GUIDE D'ADMINISTRATION

Cisco Small Business

RVS4000 Routeur de sécurité Gigabit 4 ports avec VPN

OL-23752-01

Table des matières

1

Introduction

Nous vous remercions d'avoir choisi le routeur de sécurité Gigabit 4 ports avec VPN Cisco RVS4000. Le routeur de sécurité Gigabit 4 ports avec VPN est une solution réseau avancée de partage Internet adaptée aux besoins des petites et moyennes entreprises. Comme tous les routeurs, il permet à plusieurs ordinateurs d'un bureau donné de partager une connexion Internet.

Le routeur de sécurité Gigabit 4 ports avec VPN intègre également un commutateur Ethernet 10/100/1000 4 ports en duplex intégral qui permet de connecter directement quatre ordinateurs ; vous pouvez également connecter plus de concentrateurs et de commutateurs pour étendre votre réseau à votre convenance.

La fonctionnalité de réseau privé virtuel (VPN) crée des « tunnels » cryptés sur Internet, qui vous offrent la possibilité de connecter en toute sécurité jusqu'à 5 bureaux distants et 5 utilisateurs itinérants au réseau de votre site. Les utilisateurs qui utilisent un tunnel VPN sont connectés au réseau de votre entreprise (avec un accès sécurisé aux fichiers, au courrier électronique et à votre Intranet) exactement de la même manière que s'ils se trouvaient sur votre site. Vous pouvez également utiliser les fonctionnalités VPN pour autoriser les utilisateurs de votre petit réseau à se connecter en toute sécurité à un réseau d'entreprise externe. Les fonctions QoS fournissent une qualité de voix et de vidéo constante dans l'ensemble de votre entreprise.

Le routeur de sécurité Gigabit 4 ports avec VPN peut servir de serveur DHCP et possède un pare-feu SPI et un système de détection des intrusions (IPS) puissants pour protéger vos ordinateurs contre les intrus et les attaques Internet les plus connues. Vous pouvez le configurer pour filtrer l'accès des utilisateurs internes à Internet et, grâce à ses fonctions de filtrage des adresses IP et MAC, pour spécifier qui exactement doit pouvoir accéder à votre réseau. La configuration est un jeu d'enfant grâce à l'utilitaire Web.

Ce guide d'administration vous donnera toutes les informations dont vous avez besoin pour connecter, paramétrer et configurer votre routeur.

2

Principes fondamentaux régissant la mise en réseau et la sécurité

Ce chapitre aborde les principes fondamentaux qui régissent la mise en réseau et la sécurité. Il comprend les sections suivantes :

Introduction aux réseaux locaux (LAN)

Un routeur est un périphérique réseau qui connecte ensemble deux réseaux.

Le routeur connecte le réseau local (LAN) ou le groupe d'ordinateurs de votre domicile ou de votre bureau à Internet. Le routeur traite et régule les données qui transitent entre ces deux réseaux.

La technologie de traduction d'adresses réseau (NAT) du routeur protège votre réseau d'ordinateurs de sorte que les utilisateurs sur Internet ne peuvent pas « voir » vos ordinateurs. Cette fonction préserve l'intégrité de votre LAN. Le routeur protège votre réseau en inspectant le premier paquet entrant par le port Internet, avant de le livrer à la destination finale sur l'un des ports Ethernet. Le routeur inspecte les services utilisant les ports Internet comme le serveur Web, le serveur ftp ou d'autres applications Internet et, s'il y est autorisé, il transfère le paquet à l'ordinateur approprié du côté du réseau local.

Les adresses IP

IP signifie Internet Protocol. Chaque périphérique d'un réseau IP, y compris les ordinateurs, les serveurs d'impression et les routeurs, nécessite une adresse IP pour identifier son emplacement, ou adresse, sur le réseau. Ceci concerne aussi bien les connexions LAN que les connexions Internet.

Il existe deux manières d'affecter des adresses IP à vos périphériques réseau.

Une adresse IP statique est une adresse IP fixe que vous affectez manuellement à un ordinateur ou à un autre périphérique sur le réseau. Étant donné que les adresses IP statiques restent valides tant qu'elles ne sont pas désactivées, l'utilisation d'une telle adresse vous apporte l'assurance que le périphérique correspondant gardera toujours la même adresse IP jusqu'à ce que vous décidiez de la modifier. Les adresses IP statiques sont généralement utilisées pour des périphériques réseau tels que des serveurs ou des serveurs d'impression.

Si vous souhaitez utiliser le routeur pour partager votre connexion Internet câblée ou DSL, contactez votre fournisseur d'accès Internet (FAI) pour savoir s'il a affecté une adresse IP statique à votre compte. Si tel est le cas, vous aurez besoin de cette adresse IP statique lors de la configuration du routeur. Vous pouvez obtenir cette information auprès de votre FAI.

Une adresse IP dynamique est une adresse affectée automatiquement à un périphérique sur le réseau. Ces adresses IP sont appelées dynamiques car elles ne sont affectées que temporairement à l'ordinateur ou autre périphérique. Après un certain temps, elles expirent et peuvent être modifiées. Si un ordinateur se connecte sur le réseau (ou sur Internet) et que son adresse IP dynamique a expiré, le serveur DHCP lui affecte une nouvelle adresse IP dynamique.

Un serveur DHCP peut être soit un ordinateur désigné sur le réseau, soit un autre périphérique du réseau, tel que le routeur. Par défaut, le routeur utilise le paramètre de type de connexion Internet **Obtain an IP automatically** (DHCP).

L'ordinateur ou le périphérique réseau obtenant une adresse IP est appelé client DHCP. DHCP vous évite d'avoir à affecter manuellement une adresse IP lorsqu'un nouvel utilisateur est ajouté à votre réseau.

Pour les utilisateurs DSL, de nombreux FAI peuvent vous imposer de vous connecter avec un nom d'utilisateur et un mot de passe pour accéder à Internet. Il s'agit d'un type de connexion dédié haut débit appelé PPPoE (Point to Point Protocol over Ethernet, protocole point à point sur Ethernet). Le protocole PPPoE est semblable à une connexion d'accès à distance, mais il ne compose pas de numéro téléphonique pour établir la connexion. Il fournit également au routeur une adresse IP dynamique pour établir une connexion à Internet.

Par défaut, un serveur DHCP (côté LAN) est activé sur le routeur. Si vous disposez déjà d'un serveur DHCP sur votre réseau, vous DEVEZ désactiver l'un des deux serveurs DHCP. Lorsque plusieurs serveurs DHCP sont actifs sur un réseau, des erreurs se produisent, telles que des conflits d'adresses IP. Pour désactiver le serveur DHCP sur le routeur, reportez-vous à la section Configuration de base au **Chapitre 5, « Configuration du routeur ».**

REMARQUE Comme le routeur est un périphérique qui connecte deux réseaux, il a besoin de deux adresses IP : une pour le réseau local et une pour Internet. Dans ce guide d'administration, vous trouverez des références à « l'adresse IP Internet » et à « l'adresse IP LAN ».

Comme le routeur utilise la technologie NAT, la seule adresse IP qui peut être vue depuis Internet pour votre réseau est l'adresse IP Internet du routeur. Cependant, même cette adresse IP Internet peut être bloquée, de sorte que le routeur et le réseau soient invisibles pour Internet.

Le système IPS (Intrusion Prevention System, système de prévention des intrusions)

IPS est une technologie avancée conçue pour protéger votre réseau des attaques malveillantes. IPS interagit avec votre pare-feu SPI, une liste de contrôle d'accès basée sur IP (ACL), le mécanisme NAPT (Network Address Port Translation) et votre réseau VPN (Virtual Private Network) pour vous offrir un niveau de sécurité optimal. Le système IPS se présente sous la forme d'un module en ligne intégré dans le routeur, assurant des fonctions de détection et de prévention en temps réel.

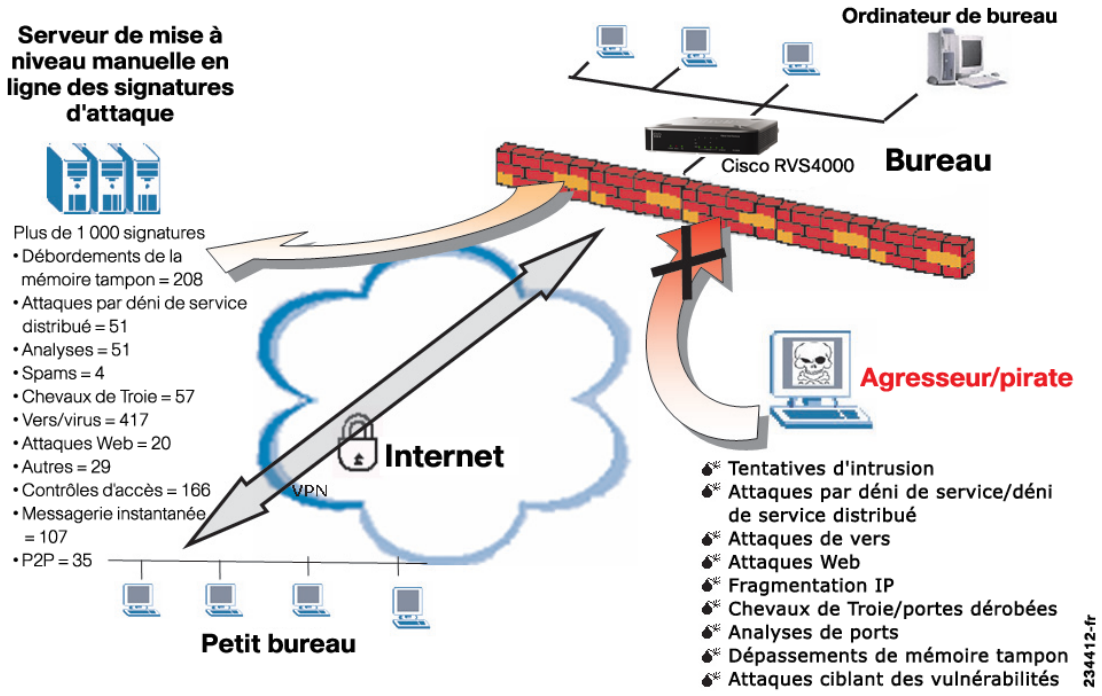
Le routeur RVS4000 est doté d'une accélération matérielle pour la mise en correspondance des modèles en temps réel afin de détecter les attaques malveillantes. Il filtre activement et abandonne les paquets TCP/UDP/ICMP/IGMP malveillants et peut réinitialiser des connexions TCP. Cette fonction empêche les attaques de vers contre les ordinateurs et les serveurs client exécutant divers systèmes d'exploitation, comme Windows, Linux et Solaris. Toutefois, ce système n'offre pas de protection contre les virus contenus dans les pièces jointes des e-mails.

