connexion établie tant qu'il y a du trafic sur la ligne. Déconnexion à l'expiration du délai d'inactivité, d'autres connections étant impossible durant la plage horaire.

Délai d'inactivité

Spécifiez la durée propre à la plage horaire.

Fréquence	Nombre de fois que la plage horaire sera appliquée.
Une fois	La plage horaire sera appliquée une seule fois

Jours de la semaine	La plage horaire sera appliquée les jours spécifiés.

Exemple

Si vous voulez que la connexion internet PPPoE soit permanente (Force On) de 9 h 00 à 18 h 00 toute la semaine et qu'elle soit impossible (Force Down) en dehors de ces heures :

Heures de bureau :  

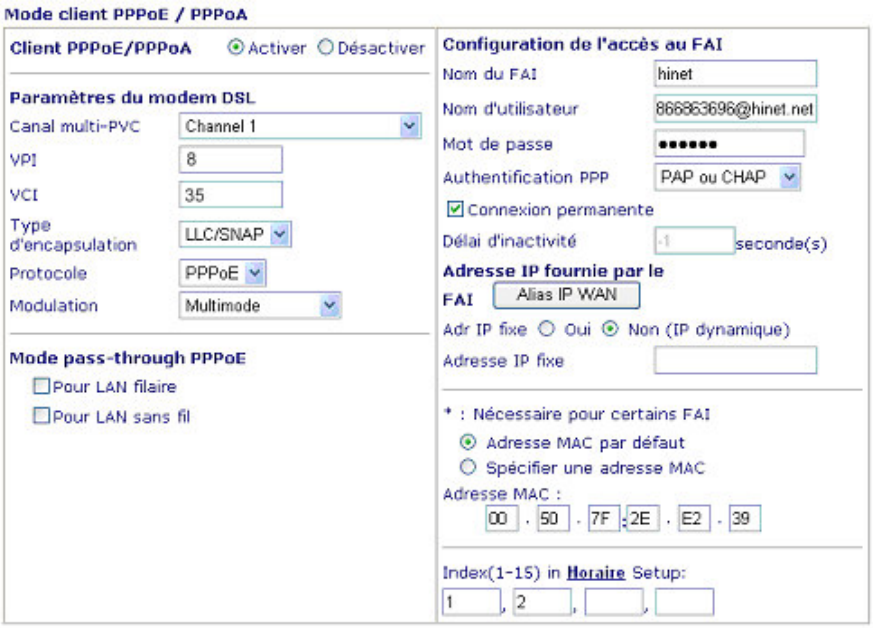
Lun - Dim **9 h 00** **à** **6 h 00**

1. Vérifiez que la connexion PPPoE fonctionne correctement et que le routeur est à l'heure (voir Réglage de l'heure).

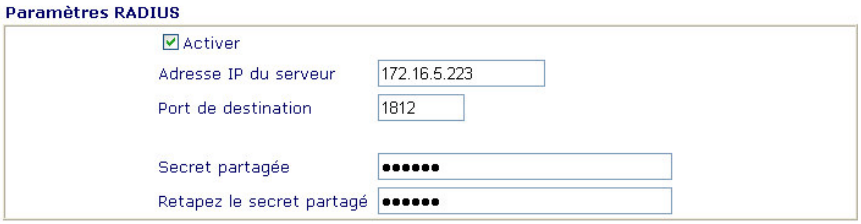
2. Configurez la connexion PPPoE en connexion permanente de 9 h 00 à 18 h 00 toute la semaine.

3. Forcez la déconnexion de 18 h 00 à 9 h 00 le jour suivant pendant toute la semaine.

4. Affectez ces deux profils au profil d'accès internet PPPoE. La connexion internet PPPoE respectera les conditions de connexion ou de déconnexion définies pour les plages horaires.



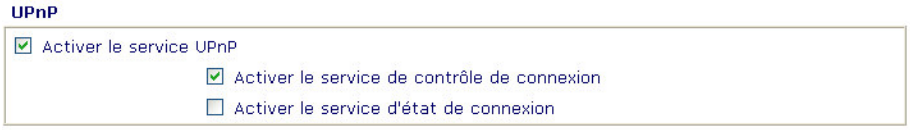
RADIUS



Activer	Cochez cette case pour activer la fonction client RADIUS
Adresse IP du serveur	Tapez l'adresse IP du serveur RADIUS
Port de destination	Numéro de port UDP utilisé par le serveur RADIUS. La valeur par défaut est 1812 (RFC 2138).
Secret partagé	Le serveur et le client RADIUS partagent un secret qui est utilisé pour authentifier les messages qu'ils s'échangent. Les deux côtés doit être configurés pour utiliser le même secret partagé.
Retaper le secret partagé	Retapez le secret partagé pour confirmer.

8.2.3 UPnP

Vous pouvez entrer les **paramètres UPNP** comme indiqué ci-dessous.

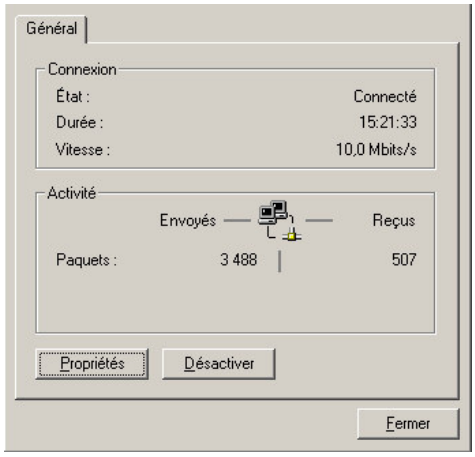


Nota: Si vous avez l'intention de faire fonctionner le service UPnP dans votre LAN, vous devez activer le service approprié pour autoriser le contrôle ci-dessus ainsi que les paramètres UPnP appropriés.

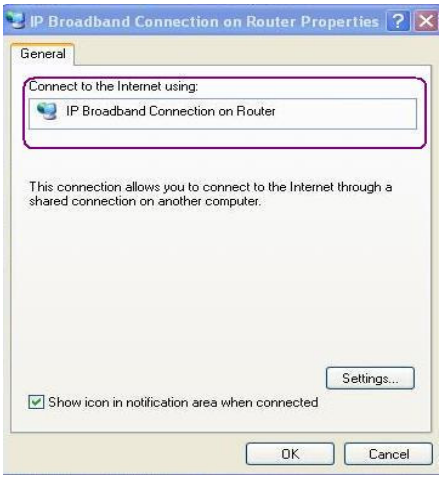
Activer le service UPnP :

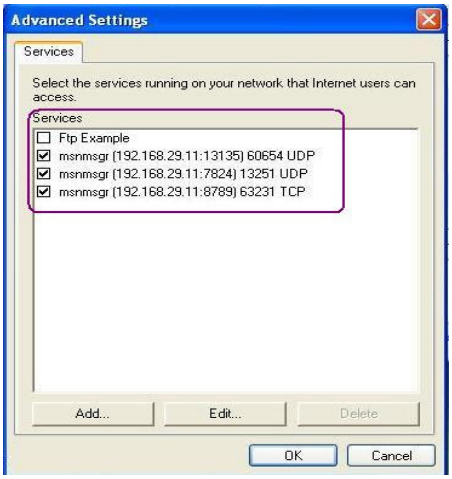
Vous pouvez activer soit le **Service de contrôle de connexion,** soit le **Service d'état de connexion**.

Cliquez sur **Internet Gateway** dans Windows XP/Favoris réseaux comme indiqué ci-dessous. Vous pourrez activer le service d'état et le service de contrôle de la connexion. La fonction NAT Traversal d'UPnP permet le fonctionnement des fonctionnalités multimédias de vos applications. Il faut paramétrer manuellement les ports ou utiliser d'autres méthodes semblables. Les écrans qui suivent montrent des exemples de cette fonctionnalité.



La fonctionnalité UPnP du routeur permet à des applications compatibles UPnP, comme MSN Messenger, de découvrir ce qu'il y a derrière un routeur NAT. L'application prendra également connaissance de l'adresse IP externe et configurera les mappages de ports sur le routeur. Cette fonctionnalité transmet ensuite les paquets des ports externes du routeur vers les ports internes utilisés par l'application.





Rappel concernant le pare feu et UPnP

Impossibilité d'utiliser la fonction UpnP avec le logiciel pare-feu

L'activation d'applications de pare-feu sur votre PC peut entraîner un mauvais fonctionnement de la fonction UPnP. Cela est dû au fait que ces applications bloquent l'accès à certains ports de réseau.

Considérations de sécurité

L'activation de la fonction UPnP sur votre réseau peut compromettre dans une certaine mesure la sécurité et peut vous faire courir certains risques. Vous devez peser soigneusement ces risques avant d'activer la fonction UpnP.

1. Certains systèmes d'exploitation Microsoft ont identifié les points faibles du protocole UPnP. Assurez-vous que vous avez appliqué les packs de service et les correctifs les plus récents.
2. Les utilisateurs non privilégiés peuvent contrôler certaines fonctions du routeur et notamment enlever et ajouter des mappages de ports.

La fonction UPnP ajoute dynamiquement des mappages de ports pour certaines applications compatibles UPnP. Lorsque les applications se terminent anormalement, ces mappages ne peuvent pas être supprimés.

8.2.4 Contrôle de QoS

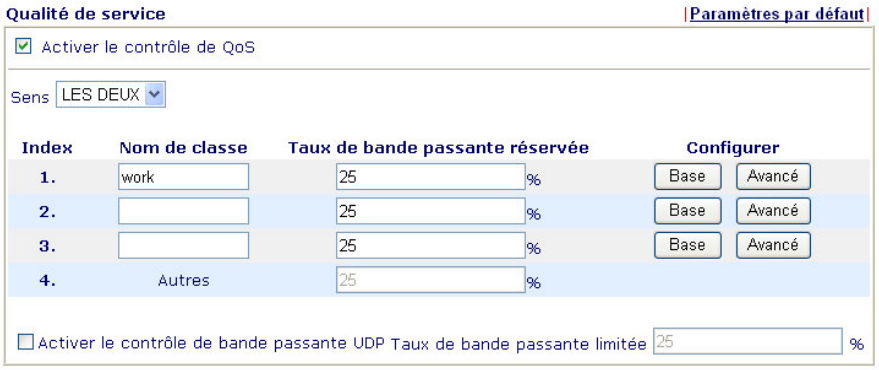
Avant de commencer

Pour un déploiement plus efficace de la QoS, vérifiez les débits montant et descendant ADSL dans **l'état en ligne** comme indiqué ci-dessous.

Les politiques de QoS suivantes sont définies sous la forme d'un rapport débit montant/débit descendant. Les paramètres dépendent de l'état du réseau.

Configuration

Cliquez sur **Application >>Qualité de service**. La fenêtre suivante apparaît.



Activer le contrôle de QoS	Pour les modèles V, le contrôle de QoS est activé par défaut.
Sens	Définit à quel type de trafic les paramètres de contrôle de QoS s'appliquent. **ENTRÉE :** trafic entrant seulement. **SORTIE :** trafic sortant seulement. **LES DEUX :** trafic entrant et trafic sortant.
Index	Le numéro d'index du groupe de paramètres de contrôle de QoS. Il y a 4 groupes au total.

Nom de classe	Définit le nom d'index de groupe.
Taux de bande passante réservée	Bande passante réservée à l'index de groupe sous la forme du rapport de **la bande passante réservée dans le sens montant à la bande passante réservée dans le sens descendant**.
Paramétrage	Il existe deux niveaux de paramétrage : **Base :** taux de bande passante réservée selon le type de service. Nous fournissons une liste des types de services courants. **Avancé :** paramétrage personnalisé du taux de bande passante réservée sur la base de l'adresse d'origine, de l'adresse de destination, du DSCP et du type de service.
Activer le contrôle de bande passante UDP	Cochez cette case et entrez le taux de bande passante limitée dans le champ de droite. Cela constitue une protection du trafic d'application du TCP car le trafic d'application UDP, comme la vidéo en flux, consomme beaucoup de bande passante.

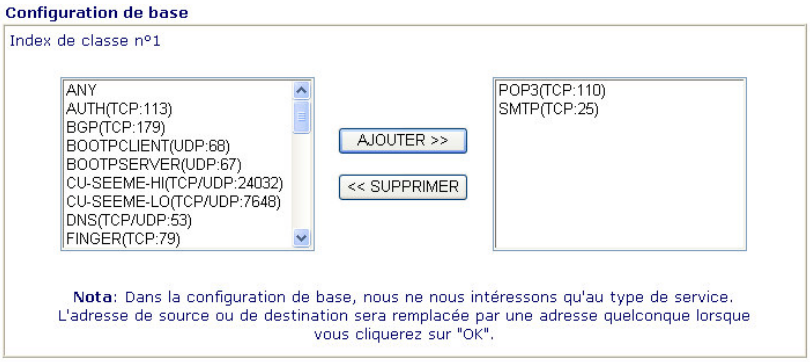
Exemple

Claudine est une télétravailleuse qui travaille quelquefois à la maison et garde des enfants. Pendant son temps de travail, elle utilise le routeur Vigor à la maison pour se connecter au serveur de l'entreprise en ville via HTTPS ou VPN pour lire ses e-mails ou accéder à la base de données interne. Pendant ce temps, les enfants utilisent Skype au salon.

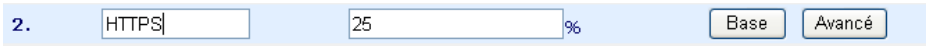
1. Vérifier que le contrôle de QoS est activé (en haut à gauche). Sélectionner LES DEUX pour Sens.

2. Entrer le nom de classe de l'index n°1. Dans cet index, Claudine va spécifier la bande passante réservée à la messagerie utilisant les protocoles POP3 et SMTP et cliquer sur le bouton Base à droite.

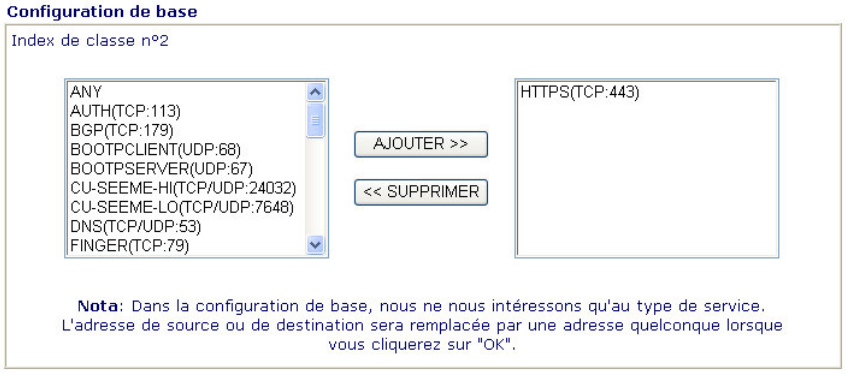
3. Sélectionner POP3 et SMTP dans la colonne de gauche et ajouter les dans la colonne de droite. Cliquer sur OK.



4. Entrer le nom de classe de l'index 2. Dans cet index, elle va spécifier la bande passante réservée pour HTTPS et cliquer sur le bouton Base à droite.

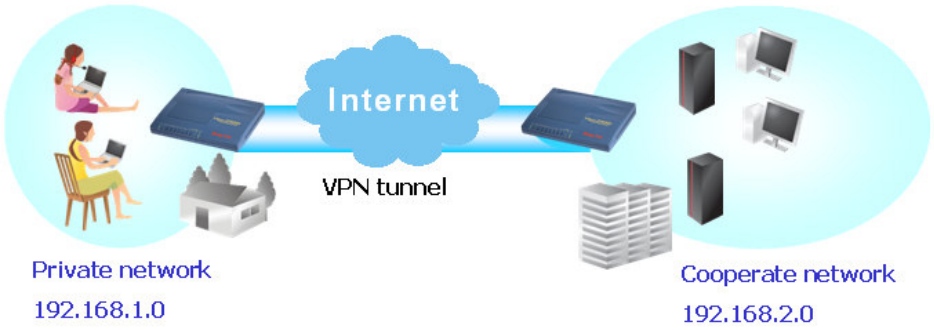


5. Sélectionner HTTPS dans la liste de la colonne de gauche et cliquer sur Ajouter pour l'ajouter dans la colonne de droite. Cliquer sur OK.



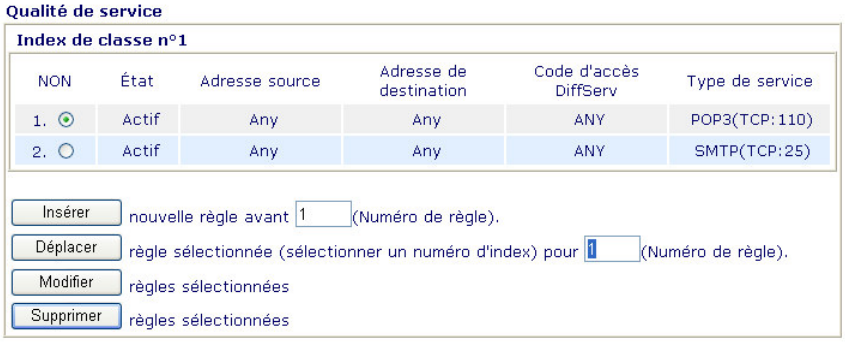
6. Cliquer sur la case Activer le contrôle de bande passante UDP en bas pour empêcher que les autres applications soient affectées par un trafic UDP dense.

7. Si Claudine s'est connectée au siège de l'entreprise à l'aide d'un tunnel de VPN (voir le Chapitre 8 VPN pour plus de détails), elle peut configurer un index pour cette connexion. Elle va entrer le nom de classe de l'index 3. Dans cet index, elle va spécifier la bande passante réservée à 1 tunnel de VPN et cliquer sur le bouton Avancé à droite.



Private network	Réseau privé
VPN tunnel	*Tunnel de VPN*
Cooperate network	*Réseau coopératif*

8. Cliquer sur Modifier pour ouvrir une nouvelle fenêtre. Cocher la case ACT, puis cliquer sur SrcEdit pour définir une adresse de sous-réseau. Cliquer sur DestEdit pour spécifier l'adresse de sous-réseau du siège. Laisser les autres champs et cliquer sur OK.



Chapitre 9

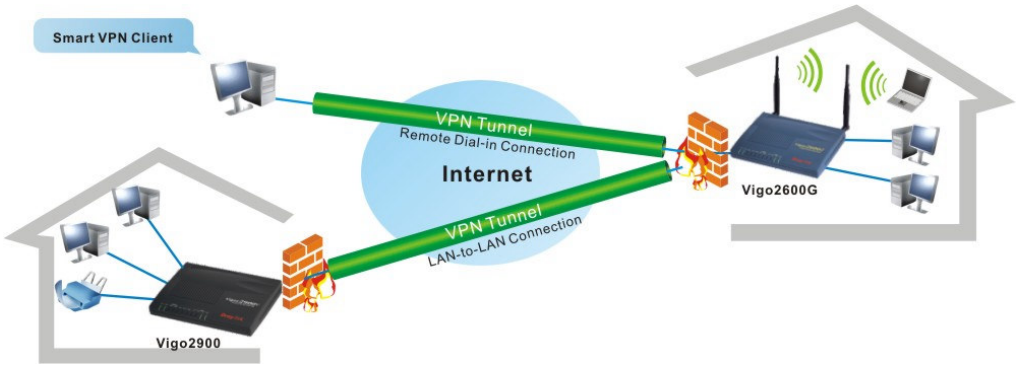
Paramétrage du VPN et de l'accès à distance/paramétrage de la gestion de certificats

9.1 Introduction

Un réseau privé virtuel (RPV ou VPN en anglais) est l'extension d'un réseau privé qui englobe des liaisons appartenant à des réseaux partagés ou publics, comme l'internet. En bref, la technologie de VPN permet l'échange de données entre deux ordinateurs via un réseau partagé ou public dans des conditions analogues à celles d'une liaison privée point à point.

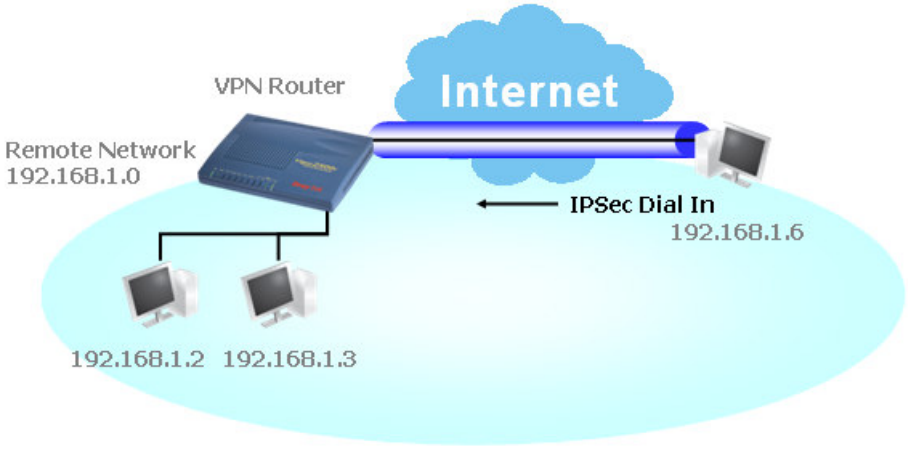
Types de VPN : accès à distance et interconnexion de LAN

Les deux types de VPN sont illustrés ci-dessous.



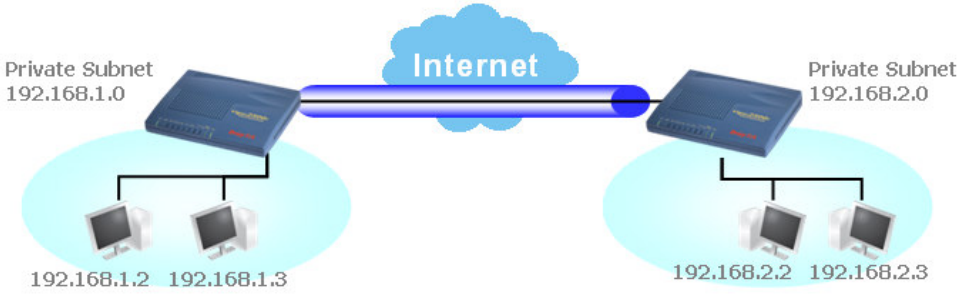
Smart VPN Client	*Client de VPN intelligent*
VPN Tunnel	*Tunnel de VPN*
Remote Dial-in Connection	*Connexion d'accès à distance*
LAN-to-LAN Connection	*Interconnexion de LAN*

- **La connexion d'accès à distance par VPN** permet à un nœud d'accès à distance, à un routeur NAT ou à un utilisateur mobile/télétravailleur d'appeler un routeur VPN via l'internet pour accéder aux ressources du réseau d'entreprise distant. L'appelant peut obtenir une adresse IP appartenant au réseau distant après un processus d'authentification et la création de tunnels de VPN et être traité comme un membre du réseau privé.



VPN Router	*Routeur VPN*
Remote Network	*Réseau distant*
IPSec Dial In	*Appel entrant IPSec*

- **L'interconnexion de LAN par VPN** permet à deux LAN indépendants situés à des endroits différents de partager les ressources, notamment l'interconnexion entre le réseau du siège et le réseau des établissements secondaires ou le domicile des télétravailleurs.