Les contrôles P2P (Peer to Peer) et IM (Instant Messaging) permettent à l'administrateur système d'empêcher les utilisateurs réseau d'utiliser ces protocoles pour communiquer avec d'autres personnes sur Internet. Les administrateurs peuvent ainsi configurer des règles d'entreprise régissant l'utilisation de leur bande passante Internet.

Le fichier des signatures est le cœur du système IPS. Il est comparable au fichier des définitions de virus du programme antivirus de votre ordinateur. IPS utilise ce fichier pour analyser les paquets qui entrent dans le routeur et agit en conséquence. Le RVS4000 possède un fichier de signatures qui comprend plus de 1 000 règles, couvrant les problématiques suivantes : attaques par déni de service/déni de service distribué (DDoS), débordements de la mémoire tampon, contrôles d'accès, analyses, chevaux de Troie, Misc., P2P, IM, virus, vers et attaques Web.

Les clients sont invités à mettre à jour régulièrement leur fichier de signatures IPS pour se protéger contre tout nouveau type d'attaque sur Internet.

Scénarios IPS



3

Planification de votre réseau privé virtuel (VPN)

Ce chapitre fournit des informations utiles pour la planification d'un VPN. Il comprend les sections suivantes :

Pourquoi ai-je besoin d'un VPN ?

La mise en réseau d'ordinateurs apporte une flexibilité qui n'existe pas lorsque l'on utilise un système archaïque, basé sur le papier. Cette flexibilité s'accompagne néanmoins d'un risque plus important pour la sécurité des données. Les pare-feu limitent ce risque. Ils aident à protéger les données localisées au sein du réseau local. Mais qu'en est-il au juste pour les données qui sortent de votre réseau local, lorsque vous envoyez des e-mails ou lorsque vous vous connectez au réseau de votre entreprise depuis un hôtel ou un bureau distant ? Comment vos données sont-elles protégées ?

La mise en œuvre d'un VPN répond à cette problématique. Les VPN, ou réseaux privés virtuels, sécurisent les données qui sortent du réseau comme si elles ne le quittaient pas.

Lorsque vous envoyez des données à l'extérieur via Internet à partir de votre ordinateur, elles sont toujours vulnérables. Vous êtes peut-être déjà équipé d'un pare-feu qui empêche la corruption ou l'interception des données situées sur votre réseau par des utilisateurs externes. Mais lorsque ces données quittent votre réseau (lorsque vous les envoyez par e-mail ou que vous communiquez sur Internet), elles ne sont plus protégées par le pare-feu.

À ce stade, vos données deviennent alors accessibles aux pirates qui utilisent diverses méthodes pour s'emparer non seulement des données que vous transmettez, mais également de vos informations de connexion au réseau et de protection. Les méthodes qu'ils emploient le plus fréquemment sont décrites ci-après.

1) Mystification d'adresses MAC (MAC Address Spoofing)

Les paquets transmis sur un réseau, soit votre réseau local, soit Internet, sont précédés d'un en-tête de paquet. Ces en-têtes de paquet contiennent les informations de source et de destination nécessaires à la bonne transmission du paquet. Un pirate peut utiliser ces informations pour usurper l'adresse MAC autorisée sur le réseau. Avec cette adresse MAC usurpée, le pirate peut également intercepter des informations destinées à un autre utilisateur.

2) Analyse des données (Data Sniffing)

Les pirates utilisent cette méthode pour intercepter les données du réseau lorsqu'elles circulent sur des réseaux non sécurisés, comme Internet. Les outils permettant ce type d'activité, tels que les analyseurs de protocole et les outils de diagnostic réseau, sont souvent intégrés aux systèmes d'exploitation et permettent de visualiser les données en clair.

3) Attaques centralisées (Man in the middle)

Une fois que le pirate a analysé ou usurpé suffisamment d'informations, il peut entreprendre une attaque centralisée. Le pirate déclenche cette attaque lorsque les données sont transmises d'un réseau à un autre, en déroutant les données vers une autre destination. Même si les données ne parviennent jamais à leur destinataire initial, l'expéditeur a l'impression que la transmission a réussi.

Il s'agit là uniquement d'un petit aperçu des méthodes utilisées par les pirates, qui ne cessent de perfectionner leurs techniques. Sans la sécurité d'un VPN, vos données sont constamment à la merci de telles attaques lorsqu'elles sont transmises via Internet. Les données transmises via Internet transitent souvent par de nombreux serveurs dans le monde avant d'arriver à destination. Ce parcours est très long pour des données non sécurisées, ce qui montre bien tout l'intérêt du VPN.

Qu'est-ce qu'un VPN ?

Un VPN, ou réseau privé virtuel, est une connexion entre deux points terminaux (routeur VPN, par exemple) situés sur différents réseaux, qui permet de sécuriser l'envoi de données privées sur un réseau partagé ou public, tel qu'Internet. Cette structure permet de créer un réseau privé capable d'envoyer des données de manière sécurisée entre ces deux emplacements ou réseaux.

L'opération nécessite la création d'un « tunnel ». Un tunnel VPN connecte les deux ordinateurs ou réseaux et permet aux données de transiter sur Internet, comme si elles ne sortaient pas de ces réseaux. Il ne s'agit évidemment pas d'un tunnel au sens propre, mais d'une connexion sécurisée qui crypte les données transmises entre les deux réseaux.

Le VPN est une alternative économique à la ligne louée, privée et dédiée pour établir un réseau privé. Utilisant des techniques de cryptage et d'authentification normalisées (IPSec, pour IP Security), le VPN crée une connexion sécurisée qui, dans les faits, fonctionne comme si vous étiez connecté directement à votre réseau local. Un VPN peut être utilisé pour créer un réseau sécurisé reliant un site central avec des bureaux distants, des télétravailleurs ou des collaborateurs itinérants (ces derniers peuvent aussi se connecter à un routeur VPN à l'aide d'un ordinateur équipé du logiciel Cisco QuickVPN Client).

Il existe deux façons très simples de créer une connexion VPN :

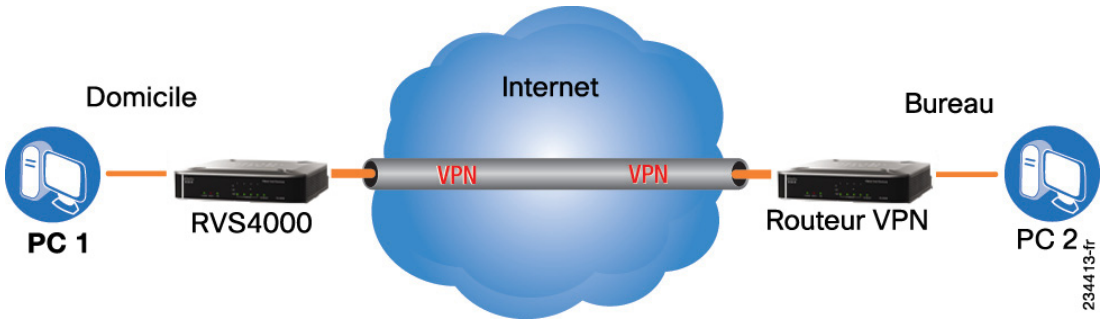
- Routeur VPN vers routeur VPN
- Ordinateur (utilisant le logiciel Cisco QuickVPN Client) vers routeur VPN

Le routeur VPN crée un « tunnel » ou un canal entre deux points terminaux, de sorte que les transmissions de données entre eux sont sécurisées. L'un de ces deux points terminaux peut être un ordinateur équipé du logiciel Cisco QuickVPN Client (reportez-vous à l'**Annexe B, « Utilisation de Cisco QuickVPN pour Windows 2000, XP ou Vista »**). Si vous choisissez de ne pas recourir au logiciel client VPN, tout ordinateur équipé du gestionnaire de sécurité IPSec intégré (Microsoft 2000 et XP) permet au routeur VPN de créer un tunnel VPN en utilisant les techniques IPSec (reportez-vous à l'**Annexe C, « Configuration d'IPSec avec un ordinateur exécutant Windows 2000 ou XP »**). D'autres versions de systèmes d'exploitation Microsoft requièrent l'installation de logiciels client VPN tiers supplémentaires qui prennent en charge IPSec.

Routeur VPN vers routeur VPN

Avec un VPN routeur VPN vers routeur VPN, un télétravailleur utilise son routeur VPN pour sa connexion permanente à Internet. Son routeur est configuré avec les paramètres VPN de son bureau. Lorsqu'il se connecte au routeur de son bureau, les deux routeurs créent un tunnel VPN, qui crypte et décrypte les données. Puisque les VPN utilisent Internet, la distance ne pose aucun problème. Grâce au VPN, le télétravailleur dispose ainsi d'une connexion sécurisée au réseau du site central de sa société, comme s'il y était physiquement connecté. Pour obtenir plus d'informations, reportez-vous à l'**Annexe D, « Tunnel VPN passerelle à passerelle ».**

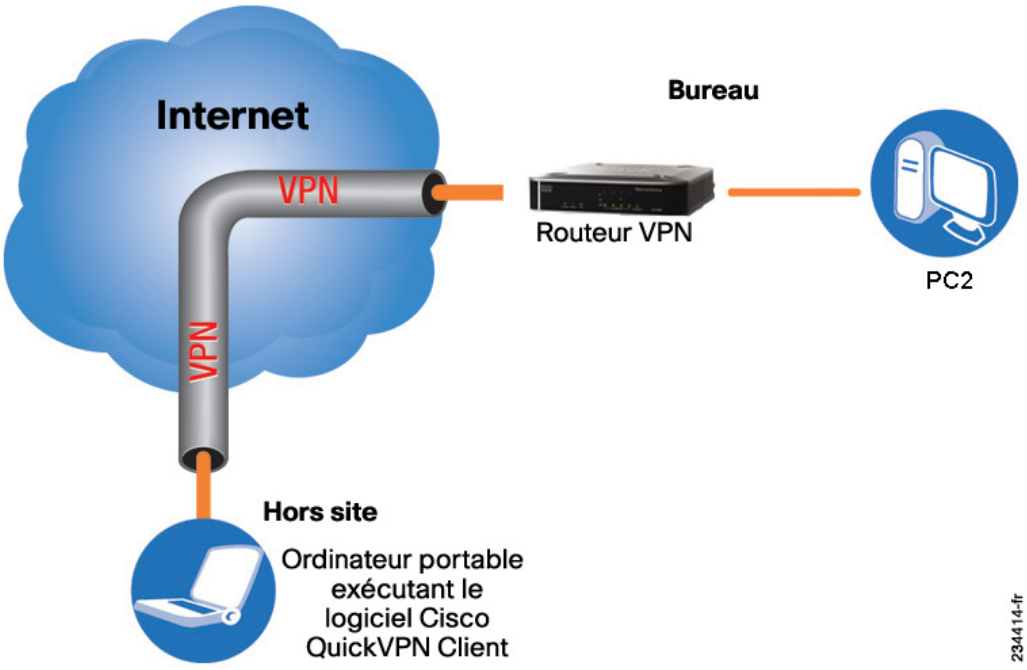
Routeur VPN vers routeur VPN



Ordinateur (utilisant le logiciel Cisco QuickVPN Client) vers routeur VPN

Dans cette illustration, vous pouvez voir un exemple de VPN ordinateur vers routeur VPN. Dans sa chambre d'hôtel, une femme d'affaires en déplacement se connecte à son FAI. Son ordinateur portable est équipé du logiciel Cisco QuickVPN Client, qui est configuré avec l'adresse IP de son bureau. Elle accède au logiciel Cisco QuickVPN Client et se connecte au routeur VPN du site central. Puisque les VPN utilisent Internet, la distance ne pose aucun problème. Grâce au VPN, cette personne dispose d'une connexion sécurisée au réseau du site central de sa société, comme si elle y était physiquement connectée.

Ordinateur vers routeur VPN



Pour obtenir des informations et des instructions supplémentaires sur la création de votre VPN, consultez le site www.cisco.com. Vous pouvez également vous reporter à l'**Annexe B, « Utilisation de Cisco QuickVPN pour Windows 2000, XP ou Vista »**, à l'**Annexe C, « Configuration d'IPSec avec un ordinateur exécutant Windows 2000 ou XP »** et à l'**Annexe D, « Tunnel VPN passerelle à passerelle ».**

4

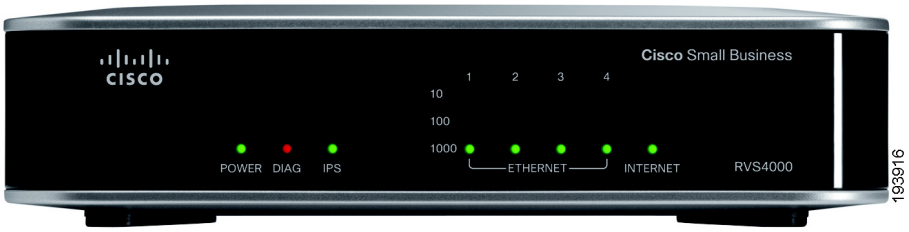
Mise en route du routeur RVS4000

Ce chapitre décrit les caractéristiques physiques du routeur RVS4000 et explique comment procéder à son installation. Il comprend les sections suivantes :

Façade

Les DEL sont situées sur la façade du routeur.

Façade



DEL POWER : stabilisée au vert lorsque le routeur est sous tension. Clignote lorsque le routeur effectue un test de diagnostic.

DEL DIAG : s'éteint lorsque le système est prêt. Clignote en rouge pendant les mises à niveau du microprogramme.

DEL IPS : stabilisée au vert lorsque la fonction IPS est activée. S'éteint lorsque la fonction IPS est désactivée. Clignote en vert lorsqu'une attaque externe est détectée. Clignote en rouge lorsqu'une attaque interne est détectée.

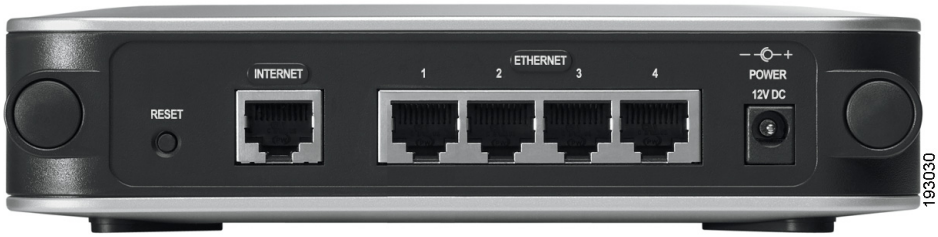
DEL des ports ETHERNET (1 à 4) : chaque port LAN est associé à trois DEL. Stabilisée au vert lorsque le routeur est connecté à un périphérique au débit indiqué, par l'intermédiaire du port correspondant (1, 2, 3 ou 4). Clignote en vert lorsque le routeur est en train d'envoyer ou de recevoir des données sur ce port.

DEL INTERNET : stabilisée au vert pour indiquer le débit de ligne du périphérique relié au port INTERNET. Clignote pour indiquer l'activité. Si le routeur est connecté à un modem câble ou DSL, la DEL 100 est généralement la seule DEL allumée. Celle-ci indique un débit de 100 Mbit/s.

Panneau arrière

Les ports ETHERNET, le port INTERNET, le bouton RESET et le port POWER sont situés sur le panneau arrière du routeur.

Panneau arrière



Bouton RESET : vous pouvez utiliser ce bouton de deux façons :

- Si le routeur rencontre des difficultés lors de la connexion à Internet, appuyez une seconde sur le bouton RESET avec la pointe d'un crayon ou avec un trombone. Cela équivaut à appuyer sur le bouton RESET de votre ordinateur, pour le faire redémarrer.
- Si le routeur rencontre des problèmes graves et que vous avez épuisé toutes les autres méthodes de dépannage, appuyez sur le bouton RESET et maintenez-le enfoncé pendant 10 secondes. Cette action rétablira les paramètres d'usine et supprimera tous les réglages effectués sur le routeur (transfert de port ou nouveau mot de passe, par exemple).

Port INTERNET : fournit une connexion WAN à un modem câble ou DSL.

Ports ETHERNET (1 à 4) : fournissent une connexion LAN à des périphériques réseau, tels que des ordinateurs, des serveurs d'impression et des commutateurs supplémentaires.

Port POWER : permet de connecter le routeur à une source d'alimentation, à l'aide de l'adaptateur secteur CA (fourni).

Dispositions possibles

Vous pouvez poser le routeur à l'horizontale, sur ses pieds en caoutchouc, sur les socles ou encore, sur un mur.

Montage sur bureau

Pour installer le routeur Cisco RVS4000 sur un bureau, positionnez-le à l'horizontale, sur ses pieds en caoutchouc.

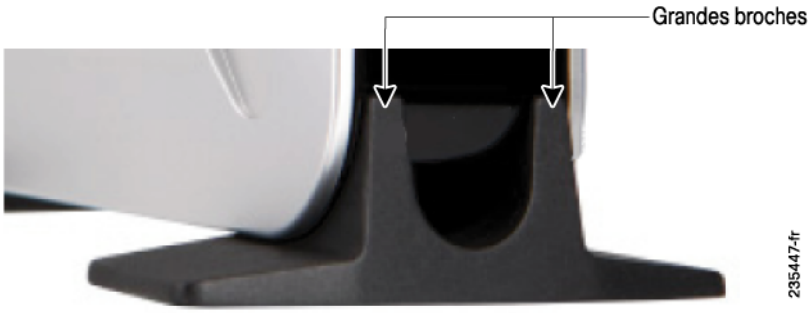
Montage sur support

Pour installer le routeur à la verticale, sur les socles fournis, procédez comme indiqué ci-après.

Pour positionner le routeur à la verticale, procédez comme suit.

ÉTAPE 1 Repérez le panneau latéral gauche du routeur.

ÉTAPE 2 Placez les broches les plus grandes de l'un des socles vers l'extérieur du routeur et insérez les petites broches dans les logements du routeur, puis poussez le socle vers le haut, jusqu'à ce qu'il s'enclenche dans le routeur.



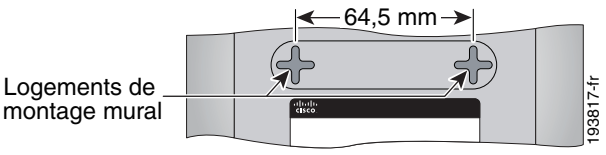
ÉTAPE 3 Répétez l'étape 2 avec le deuxième socle.

Contre un mur

Pour installer le routeur Cisco RVS4000 contre un mur, procédez comme suit.

ÉTAPE 1 Déterminez l'endroit du mur où vous souhaitez installer le routeur et placez-y deux vis (non fournies) à environ 64,5 mm de distance l'une de l'autre.

ÉTAPE 2 Placez le routeur de sorte que le panneau arrière soit dirigé vers le haut (pour un montage à la verticale), alignez sur les deux vis les logements en étoile de montage mural, qui sont situés au bas du point d'accès.



ÉTAPE 3 Placez les logements de montage mural au-dessus des vis, puis faites glisser le routeur vers le bas, jusqu'à introduire doucement les têtes de vis dans ces logements.