Private Subnet	*Sous-réseau privé*

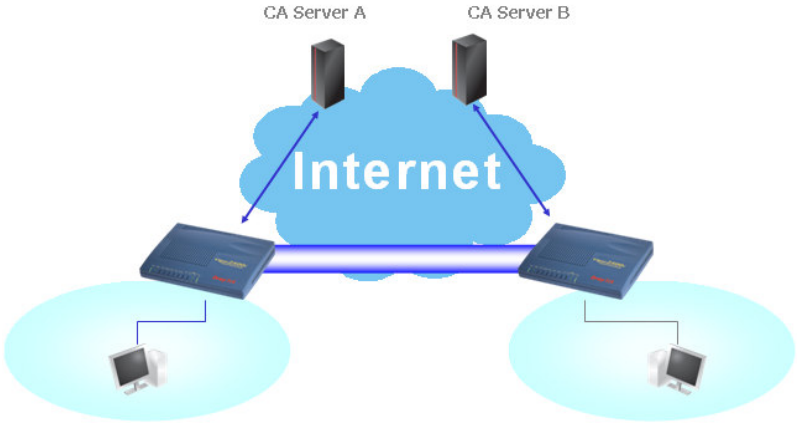
Protocoles utilisés pour chaque type de VPN

Le routeur Vigor prend en charge plusieurs normes de VPN. Chacune a des caractéristiques différentes qui offrent des fonctionnalités de VPN spécifiques.

- **Les protocoles de sécurisation IP (IPSec)** ont été élaborés par l'Internet Engineering Task Force (IETF) pour l'échange sécurisé de paquets au niveau de la couche réseau dans un réseau IP partagé. Un protocole hybride, appelé **protocole d'échange de clé internet (IKE)**, fournit des services comme l'authentification des homologues IPSec, la négociation des paramètres d'association de sécurité IPSec et IKE et l'établissement des clés pour les algorithmes de cryptage utilisés par IPSec. On peut en outre distinguer différents types d'authentification selon les méthodes :

  - **La clé prépartagée** est configurée manuellement sur chaque homologue IPSec. Chaque homologue calcule et envoie une valeur hachée. Si l'homologue récepteur peut créer indépendamment la même valeur hachée à l'aide de sa clé prépartagée, ce qui prouve qu'il a la même clé que l'homologue émetteur, l'authentification est faite.

  - **Des signatures numériques (certificats X.509)** sont utilisées avec le protocole IKE lorsque l'authentification nécessite des clés publiques. Ce certificat est un identifiant numérique donné à chaque machine par des serveurs d'autorité de certification (AC). Deux machines échangent leur certificat numérique pour prouver leur identité avant de commencer à communiquer.



CA Server A	*Serveur d'AC A*
CA Server B	*Serveur d'AC B*

- **Le protocole de tunnel point à point (PPTP)** est un protocole point à point (PPP) élaboré par Microsoft. Lors d'une session de transport (TCP/IP ou NetBIOS), un tunnel est établi pour envoyer les paquets PPP au serveur d'accès à distance (RAS) sur l'internet. L'authentification des utilisateurs s'effectue à l'aide des protocoles existants : PAP et CHAP. MS-CHAP prend en charge le hachage MD4 ainsi que le cryptage DES. Le protocole PPTP assure l'accès sécurisé sur l'internet avec un secret partagé, forme hachée de l'identité des utilisateurs, qui est validé par les deux extrémités. La connexion de VPN PPTP est compatible avec toutes les plates-formes Windows dotées du protocole PPTP.
- **Le protocole de tunnel de couche 2 (L2TP)** est un autre protocole de tunnel point à point (PPP) élaboré par Microsoft et par Cisco. Il combine le meilleur de deux protocoles de tunnel existants : PPTP de Microsoft et L2F de Cisco. Comme PPTP, L2TP nécessite que les routeurs du FAI prennent en charge le protocole.
- **Le protocole L2TP sur IPSec** met en œuvre L2TP avec une politique IPSec. Les protocoles L2TP et L2TP sur IPSec sont compatibles avec Windows 2000 et XP.

Mode transit de VPN (pass-through)

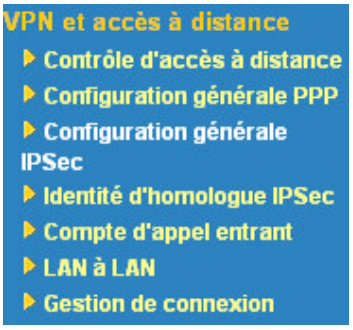
Si vous ajoutez un routeur Vigor à une structure existante qui comporte un routeur dédié au VPN, il faut laisser les tunnels de VPN transiter par le routeur Vigor. Vous pouvez ajouter des mécanismes de contrôle en fonction du type de tunnel de VPN. Par exemple, vous pouvez autoriser le transit des services de VPN IPSec et L2TP et interdire le transit des services de VPN PPTP.

Fonctionnalités liées au RNIS (modèles I)

Pour ceux qui ont des connexions RNIS, des fonctionnalités liés au RNIS, comme l'appel entrant RNIS ou l'appel entrant et l'appel sortant dans le cas de l'interconnexion de LAN, peuvent être configurées. Le RNIS met en œuvre également des connexions PPP pour l'authentification et la facturation. Le rappel automatique permet au routeur Vigor de l'entreprise de partager le coût de connexion.

9.2 Paramètres

Cette section explique les possibilités offertes par le VPN et l'accès à distance. Utilisez les liens du menu pour configurer le VPN et l'accès à distance ainsi que les fonctions de gestion de certificats.



9.2.1 Gestion de certificats

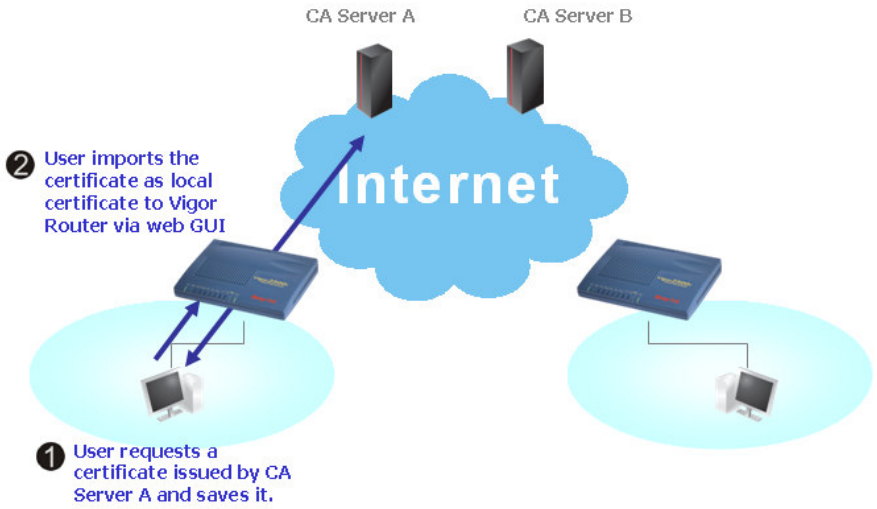
Un certificat numérique est un identifiant électronique délivré par une autorité de certification (AC). Il contient des informations telles que votre nom, un numéro de série, des dates d'expiration, etc., et la signature numérique de l'autorité de certification afin qu'un destinataire puisse vérifier que le certificat est authentique. Le routeur Vigor prend en charge les certificats numériques conformes à la norme X.509.

Une entité voulant utiliser des certificats numériques doit d'abord demander un certificat à un serveur d'AC. Il doit également se procurer les certificats d'autres serveurs d'AC de confiance afin de pouvoir authentifier l'homologue avec des certificats émis par ces serveurs d'AC de confiance.

Ici, vous pouvez créer et gérer des certificats numériques locaux et des certificats d'AC de confiance.

N'oubliez pas de mettre le routeur à l'heure avant d'utiliser le certificat pour que la période de validité du certificat soit correcte.

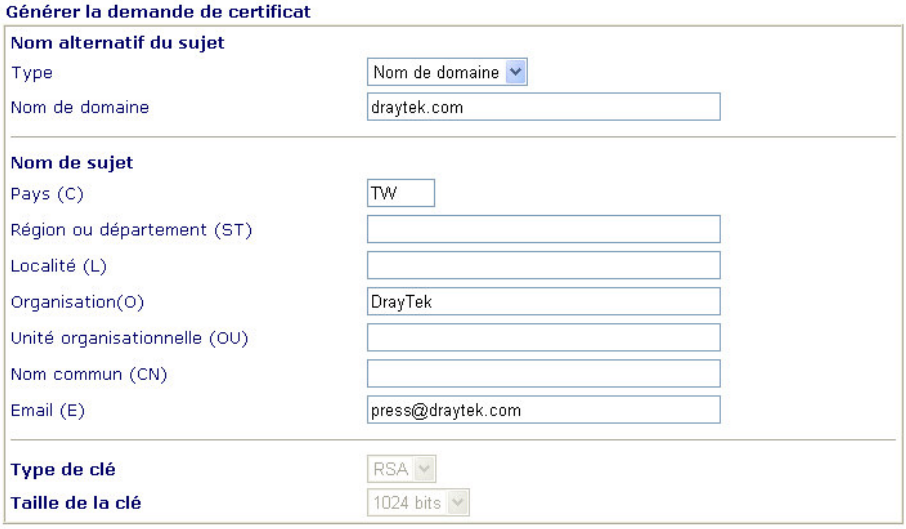
Demande de certificat à un serveur d'AC



CA Server A	*Serveur d'AC A*
CA Server B	*Serveur d'AC B*
User requests a certificate issued by CA Server A and saves it.	*L'utilisateur demande un certificat émis par le serveur d'AC A et l'enregistre.*
User imports the certificate as local certificate to Vigor Router via web GUI.	*L'utilisateur importe le certificat en tant que certificat local du routeur Vigor via l'interface utilisateur web.*

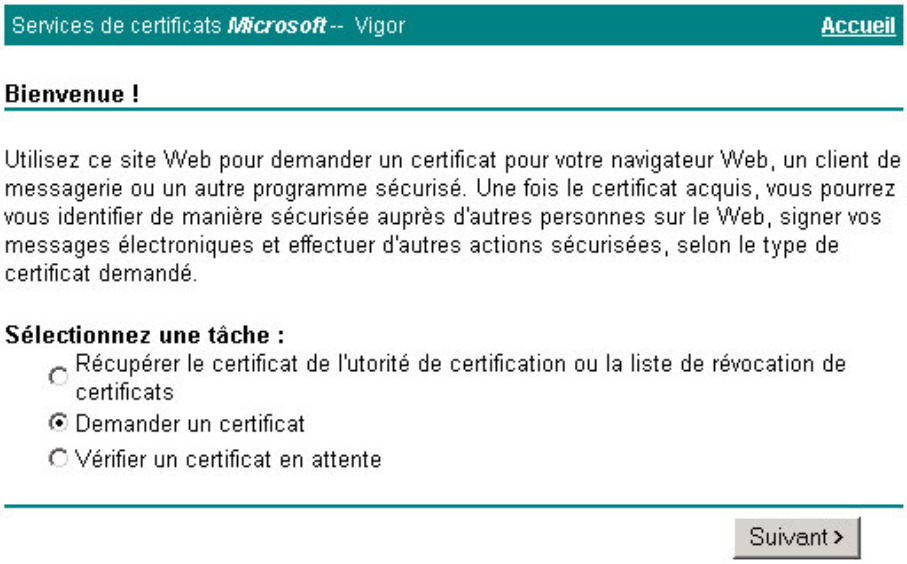
Étape 1 : Cliquez sur **Certificat local** pour avoir l'écran ci-dessous. Vous pouvez cliquer sur le bouton **GÉNÉRER** pour commencer à éditer une demande de certificat.

Étape 2 : Entrez les informations voulues dans la demande de certificat.

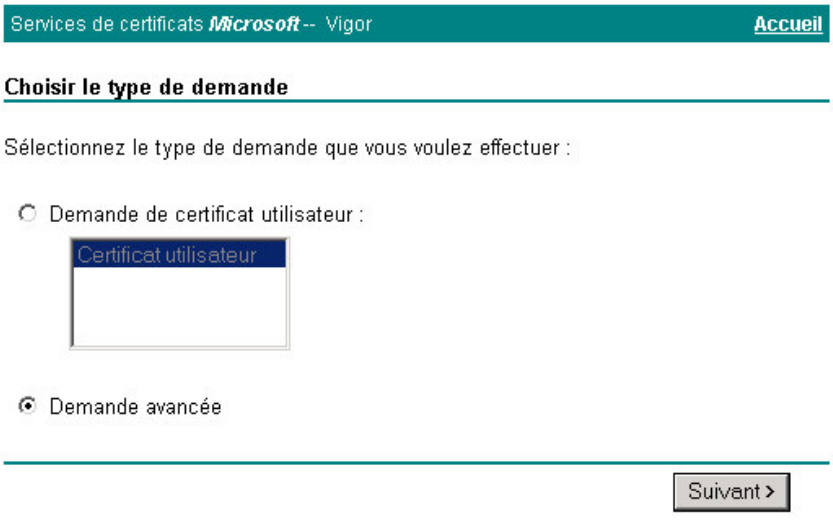


Étape 3 : Copiez et enregistrez la demande de certificat local X509 sous la forme d'un fichier texte.

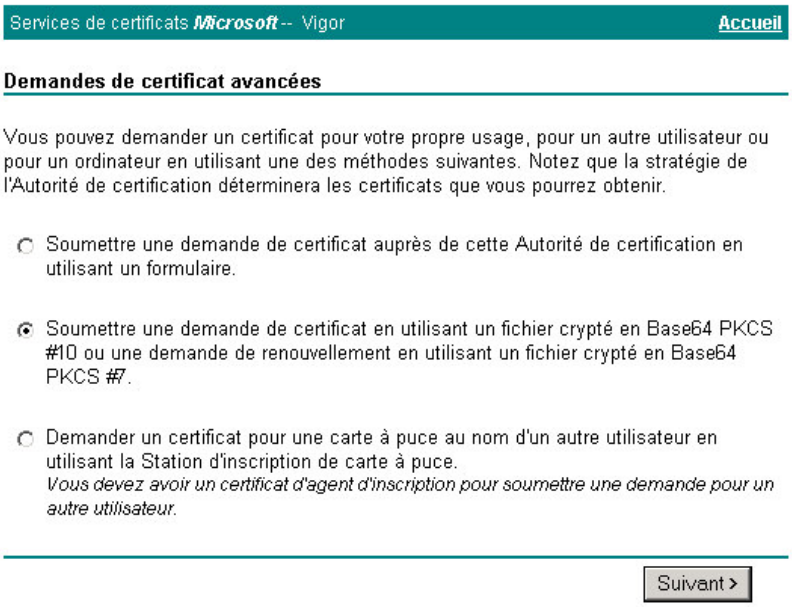
Étape 4 : Connectez-vous au serveur d'AC à l'aide du navigateur internet. Suivez les instructions. Nous allons prendre l'exemple d'un serveur d'AC Windows 2000. Sélectionnez **Demander un certificat**.



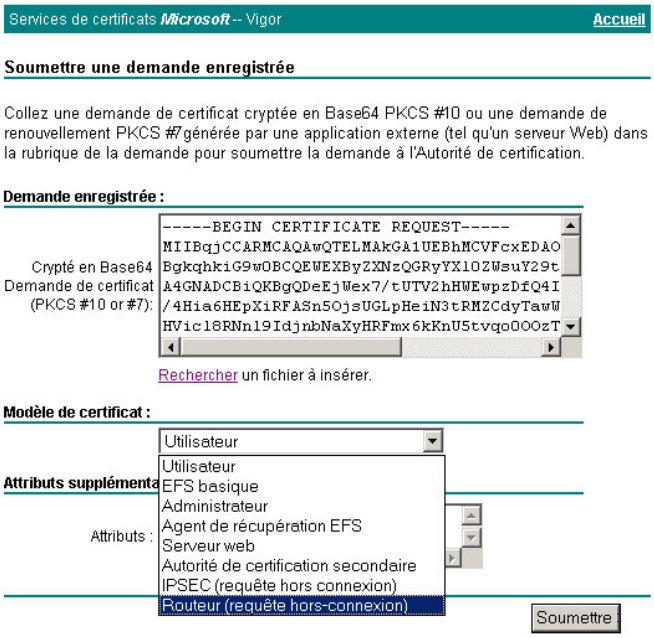
Sélectionnez **Demande avancée**.



Sélectionnez **Soumettre une demande de certificat en utilisant un fichier crypté en Base64 PKCS #10 ou une demande de renouvellement en utilisant un fichier crypté en Base64 PKCS #7**.



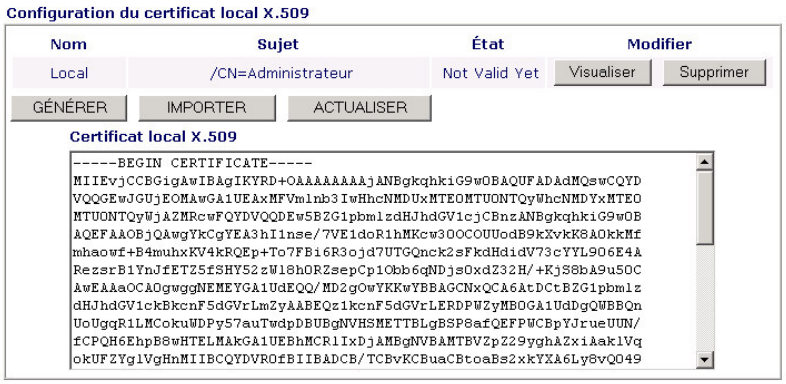
Importez le fichier texte de demande de certificat local X509. Sélectionnez **Routeur (demande hors connexion)** ou **IPSec (demande hors connexion)** ci-dessous.



Le serveur vous délivre un certificat. Sélectionnez **Crypté en Base64** et **Télécharger le certificat CA**.

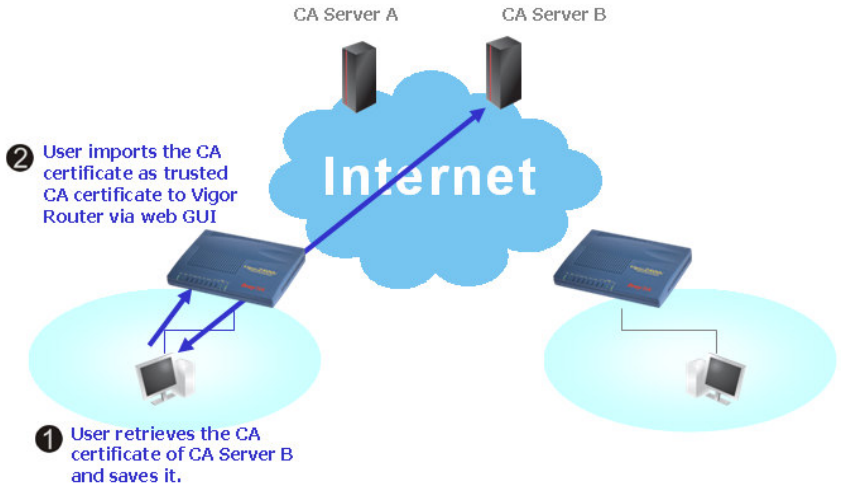
Vous obtenez un certificat (fichier .cer) que vous pouvez enregistrer.

Étape 5 : Retournez au routeur Vigor, cliquez sur **Certificat local**. Cliquez sur le bouton **IMPORTER** et recherchez le fichier .cer sur le routeur Vigor. Cela fait, cliquez sur ACTUALISER. La fenêtre suivante apparaît avec « ------BEGIN CERTIFICATE------..... ».



Vous pouvez visualiser les informations du certificat en cliquant sur le bouton **Visualiser**.

Demande de certificat à définir comme certificat de confiance



CA Server A	*Serveur d'AC A*
CA Server B	*Serveur d'AC B*
User retrieves the CA certificate of CA Server B and saves it.	*L'utilisateur récupère le certificat du serveur d'AC B et l'enregistre.*
User imports the CA certificate as trusted CA certificate to Vigor Router via web GUI.	*L'utilisateur importe le certificat comme certificat de confiance sur le routeur Vigor via l'interface utilisateur web.*

Étape 1 : À l'aide du navigateur internet, connectez-vous au serveur d'AC dont vous voulez récupérer le certificat. Cliquez sur **Récupérer le certificat de l'autorité de certification ou la liste de révocation de certificats**.

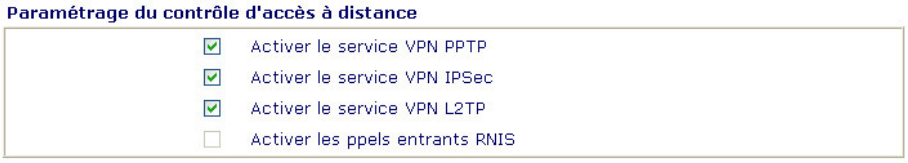
Étape 2 : Sous **Choisir un fichier à télécharger**, cliquez sur **Courant** sur **Crypté en Base64** et sur **Télécharger le certificat CA** pour enregistrer le fichier .cer.

Étape 3 : Retournez au routeur Vigor, sélectionnez **Certificat d'AC de confiance**. Cliquez sur le bouton **IMPORTER** et recherchez le fichier .cer sur le routeur Vigor. Cela fait, cliquez sur Actualiser. L'écran suivant apparaît.

Vous pouvez visualiser les informations du certificat en cliquant sur le bouton **Visualiser**.

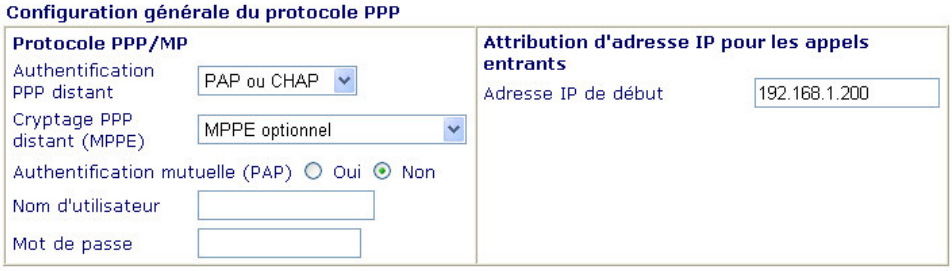
9.2.2 Paramétrage du contrôle d'accès à distance

Activez le service VPN dont vous avez besoin. Si vous voulez faire fonctionner un serveur VPN dans votre LAN, vous devez désactiver le service VPN du routeur Vigor pour autoriser le mode transit de VPN, ainsi que les paramètres NAT appropriés, comme les paramètres DMZ ou d'ouverture de ports. Activez l'accès à distance RNIS si besoin est.



9.2.3 Configuration générale du protocole PPP

Ce sous-menu s'applique uniquement aux connections PPP, comme PPTP, L2TP, L2TP sur IPSec.



Protocole PPP/MP

Authentification PPP distant	**PAP seulement :** Choisissez cette option pour que le routeur authentifie les utilisateurs distants avec le protocole PAP. **PAP ou CHAP :** Si vous choisissez cette option, le routeur tentera d'authentifier les utilisateurs distants d'abord avec le protocole CHAP. Si l'utilisateur distant ne prend pas en charge ce protocole, le routeur utilisera le protocole PAP pour l'authentification.
Cryptage PPP distant (MPPE)	**MPPE optionnel :** Cette option signifie que la méthode de cryptage MPPE sera employée facultativement par le routeur pour l'utilisateur distant. Si l'utilisateur distant ne prend pas en charge l'algorithme de cryptage MPPE, le routeur transmettra « paquets non cryptés par MPPE ». Autrement, l'algorithme de cryptage MPPE sera utilisé. **Nécessite MPPE (40/128bits) :** Choisissez cette option pour que le routeur crypte les paquets à l'aide de l'algorithme de cryptage MPPE. L'utilisateur distant utilisera un cryptage sur 40 bits avant d'utiliser un cryptage sur 128 bits. En d'autres termes, si le cryptage MPPE sur 40 bits n'est pas disponible, c'est le cryptage sur 128 bits qui sera appliqué aux données. **MPPE maximum :** Cette option indique que le routeur utilisera le cryptage MPPE sur 128 bits.
Authentification mutuelle (PAP)	La fonction d'authentification mutuelle est surtout utilisée pour communiquer avec d'autres routeurs ou clients qui ont besoin d'une authentification bidirectionnelle pour renforcer la sécurité, par exemple, les routeurs Cisco. Par conséquent, vous devez activer cette fonction si le routeur homologue demande une authentification mutuelle. Dans ce

	cas, vous devez également spécifier le **nom d'utilisateur** et le **mot de passe** de l'homologue.