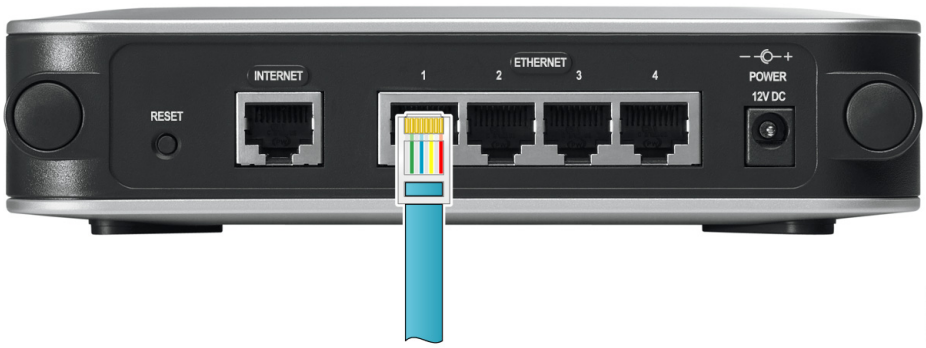
Installation du routeur

Pour préparer le routeur en vue de son installation, procédez comme suit :

- Obtenez les informations de configuration spécifiques à votre type de connexion Internet, auprès de votre fournisseur d'accès à Internet (FAI).
- Mettez hors tension l'ensemble des éléments matériels de votre réseau, notamment le routeur, les ordinateurs et le modem câble ou DSL.

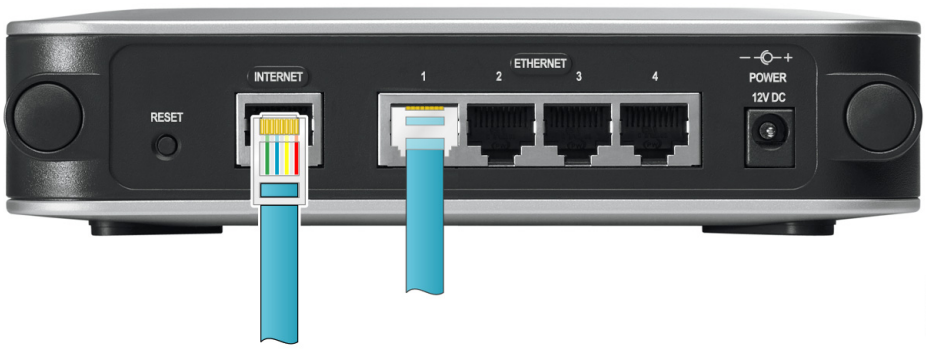
Pour installer le matériel, suivez les étapes détaillées dans cette section.

ÉTAPE 1 Reliez une extrémité d'un câble réseau Ethernet à l'un des ports LAN (numérotés 1 à 4) situés à l'arrière du routeur. Branchez l'autre extrémité de ce câble sur le port ETHERNET d'un ordinateur.



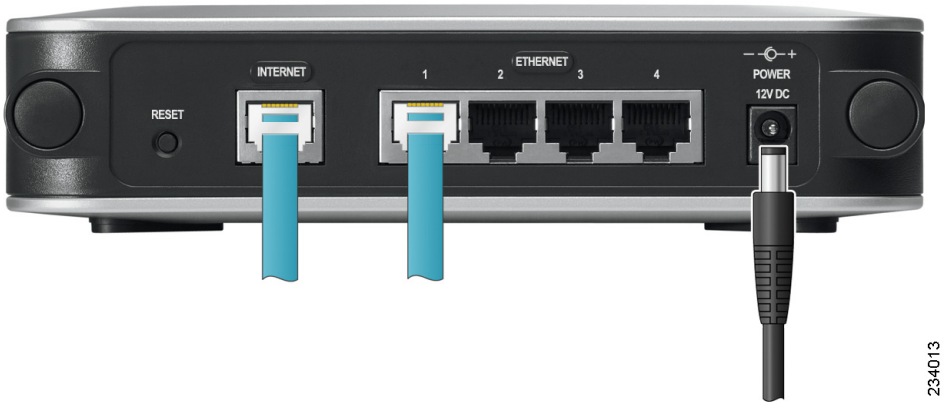
ÉTAPE 2 Répétez l'étape 1 pour connecter jusqu'à quatre ordinateurs, commutateurs ou autres périphériques réseau au routeur.

ÉTAPE 3 Branchez une extrémité d'un câble réseau Ethernet sur votre modem câble ou DSL et l'autre extrémité, sur le port INTERNET situé à l'arrière du routeur.



ÉTAPE 4 Mettez sous tension le modem câble ou DSL.

ÉTAPE 5 Branchez l'adaptateur secteur sur le port POWER du routeur, puis branchez l'autre extrémité sur une prise électrique.



ÉTAPE 6 Les DEL POWER et INTERNET, situées sur la façade, s'allument en vert dès que l'adaptateur secteur est correctement branché.

ÉTAPE 7 Allumez les ordinateurs.

L'installation matérielle du routeur est maintenant terminée.

Configuration du routeur

Pour configurer le RVS4000, connectez un ordinateur au routeur et lancez l'utilitaire de configuration.

REMARQUE Avant de configurer le routeur, vérifiez que vos ordinateurs sont configurés de telle manière que le routeur peut leur attribuer automatiquement une adresse IP (ou TCP/IP).

ÉTAPE 1 Ouvrez un navigateur Web comme Internet Explorer ou Mozilla Firefox.

ÉTAPE 2 Dans le champ Adresse, saisissez **192.168.1.1,** puis appuyez sur **Entrée**.

ÉTAPE 3 Dans les champs User Name et Password, saisissez **admin**.

Les nom d'utilisateur et mot de passe par défaut sont **admin**.

ÉTAPE4 Cliquez sur **OK**.

Pour plus de sécurité, nous vous recommandons de définir ultérieurement un nouveau mot de passe, dans la page *Administration > Management* de l'utilitaire de configuration.

ÉTAPE 5 L'utilitaire de configuration s'affiche avec le menu Setup et Summary sélectionnés. Cliquez sur **WAN,** dans le menu Setup.

ÉTAPE 6 Si votre FAI (généralement un FAI câble) l'exige, remplissez les champs Host Name et Domain Name et les champs MTU et MTU Size. Sinon, conservez les valeurs par défaut.

ÉTAPE 7 Dans l'écran WAN, choisissez un type de connexion Internet, à partir du menu déroulant. Des procédures de configuration supplémentaires peuvent s'avérer nécessaires, selon le type de connexion Internet sélectionné.

Les différents types de connexion Internet sont répertoriés ci-après.

Automatic Configuration - DHCP : si vous vous connectez à votre fournisseur d'accès Internet au moyen d'une adresse DHCP ou d'une adresse IP dynamique, conservez ce paramètre par défaut.

Static IP : si votre fournisseur d'accès Internet vous attribue une adresse IP statique, sélectionnez Static IP dans le menu déroulant. Remplissez les champs Internet IP Address, Subnet Mask, Default Gateway et DNS. Saisissez au moins une adresse DNS.

PPPoE : si vous vous connectez via le protocole PPPoE, sélectionnez PPPoE dans le menu déroulant. Renseignez les champs User Name et Password.

PPTP : le type PPTP est utilisé uniquement en Europe. Si vous utilisez une connexion PPTP, demandez les informations de configuration nécessaires à votre FAI.

Heartbeat Signal : le type Heartbeat Signal est principalement utilisé en Australie. Demandez les informations de configuration nécessaires à votre FAI.

L2TP : le type L2TP est surtout utilisé en Europe. Demandez les informations de configuration nécessaires à votre FAI.

ÉTAPE 8 Lorsque tous vos paramètres de connexion Internet sont corrects, cliquez sur **Save**.

ÉTAPE 9 Redémarrez votre ordinateur ou mettez-le sous tension, pour obtenir la nouvelle configuration du routeur.

ÉTAPE 10 Pour tester la configuration, ouvrez votre navigateur Web à partir de n'importe quel ordinateur, puis saisissez www.cisco.com/smb.

Félicitations ! L'installation du routeur est terminée.

REMARQUE Pour obtenir plus d'informations sur les paramètres et options de sécurité avancés, reportez-vous au **Chapitre 5, « Configuration du routeur ».**

5

Configuration du routeur

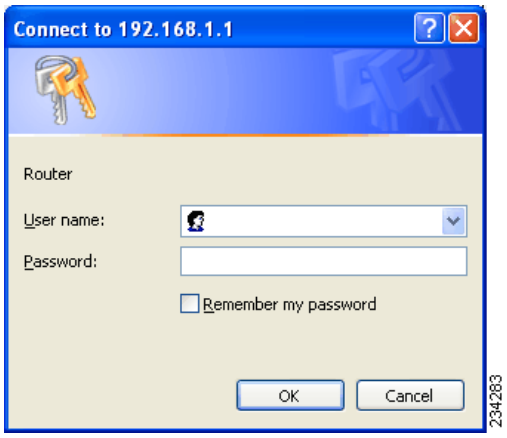
Ce chapitre décrit la procédure à suivre pour configurer les fonctions suivantes du routeur :

Configurez le routeur au moyen de l'utilitaire de configuration Web intégré. Pour accéder à l'utilitaire de configuration du routeur, ouvrez votre navigateur Web et saisissez **http://192.168.1.1** dans le champ Adresse. Appuyez sur la touche **Entrée**. La fenêtre *Login* s'affiche.

REMARQUE L'adresse IP par défaut est **192.168.1.1**. Si l'adresse IP par défaut a été modifiée via DHCP ou l'interface de la console, saisissez l'adresse IP attribuée au lieu de celle-ci.

La première fois que vous ouvrez l'utilitaire de configuration, entrez **admin (**nom d'utilisateur par défaut) dans le champ *Username* et **admin** également dans le champ *Password*. Cliquez sur le bouton **OK**. Vous pouvez modifier le mot de passe par la suite dans la fenêtre *Administration* > *Management*.

Fenêtre Login



Une fois que vous êtes connecté, l'utilitaire de configuration s'ouvre. Les menus s'affichent sous la forme de liens dans le volet de navigation situé à gauche de l'écran. Lorsque vous sélectionnez un menu, une liste de fenêtres s'affiche. Pour exécuter une fonction spécifique, sélectionnez un menu, puis la fenêtre adéquate. Par défaut, la fenêtre *Summary* du menu Setup apparaît une fois que vous êtes connecté.

Les sections qui suivent décrivent les menus et les fenêtres de l'utilitaire. Par souci de concision, les noms des fenêtres sont indiqués au format *Menu > Fenêtre*.

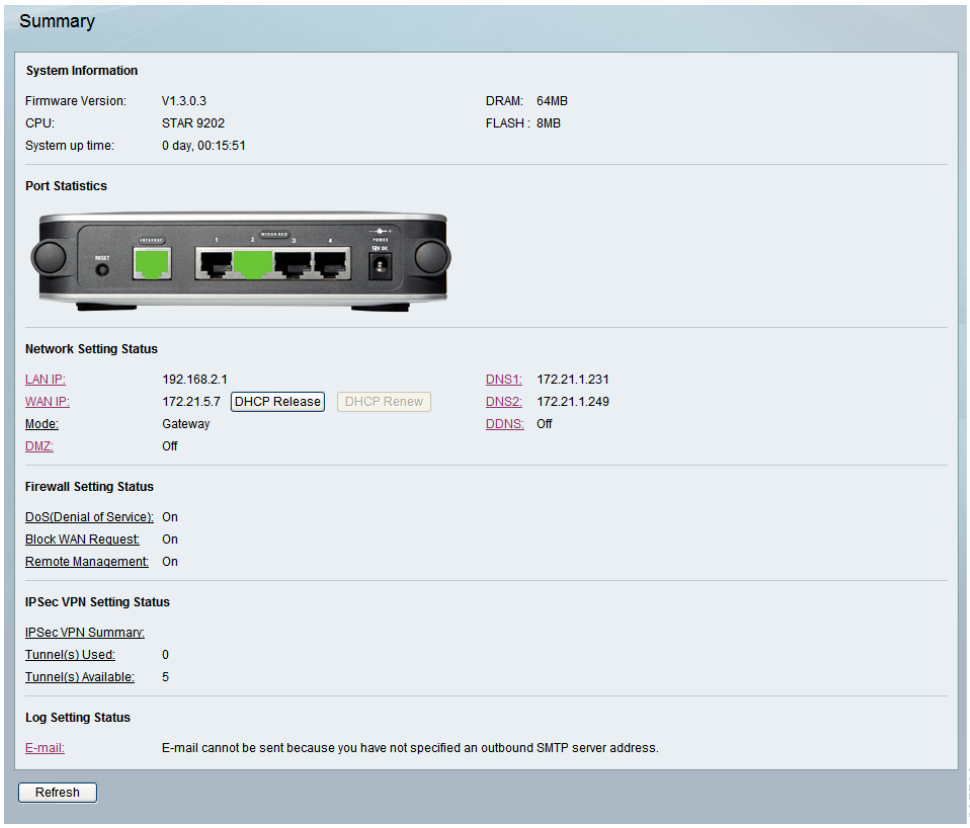
Setup

Utilisez le menu Setup pour accéder aux fonctions de configuration de base du routeur. Vous pouvez utiliser le routeur avec la plupart des configurations réseau, sans modification des valeurs par défaut. Certains utilisateurs devront peut-être entrer des informations supplémentaires pour se connecter à Internet via un FAI (fournisseur d'accès Internet) ou via une porteuse haut débit (DSL, modem câble).

Setup > Summary

La fenêtre *Setup > Summary* affiche un résumé en lecture seule des informations de base du routeur. Cliquez sur un lien hypertexte (texte souligné) pour ouvrir une page connexe permettant de mettre à jour ces informations.

Setup > Summary



System Information

Firmware Version : indique la version de microprogramme actuelle du routeur.

CPU : indique le type d'UC (unité centrale) du routeur.

System up time : indique le temps écoulé depuis la dernière réinitialisation du routeur.

DRAM : indique la capacité de mémoire DRAM installée dans le routeur.

FLASH : affiche la capacité de mémoire Flash installée dans le routeur.

Port Statistics

Cette section fournit des informations d'état sur les ports Ethernet du routeur à l'aide de codes couleur :

- **Vert** : indique que le port dispose d'une connexion.
- **Noir** : indique que le port ne dispose pas de connexion.

Network Setting Status

LAN IP : adresse IP de l'interface LAN du routeur.

WAN IP : adresse IP de l'interface WAN du routeur. Si cette adresse a été attribuée au moyen de DHCP, cliquez sur **DHCP Release** pour la libérer ou sur **DHCP Renew** pour la renouveler.

Mode : mode de fonctionnement, à savoir **Gateway** ou **Router**.

Gateway : adresse de passerelle, c'est-à-dire l'adresse IP du serveur de votre FAI.

DNS 1-2 : adresses IP du ou des serveurs DNS (Domain Name System, système de noms de domaine) que le routeur utilise.

DDNS : indique si la fonction DDNS (Dynamic Domain Name System, système de noms de domaine dynamique) est activée.

DMZ : indique si la fonction d'hébergement DMZ est activée.

Firewall Setting Status

DoS (Denial of Service) : indique si la fonction de protection contre les attaques DoS (Denial of Service, déni de service) est activée.

Block WAN Request : indique si la fonction de blocage des requêtes WAN est activée.

Remote Management : indique si la fonction de gestion à distance est activée.

IPSec VPN Setting Status

IPSec VPN Summary : cliquez sur le lien hypertexte **IPSec VPN Summary** pour afficher la fenêtre *VPN > Summary*.

Tunnel(s) Used : affiche le nombre de tunnels VPN (Virtual Private Network, réseau privé virtuel) en cours d'utilisation.

Tunnel(s) Available : affiche le nombre de tunnels VPN disponibles.

Log Setting Status

E-mail : si le message *Email cannot be sent because you have not specified an outbound SMTP server address* est affiché, cela signifie que vous n'avez pas configuré le serveur de messagerie. Cliquez sur le lien hypertexte **E-mail** pour afficher la fenêtre *Administration > Log* où vous pouvez configurer le serveur de messagerie SMTP.

Setup > WAN

Internet Connection Type

Le routeur prend en charge six types de connexions. Chaque fenêtre *Setup > WAN* et les fonctionnalités disponibles diffèrent en fonction du type de connexion sélectionnée.

Automatic Configuration—DHCP

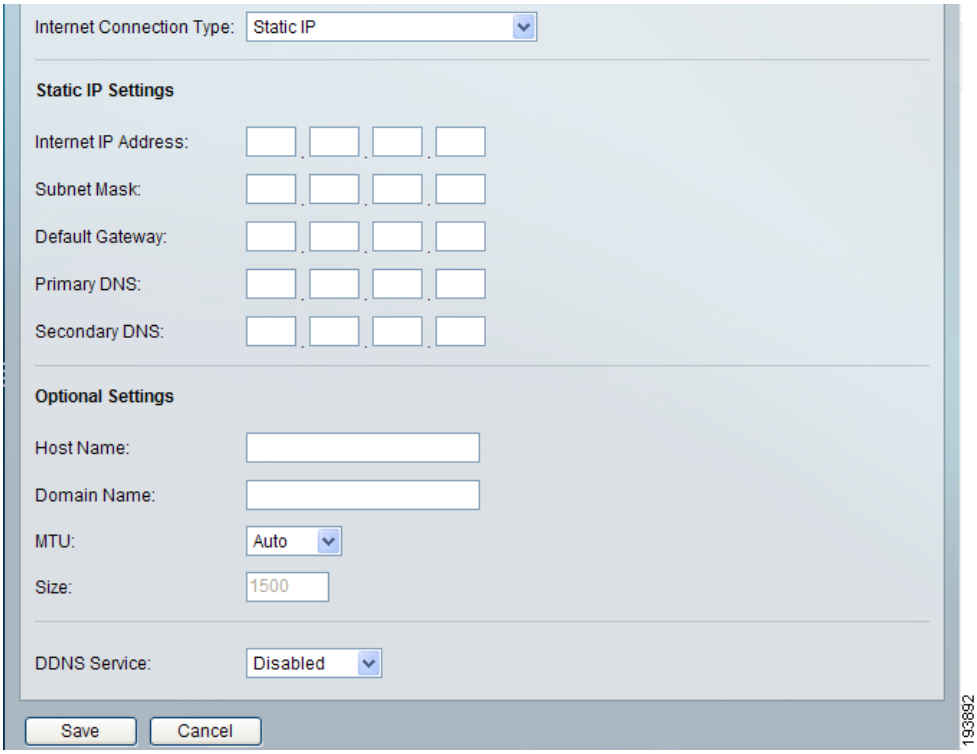
Par défaut, le type de configuration du routeur est réglé sur **Automatic Configuration—DHCP**. Ne conservez cette option que si votre FAI prend en charge le protocole DHCP ou si vous vous connectez via une adresse IP dynamique.

Automatic Configuration—DHCP

Static IP

Si votre connexion utilise une adresse IP permanente pour la connexion à Internet, sélectionnez **Static IP.**

Static IP



Internet IP Address : adresse IP du routeur, telle qu'elle est vue depuis le WAN (Wide-Area Network, réseau étendu) ou depuis Internet. Votre FAI peut vous fournir l'adresse IP que vous devez spécifier dans ce champ.

Subnet Mask : masque de sous-réseau du routeur, tel qu'il est vu par les utilisateurs externes sur Internet (y compris votre FAI). Votre FAI peut vous indiquer le masque de sous-réseau à spécifier.

Default Gateway : votre FAI peut vous fournir l'adresse de la passerelle par défaut (il s'agit en fait de l'adresse IP du serveur du FAI).