Attribution d'adresse IP pour les appels entrants

Adresse IP de début	Entrez une adresse IP de début pour la connexion PPP entrante. Vous pouvez choisir une adresse >IP du réseau privé local. Par exemple, si le réseau privé local est 192.168.1.0/255.255.255.0, vous pouvez choisir 192.168.1.200 comme adresse IP de début. Les adresses 192.168.1.200 et 192.168.1.201 sont réservées aux appels entrants RNIS.

9.2.4 Configuration générale IPSec

Dans **Configuration générale IPSec,** on distingue deux parties principales.

La négociation IKE/IPSec comporte deux phases.

- Phase 1 : négociation des paramètres IKE, notamment les paramètres de cryptage, de hachage, Diffie-Hellman et de durée de vie pour protéger l'échange IKE qui suit, l'authentification des deux interlocuteurs à l'aide d'une clé prépartagée ou d'une signature numérique (X.509). L'interlocuteur qui entame la négociation propose toutes ses règles à l'interlocuteur distant, puis celui-ci tente de trouver une correspondance prioritaire avec ses règles. À la fin, un tunnel sécurisé est établi pour la phase 2 IKE.

- Phase 2 : négociation des méthodes de sécurisation IPSec, notamment l'en-tête d'authentification (AH) et/ou la charge utile de sécurité d'encapsulation (ESP) pour l'échange IKE suivant et le contrôle mutuel de l'établissement du tunnel sécurisé.

L'en-tête d'authentification (AH) assure l'authentification des données et l'intégrité des paquets IP échangés par les homologues VPN. Pour cela, une fonction de hachage à sens unique est appliquée aux paquets pour créer un condensé de message. Ce condensé est placé dans l'AH et transmis avec les paquets. Côté réception, l'homologue applique la même fonction de hachage aux paquets et compare la valeur avec celle de l'AH reçu.

La charge utile de sécurité d'encapsulation (ESP) est un protocole de sécurisation qui assure la confidentialité et la protection des données avec un service optionnel d'authentification et de détection de rejet. Le routeur Vigor prend en charge l'ESP pour le cryptage de la charge utile. Dans IPSec, il y a deux modes de cryptage : transport et tunnel. Le

mode transport crypte uniquement la partie données, c'est-à-dire la charge utile, de chaque paquet, mais non l'en-tête. Le mode transport est utilisé avec le protocole L2TP sur IPSec. Le mode tunnel, plus sûr, crypte à la fois l'en-tête et la charge utile. Le mode tunnel est utilisé par le protocole IPSec. L'ESP peut être utilisé seul ou avec AH.

Méthode d'authentification IKE

Cette méthode s'applique généralement à un utilisateur distant ou à un nœud d'interconnexion de LAN qui utilise une adresse IP dynamique et des connexions de VPN liées à IPSec, comme L2TP sur IPSec et les tunnels IPSec.

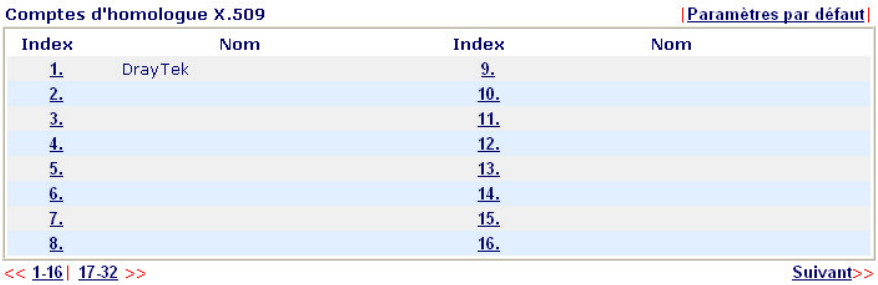
Clé prépartagée	Le routeur Vigor prend actuellement en charge uniquement l'authentification par clé prépartagée. **Clé prépartagée :** Spécifiez une clé pour l'authentification IKE. **Retapez la clé prépartagée :** Confirmez la clé prépartagée.

Méthode de sécurisation IPSec

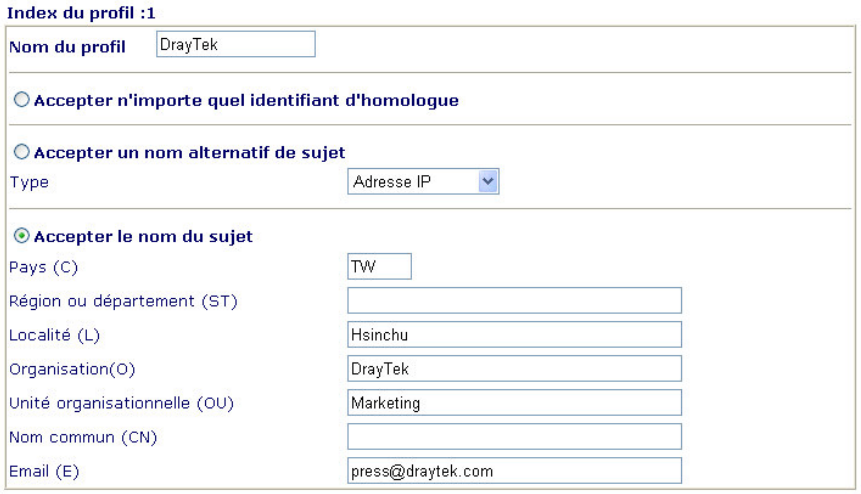
Moyenne	**En-tête d'authentification (AH)** : les données seront authentifiées mais non cryptées. Par défaut, cette option est active.
Élevée	**Charge utile de sécurité d'encapsulation (ESP)** : la charge utile (les données) sera cryptée et authentifiée. Vous pouvez choisir un algorithme de cryptage : DES, 3DES et AES.

9.2.5 Identité d'homologue IPSec

Pour utiliser un certificat numérique pour l'authentification d'un homologue en mode interconnexion de LAN ou accès à distance, vous pouvez éditer une table de certificats d'homologue. Le routeur permet de spécifier 32 certificats numériques pour les appels entrants.



Pour éditer un certificat numérique, cliquez sur le numéro d'index correspondant. Il existe trois niveaux de sécurité pour l'authentification des signatures numériques : remplissez chaque champ nécessaire pour authentifier l'homologue distant. L'explication suivante vous aidera à remplir tous les champs nécessaires.



Index de profil

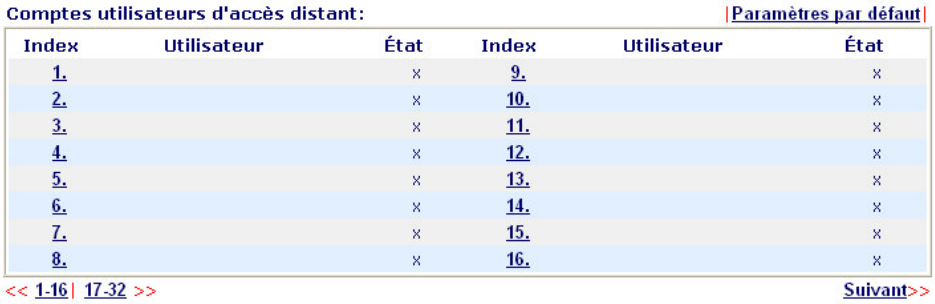
Accepter n'importe quel identifiant d'homologue	Cliquez pour accepter n'importe quel homologue, quel que soit son identifiant.
Accepter un nom alternatif de sujet	Cliquez pour vérifier un champ spécifique de la signature numérique afin d'accepter l'homologue qui a une valeur concordante. Le champ peut être **Adresse IP, Domaine**

	ou **Adresse e-mail**.
Accepter un nom de sujet	Cliquez pour vérifier des champs spécifiques de la signature numérique afin d'accepter l'homologue qui a une valeur concordante. Les champs peuvent être les suivants : **Pays (C), Région ou département (ST), Localité (L), Organisation (O), Unité organisationnelle (OU), Nom commun (CN)** et **E-mail (E)**.

9.2.6 Utilisateur distant

Ici, vous pouvez gérer l'accès à distance à l'aide d'une table de profils d'utilisateur distant permettant d'authentifier l'utilisateur et d'établir la connexion de VPN. Vous pouvez définir des paramètres comme identifiant d'homologue, le type de connexion (RNIS, VPN avec PPTP, tunnel IPSec, L2TP ou L2TP sur IPSec), les méthodes de sécurisation correspondantes, etc.

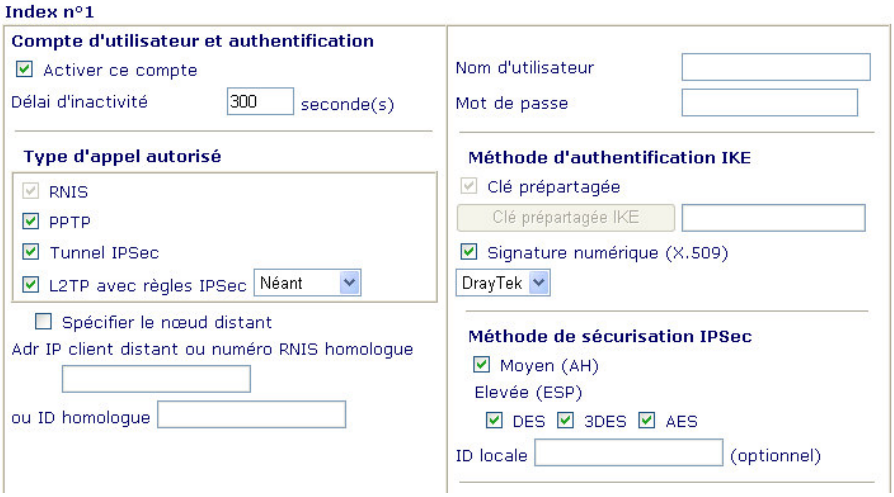
Le routeur permet de créer 32 comptes d'utilisateur distant. En outre, vous pouvez étendre les comptes utilisateurs au serveur RADIUS grâce à la fonction client RADIUS intégré. L'écran récapitulatif est représenté ci-dessous.



Comptes utilisateurs d'accès distant

Paramètres par défaut	Cliquez ici pour effacer tous les numéros d'index.
Utilisateur	Affiche le nom d'utilisateur de l'utilisateur distant ou du profil d'interconnexion de LAN. Le symbole ??? signifie que le profil est vide.
État	Affiche l'état de l'accès de l'utilisateur distant spécifié. V indique que l'utilisateur distant est actif. X indique que l'utilisateur distant est inactif.

Cliquez sur chaque numéro d'index pour éditer l'un des profils d'utilisateur distant. **Pour chaque type d'appel entrant, vous devez remplir les différents champs à droite.** Si les champs sont grisés, c'est que vous pouvez les laisser de côté. L'explication qui suit vous aidera à remplir tous les champs nécessaires.



Authentification de compte utilisateur

Activer ce compte	**Délai d'inactivité :** Délai d'inactivité à l'expiration duquel le routeur déconnectera l'utilisateur distant. Par défaut, le délai d'inactivité est de 300 secondes.

Type d'appel entrant autorisé

Type	**RNIS :** Permet d'établir une connexion RNIS. Vous pouvez également paramétrer la fonction de rappel automatique. Vous devez spécifier le nom d'utilisateur et le mot de passe de l'utilisateur distant. **PPTP :** Permet à l'utilisateur distant d'établir une connexion de VPN PPTP via l'internet. Vous devez spécifier le nom de l'utilisateur et le mot de passe de l'utilisateur distant. **Tunnel IPSec :** Permet à l'utilisateur distant d'établir une connexion de VPN IPSec via l'internet. **L2TP:** Permet à l'utilisateur distant d'établir une connexion de VPN L2TP via l'internet. Vous pouvez sélectionner L2TP ou L2TP sur IPSec. ➢ **Néant :** ne pas appliquer la politique IPSec. En conséquence, la connexion de VPN L2TP sans politique IPSec peut être considérée comme une connexion L2TP pure.

	➢ **Souhaitée :** appliquer d'abord la politique IPSec si elle est applicable pendant la négociation. Sinon, la connexion de VPN devient une connexion L2TP pure. ➢ **Imposée :** appliquer systématiquement la politique IPSec à la connexion L2TP. Vous devez spécifier le nom de l'utilisateur et le mot de passe de l'utilisateur distant.
Nom d'utilisateur	Ce champ est applicable lorsque vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. Il l'est également si vous sélectionnez RNIS.
Mot de passe	Ce champ est applicable lorsque vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. Il l'est également si vous sélectionnez RNIS.
Spécifier le nœud distant	**Cocher la case :** vous pouvez spécifier l'adresse IP de l'utilisateur distant ou l'identifiant d'homologue. Si vous avez sélectionné RNIS, tapez le numéro RNIS d'homologue. Vous devez également spécifier les méthodes de sécurisation correspondantes à droite. **Décocher la case :** le type de connexion que vous avez sélectionné plus haut appliquera les méthodes d'authentification et de sécurisation définies dans les **Paramètres généraux**.

Méthode d'authentification IKE

Ce groupe de champs est applicable aux tunnels IPSec et à L2TP avec politique IPSec **lorsque vous spécifiez l'adresse IP du nœud distant**. La seule exception est la signature numérique (X.509) qui peut être spécifiée lorsque vous sélectionnez le tunnel IPSec avec ou sans l'adresse IP du nœud distant.

Clé prépartagée	Entrez une clé prépartagée (1 à 63 caractères).
Signature numérique (X.509)	Sélectionnez une signature numérique préétablie dans les profils d'ID homologue X.509.

Méthode de sécurisation IPSec

Ce groupe de champs est obligatoire pour les tunnels IPSec et L2TP avec politique IPSec lorsque vous spécifiez le nœud distant.

Moyenne	**En-tête d'authentification (AH)** : les données seront authentifiées mais non cryptées. Par défaut, cette option est active.
Élevée	**Charge utile de sécurité d'encapsulation (ESP)** : la charge utile (les données) sera cryptée et authentifiée. Vous pouvez choisir un algorithme de cryptage : DES, 3DES et AES.
ID local	Spécifiez un identifiant local à utiliser pour le paramétrage des appels entrants dans le profil d'interconnexion de LAN. Cette information est facultative.

Fonction de rappel automatique

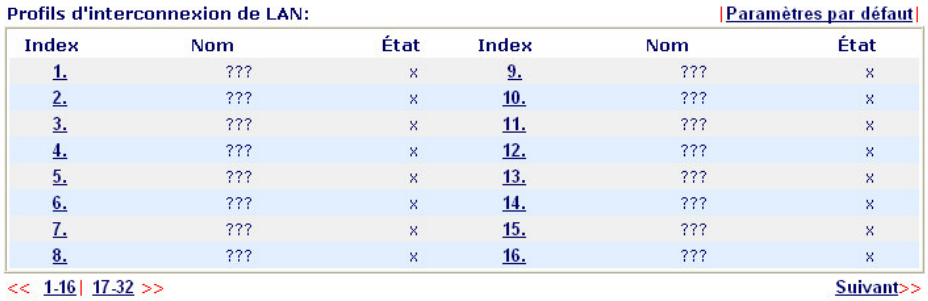
La fonction de rappel automatique n'est applicable qu'aux appels entrants RNIS. Le coût de la connexion est facturé au propriétaire du routeur.

Cocher pour activer la fonction de rappel automatique	Active la fonction de rappel automatique.
Spécifier le numéro de rappel automatique	Cette option est destinée à renforcer la sécurité. Si elle est activée, le routeur rappelle UNIQUEMENT le **numéro de rappel automatique spécifié**.
Cocher pour activer le contrôle de crédit de rappel automatique	Par défaut, la fonction de rappel automatique comporte une limite de temps. Une fois le crédit de rappel automatique épuisé, le mécanisme de rappel automatique est désactivé automatiquement. **Crédit de rappel automatique (unité : minutes) :** spécifiez le crédit de rappel automatique de l'utilisateur distant. Ce crédit est diminué automatiquement à chaque connexion de rappel automatique.

9.2.7 Interconnexion de LAN

Vous pouvez gérer des interconnexions de LAN à l'aide d'une table de profils d'interconnexion. Vous pouvez définir des paramètres d'appel entrant ou sortant, des identifiants de connexion, des types de connexion (RNIS, VPN avec PPTP, tunnel IPSec, L2TP ou L2TP sur IPSec), les méthodes de sécurisation correspondantes, etc.

Le routeur Vigor permet de créer 32 profils, ce qui implique la prise en charge de 32 tunnels de VPN simultanés. La table des profils d'interconnexion de LAN est représentée ci-dessous.


Profils d'interconnexion de LAN: |Paramètres par défaut|

Index	Nom	État	Index	Nom	État
1.	???	x	9.	???	x
2.	???	x	10.	???	x
3.	???	x	11.	???	x
4.	???	x	12.	???	x
5.	???	x	13.	???	x
6.	???	x	14.	???	x
7.	???	x	15.	???	x
8.	???	x	16.	???	x

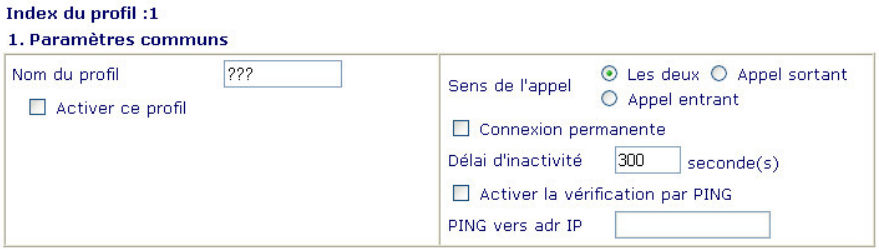
<< 1-16 | 17-32 >> Suivant>>

Profils d'interconnexion de LAN

Paramètres par défaut	Cliquez pour effacer tous les numéros d'index.
Nom	Affiche le nom du profil d'interconnexion de LAN. ??? signifie que le profil est vide.
État	Affiche l'état du profil. V indique que le profil est actif, X indique que le profil est inactif.

Cliquez sur chaque numéro d'index pour éditer un profil d'interconnexion de LAN. Chaque profil d'interconnexion de LAN comprend 4 sous-groupes de paramètres. Pour le sous-groupe Type d'appel entrant, il faut remplir les différents champs correspondants à droite. Si les champs sont grisés, c'est que vous pouvez les laisser tels que. L'explication suivante vous aidera à remplir les champs nécessaires.

Paramètres communs

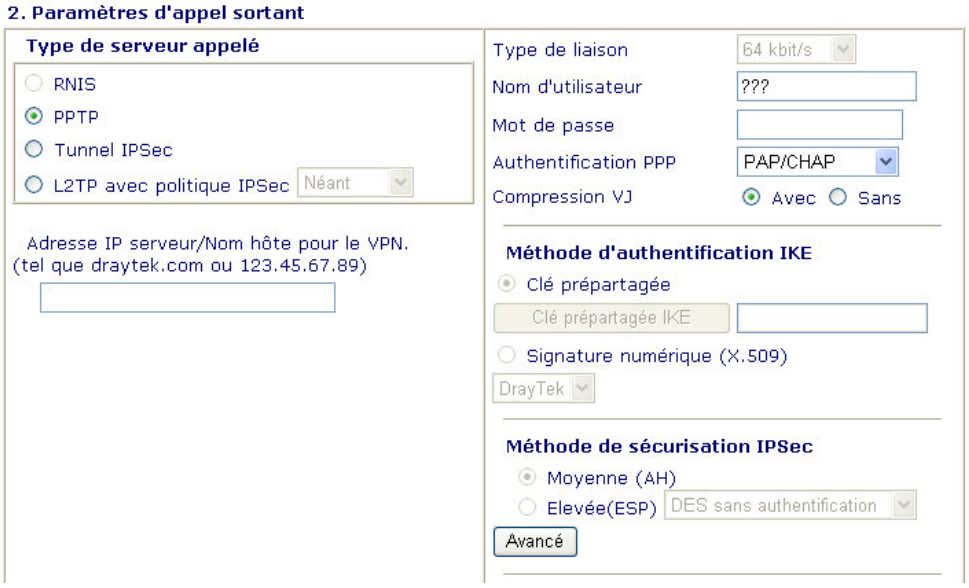


Nom du profil	Spécifiez un nom pour le profil d'interconnexion de LAN.
Activer ce profil	Cochez cette case pour activer le profil.
Sens de l'appel	Spécifiez le sens des appels pour ce profil d'interconnexion de LAN. **Les deux** : appels sortants et entrants **Sortants** : appels sortants seulement **Entrants :** appels entrants seulement.
Connexion permanente ou délai d'inactivité	**Connexion permanente :** cochez cette case pour que le routeur maintienne la connexion de VPN en permanence. **Délai d'inactivité :** la valeur par défaut est 300 secondes. Si la connexion est restée inactive jusqu'à l'expiration du délai d'inactivité, le routeur la libère.
Vérification par PING	Cette fonction permet au routeur de déterminer l'état de la connexion de VPN IPSec. Elle est particulièrement utile en cas d'interruption anormale du tunnel IPSec. Pour plus de détails, reportez-vous aux nota ci-dessous. Cochez cette case pour autoriser la transmission de paquets PING à une adresse IP spécifiée. **PING vers IP :** entrez l'adresse IP de l'hôte distant situé à l'autre extrémité du tunnel de VPN.

Activer la vérification par PING : option utilisée pour traiter les interruptions anormales de connexions de VPN IPSec. Cette option permet de connaître l'état d'une connexion de VPN et d'apprécier l'opportunité de la rétablir.

Normalement, si l'un des homologues VPN veut libérer la connexion, il doit échanger des paquets avec l'autre pour l'informer. Toutefois, si l'homologue distant libère la connexion sans préavis, le routeur Vigor ne s'en apercevra pas. Pour résoudre ce problème, le routeur Vigor vérifie l'état de la connexion de VPN en envoyant continuellement des paquets PING à l'hôte distant.

Paramètres d'appel sortant



Type de serveur appelé	Sélectionnez l'un des quatre types suivants. **RNIS :** établissement d'une connexion RNIS sortante avec le serveur. Vous devez paramétrer le type de liaison ainsi que le nom d'utilisateur et le mot de passe pour l'authentification du serveur distant. Vous pouvez également paramétrer la fonction de rappel automatique (CBCP). **PPTP :** établissement d'une connexion de VPN PPTP avec le serveur via l'internet. Vous devez spécifier le nom d'utilisateur et le mot de passe pour authentifier le serveur distant. **Tunnel IPSec :** établissement d'une connexion de VPN IPSec avec le serveur via l'internet. **L2TP :** établissement d'une connexion de VPN L2TP via l'internet. Vous pouvez sélectionner L2TP seul ou L2TP avec IPSec. ➢ **Néant :** ne pas appliquer la politique IPSec. En conséquence, la connexion de VPN L2TP sans politique IPSec peut être considérée comme une connexion L2TP pure. ➢ **Souhaitée :** appliquer d'abord la politique IPSec si elle est applicable lors de la négociation. Sinon, la connexion de VPN devient une connexion L2TP pure. ➢ **Imposée :** appliquer systématiquement à la connexion L2TP.