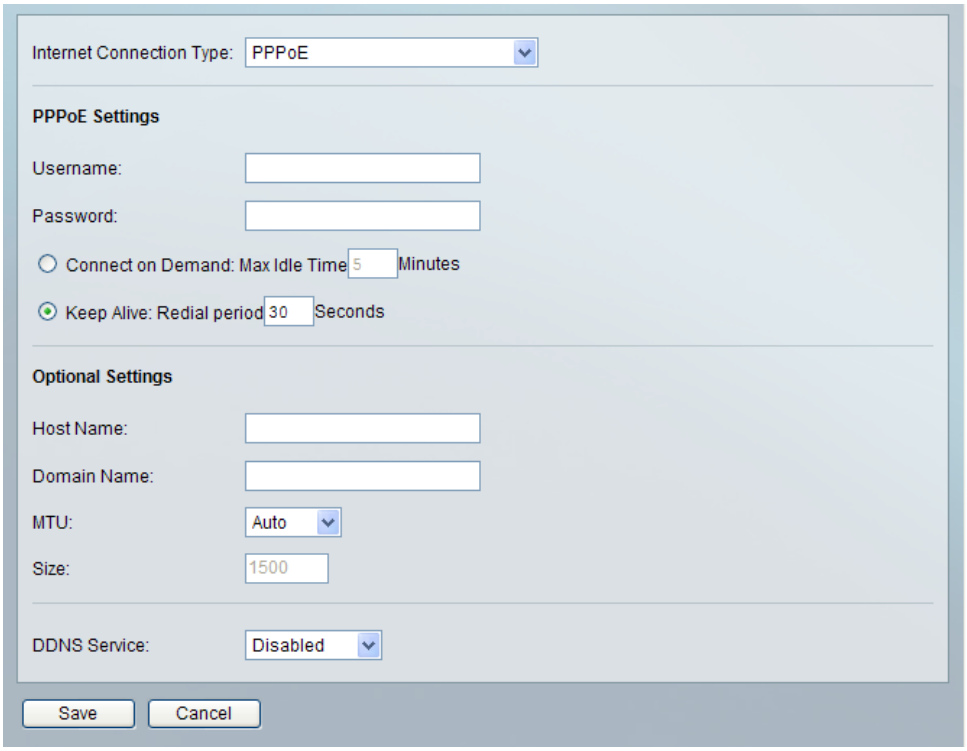
Primary DNS (obligatoire) et Secondary DNS (facultatif) : votre FAI peut vous fournir au moins une adresse IP de serveur DNS.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

PPPoE

Certains FAI DSL utilisent le protocole PPPoE (Point-to-Point Protocol over Ethernet) pour établir des connexions Internet. Si vous êtes connecté à Internet via une ligne DSL, vérifiez auprès de votre FAI s'il utilise ce protocole. Si c'est le cas, activez PPPoE.

PPPoE



Username et Password : saisissez le nom d'utilisateur et le mot de passe fournis par votre FAI.

Connect on Demand: Max Idle Time : vous pouvez configurer le routeur pour qu'il ferme la connexion Internet après une période d'inactivité spécifiée (Max Idle Time) et qu'il la rétablisse automatiquement lorsque vous tentez d'accéder à nouveau à Internet. Pour activer la fonctionnalité de connexion à la demande, sélectionnez l'option **Connect on Demand** et, dans le champ *Max Idle Time*, entrez le nombre de minutes d'inactivité devant s'écouler avant que le routeur mette automatiquement fin à la connexion Internet.

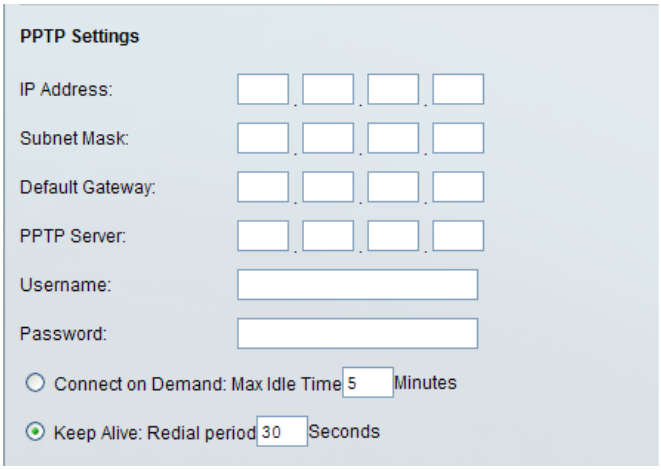
Keep Alive: Redial period : lorsque cette option est sélectionnée, le routeur procède régulièrement à une vérification de la connexion Internet. Si vous êtes déconnecté, le routeur rétablit alors automatiquement votre connexion. Si vous souhaitez sélectionner cette option, cliquez sur le bouton radio **Keep Alive**. Dans le champ *Redial period*, indiquez la fréquence à laquelle le routeur doit vérifier votre connexion Internet. Par défaut, le temps devant s'écouler avant rappel est de **30** secondes.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

PPTP

Le protocole PPTP (Point-to-Point Tunneling Protocol) est un service concernant uniquement les connexions en Europe et en Israël.

PPTP



IP Address : adresse IP du routeur, telle qu'elle est vue depuis le WAN ou depuis Internet. Votre FAI peut vous fournir l'adresse IP que vous devez spécifier dans ce champ.

Subnet Mask : masque de sous-réseau du routeur, tel qu'il est vu par les utilisateurs externes sur Internet (y compris votre FAI). Votre FAI peut vous indiquer le masque de sous-réseau à spécifier.

Default Gateway : votre FAI peut vous fournir l'adresse de passerelle par défaut à spécifier.

PPTP Server : saisissez l'adresse IP du serveur PPTP.

Username et Password : saisissez le nom d'utilisateur et le mot de passe fournis par votre FAI.

Connect on Demand: Max Idle Time : vous pouvez configurer le routeur pour qu'il ferme la connexion Internet après une période d'inactivité spécifiée (Max Idle Time) et qu'il la rétablisse automatiquement lorsque vous tentez d'accéder à nouveau à Internet. Pour activer la fonctionnalité de connexion à la demande, sélectionnez l'option **Connect on Demand** et, dans le champ *Max Idle Time*, entrez le nombre de minutes d'inactivité devant s'écouler avant que le routeur mette automatiquement fin à la connexion Internet.

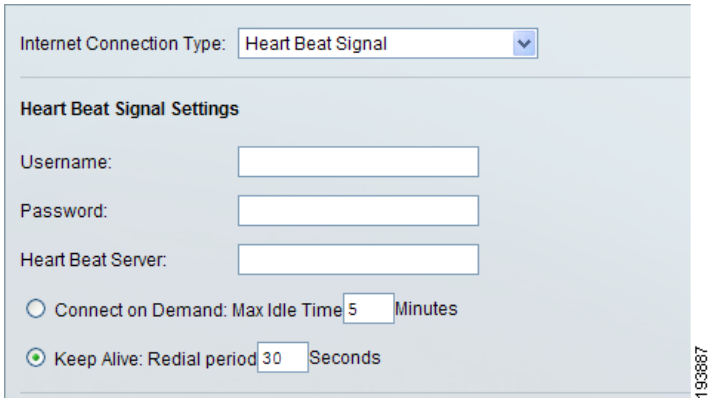
Keep Alive: Redial period : lorsque cette option est sélectionnée, le routeur procède régulièrement à une vérification de la connexion Internet. Si vous êtes déconnecté, le routeur rétablit alors automatiquement votre connexion. Si vous souhaitez sélectionner cette option, cliquez sur le bouton radio **Keep Alive**. Dans le champ *Redial period*, indiquez la fréquence à laquelle le routeur doit vérifier votre connexion Internet. Par défaut, le temps devant s'écouler avant rappel est de **30** secondes.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

Heart Beat Signal (HBS)

Heart Beat Signal est un service utilisé en Australie. Demandez les informations de configuration nécessaires à votre FAI.

Heart Beat Signal (HBS)



Username et Password : saisissez le nom d'utilisateur et le mot de passe fournis par votre FAI.

Heart Beat Server : saisissez l'adresse IP du serveur Heart Beat.

Connect on Demand: Max Idle Time : vous pouvez configurer le routeur pour qu'il ferme la connexion Internet après une période d'inactivité spécifiée (Max Idle Time) et qu'il la rétablisse automatiquement lorsque vous tentez d'accéder à nouveau à Internet. Pour activer la fonctionnalité de connexion à la demande, sélectionnez l'option **Connect on Demand** et, dans le champ *Max Idle Time*, entrez le nombre de minutes d'inactivité devant s'écouler avant que le routeur mette automatiquement fin à la connexion Internet.

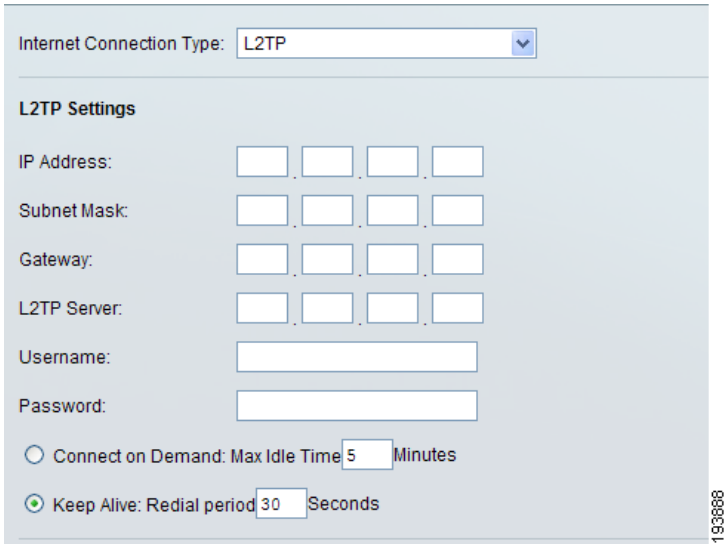
Keep Alive: Redial period : lorsque cette option est sélectionnée, le routeur procède régulièrement à une vérification de la connexion Internet. Si vous êtes déconnecté, le routeur rétablit alors automatiquement votre connexion. Si vous souhaitez sélectionner cette option, cliquez sur le bouton radio **Keep Alive**. Dans le champ *Redial period*, indiquez la fréquence à laquelle le routeur doit vérifier votre connexion Internet. Par défaut, le temps devant s'écouler avant rappel est de **30** secondes.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

L2TP

Le protocole **L2TP (Layer 2 Tunneling Protocol)** est un service qui « tunnelise » le protocole PPP (Point-to-Point Protocol) via Internet. Il est principalement utilisé dans les pays européens. Demandez les informations de configuration nécessaires à votre FAI.

L2TP



IP Address : adresse IP du routeur, telle qu'elle est vue depuis le WAN ou depuis Internet. Votre FAI peut vous fournir l'adresse IP que vous devez spécifier dans ce champ.

Subnet Mask : masque de sous-réseau du routeur, tel qu'il est vu par les utilisateurs externes sur Internet (y compris votre FAI). Votre FAI peut vous indiquer le masque de sous-réseau à spécifier.

Gateway : votre FAI peut vous fournir l'adresse de passerelle par défaut à spécifier.

L2TP Server : saisissez l'adresse IP du serveur L2TP.

Username et Password : saisissez le nom d'utilisateur et le mot de passe fournis par votre FAI.

Connect on Demand: Max Idle Time : vous pouvez configurer le routeur pour qu'il ferme la connexion Internet après une période d'inactivité spécifiée (Max Idle Time) et qu'il la rétablisse automatiquement lorsque vous tentez d'accéder à nouveau à Internet. Pour activer la fonctionnalité de connexion à la demande, sélectionnez l'option **Connect on Demand** et, dans le champ *Max Idle Time*, entrez le nombre de minutes d'inactivité devant s'écouler avant que le routeur mette automatiquement fin à la connexion Internet.

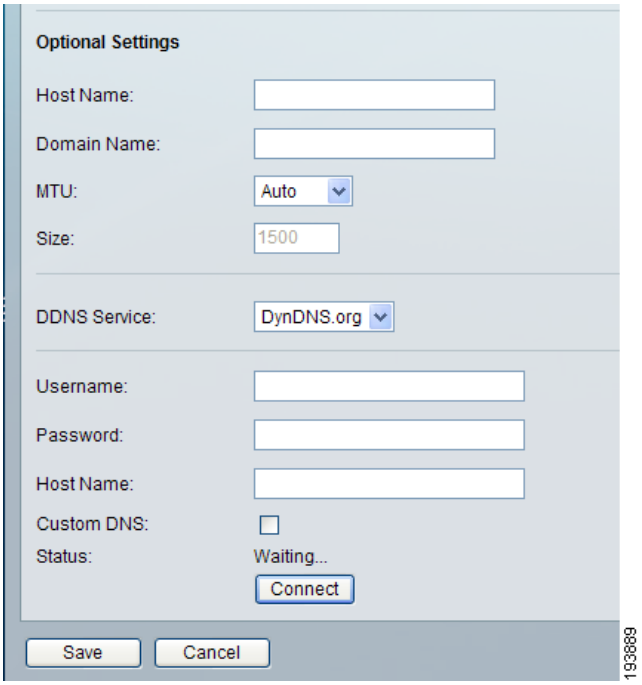
Keep Alive: Redial period : lorsque cette option est sélectionnée, le routeur procède régulièrement à une vérification de la connexion Internet. Si vous êtes déconnecté, le routeur rétablit alors automatiquement votre connexion. Si vous souhaitez sélectionner cette option, cliquez sur le bouton radio **Keep Alive**. Dans le champ *Redial period*, spécifiez la fréquence à laquelle le routeur doit vérifier votre connexion Internet. Par défaut, le temps devant s'écouler avant rappel est de **30** secondes.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

Optional Settings (requis par certains FAI)

Votre FAI peut exiger certains de ces paramètres. Renseignez-vous auprès de votre FAI avant d'effectuer des modifications.

Optional Settings



Host Name : certains FAI (les fournisseurs de services câblés généralement) exigent un nom d'hôte à des fins d'identification. Vous devrez peut-être vérifier auprès de votre FAI que votre service Internet haut débit a été configuré à l'aide d'un nom d'hôte. Dans la plupart des cas, vous pouvez laisser ce champ vide.

Domain Name : certains FAI (les fournisseurs de services câblés généralement) exigent un nom de domaine à des fins d'identification. Vous devrez peut-être vérifier auprès de votre FAI que votre service Internet haut débit a été configuré à l'aide d'un nom de domaine. Dans la plupart des cas, vous pouvez laisser ce champ vide.

MTU : Maximum Transmission Unit, ou unité de transmission maximale. Il s'agit de la taille de paquet maximale autorisée pour la transmission Internet. Sélectionnez Manual si vous souhaitez entrer manuellement la taille maximale de paquet qui sera transmise. Si vous préférez que le routeur sélectionne la valeur MTU optimale pour votre connexion Internet, conservez le paramètre par défaut, **Auto**.

Size : cette option est activée lorsque Manual est sélectionné dans le champ MTU. Il est recommandé d'affecter une valeur comprise entre 1200 et 1500 ; toutefois, vous pouvez entrer une valeur comprise entre 128 et 1500.

DDNS Service : le service DDNS est désactivé par défaut. Pour activer le service DDNS, procédez comme suit :

Connect : le bouton **Connect** est affiché lorsque DDNS est activé. Cliquez sur ce bouton pour contacter le serveur DDNS afin de mettre à jour manuellement vos informations d'adresse IP. La zone Status de cette fenêtre est également mise à jour.

ÉTAPE 1 Souscrivez à un service DDNS :

- DynDNS : vous pouvez souscrire à un service DDNS sur le site www.dyndns.org, en entrant votre nom d'utilisateur, votre mot de passe et votre nom d'hôte.
- TZO : vous pouvez souscrire à un service DDNS sur le site www.tzo.com, en entrant votre adresse électronique, votre mot de passe et votre nom de domaine.

ÉTAPE 2 Sélectionnez votre fournisseur de service DDNS.

ÉTAPE 3 Configurez les champs suivants :

- User Name (DynDNS) ou Email address (TZO)
- Mot de passe
- Host Name (DynDNS) ou Domain name (TZO)
- Custom DNS (DynDNS)

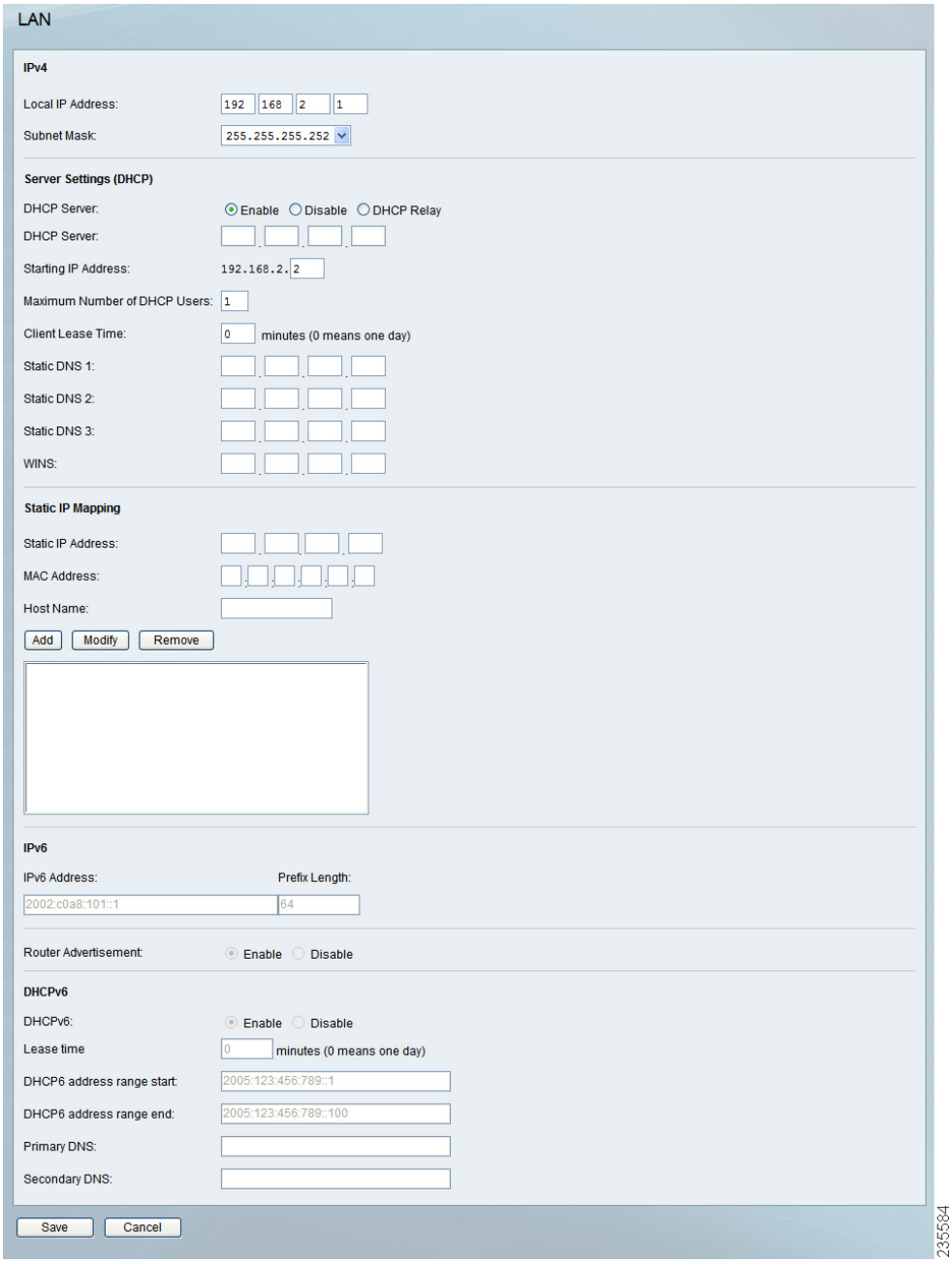
ÉTAPE 4 Cliquez sur **Save**.

Le routeur indique alors au service DDNS votre adresse IP (Internet) WAN actuelle ; il répète cette opération chaque fois que cette adresse change. Si vous utilisez TZO, ne recourez PAS au logiciel TZO pour effectuer la « mise à jour d'adresse IP ».