	Vous devez spécifier le nom d'utilisateur et le mot de passe pour l'authentification du serveur distant.
Nom d'utilisateur	Ce champ est applicable si vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. Il l'est également si vous sélectionnez RNIS.
Mot de passe	Ce champ est applicable si vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. Il l'est également si vous sélectionnez RNIS.
Authentification PPP	Ce champ est applicable si vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. Il l'est également si vous sélectionnez RNIS. Normalement PAP/CHAP assure la compatibilité la plus large.
Compression VJ	Ce champ est applicable si vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. Il l'est également si vous sélectionnez RNIS. La compression VJ est utilisée pour la compression de l'en-tête de protocole TCP/IP. Normalement **Oui** pour améliorer l'utilisation de la bande passante.
Numéro d'appel pour le RNIS ou adresse IP de serveur/nom d'hôte pour le VPN	Vous devez spécifier l'adresse IP du serveur de VPN distant ou le nom d'hôte. Tapez le numéro RNIS d'homologue si vous sélectionnez RNIS. Par ailleurs, vous devez spécifier les méthodes de sécurisation correspondantes à droite.

Méthode d'authentification IKE

Ce champ est applicable aux tunnels IPSec et à L2TP avec politique IPSec.

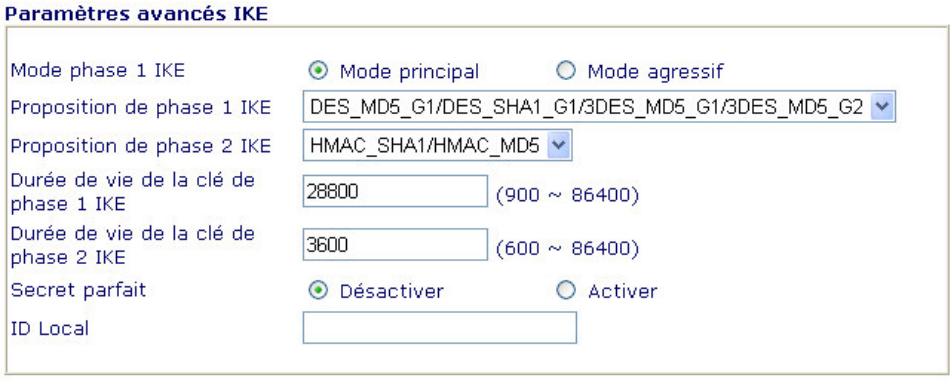
Clé prépartagée	Entrez une clé prépartagée (1 à 63 caractères).
Signature numérique (X.509)	Sélectionnez une signature numérique préétablie dans les profils d'ID homologue X.509.

Méthode de sécurisation IPSec

Ce champs est obligatoire pour les tunnels IPSec et pour L2TP avec politique IPSec.

Moyenne	**En-tête d'authentification (AH)** : les données seront authentifiées mais non cryptées. Par défaut, cette option est active.
Élevée	**Charge utile de sécurité d'encapsulation (ESP)** : la charge utile (les données) sera cryptée et authentifiée. Sélectionner un algorithme de cryptage : **DES sans authentification :** utiliser l'algorithme de cryptage DES sans authentification. **DES avec authentification :** utiliser l'algorithme de cryptage DES avec authentification. **3DES sans authentification :** utiliser l'algorithme de cryptage 3DES sans authentification. **3DES avec authentification :** utiliser l'algorithme de cryptage 3DES et appliquer l'algorithme d'authentification MD5 ou SHA-1. **AES sans authentification :** utiliser l'algorithme de cryptage AES sans authentification. **AES avec authentification :** utiliser l'algorithme de cryptage AES et appliquer l'algorithme d'authentification MD5 ou SHA-1.

La fenêtre des paramètres avancés est représentée ci-dessous.



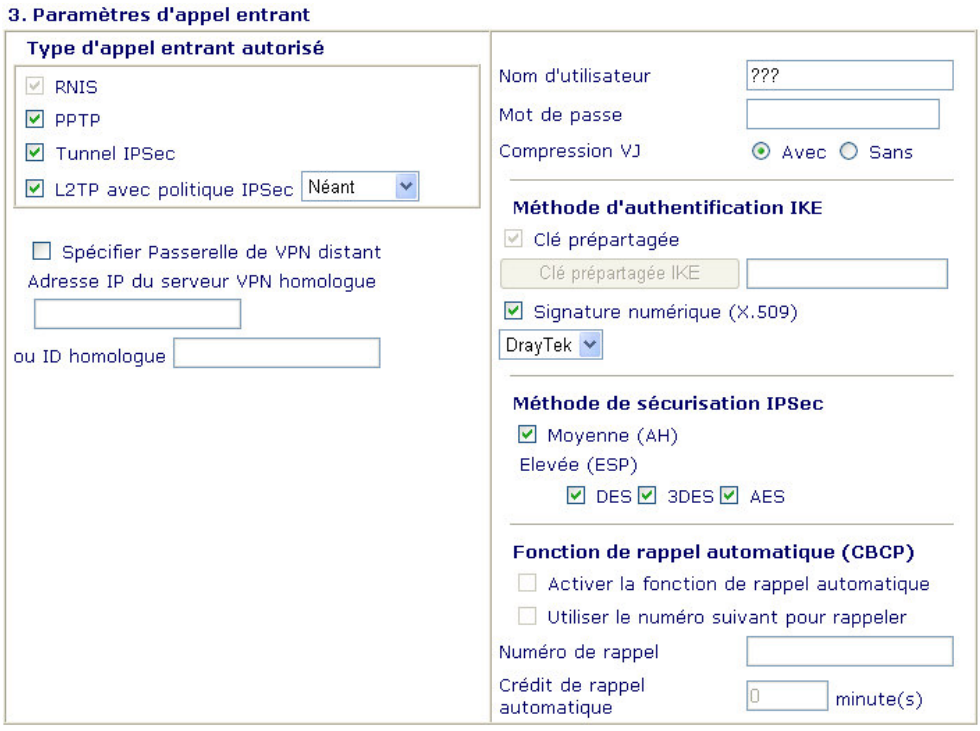
Avancé	Spécifiez le mode, la proposition et la durée de vie des clés pour chaque phase IKE. **Mode phase 1 IKE :** mode principal et mode agressif. Il s'agit d'échanger des propositions de sécurisation pour créer un canal sécurisé. Le mode principal est plus sûr que le mode agressif car les échanges sont plus nombreux dans un canal sécurisé pour établir une session IPSec. Toutefois, le mode agressif est plus rapide. Le mode par défaut est le mode principal. **Proposition de phase 1 IKE :** proposer aux homologues de VPN les mécanismes d'authentification et algorithmes de cryptage locaux et obtenir un retour pour trouver une correspondance. Il existe deux options pour le mode agressif et neuf options pour le mode principal. Nous suggérons de choisir l'option qui couvre le plus grand nombre d'algorithmes **Proposition de phase 2 IKE :** proposer aux homologues de VPN les algorithmes disponibles locaux et obtenir un retour pour trouver une correspondance. Il existe trois options pour les deux modes. Nous suggérons de choisir l'option qui couvre le plus grand nombre d'algorithmes. **Durée de vie de la clé de phase 1 IKE :** pour des raisons de sécurité, la durée de vie de la clé doit être définie. La valeur par défaut est de 28800 secondes. Vous pouvez spécifier une valeur comprise entre 900 et 86400 secondes. **Durée de vie de la clé de phase 2 IKE :** pour des raisons de sécurité, la durée de vie de la clé doit être définie. La valeur par défaut est de 3600 seconds. Vous pouvez spécifier une valeur comprise entre 600 et 86400 secondes **Secret parfait (PFS) :** la clé de phase 1 IKE est réutilisée pour éviter la complexité des calculs de la phase 2. Par défaut, cette fonction est inactive. **ID local :** en mode agressif, l'ID local est l'adresse IP qui sert pour l'authentification avec le serveur de VPN distant.

Fonction de rappel automatique (modèles I)

La fonction de rappel automatique fournit un service de rappel automatique pour les utilisateurs distants RNIS dans le cadre du protocole PPP. Le coût de la connexion est facturé au propriétaire du routeur.

Demander à l'homologue distant de rappeler	Activez cette option pour que le routeur demande à l'homologue distant de rappeler.
Fournir le numéro RNIS à l'homologue distant	Dans le cas où l'homologue distant demande au routeur Vigor de rappeler, le numéro RNIS local est fourni à l'homologue distant. Cliquez ici pour que le routeur Vigor envoie le numéro RNIS au routeur distant.

Paramètres d'appel entrant



Type d'appel entrant autorisé	**RNIS :** Permet d'établir une connexion RNIS. Vous pouvez également paramétrer la fonction de rappel automatique. Vous devez spécifier le nom d'utilisateur et le mot de passe de l'utilisateur distant.

	PPTP : Permet à l'utilisateur distant d'établir une connexion de VPN PPTP via l'internet. Vous devez spécifier le nom de l'utilisateur et le mot de passe de l'utilisateur distant. **Tunnel IPSec :** Permet à l'utilisateur distant d'établir une connexion de VPN IPSec via l'internet. **L2TP:** Permet à l'utilisateur distant d'établir une connexion de VPN L2TP via l'internet. Vous pouvez sélectionner L2TP ou L2TP sur IPSec. ➢ **Néant :** ne pas appliquer la politique IPSec. En conséquence, la connexion de VPN L2TP sans politique IPSec peut être considérée comme une connexion L2TP pure. ➢ **Souhaitée :** appliquer d'abord la politique IPSec si elle est applicable pendant la négociation. Sinon, la connexion de VPN devient une connexion L2TP pure. ➢ **Imposée :** appliquer systématiquement la politique IPSec à la connexion L2TP. Vous devez spécifier le nom de l'utilisateur et le mot de passe de l'utilisateur distant.
Nom d'utilisateur	Ce champ est applicable lorsque vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. Il l'est également si vous sélectionnez RNIS.
Mot de passe	Ce champ est applicable lorsque vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. Il l'est également si vous sélectionnez RNIS.
Compression VJ	La compression VJ est utilisée pour la compression de l'en-tête de protocole TCP/IP. Ce champ est applicable lorsque vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. Il l'est également si vous sélectionnez RNIS.
Spécifier le CLID RNIS ou le numéro RNIS d'homologue de passerelle de VPN ou l'adresse IP du serveur de VPN homologue	**Cocher la case :** vous pouvez spécifier l'adresse IP de l'utilisateur distant ou l'identifiant d'homologue. Si vous avez sélectionné RNIS, tapez le numéro RNIS d'homologue. Vous devez également spécifier les méthodes de sécurisation correspondantes à droite. **Décocher la case :** le type de connexion que vous avez sélectionné plus haut appliquera les méthodes d'authentification et de sécurisation définies dans les Paramètres généraux.

Méthode d'authentification IKE

Ce groupe de champs est applicable aux tunnels IPSec et à L2TP avec politique IPSec **lorsque vous spécifiez le CLID RNIS, un numéro RNIS d'homologue de passerelle de VPN distante ou une adresse IP de serveur de VPN d'homologue**. La seule exception est la signature numérique (X.509) que vous pouvez spécifier lorsque vous sélectionnez le mode tunnel IPSec avec ou sans le CLID ou l'adresse IP du nœud distant.

Clé prépartagée	Entrez une clé prépartagée (1 à 63 caractères).
Signature numérique (X.509)	Sélectionnez une signature numérique préétablie dans les profils d'ID homologue X.509.

Méthode de sécurisation IPSec

Ce groupe de champs est obligatoire pour les tunnels IPSec et pour L2TP avec politique IPSec lorsque vous spécifiez le nœud distant.

Moyenne	**En-tête d'authentification (AH)** : les données seront authentifiées mais non cryptées. Par défaut, cette option est active.
Élevée	**Charge utile de sécurité d'encapsulation (ESP)** : la charge utile (les données) sera cryptée et authentifiée. Vous pouvez choisir un algorithme de cryptage : DES, 3DES et AES.

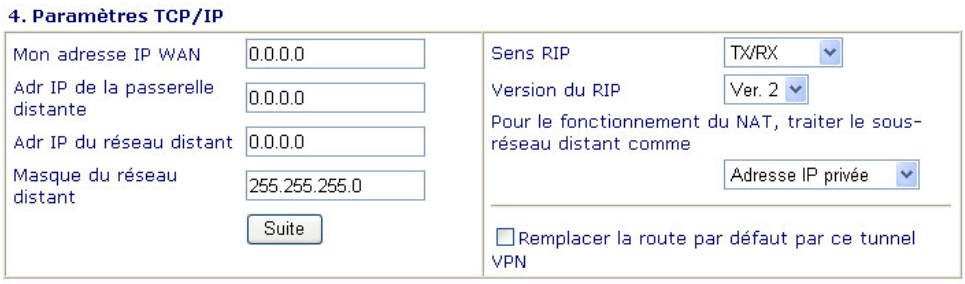
Fonction de rappel automatique

La fonction de rappel automatique n'est applicable qu'aux appels entrants RNIS. Le coût de la connexion est facturé au propriétaire du routeur.

Cocher pour activer la fonction de rappel automatique	Active la fonction de rappel automatique.
Spécifier le numéro de rappel automatique	Cette option est destinée à renforcer la sécurité. Si elle est activée, le routeur rappelle UNIQUEMENT le **numéro de rappel automatique spécifié**.

Cocher pour activer le contrôle de crédit de rappel automatique	Par défaut, la fonction de rappel automatique comporte une limite de temps. Une fois le crédit de rappel automatique épuisé, le mécanisme de rappel automatique est désactivé automatiquement. **Crédit de rappel automatique (unité : minutes) :** spécifiez le crédit de rappel automatique de l'utilisateur distant. Ce crédit est diminué automatiquement à chaque connexion de rappel automatique. Avec la valeur par défaut 0, la période de rappel automatique n'est pas limitée.

Paramètres TCP/IP

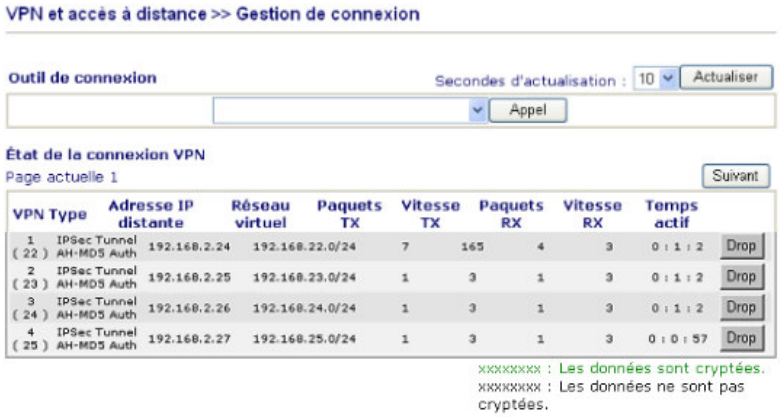


Mon adresse IP WAN	Ce champ est applicable uniquement lorsque vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. La valeur par défaut est 0.0.0.0. Le routeur Vigor obtient une adresse IP WAN du routeur distant pendant la phase de négociation IPCP. Si l'adresse IP WAN est fixée par le routeur distant, spécifiez ici l'adresse IP fixe.
Ad. IP de la passerelle distante	Ce champ est applicable uniquement lorsque vous sélectionnez PPTP ou L2TP avec ou sans politique IPSec. La valeur par défaut est 0.0.0.0. Le routeur Vigor obtient une adresse IP de passerelle distante du routeur distant pendant la phase de négociation IPCP. Si l'adresse IP de WAN est fixée par le routeur distant, spécifiez ici l'adresse IP fixe.
Adr. IP du réseau distant/Masque du réseau distant	Ajoute un routeur statique pour aiguiller tout le trafic destiné à cette adresse IP de réseau distant ou à ce masque de réseau distant via la connexion de VPN.

Suite	Ajoute un routeur statique pour aiguiller tout le trafic destiné à cette adresse IP de réseau distant ou à ce masque de réseau distant via la connexion de VPN. Généralement utilisé lorsqu'il y a plusieurs sous-réseaux derrière le routeur de VPN distant.
Sens RIP	L'option spécifie le sens des paquets RIP (Routing Information Protocol). Vous pouvez activer/désactiver l'un des sens. Il y a quatre options : TX/RX, TX seulement, RX seulement et Désactiver.
Version du RIP	Sélectionnez la version du protocole RIP. Spécifiez Ver. 2 pour que la compatibilité soit la plus large possible.
Pour le fonctionnement du NAT, traiter le sous-réseau distant comme	Lorsqu'il communique avec le sous-réseau distant, le routeur peut le traiter comme un sous-réseau privé envoyant des paquets avec l'adresse IP¨privée du routeur ou le traiter comme un sous-réseau public envoyant des paquets avec l'adresse IP publique du routeur.

9.2.8 Gestion des connexions

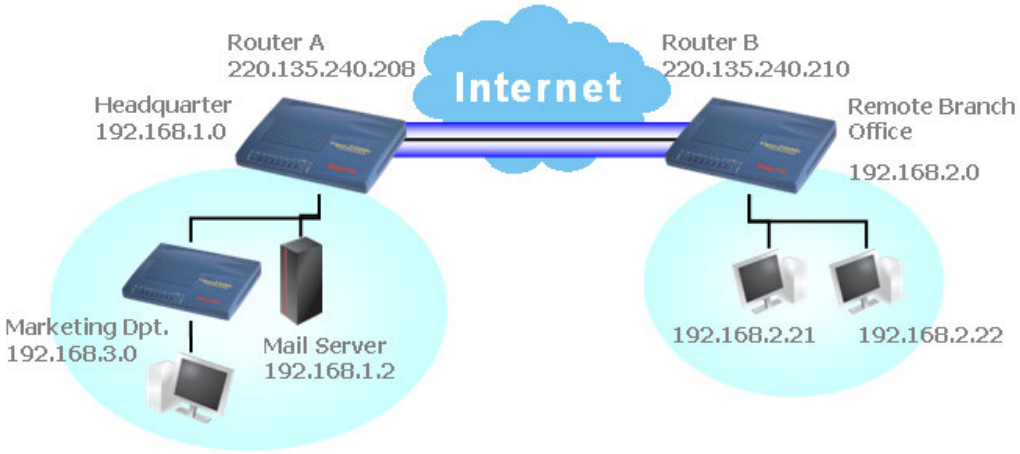
Le tableau récapitulatif de toutes les connexions de VPN est donné ci-dessous. Vous pouvez libérer n'importe quelle connexion de VPN en cliquant sur le bouton Suppr. Vous pouvez également utiliser l'outil d'appel sortant et cliquez sur le bouton Appel.



9.2.9 Exemples

Création d'une interconnexion de LAN entre un établissement secondaire et le siège

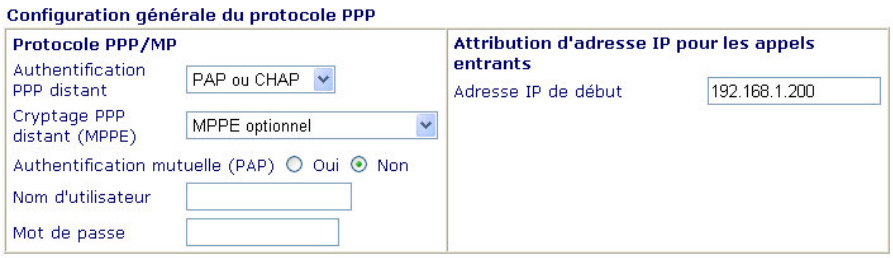
Vous pouvez vouloir établir une connexion sécurisée entre un établissement secondaire et le siège. Selon la structure de réseau illustrée ci-dessous, créez un profil d'interconnexion de LAN. Les deux réseaux (LAN) ne doivent pas avoir la même adresse réseau.



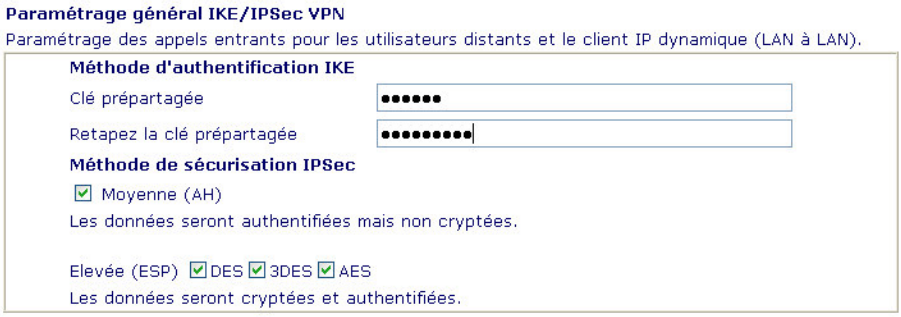
Router A	*Routeur A*
Router B	*Routeur B*
Headquarter	*Siège*
Remote Branch Office	*Établissement secondaire*
Marketing Dpt.	*Service marketing*
Mail Server	*Serveur de messagerie*

Paramétrage du routeur A au siège :

1. Sélectionnez **Contrôle d'accès à distance** pour activer le service de VPN nécessaire.
2. Puis,
   - ➢ Pour utiliser les services PPP comme PPTP, L2TP ou RNIS, définissez les paramètres généraux dans **Configuration générale PPP**.

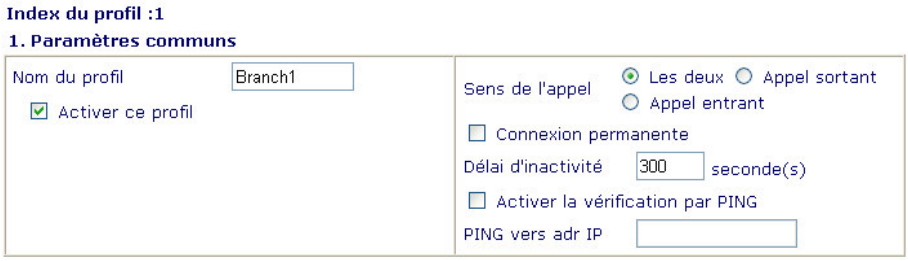


➢ Pour utiliser un service basé sur IPSec, comme IPSec ou L2TP avec politique IPSec, définissez les paramètres généraux dans **Configuration générale IPSec**, notamment la clé prépartagée connue des deux correspondants.



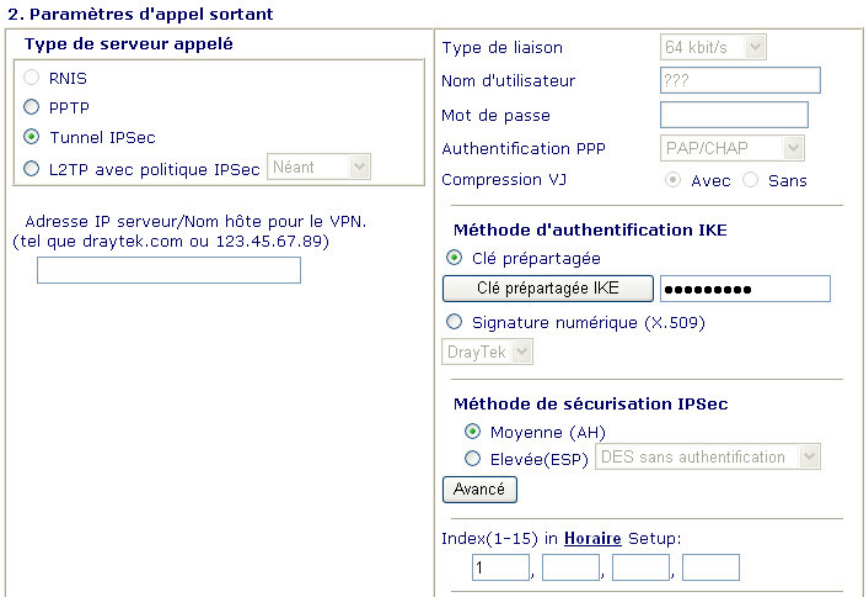
3. Sélectionnez **LAN à LAN**. Cliquez sur un numéro d'index pour éditer un profil.

4. Définissez les **Paramètres communs** comme indiqué ci-dessous. Vous devez activer les deux connexions de VPN car n'importe lequel des correspondants peut déclencher la connexion de VPN.

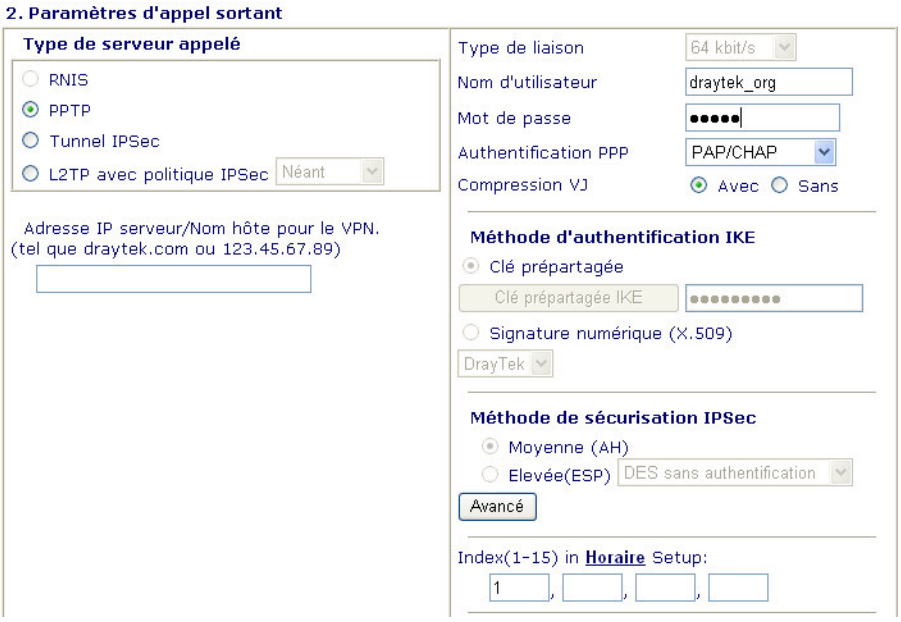


5. Définissez les paramètres d'appel sortant pour vous connecter en mode agressif au routeur B avec la méthode d'appel sortant sélectionnée.

➢ Si un service basé sur IPSec est sélectionné, vous devez également spécifier l'adresse IP d'homologue distant, la méthode d'authentification IKE et la méthode de sécurisation IPSec pour cette connexion sortante.



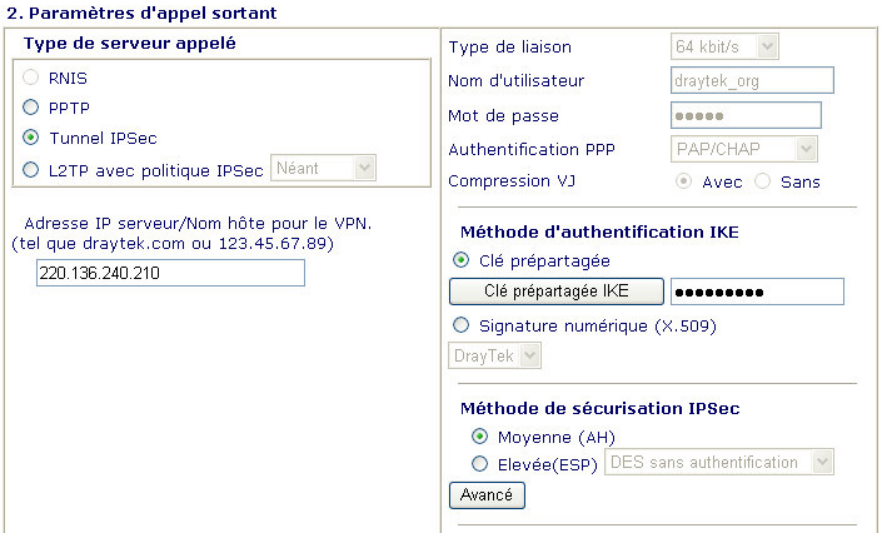
➢ Si un service basé sur PPP est sélectionné, vous devez également spécifier l'adresse IP de l'homologue distant, le nom d'utilisateur, le mot de passe, l'authentification PPP et la compression VJ pour cette connexion sortante.



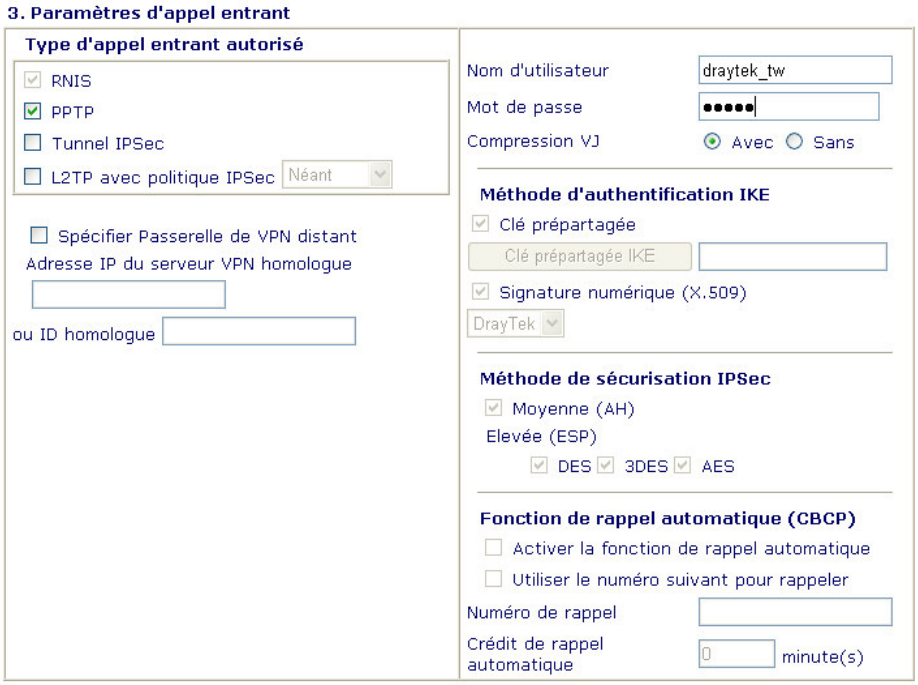
6. Définissez les paramètres d'appel entrant pour permettre au routeur B d'appeler la connexion de VPN.

➢ Si un service basé sur IPSec est sélectionné, vous pouvez également spécifier l'adresse IP d'homologue distant, la méthode d'authentification IKE et la méthode de sécurisation IPSec pour

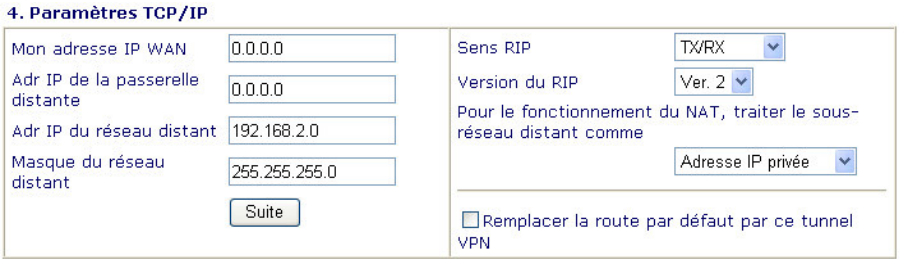
cette connexion entrante. Autrement, les **paramètres généraux IPSec** seront appliqués.



➢ Si un service basé sur PPP est sélectionné, vous devez également spécifier l'adresse IP d'homologue distant, le nom de l'utilisateur, le mot de passe et la compression VJ pour cette connexion entrante.

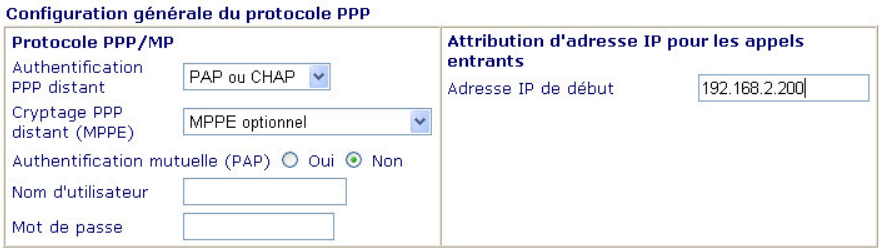


7. Enfin, spécifiez l'adresse IP de réseau distant et le sous-réseau dans les **Paramètres de réseau TCP/IP** pour que le routeur A puisse aiguiller les paquets destinés au réseau distant vers le routeur B via la connexion de VPN.

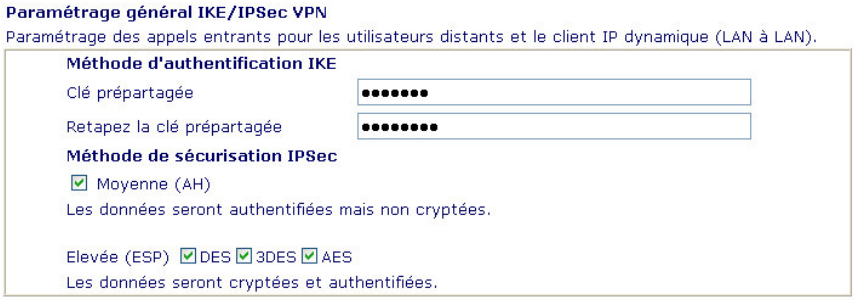


Paramétrage du routeur B de l'établissement secondaire :

8. Sélectionnez **Contrôle d'accès à distance** pour activer le service de VPN nécessaire.
9. Puis,
   - Pour utiliser les services PPP comme PPTP, L2TP ou RNIS, définissez les paramètres généraux dans **Configuration générale PPP**.

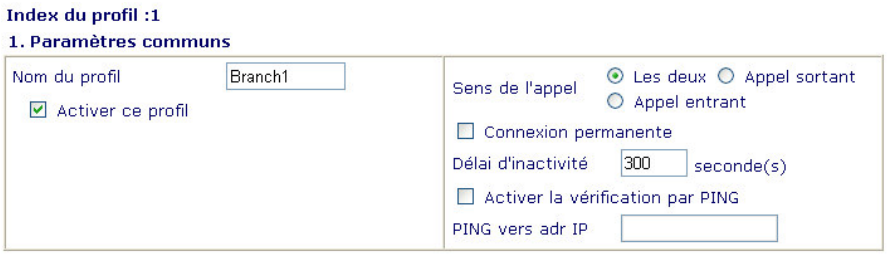


   - Pour utiliser un service basé sur IPSec, comme IPSec ou L2TP avec politique IPSec, définissez les paramètres généraux dans **Configuration générale IPSec**, notamment la clé prépartagée connue des deux correspondants.



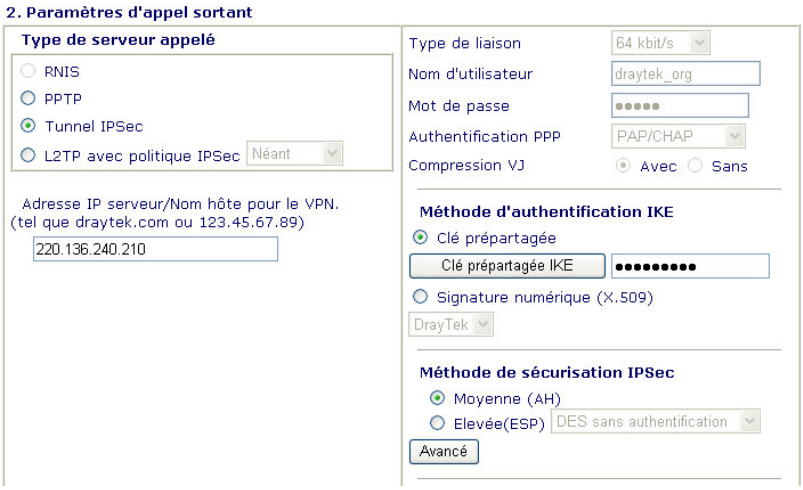
10. Sélectionnez **LAN à LAN**. Cliquez sur un numéro d'index pour éditer un profil.

11. Définissez les **Paramètres communs** comme indiqué ci-dessous. Vous devez activer les deux connexions de VPN car n'importe lequel des correspondants peut déclencher la connexion de VPN.

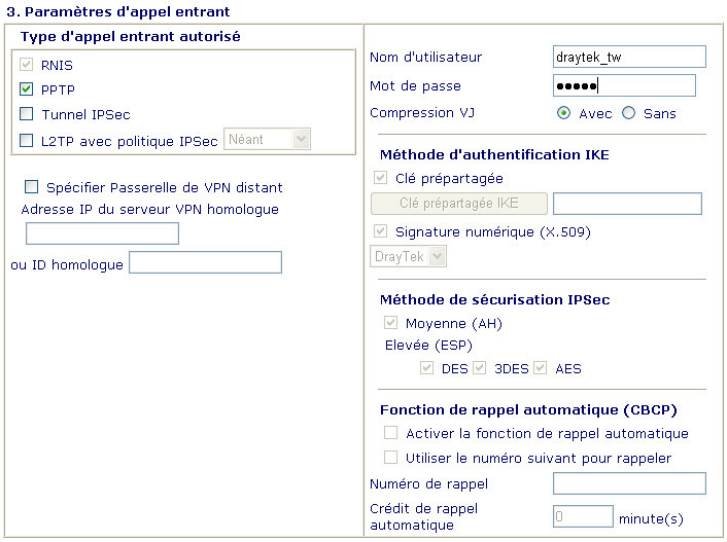


12. Définissez les paramètres d'appel sortant pour vous connecter en mode agressif au routeur B avec la méthode d'appel sortant sélectionnée.

- Si un service basé sur IPSec est sélectionné, vous devez également spécifier l'adresse IP d'homologue distant, la méthode d'authentification IKE et la méthode de sécurisation IPSec pour cette connexion sortante.

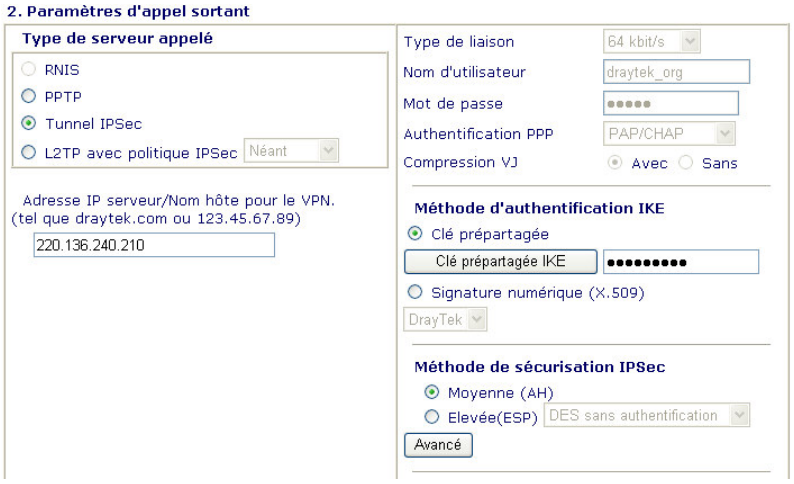


- Si un service basé sur PPP est sélectionné, vous devez également spécifier l'adresse IP de l'homologue distant, le nom d'utilisateur, le mot de passe, l'authentification PPP et la compression VJ pour cette connexion sortante.

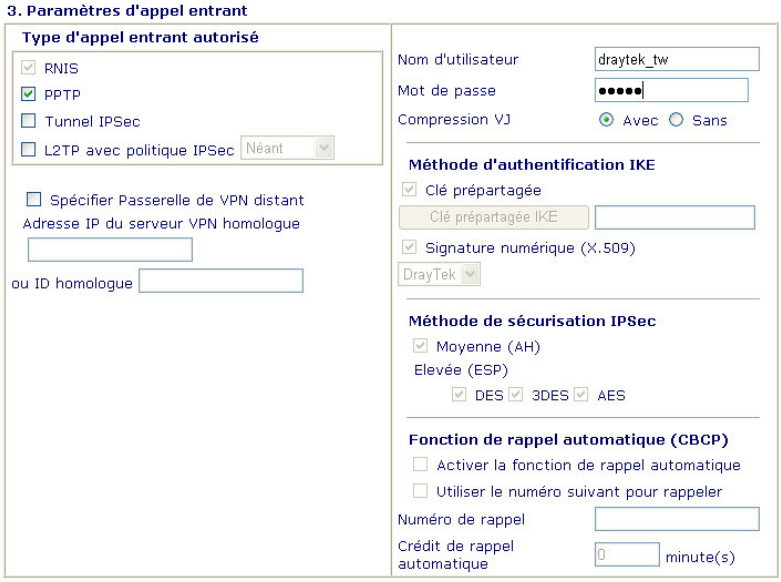


13. Définissez les paramètres d'appel entrant pour permettre au routeur B d'appeler la connexion de VPN.

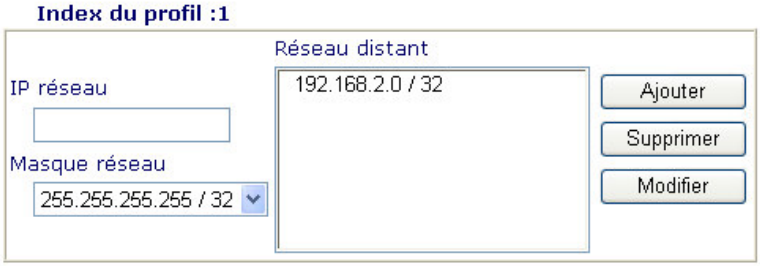
- Si un service basé sur IPSec est sélectionné, vous pouvez également spécifier l'adresse IP d'homologue distant, la méthode d'authentification IKE et la méthode de sécurisation IPSec pour cette connexion entrante. Autrement, les **paramètres généraux IPSec** seront appliqués.



➢ Si un service basé sur PPP est sélectionné, vous devez également spécifier l'adresse IP d'homologue distant, le nom de l'utilisateur, le mot de passe et la compression VJ pour cette connexion entrante.

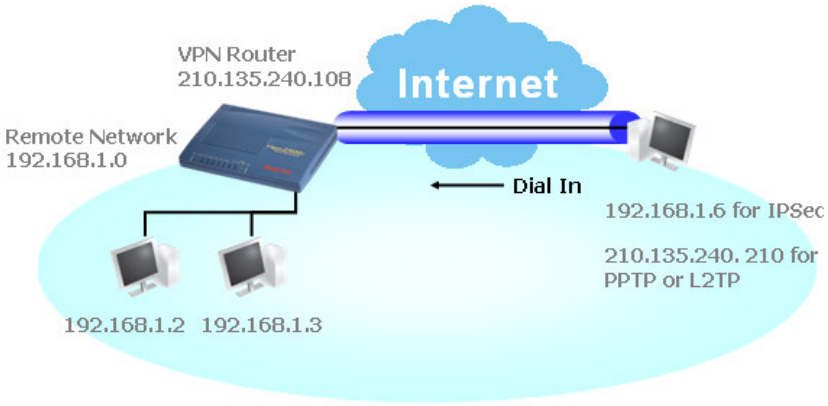


14. Enfin, spécifiez l'adresse IP de réseau distant et le sous-réseau dans les **Paramètres de réseau TCP/IP** pour que le routeur B puisse aiguiller les paquets destinés au réseau distant vers le routeur A via la connexion de VPN.



Création d'une connexion d'utilisateur distant entre télétravailleur et siège

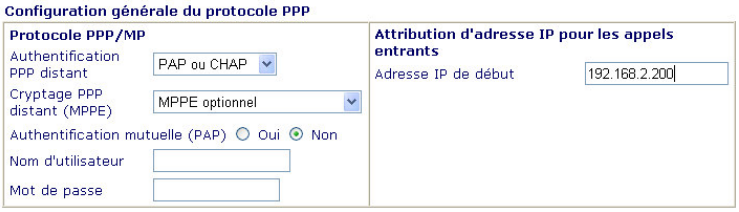
Autre cas courant, un télétravailleur veut se connecter au réseau d'entreprise en toute sécurité. Selon la structure de réseau, vous pouvez créer un profil d'utilisateur distant et installez le client de VPN intelligent sur l'hôte distant.



VPN Router	*Routeur de VPN*
Remote Network	*Réseau distant*
Dial In	*Appel entrant*
192.168.1.6 for IPSec	*192.168.1.6 pour IPSec*
210.135.240.210 for PPTP or L2TP	*210.135.240.210 pour PPTP ou L2TP*

Paramétrage du routeur de VPN au siège :

1. Sélectionnez **Contrôle d'accès à distance** pour activer le service de VPN nécessaire.
2. Puis,
   - Pour utiliser les services PPP comme PPTP, L2TP ou RNIS, définissez les paramètres généraux dans **Configuration générale PPP**.

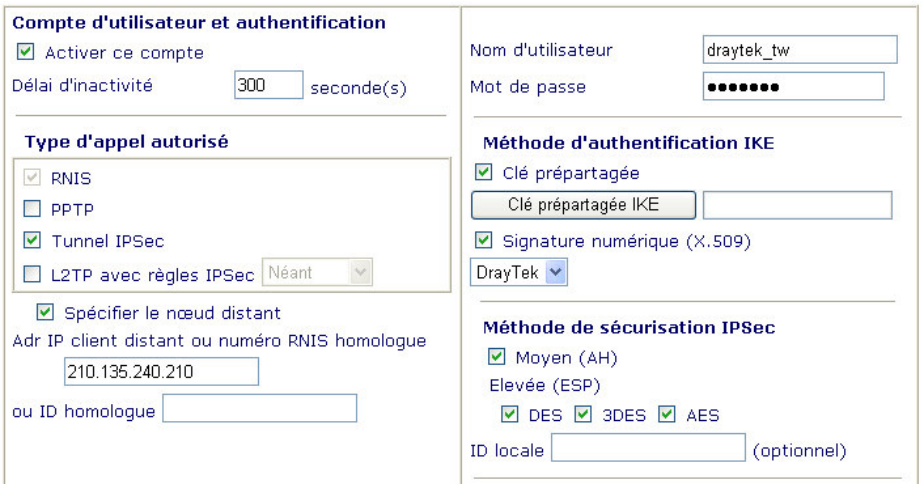


   - Pour utiliser un service basé sur IPSec, comme IPSec ou L2TP avec politique IPSec, définissez les paramètres généraux dans **Configuration générale IPSec**, notamment la clé prépartagée connue des deux correspondants.

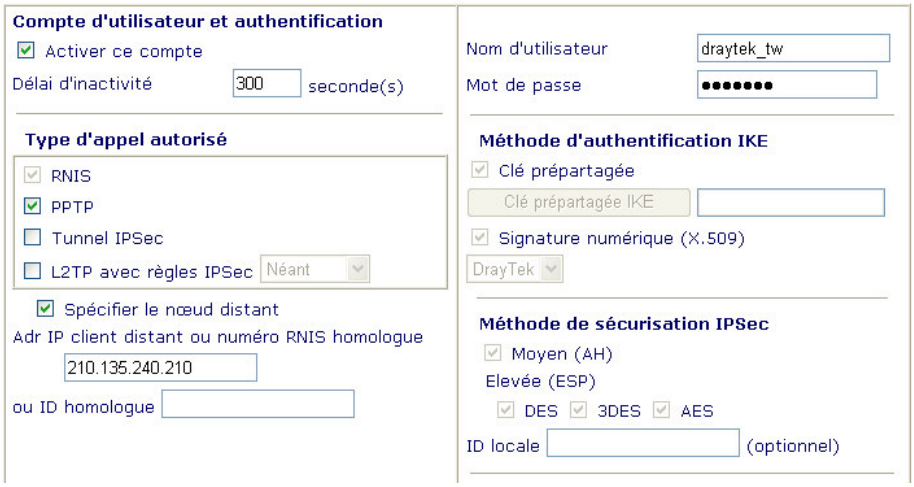
3. Sélectionnez **Comptes d'appel entrant**. Cliquez sur un numéro d'index pour éditer un profil.

4. Définissez les paramètres d'appel entrant pour permettre à l'utilisateur distant d'établir la connexion de VPN.

➢ Si un service basé sur IPSec est sélectionné, vous pouvez également spécifier l'adresse IP d'homologue distant, la méthode d'authentification IKE et la méthode de sécurisation IPSec pour cette connexion entrante. Autrement, les **paramètres généraux IPSec** seront appliqués.

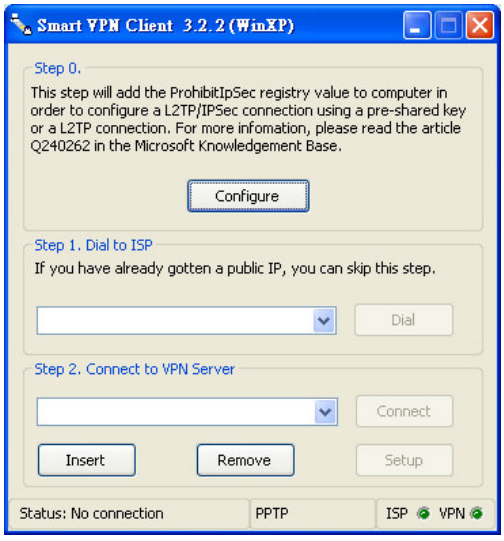


➢ Si un service basé sur PPP est sélectionné, vous devez également spécifier l'adresse IP d'homologue distant, le nom de l'utilisateur, le mot de passe et la compression VJ pour cette connexion entrante.



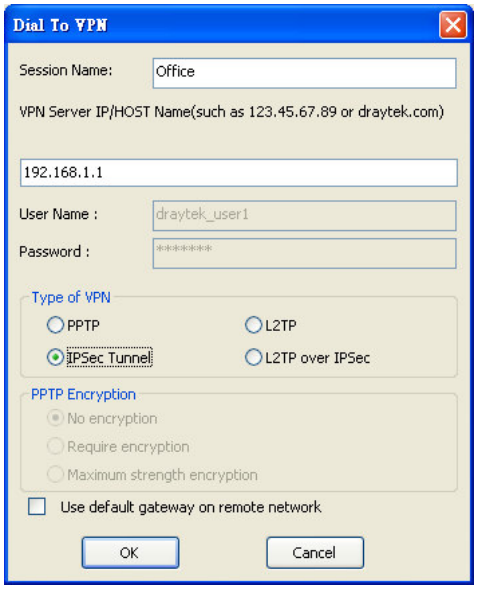
Paramétrage de l'hôte distant :

5. Dans le cas de Win98/ME, vous pouvez utiliser « Accès réseau à distance » pour créer le tunnel PPTP vers le routeur Vigor. Dans le cas de Win2000/XP, utilisez « Network and Dial-up connections » ou « Smart VPN Client » pour vous aider à créer un tunnel pour PPTP, L2TP et L2TP sur IPSec. Vous trouverez ce logiciel complémentaire sur le CD-ROM ou au centre de téléchargement www.draytek.com. Procédez à l'installation en suivant les instructions.
6. Après l'installation, vous devez cliquer sur le bouton **Étape 0. Configurer**. Redémarrez l'hôte.

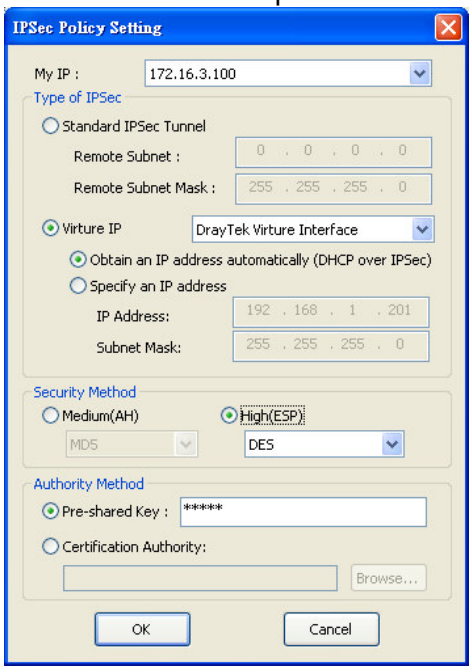


7. Dans l'**Étape 2. Se connecter au serveur de VPN**, cliquez sur le bouton **Insérer** pour ajouter une nouvelle entrée.

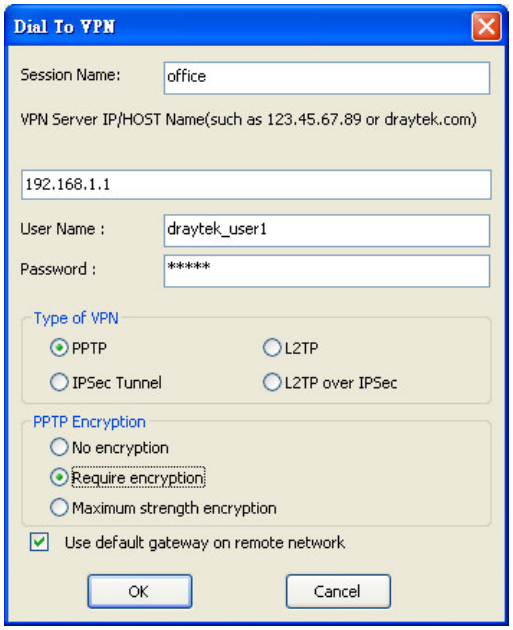
➢ Si un service basé sur IPSec est sélectionné comme indiqué ci-dessous,



Vous pouvez également spécifier la méthode que vous utilisez pour obtenir l'adresse IP, la méthode de sécurisation et la méthode d'authentification. Si la clé prépartagée est sélectionnée, elle doit concorder avec celle paramétrée dans le routeur de VPN.



➢ Si un service basé sur PPP est sélectionné, vous devez également spécifier l'adresse IP du serveur de VPN distant, le nom de l'utilisateur, le mot de passe et la méthode de cryptage. Le nom d'utilisateur et le mot de passe doivent concorder avec ceux paramétrés dans le routeur de VPN. Si vous utilisez la passerelle par défaut sur le réseau distant, tous les paquets de l'hôte distant seront aiguillés vers le serveur de VPN, puis transmis à l'internet. L'hôte distant semblera fonctionner au sein du réseau d'entreprise.



8. Cliquez sur le bouton **Se connecter** pour établir la connexion. Lorsque la connexion est établie, vous verrez un voyant vert dans l'angle inférieur droit.

Chapitre 10
Paramètres RNIS

10.1 Introduction

Ce chapitre traite **des paramètres RNIS, de la connexion à un seul FAI, de la connexion à deux FAI, du TA virtuel (CAPI) et des paramètres de contrôle d'appel et PPP/MP.**

10.2 Paramètres

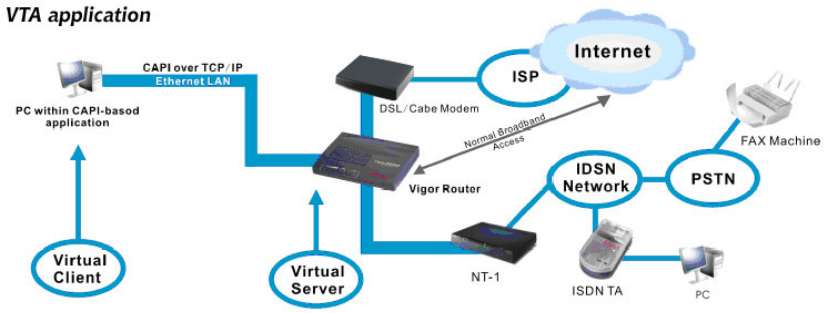
Cliquez sur **Paramétrage des applications** pour ouvrir la page de paramétrage.

Connexion à un ou deux FAI

Sélectionnez **Connexion à un seul FAI** si vous accédez à l'internet par l'intermédiaire d'un seul FAI. Sélectionnez **Connexion à deux FAI** si vous avez deux FAI. Vous pourrez vous connecter simultanément aux deux FAI. Cette fonction est utilisée principalement pour les FAI qui ne prennent pas en charge le protocole PPP multilien (ML-PPP). Dans un tel cas, la connexion à deux FAI peut porter le débit des canaux RNIS à 128 kbit/s.

TA virtuel

L'adaptateur de terminal virtuel (TA virtuel) est un logiciel « CAPI » qui peut simuler un adaptateur de terminal RNIS installé sur votre ordinateur. Vous pouvez installer le logiciel CAPI pour des applications d'accès commuté, de télécopie ou de téléphonie, selon les fonctionnalités du logiciel installé. Pour utiliser la fonctionnalité TA virtuel, téléchargez les pilotes VTA (disponibles uniquement pour Windows 98SE/2000/XP) à l'adresse http://www.draytek.com/support/download.php. Lorsqu'un hôte local ou un PC du réseau utilise un logiciel CAPI courant, comme RVS-COM ou BVRP, pour accéder au routeur, il peut fonctionner comme un TA RNIS local pour envoyer ou recevoir des télécopies sur la ligne RNIS. C'est essentiellement un modèle de réseau client-serveur. Le serveur TA virtuel intégré gère l'établissement et la libération des connexions. Le client TA virtuel, qui est l'hôte ou le PC local, crée un pilote CAPI pour relayer les messages CAPI entre les applications et le module CAPI du routeur.



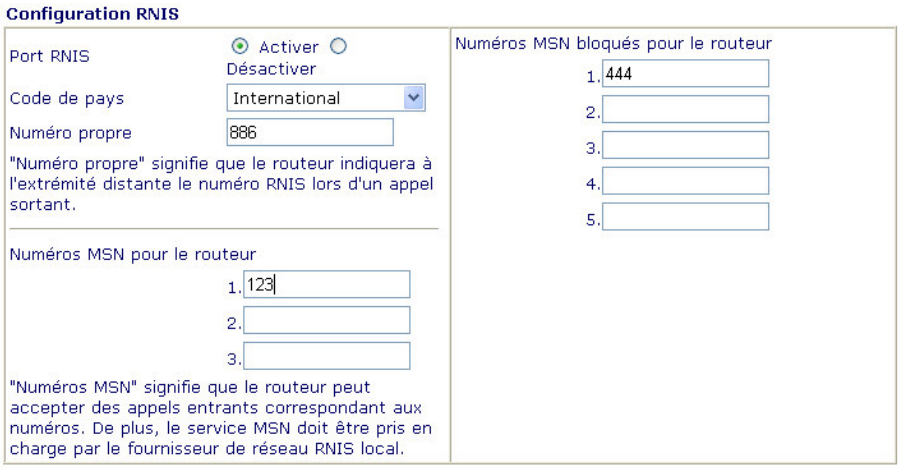
VTA application	*Application de TA virtuel*
CAPI over TCP/IP	*CAPI sur TCP/IP*
PC within CAPI-based application	*PC de l'application CAPI*
Virtual Client	*Client virtuel*
Virtual Server	*Serveur virtuel*
Vigor Router	*Routeur Vigor*
DSL/Cable Modem	*Modem DSL/câble*
ISP	*FAI*
FAX Machine	*Télécopieur*
PSTN	*RTPC*
ISDN Network	*Réseau RNIS*
ISDN TA	*TA RNIS*

Comme le montre le scénario d'application ci-dessus, le client TA virtuel peut appeler un télécopieur, un TA RNIS, etc. ou recevoir un appel. Cliquez sur **TA virtuel (CAPI distant)** dans **Installation rapide** pour configurer les fonctionnalités de TA virtuel.

Contrôle d'appel et PPP/MP

Certaines applications nécessitent que le routeur (seulement dans le cas des modèles RNIS) soit activé à distance ou puisse être connecté au FAI par l'intermédiaire de l'interface RNIS. Les routeurs Vigor permettent aux utilisateurs d'appeler le routeur et de lui demander de se connecter au FAI. Ainsi, un télétravailleur peut accéder au réseau distant pour utiliser des ressources. Bien sûr, il faut une adresse IP fixe pour la connexion WAN et exposer certaines ressources internes pour les utilisateurs distants (FTP, WWW).

10.2.1 Paramètres RNIS



Port RNIS

Cliquez sur **Activer** pour ouvrir le port RNIS et sur **Désactiver** pour le fermer.

Code du pays

Pour que le routeur fonctionne correctement sur votre réseau RNIS local, vous devez choisir le bon code de pays.

Numéro propre

Tapez votre numéro RNIS. À chaque appel sortant, le numéro sera envoyé au destinataire.

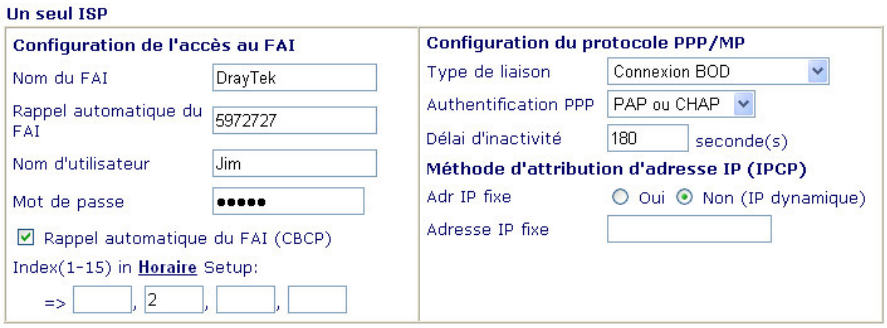
Numéros MSN bloqués pour le routeur

Tapez les numéros MSN dans les champs pour empêcher le routeur d'appeler ces numéros.

Numéros MSN pour le routeur

Le routeur accepte uniquement les appels entrants dont le numéro concorde. De plus, le fournisseur de réseau RNIS local doit prendre en charge les services MSN. Le routeur permet de spécifier trois numéros MSN. À noter que les services MSN doivent être fournis par vos opérateurs de télécommunications locaux. Par défaut, la fonction MSN est désactivée. Si vous laissez les champs vides, tous les appels entrants seront acceptés.

10.2.2 Connexion à un seul FAI et connexion à deux FAI



Configuration de l'accès au FAI

Nom du FAI	Tapez le nom de votre FAI.
Numéro d'appel	Tapez le numéro d'accès RNIS fourni par votre FAI.
Nom d'utilisateur	Tapez le nom d'utilisateur fourni par votre FAI.
Mot de passe	Tapez le mot de passe fourni par votre FAI.
Demander le rappel automatique (CBCP)	Si votre FAI prend en charge la fonction de rappel automatique, cochez cette case pour activer le protocole CBCP pendant la négociation PPP.
Plages horaires (1-15)	Entrez le numéro d'index des plages horaires pour contrôler l'accès à l'internet selon les plages horaires préconfigurées.

Configuration PPP/MP

Type de liaison	Tapez le nom de votre FAI. **Désactivation de la liaison :** désactivation de la connexion RNIS. **Connexion à 64 kbit/s :** utilisation d'un canal B RNIS pour l'accès à l'internet. **Connexion à 128 kbit/s :** utilisation des deux canaux B RNIS pour l'accès à l'internet. **Connexion BOD :** BOD signifie « bandwidth-on-demand » (bande passante à la demande). Le routeur utilise uniquement un canal B lorsque le trafic est faible. Lorsque le canal B arrive à saturation, l'autre canal B est activé automatiquement. Pour plus de détails sur le paramétrage BOD, se reporter à Configuration avancée > Paramétrage du contrôle d'appel et PPP/MP.
Authentification PPP	**PAP seulement :** configuration de la session PPP pour l'utilisation du protocole PAP pour la négociation du nom d'utilisateur et du mot de passe avec le FAI. **PAP ou CHAP :** configuration de la session PPP pour l'utilisation des protocoles PAP ou CHAP pour négocier le nom d'utilisateur et le mot de passe avec le FAI.

Délai d'inactivité	Le routeur se déconnecte au bout d'un certain temps d'inactivité. La valeur par défaut est 180 secondes. Si vous spécifiez 0, la connexion RNIS au FAI est permanente.

Méthode d'attribution des adresses IP (IPCP)

***Paramètres IP fixe et Adresse IP fixe* :**

Dans la plupart des environnements, vous ne devriez pas avoir à modifier ces paramètres car la plupart des FAI fournissent une adresse IP dynamique au routeur lorsqu'il se connecte. Si votre FAI fournit une adresse IP fixe, cliquez sur **Oui** et tapez l'adresse IP dans le champ **Adresse IP fixe**.

10.2.3 TA virtuel (CAPI distant)

Avant de passer à la configuration du TA virtuel, notez les limites suivantes :

1. Le client TA virtuel n'est utilisable qu'avec les plates-formes MicrosoftTM Windows 95 OSR2.1/98/98SE/Me/2000.
2. Le client TA virtuel n'est utilisable qu'avec le protocole CAPI 2.0 et n'a pas de moteur fax intégré.
3. Une interface au débit de base RNIS comporte deux canaux B. Le nombre maximal de clients actifs est également de 2.
4. Avant de configurer le TA virtuel, vous devez spécifier le bon code de pays dans les **Paramètres RNIS**.

Installation d'un client TA virtuel

1. Mettez en place le CD-ROM fourni avec votre routeur Vigor. Recherchez l'outil **VTA Client** dans le menu Utility et cliquez sur le bouton Install.
2. Suivez les instructions qui s'affichent. À la fin, vous êtes invité à redémarrer votre ordinateur. Cliquez sur **OK** pour redémarrer votre ordinateur.
3. Après le redémarrage de l'ordinateur, il y a une icône VT dans la barre des tâches (généralement en bas à droite de l'écran, près de l'horloge).

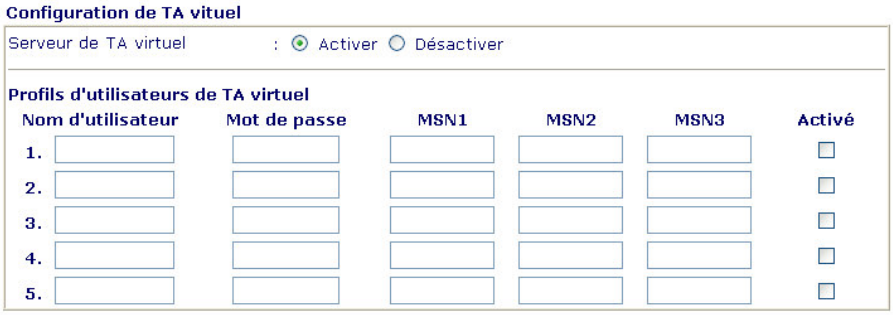
Si le texte de l'icône est VERT, le client TA virtuel est connecté au serveur TA virtuel et vous pouvez lancer votre logiciel CAPI et utilisez le client pour accéder au routeur. Si le texte de l'icône est ROUGE, c'est que le client n'est pas connecté au serveur. Vérifiez la connexion

Ethernet physique.

Configuration d'un client-serveur TA virtuel

Comme l'application de TA virtuel est un modèle de réseau client-serveur, vous devez la configurer aux deux extrémités pour que votre application de TA virtuel fonctionne correctement.

Par défaut, le serveur TA virtuel est activé et les champs nom d'utilisateur/mot de passe sont vides. N'importe quel client TA virtuel peut se connecter au serveur. Une fois qu'un champ nom d'utilisateur/mot de passe a été rempli, le serveur TA virtuel autorise uniquement les clients dont le nom d'utilisateur/mot de passe est correct à se connecter. L'écran de configuration du TA virtuel est présenté ci-dessous.



Serveur TA virtuel

Activer	Cliquez pour activer le serveur.
Désactiver	Cliquez pour désactiver le serveur. Toutes les applications de TA virtuel se termineront.

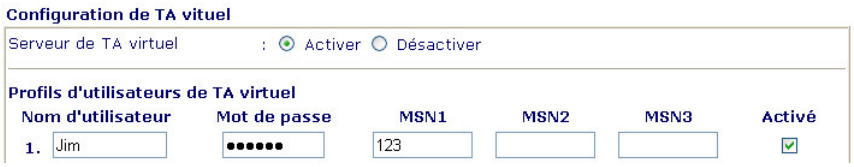
Profils d'utilisateur de TA virtuel

Nom d'utilisateur	Tapez le nom d'utilisateur d'un client spécifique.
Mot de passe	Tapez le mot de passe d'un client spécifique.
MSN 1/2/3	MSN est l'abréviation de Multiple Subscriber Number. Cela signifie que vous pouvez disposer de plusieurs numéros RNIS sur une seule ligne d'abonné. Ce service est fourni par votre opérateur de télécommunications. Spécifiez les numéros MSN pour un client spécifique. Si vous n'avez pas de service MSN, laissez ce champ vide.
Active	Cliquez pour permettre au client d'accéder au serveur.

Exemple de connexion client-serveur VTA

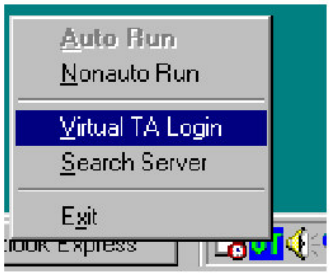
À noter que la création d'un unique compte d'accès limitera l'accès au serveur TA virtuel au détenteur du compte spécifié. Dans cet exemple, nous supposons que vous n'avez pas obtenu le service MSN de votre fournisseur de réseau RNIS.

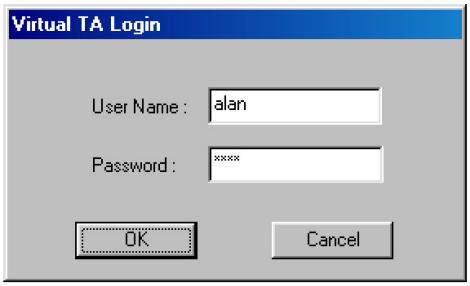
1. Sur le serveur : cliquez sur **Configuration de TA virtuel (CAPI distant)** et remplissez les champs Nom d'utilisateur et Mot de passe. Cochez la case **Active** pour activer le compte.



2. Sur le client : faites un clic droit sur l'icône VT. Le menu suivant apparaît.

3. Cliquez sur Virtual TA Login pour lancer la boîte de connexion.





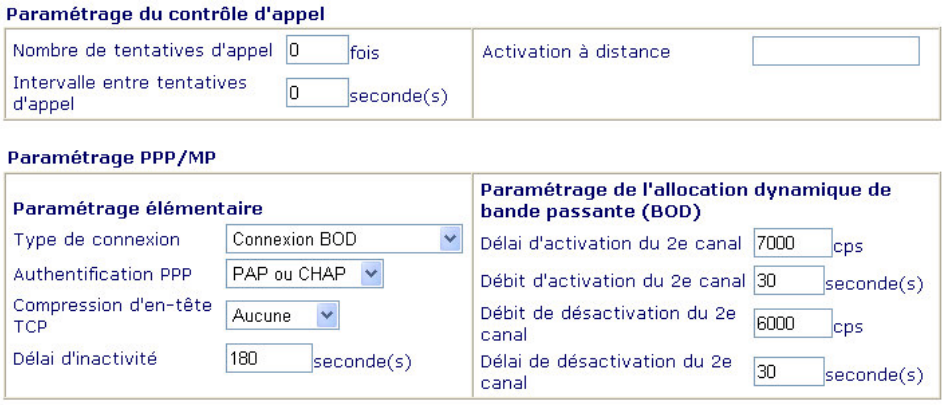
4. Tapez le Nom d'utilisateur et le Mot de passe, puis cliquez sur **OK**. Peu de temps après, le texte de l'icône VT devient vert.

5. Si vous avez demandé un service MSN, le serveur TA virtuel peut déterminer quel client a le numéro MSN spécifié. À l'arrivée d'un appel, le serveur informe le client approprié. Si nous avons tapé le numéro MSN spécifié « 123 » dans le client VTA, le serveur TA virtuel envoie un avis au client VTA, le logiciel CAPI reçoit lui aussi l'avis. Si le numéro MSN est incorrect, le logiciel n'accepte pas l'appel entrant.

10.2.4 Contrôle d'appel et PPP/MP

Nous allons maintenant configurer le contrôle d'appel et PPP/MP.

Cliquez sur **Paramétrage du contrôle d'appel et PPP/MP**. L'écran suivant apparaît.



Paramétrage du contrôle d'appel

Nombre de tentatives d'appel	C'est le nombre de tentatives d'appel par paquet déclenché. Un paquet déclenché est le paquet dont la destination est extérieure au réseau local. Par défaut, il n'est pas effectué de nouvelle tentative d'appel. Si la valeur 5 est spécifiée, pour chaque paquet déclenché, le routeur appelle 5 fois jusqu'à ce qu'il soit connecté au FAI ou au routeur d'accès à distance.
Intervalle entre tentatives d'appel	Intervalle entre tentatives d'appel. Par défaut, l'intervalle est de 0 seconde.
Activation à distance	Un numéro de téléphone est tapé dans le champ Activation à distance pour activer la fonction d'activation à distance. Si le routeur accepte un appel du numéro 12345678, il met fin immédiatement à l'appel entrant et appelle le FAI.

À noter que la **Connexion à un seul FAI** doit être préconfigurée correctement.

Connexion sortante PPP/MP

Paramétrage de base

Type de liaison	Comme le RNIS comporte deux canaux B (64 kbit/s par canal), vous pouvez spécifier si vous voulez utiliser un canal B, deux canaux B ou la bande passante à la demande (BOD). Il y a quatre options : désactivation de la liaison, connexion à 64 kbit/s, connexion à 128 kbit/s, connexion BOD.
Authentification PPP	Spécifiez la méthode d'authentification PPP pour les connexions PPP/MP. PAP/CHAP assure une meilleure compatibilité.
Compression de l'en-tête TCP	**Compression VJ** : utilisée pour la compression de l'en-tête TCP/IP. Sélectionnez Oui pour améliorer l'utilisation de la bande passante.
Délai d'inactivité	Comme notre liaison RNIS est du type « Appel à la demande », la connexion n'est déclenchée que lorsqu'elle est nécessaire.

Paramétrage de la fonction bande passante à la demande (BOD)

La bande passante à la demande concerne le protocole PPP multilien (ML-PPP ou MP). Les paramètres ne sont pris en compte que si vous choisissez **Connexion BOD** comme **type de liaison**.

Le RNIS utilise généralement un canal B pour accéder à l'internet ou au réseau distant lorsque vous choisissez Connexion BOD comme type de liaison. Le routeur utilise les paramètres suivants pour décider de l'activation ou de la désactivation du canal B supplémentaire. À noter que le paramètre **cps** (caractères par seconde) mesure l'utilisation globale de la liaison.

Délai d'activation du 2e canal et débit d'activation du 2e canal	Ces paramètres précisent les conditions d'activation du 2e canal. Si le temps d'utilisation du 1e canal dépasse le débit d'activation du 2e canal pendant un temps supérieur au délai d'activation du 2e canal, le 2e canal est activé. Le débit total de la liaison est alors de 128 kbit/s (deux canaux B).
Débit de désactivation du 2e canal et délai d'activation du 2e canal	Ces paramètres précisent les conditions de désactivation du 2e canal. Si le taux d'utilisation des deux canaux B est inférieur au débit de désactivation du 2e canal, et ce, pendant un temps supérieur au délai de désactivation du 2e canal, le 2e canal est désactivé. Par suite, le débit total de la liaison est de 64 kbit/s (un canal B).

Chapitre 11 Paramètres du LAN sans fil (pour les modèles G)

11.1 Introduction

Ces dernières années, le marché des télécommunications sans fil a connu un essor extraordinaire. La technologie sans fil permet actuellement de joindre pratiquement n'importe quel point du globe terrestre. Des centaines de millions de personnes échangent des informations à l'aide de produits de télécommunication sans fil. Le modèle Vigor G, le routeur sans fil Vigor, est conçu pour maximiser la souplesse et l'efficacité des communications pour les professions indépendantes et les particuliers. N'importe quelle personne autorisée peut amener un PDA ou un ordinateur bloc-notes sans fil dans une salle de conférence sans avoir à poser un câble réseau ou à percer des trous. Le LAN sans fil procure une haute mobilité aux utilisateurs, leur permettant d'accéder simultanément à toutes les fonctionnalités du LAN et à l'internet.

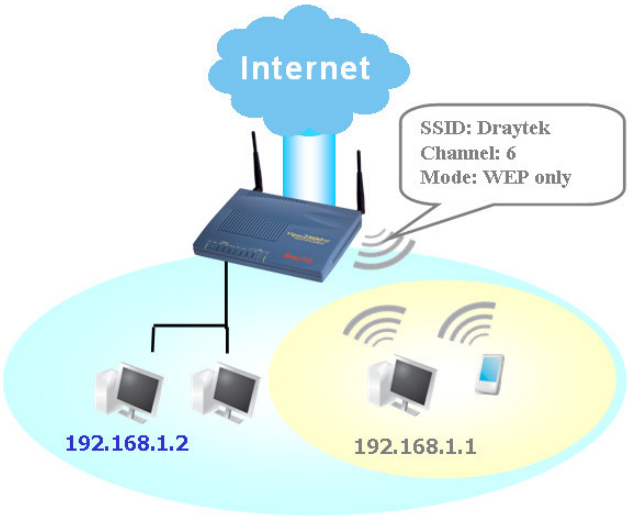
Augmenter votre débit sans fil

Les routeurs sans fil Vigor sont dotés d'une interface LAN sans fil conforme au protocole IEEE 802.11g. Pour améliorer encore les performances, le routeur Vigor est également doté de la technologie sans fil évoluée Super G™ qui permet d'atteindre 108 Mbit/s*. Vous pouvez enfin profiter de la musique et de la vidéo en flux.

* Le débit effectif varie selon divers facteurs, notamment le volume de trafic sur le réseau, la bande passante consommée hors charge utile et les matériaux de construction des bâtiments.

Principes de base du LAN sans fil

En mode infrastructure, le routeur sans fil Vigor sert de point d'accès (AP) en se connectant à de nombreux clients sans fil ou stations (STA). Toutes les stations partagent la même connexion à internet avec d'autres hôtes filaires par l'intermédiaire du routeur sans fil Vigor. Les **Paramètres généraux** définissent notamment le SSID du réseau sans fil, le canal radio du routeur, etc.



SSID: Draytek	*SSID : Draytek*
Channel: 6	*Canal : 6*
Mode: WEP only	*Mode : WEP seulement*

Plus sécurisé que jamais

Cryptage matériel en temps réel

Le routeur Vigor est doté d'un moteur de cryptage AES matériel qui assure le plus haut degré de protection.

Choix complet de normes de sécurisation

Pour assurer la sécurité et la confidentialité de vos communications sans fil, nous fournissons plusieurs normes qui ont la faveur du marché.

Le cryptage WEP (Wireless Equivalent Privacy) crypte chaque trame transmise par radio à l'aide d'une clé de 64 bits ou de 128 bits. Normalement, le point d'accès préétablit un jeu de quatre clés et communique avec chaque station en utilisant l'une de ces quatre clés.

Le cryptage WPA (Wi-Fi Protected Access), le mécanisme de sécurisation dominant dans l'industrie, a deux formes : WPA-personnel ou WPA Pre-Share Key (WPA/PSK) et WPA-entreprise ou WPA/802.1x.

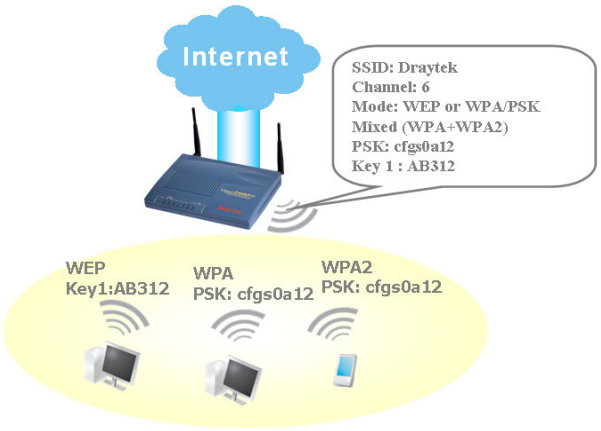
Dans WPA-personnel, une clé préétablie est utilisée pour le cryptage pendant la transmission des données. Le WPA utilise le protocole d'intégrité de clé temporelle (TKIP) pour le cryptage, tandis que WPA2 utilise AES. WPA-entreprise combine le cryptage et l'authentification.

Comme le WEP s'est avéré vulnérable, vous pouvez envisager d'utiliser WPA pour une meilleure sécurité. Choisissez le mécanisme

de sécurisation qui correspond à vos besoins.

Quels que soient les mécanismes de sécurisation que vous choisissez, ils amélioreront tous la protection des données radio et/ou la confidentialité de vos réseaux sans fil. Le routeur sans fil Vigor est très souple et peut prendre en charge de multiples connexions sécurisées mettant en œuvre simultanément WEP et WPA.

Exemple 1

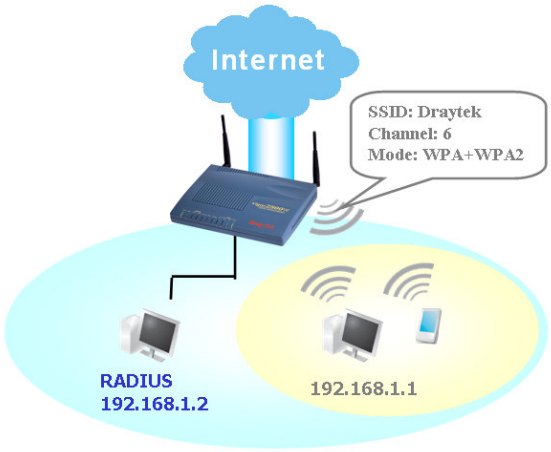


SSID: Draytek	*SSID : Draytek*
Channel: 6	*Canal : 6*
Mode: WEP or WPA/PSK	*Mode : WEP ou WPA/PSK*
Mixed (WPA+WPA2)	*Mixte : (WPA+WPA2)*
PSK: cfgs0a12	*PSK : cfgs0a12*
Key 1: AB312	*Clé 1 : AB312*
Key 1	*Clé 1*

Exemple 2

SSID: Draytek	*SSID : Draytek*
Channel: 6	*Canal : 6*
Mode: WPA/PSK only	*Mode : WPA/PSK seulement*
WPA2 only	*WPA2 seulement*
Pre-shared key: cfgs0a12	*Clé prépartagée : cfgs0a12*

Exemple 3



SSID: Draytek	*SSID : Draytek*
Channel: 6	*Canal : 6*
Mode: WPA+WPA2	*Mode : WPA+WPA2*

Séparation du sans fil et du filaire

Isolement de WLAN vous permet d'isoler votre LAN sans fil du LAN filaire pour des raisons de mise en quarantaine ou de limitation d'accès. Il s'ensuit qu'aucune communication n'est possible entre les deux LAN. À titre d'exemple, vous pouvez configurer un LAN sans fil uniquement pour les visiteurs de manière qu'ils puissent se connecter à l'internet sans craindre une fuite d'informations confidentielles. Vous pouvez aussi ajouter un filtre d'adresse MAC pour isoler un utilisateur particulier du LAN filaire.

Gestion de stations sans fil

La **liste des stations** affiche toutes les stations de votre réseau sans fil et l'état de connexion. En outre, vous pouvez utiliser la fonction **Contrôle d'accès MAC** pour autoriser uniquement la connexion à un utilisateur de confiance. Le **Contrôle de débit station** peut attribuer des débits descendant/montant spécifiques à chaque STA.

Découverte de point d'accès voisin

La découverte de point d'accès est une fonction que l'on trouve généralement dans un utilitaire de client sans fil pour trouver un point d'accès. Le routeur sans fil Vigor exploite cette fonctionnalité pour assurer la qualité et la sécurité des communications sans fil. Vous pouvez sélectionner le canal le moins encombré ou le moins brouillé pour constituer votre réseau sans fil. Vous pouvez sélectionner l'AP homologue WDS sur la base de l'adresse MAC.

11.2 Paramètres

Nous allons décrire les possibilités du LAN sans fil et les configurations web correspondantes. Utilisez le lien du menu pour configurer la fonction LAN sans fil. Certaines fonctions sont susceptibles d'évoluer.

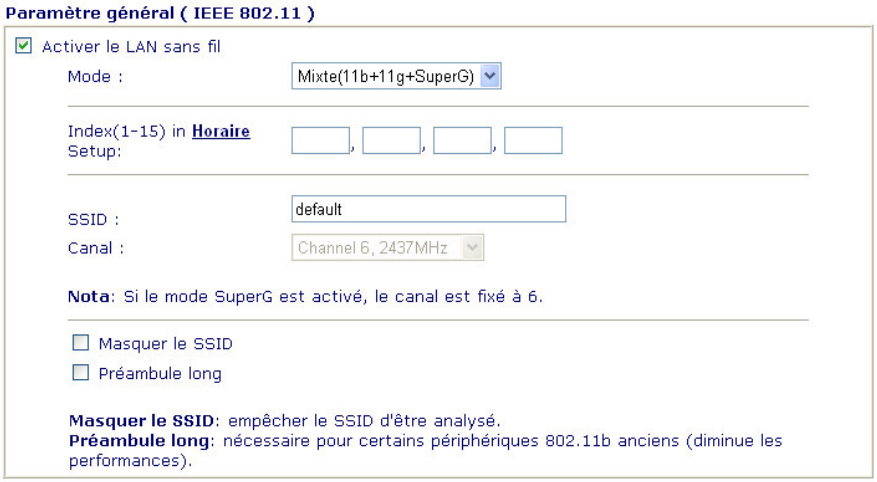
Vérification de l'état du réseau sans fil

Cliquez sur « **Maintenance du système>>État du système** ». Les informations suivantes s'affichent :

Cette page web affiche les informations du LAN sans fil, notamment l'**adresse MAC**, le **domaine de fréquence** et la **version du logiciel**. Le **domaine de fréquence** peut être l'Europe (13 canaux utilisables), les États-Unis (11 canaux utilisables), etc. Les canaux disponibles pris en charge par les produits sans fil varient suivant les pays. La **version du logiciel** fournit des informations sur le pilote WLAN.

11.2.1 Paramètres généraux

Cliquez sur **Paramètres généraux**. La fenêtre suivante apparaît.



Activer le LAN sans fil

Cochez la case pour activer la fonction sans fil.

Mode

Sélectionner un mode sans fil approprié.

Mixte (11b+11g+SuperG)	Le routeur communique simultanément avec les stations 802.11b, 802.11g et Super G.
Mixte (11b+11g)	Le routeur communique simultanément avec les stations 802.11b et 802.11g.
Super G seulement	Le routeur ne communique qu'avec les stations Super G.
11g seulement	Le routeur communique uniquement avec les stations 802.11g.
11b seulement	Le routeur communique uniquement avec les stations 802.11b.

Plages horaires

Vous pouvez limiter le fonctionnement du LAN sans fil à certaines plages horaires. Vous pouvez choisir jusqu'à 4 plages horaires parmi les 15 définies dans **Applications >> Plages horaires**. Par défaut, ce champ est vide et la fonction est activée en

permanence.

SSID et canal

Par défaut, le SSID est « valeur par défaut ». Nous vous suggérons de le changer.

SSID	Identifie le LAN sans fil. Le SSID peut se composer d'un nombre quelconque de caractères ou de divers caractères spéciaux.
Canal	Le canal radio du LAN sans fil. Le canal par défaut est 6. Vous pouvez en spécifier un autre si le canal sélectionné est gravement perturbé.

Masquer le SSID

Cochez cette case pour prévenir toute scrutation malveillante et rendre difficile à des clients non autorisés de joindre votre LAN sans fil. Selon l'utilitaire sans fil, l'utilisateur pourra visualiser les informations à l'exception du SSID ou n'avoir aucune information concernant le routeur sans Vigor.

Préambule long

Cette option définit la longueur du champ de synchronisation d'un paquet 802.11. La plupart des réseaux sans fil modernes utilisent un préambule court constitué d'un champ de synchronisation de 56 bits au lieu d'un préambule long de 128 bits. Toutefois, certains équipements de réseau sans fil 11b originel ne prennent en charge que le préambule long. Cochez la case **Préambule long** s'il cela est nécessaire pour communiquer avec ce type d'équipement.

11.2.2 Sécurité

Cliquez sur **Paramètres de sécurité**. Une nouvelle fenêtre s'ouvre.

Mode

Sélectionnez un mode de cryptage approprié pour améliorer la sécurité et la confidentialité de vos paquets de données sans fil.

Désactiver	Désactive le mécanisme de cryptage.
WEP seulement	Accepte uniquement les clients WEP. La clé doit être tapée dans WEP Key.
WEP/802.1x seulement	Accepte les clients WEP avec authentification 802.1x. Comme la clé est négociée automatiquement pendant l'authentification, le champ Clé est inactif.
WEP ou WPA/PSK	Accepte les clients WEP et WPA avec une clé valide. Seul Mixte (WPA+WPA2) est applicable si vous sélectionnez WPA/PSK.
WEP/802.1x ou WPA/802.1x	Accepte les clients WEP ou WPA avec authentification 802.1x. Si vous sélectionnez WPA/PSK, seul Mixte (WPA+WPA2) est applicable. Comme la clé est négociée automatiquement pendant l'authentification, le champ Clé est inactif.
WPA/PSK	Accepte les clients WPA. La clé doit être tapée dans

seulement	PSK. N'oubliez pas de sélectionner le type de WPA pour définir Mixte ou WPA2 seulement.
WPA/802.1x seulement	Accepte les clients WPA avec authentification 802.1x. N'oubliez pas de sélectionner le type de WPA pour définir Mixte ou WPA2 seulement. Comme la clé est négociée automatiquement pendant l'authentification, le champ Clé est inactif.

WPA

WPA crypte chaque trame transmise par radio à l'aide de la clé entrée manuellement dans le champ ou négociée automatiquement via l'authentification 802.1x.

Type	Choisissez entre **Mixte (WPA+WPA2)** et **WPA2 seulement**.
Clé partagée (PSK)	Entrez **8 à 63** caractères ASCII, par exemple 012345678 (soit 64 chiffres hexadécimaux commençant par 0x, par exemple « 0x321253abcde... »)

WEP

64 bits	Pour le WEP 64 bits, entrez **5** caractères ASCII, comme 12345 (ou 10 chiffres hexadécimaux commençant par 0x, par exemple 0x4142434445F).
128 bits	Pour le WEP 128 bits, entrez **13** caractères ASCII, comme ABCDEFGHIJKLM (ou 26 chiffres hexadécimaux commençant par 0x, par exemple 0x41424344454647484 94A4B4C4D)

Tous les équipements sans fil doivent prendre en charge le même nombre de bits de cryptage WEP et avoir la même clé. Quatre clés peuvent être entrées ici mais seule une clé peut être sélectionnée à un moment donné. Les clés peuvent être entrées en ASCII ou en hexadécimal. Vérifiez la clé que vous voulez utiliser.

11.2.3 Contrôle d'accès

Pour renforcer la sécurité d'accès sans fil, la fonction de **Contrôle d'accès** vous permet de limiter l'accès au réseau à l'aide de l'adresse MAC du client sans fil. Seule l'adresse MAC valable configurée peut accéder au LAN sans fil. En cliquant sur **Contrôle d'accès**, vous obtenez une nouvelle page web qui vous permet d'éditer les adresses MAC de clients pour contrôler leur droit d'accès.

Activer le contrôle d'accès

Cochez cette case pour activer la fonction de contrôle d'accès par adresse MAC.

Politique

Activer le filtre d'adresse MAC	Sélectionnez cette option pour activer le filtre d'adresse MAC. Vous pouvez ensuite ajouter manuellement des adresses MAC de client dans la zone du dessous.
Isoler le WLAN du LAN	Sélectionnez cette option pour isoler le LAN sans fil du LAN sur la base de la liste d'adresses MAC.

Filtre d'adresse MAC

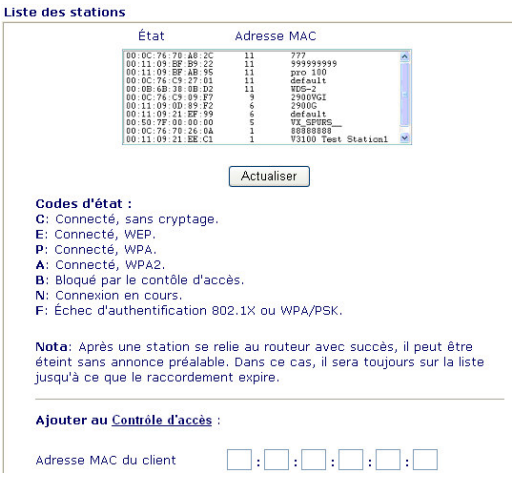
Adresse MAC du client	Entrez manuellement l'adresse MAC du client sans fil.
Attribut	(Aucun) : sélectionnez Aucun pour permettre au client sans fil de l'adresse MAC de se connecter au routeur sans fil Vigor. v : cochez cette case pour appliquer le VPN à la connexion du client sans fil de l'adresse MAC. s : cochez cette case pour isoler du LAN la connexion sans fil du client sans fil de l'adresse MAC. Cliquez sur **Modifier** pour appliquer la modification à l'adresse MAC sélectionnée.

Il y a quatre boutons (Ajouter, Supprimer, Modifier et Annuler) pour l'édition d'une adresse MAC.

Ajouter	Ajouter une nouvelle adresse MAC à la liste.
Supprimer	Supprimer l'adresse MAC sélectionnée de la liste.
Modifier	Modifier l'adresse MAC sélectionnée.
Annuler	Annuler le contrôle d'accès.
Supprimer tout	Supprimer toutes les adresses MAC.
OK	Enregistrer la liste de contrôle d'accès.

11.2.4 Découverte d'AP

Pour découvrir tous les points d'accès du voisinage, cliquez sur **Scruter**.



Liste de point d'accès

La liste de points d'accès affiche tous les points d'accès du voisinage.

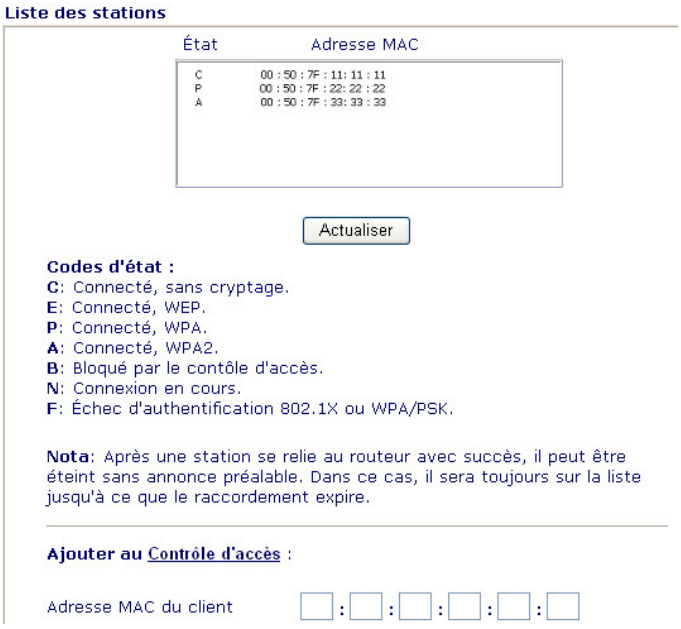
BSSID	Ajouter une nouvelle adresse MAC à la liste.
Canal	Supprimer l'adresse MAC sélectionnée de la liste.
SSID	Modifier l'adresse MAC sélectionnée.

Statistiques

Statistiques des points d'accès du voisinage pour chaque canal.

11.2.5 Liste des stations

La liste des stations permet de connaître des clients sans fil qui se connectent actuellement avec leur code d'état. La signification des codes est indiquée au-dessous. Pour le **contrôle d'accès**, vous pouvez sélectionner station WLAN et cliquez sur **Ajouter au contrôle d'accès**.



Chapitre 12 Maintenance du système

12.1 Introduction

L'état du système fournit les paramètres réseau de base du routeur Vigor, notamment les informations relatives aux interfaces LAN et WAN. Vous pouvez également obtenir des informations sur la version actuelle du logiciel.

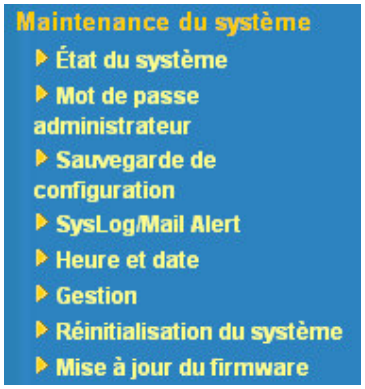
La **sauvegarde de la configuration** vous permet de conserver les configurations de votre routeur sous la forme de fichiers ou de restaurer les configurations avec ces fichiers. Le routeur vous permet de sauvegarder ou de restaurer la configuration d'une manière très simple via l'internet.

Par défaut, le routeur peut être configuré et géré à l'aide de n'importe quel client Telnet ou de n'importe quel navigateur internet fonctionnant sous n'importe quel système d'exploitation. Aucun logiciel supplémentaire n'est nécessaire. Toutefois, dans certains environnements spécifiques, vous pouvez modifier les numéros de port pour le serveur Telnet ou http intégré, créer des listes de contrôle d'accès pour protéger le routeur ou empêcher l'administrateur système de se connecter à l'internet.

Par ailleurs, à l'aide des fonctions de **réinitialisation du système** et de **mise à jour du logiciel**, vous pouvez réinitialiser le système après certaines opérations de paramétrage et mettre à jour le logiciel via TFTP.

12.2 Paramètres

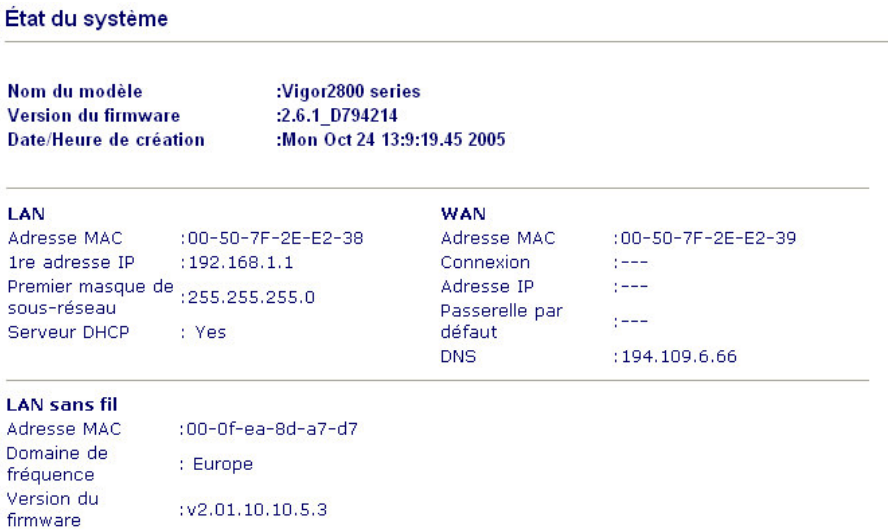
Cliquez sur **Maintenance du système** pour ouvrir la page de paramétrage.



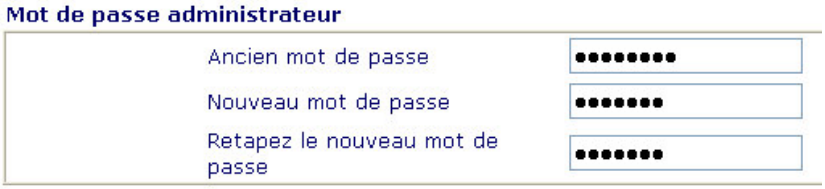
État du système	Affichage de l'état du système.
Mot de passe administrateur	Définition ou modification du mot de passe.
Sauvegarde des configurations	Restauration d'un fichier de configuration ou sauvegarde de la configuration courante.
SysLog/Mail Alert	Définition du serveur SysLog auquel le routeur fournit des informations. Définition du serveur SNMTP auquel le routeur fournit des « mail alerts ».
Date et heure	Réglage de l'heure à partir du PC ou d'un serveur NTP.
Gestion	Paramétrages du contrôle d'accès de gestion, SNMP et de port.
Réinitialisation du système	Réinitialisation du système.
Mise à jour du firmware	Mise à jour du logiciel via TFTP

12.2.1 État du système

Dans **État du système**, vous pouvez visualiser les informations suivantes.



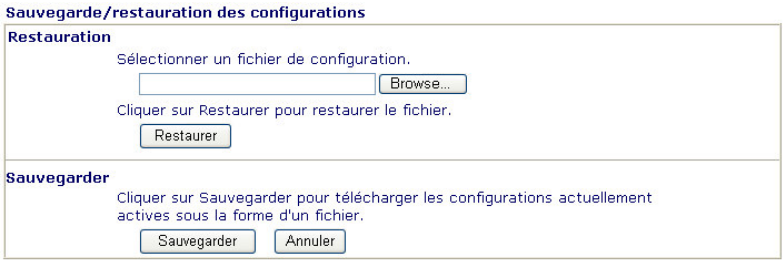
12.2.2 Mot de passe administrateur



Vous pouvez réinitialiser le mot de passe administrateur.

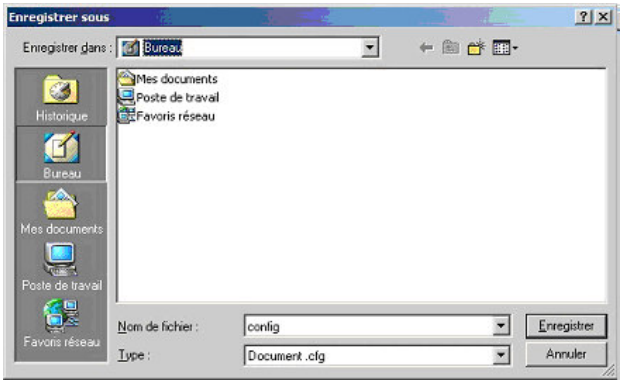
12.2.3 Sauvegarde des configurations

1. Allez à **Maintenance du système** > **Sauvegarde des configurations**. Les fenêtres suivantes apparaissent.



2. Cliquez sur le bouton Sauvegarder.

3. Cliquez sur le bouton OK pour enregistrer la configuration sur la forme dans un fichier. Le nom du fichier par défaut est **config.cfg**. Vous pouvez lui donner un autre nom.



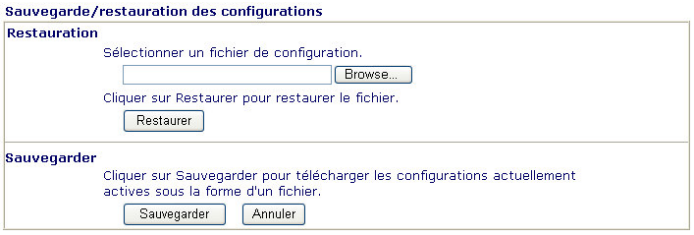
4. Cliquez sur le bouton **Enregistrer.** La configuration est téléchargée automatiquement sur votre ordinateur sous la forme d'un fichier **config.cfg**.

L'exemple ci-dessus vaut pour les plateformes **Windows**. La plateforme **Mac** ou **Linux** donne des fenêtres différentes mais la fonction de sauvegarde est la même.

Restaurer la configuration à partir d'un fichier de configuration

1. Allez à **Maintenance du système** > **Sauvegarde des configurations**. Les fenêtres suivantes apparaissent.

2. Cliquez sur le bouton **Parcourir** pour choisir le fichier de configuration correct.



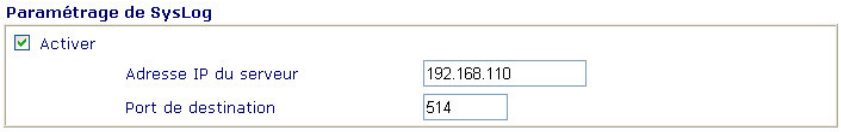
3. Cliquez sur le bouton **Restaurer** et attendez quelques secondes. Vous êtes informé du succès de la restauration.

12.2.4 SysLog/Mail Alert

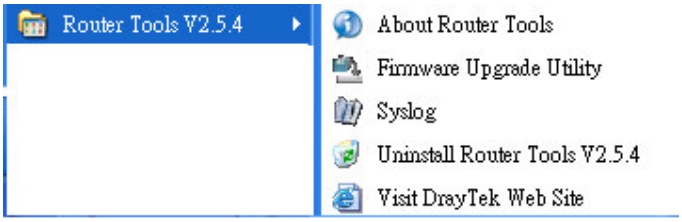
SysLog

La fonction SysLog aide les utilisateurs à surveiller le routeur. Inutile d'aller dans le configurateur web du routeur ou de se procurer des équipements de débogage.

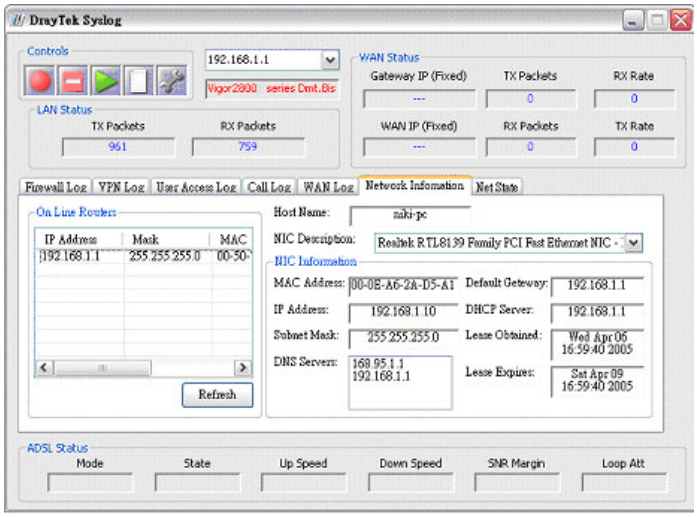
1. Spécifiez l'adresse IP du serveur SysLog.



2. Installez les outils du routeur dans l'utilitaire avec le CD fourni. Dans le menu des programmes, cliquez sur **Outils du routeur>>SysLog**.



3. Sélectionnez le routeur que vous voulez surveiller. La fenêtre SysLog s'affiche. Dans **Network Information**, sélectionnez la carte réseau utilisée pour se connecter au routeur. Autrement, vous ne pourrez pas obtenir d'informations du routeur.



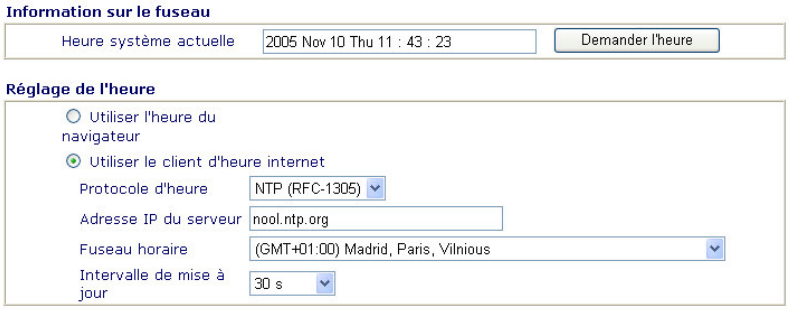
Mail Alert

La fonction Mail Alert avertit de l'apparition d'évènements spécifiques.

Serveur SMTP	Spécifiez l'adresse IP du serveur SMTP de messagerie.
Envoyer à	Spécifiez l'adresse e-mail du destinataire.
Chemin de retour	Spécifiez l'adresse e-mail de l'émetteur.

12.2.5 Réglage de l'heure et de la date

Il s'agit de spécifier où le routeur doit obtenir l'heure et la date.



Informations horaires

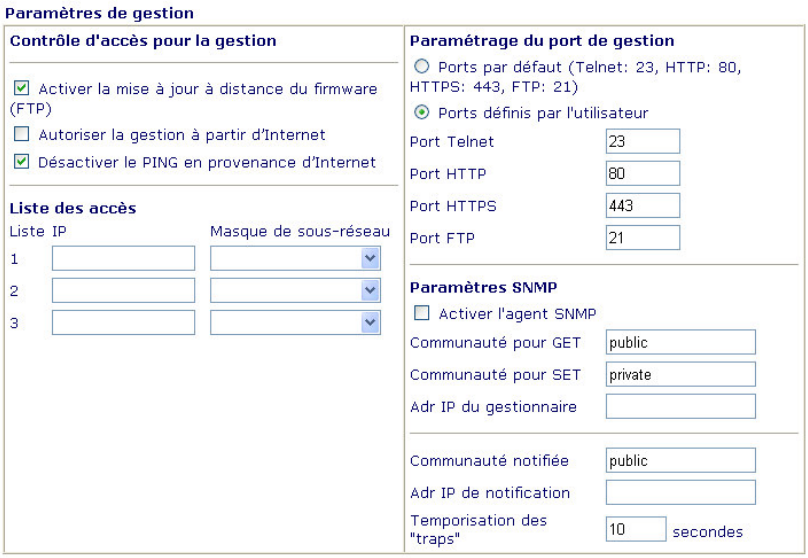
Cliquez sur Demander l'heure pour obtenir l'heure actuelle.

Réglage de l'heure

Utiliser l'heure du navigateur	Sélectionnez l'heure à votre PC.
Utiliser le client d'heure internet	Sélectionnez l'heure à un serveur d'heure sur internet à l'aide du protocole défini.

12.2.6 Gestion

Cliquez sur **Paramètres de gestion**. La page de paramétrage suivante apparaît.



Contrôle d'accès pour la gestion

Numéro de port utilisé pour envoyer/recevoir des messages SIP. La valeur par défaut est 5060 et doit correspondre au registre homologue pour les appels VoIP.

Autoriser la mise à jour à distance du firmware	Cliquez sur la case pour autoriser la mise à jour à distance du firmware via le protocole de transfert de fichier (FTP).
Autoriser la gestion à partir de l'internet	Cochez la case pour autoriser les administrateurs système à se connecter à partir de l'internet. Par défaut, la connexion n'est pas autorisée.
Désactiver le PING en provenance de l'internet	Cochez la case pour rejeter tous les paquets PING provenant de l'internet. Pour des raisons de sécurité, cette fonction est activée par défaut.

Liste d'accès

Vous pouvez spécifier que l'administrateur système peut se connecter uniquement à partir d'un hôte ou d'un réseau spécifique défini dans la liste. Vous pouvez définir jusqu'à trois adresses IP/masques de sous-réseau.

IP	Adresse IP autorisée à se connecter au routeur.
Masque de sous-réseau	Masque de sous-réseau autorisé à se connecter au routeur.

Paramétrage du port de gestion

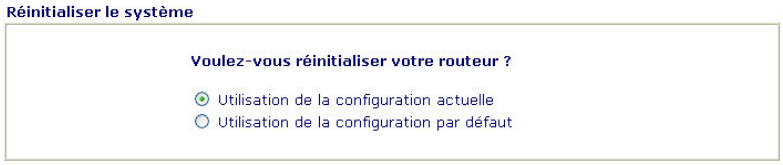
Ports par défaut	Cochez la case pour utiliser les numéros de ports standard pour les serveurs Telnet et HTTP.
Ports définis par l'utilisateur	Cochez la case pour spécifier des numéros de port définis par l'utilisateur pour les serveurs Telnet, HTTP, HTTPS, FTP.

Paramétrage SNMP

Communauté pour GET	Nom que l'agent SNMP a utilisé pour exécuter l'action « Get ». La valeur par défaut est « public ».
Communauté pour SET	Nom que l'agent SNMP a utilisé pour exécuter l'action « Set ». La valeur par défaut est « privé ».
Adr IP du gestionnaire	Laissez le champ vide pour permettre à n'importe quel hôte d'exécuter une action « Get » ou « Set ». Spécifiez l'adresse IP de l'hôte, si besoin est.
Communauté notifiée	Nom que l'agent SNMP à utiliser pour contacter la communauté notifiée afin d'exécuter l'action « Set ». La valeur par défaut est « public ».
Adr IP de notification	Adresse IP de l'hôte que le routeur doit notifier.

12.2.7 Réinitialisation du système

Le configurateur web peut être utilisé pour redémarrer votre routeur. Cliquez sur **Réinitialisation du système** dans le menu principal pour ouvrir la page suivante.



Si vous voulez réinitialiser le routeur avec la configuration courante, cochez **Utiliser la configuration courante** et cliquez sur **OK**. Pour rétablir les paramètres par défaut du routeur, cochez **Utiliser la configuration par défaut** et cliquez sur **OK**. La réinitialisation prend 5 secondes.

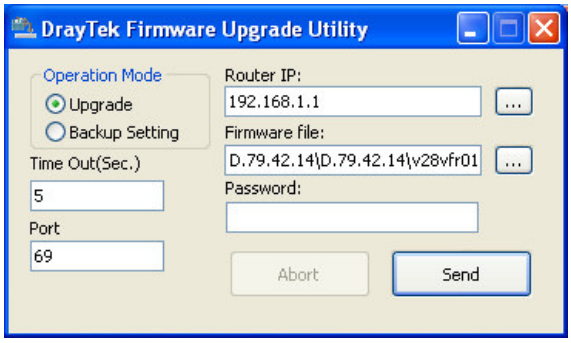
12.2.8 Mise à jour du firmware

Vous devrez trouver la dernière version du firmware aux adresses suivantes :

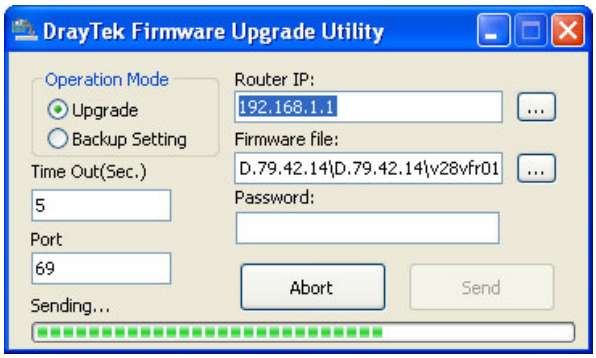
- Site web www.draytek.com (ou site web de DrayTek local)
- Site FTP ftp://ftp.draytek.com

Pour mettre à jour facilement le firmware du routeur Vigor, il vous faut installer les Router Tools. Il s'agit d'un logiciel d'application gratuit fourni avec le CD-ROM du produit. Vous pouvez également le trouver sur le site web de DrayTek.

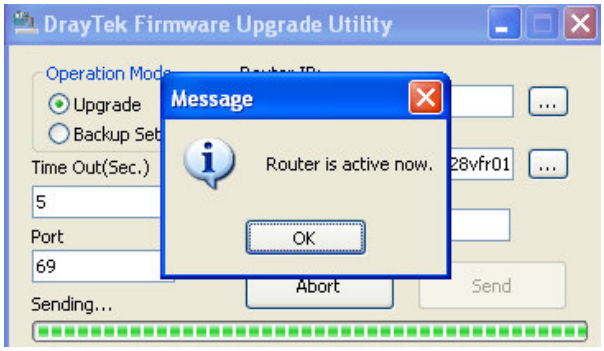
1. Connectez votre routeur Vigor et assurez-vous que vous pouvez naviguer.
2. Installez les routeur Tools. L'écran ci-dessous doit apparaître. (*Écran Windows*)
3. Puis la fenêtre suivante apparaît. Tapez l'adresse IP du routeur dans le champ **Router IP**. Cliquez sur « … » à droite pour laisser le programme rechercher les routeurs Vigor. Vous devez également préciser l'emplacement du firmware sur votre PC. Le champ **Mot de passe** doit être rempli si vous avez défini un mot de passe lors de l'installation du routeur.



La mise à jour commence et son état est indiqué par la barre d'avancement.



Une fois la mise à jour achevée, attendez environ 30 secondes et le routeur est prêt (voyant ACT se remet à clignoter normalement.



Chapitre 13
Paramétrage des diagnostics

13.1 Introduction

Les outils de diagnostic vous permettent de visualiser ou de diagnostiquer l'état de votre routeur Vigor.

13.2 Paramètres

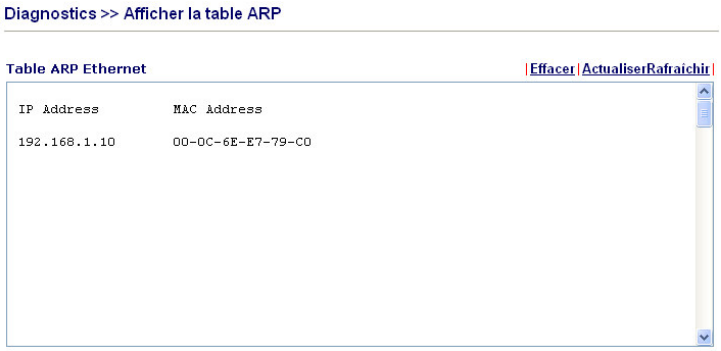
Cliquez sur **Diagnostics** pour ouvrir la page de paramétrage.

13.2.1 Connexion WAN

Mode/État de l'accès à haut débit	Affiche le mode et l'état de l'accès à haut débit. Si la connexion est inactive, "**---**" est affiché.
Adresse IP WAN	Adresse IP WAN pour la connexion active.
Appel PPPoE ou PPTP	Cliquez sur cette option pour que routeur établisse une connexion PPPoE ou PPTP.

13.2.2 Table de cache ARP

Cliquez sur **Visualiser la table de cache ARP** pour visualiser le contenu du cache ARP du routeur. La table affiche la correspondance entre une adresse matérielle Éthernet (adresse MAC) et une adresse IP.



Actualiser : Cliquez pour recharger la page.

13.2.3 Table DHCP

Cette fonction fournit des informations sur les adresses IP attribuées. Ces informations sont utiles pour diagnostiquer les problèmes de réseau, comme les conflits d'adresse IP, etc.