Setup > LAN

La fenêtre *Setup > LAN* vous permet de modifier les paramètres LAN (Local-Area Network, réseau local) du routeur.

Setup > LAN



VLAN : sélectionnez le VLAN (Virtual Local-Area Network, réseau local virtuel) du serveur DHCP dans le menu déroulant.

REMARQUE Cette option apparaît uniquement si vous avez créé au moins un VLAN dans la fenêtre *L2 Switch > Create VLAN*.

IPv4

Cette section affiche l'adresse IP locale et le masque de sous-réseau du routeur. Dans la plupart des cas, vous pouvez conserver les valeurs par défaut.

Local IP Address : la valeur par défaut est 192.168.1.1.

Subnet Mask : la valeur par défaut est 255.255.255.0.

Server Settings (DHCP)

Il est possible d'utiliser le routeur en tant que serveur DHCP (Dynamic Host Configuration Protocol) de votre réseau. Ce serveur affecte automatiquement une adresse IP à chaque ordinateur du réseau. À moins que vous ne disposiez déjà d'un serveur DHCP, il est recommandé de laisser la fonction de serveur DHCP activée pour le routeur.

DHCP Server : DHCP est activé par défaut. Si vous disposez déjà d'un serveur DHCP sur votre réseau ou si vous ne souhaitez utiliser aucun serveur DHCP, cliquez sur le bouton **Disable** (aucune autre fonctionnalité DHCP n'est alors disponible). Si vous disposez déjà d'un serveur DHCP sur votre réseau et que vous souhaitez utiliser ce routeur comme relais pour ce serveur DHCP, sélectionnez **DHCP Relay**, puis entrez l'adresse IP du serveur DHCP. Si vous désactivez DHCP, affectez une adresse IP statique au routeur.

Starting IP Address : saisissez la valeur de début que devra utiliser le serveur DHCP pour la publication des adresses IP. Cette valeur doit être 192.168.1.2 ou supérieure, mais inférieure à 192.168.1.254, car l'adresse IP par défaut du routeur est 192.168.1.1, et 192.168.1.255 correspond à l'adresse IP de diffusion.

Maximum Number of DHCP Users : saisissez le nombre maximal d'ordinateurs auxquels le serveur DHCP peut attribuer des adresses IP. Ce nombre ne peut pas être supérieur à 253. Pour déterminer la plage d'adresses IP DHCP, ajoutez l'adresse IP de début (100, par exemple) au nombre d'utilisateurs DHCP.

Client Lease Time : période pendant laquelle un client DHCP peut conserver l'adresse IP qui lui est attribuée avant d'envoyer une demande de renouvellement au serveur DHCP.

Static DNS 1-3 : le cas échéant, entrez la ou les adresses IP de votre ou vos serveurs DNS.

WINS (Windows Internet Naming Service) offre un service d'attribution de noms (similaire à DNS) au sein des réseaux Windows. Si vous optez pour un serveur WINS, saisissez son adresse IP dans ce champ. Sinon, laissez-le vide.

Static IP Mapping

La section Static IP Mapping sert à lier une adresse IP spécifique à une adresse MAC spécifique. Ceci permet aux utilisateurs WAN externes d'accéder plus facilement aux serveurs LAN signalés par le biais du transfert de port NAPT. Vous pouvez définir jusqu'à 50 entrées.

Static IP Address : saisissez l'adresse IP à mapper.

MAC Address : saisissez l'adresse MAC à mapper.

Host Name : saisissez le nom d'hôte à mapper.

Cliquez sur **Add** pour créer l'entrée et l'ajouter à la liste. Pour modifier une entrée existante, sélectionnez-la dans la liste, modifiez le ou les champs voulus, puis cliquez sur **Modify**. Pour supprimer une entrée, sélectionnez-la et cliquez sur **Remove**.

IPv6

IPv6 Address : si votre réseau utilise IPv6, entrez l'adresse IPv6 appropriée dans ce champ.

Prefix Length : saisissez la longueur de préfixe IPv6 adéquate.

Router Advertisement : lorsque cette option est activée, elle permet la configuration automatique des adresses IP des hôtes IPv6 à l'aide de la fonctionnalité de diffusion de préfixe IPv6 du routeur.

DHCPv6

Pour activer la fonctionnalité DHCP v6, sélectionnez **Enable**. Pour désactiver DHCP v6, sélectionnez **Disable**.

Lease time : saisissez la durée du bail en minutes.

DHCP6 address range start : saisissez l'adresse IP DHCP v6 de début de plage.

DHCP6 address range end : saisissez l'adresse IP DHCP v6 de fin de plage.

Primary DNS : saisissez l'adresse du serveur DNS DHCP v6 principal.

Secondary DNS : saisissez l'adresse du serveur DNS DHCP v6 secondaire.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

Setup > DMZ

Vous pouvez configurer une DMZ (Demilitarized Zone, zone démilitarisée) afin de permettre à un ordinateur local d'accéder à Internet en vue d'utiliser un service particulier, de vidéoconférence ou de jeux sur Internet, par exemple. Tandis que le transfert de plage de ports ne permet de transférer que dix plages de ports au maximum, l'hébergement DMZ permet de transférer simultanément tous les ports d'un ordinateur.

Setup > DMZ

DMZ Hosting : la fonctionnalité d'hébergement DMZ permet à un ordinateur local d'accéder à Internet en vue d'utiliser un service spécifique de vidéoconférence ou de jeux sur Internet, par exemple. Pour activer cette fonctionnalité, sélectionnez **Enable**. Pour la désactiver, sélectionnez **Disable**.

DMZ Host IP Address : pour octroyer l'accès à Internet à un ordinateur, saisissez son adresse IP.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

Setup > MAC Address Clone

Avec certains FAI, vous devez obligatoirement enregistrer une adresse MAC. Cette fonctionnalité permet de « cloner » l'adresse MAC de votre carte réseau vers le routeur et vous évite d'appeler votre FAI pour transformer l'adresse MAC enregistrée en adresse MAC du routeur. L'adresse MAC du routeur est un code à 12 chiffres attribué à un composant matériel unique en vue de son identification.

Setup > MAC Address Clone

MAC Address Clone : sélectionnez **Enabled** ou **Disabled** dans la liste déroulante.

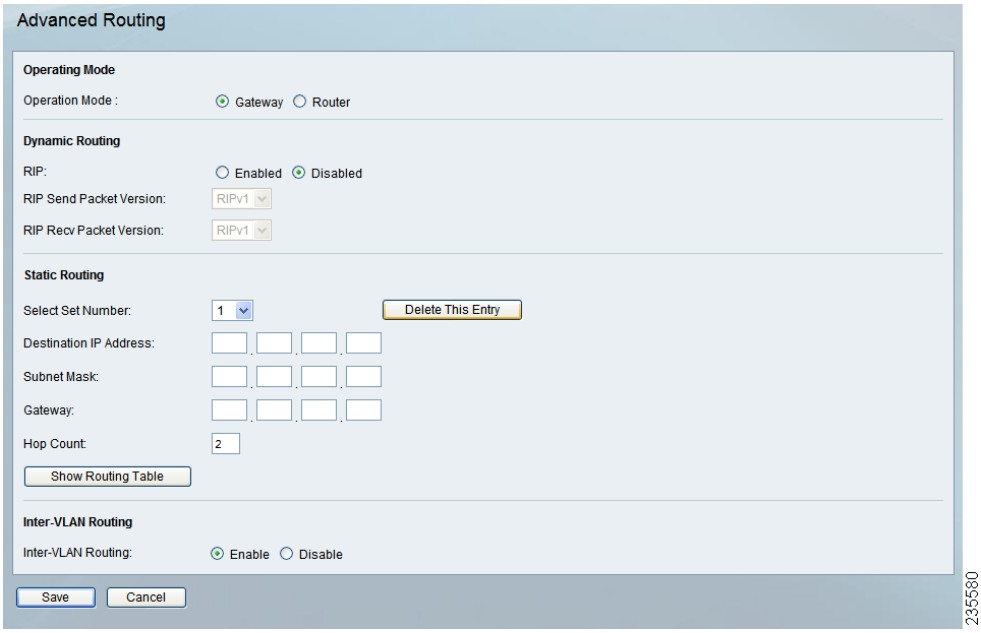
MAC Address : saisissez l'adresse MAC enregistrée auprès de votre FAI dans ce champ.

Clone My PC's MAC : si vous avez sélectionné Enabled en regard de MAC Address Clone, cliquez sur ce bouton pour copier l'adresse MAC de la carte réseau de l'ordinateur que vous utilisez pour la connexion à l'interface Web.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

Setup > Advanced Routing

Setup > Advanced Routing



Operating Mode

Operation Mode : sélectionnez le mode de fonctionnement de ce routeur.

- **Gateway** : le mode Passerelle est le mode de fonctionnement normal. Il permet à tous les périphériques du LAN de partager la même adresse IP (Internet) WAN. En mode Passerelle, le mécanisme NAT (Network Address Translation, traduction d'adresses réseau) est activé.
- **Router** : en mode Routeur, vous devez soit utiliser un autre routeur en tant que passerelle Internet, soit affecter à tous les ordinateurs de votre réseau local des adresses IP Internet (fixes). Dans ce mode, le mécanisme NAT est désactivé.

Dynamic Routing

Vous pouvez utiliser la fonctionnalité de routage dynamique pour permettre au routeur de s'adapter automatiquement aux modifications physiques intervenant dans la topologie du réseau. Le routeur peut utiliser le protocole RIP dynamique pour calculer l'itinéraire le plus efficace pour l'acheminement des paquets de données du réseau entre la source et la destination, d'après les chemins les plus courts. Le protocole RIP transmet régulièrement les informations de routage aux autres routeurs du réseau.

RIP (Routing Information Protocol) : si vous souhaitez que le routeur utilise le protocole RIP, sélectionnez **Enabled** ; sinon, conservez le paramètre par défaut, à savoir **Disabled**.

RIP Send Packet Version : choisissez le protocole à utiliser pour l'envoi des données sur le réseau, à savoir **RIPv1** ou **RIPv2**. La version choisie doit être prise en charge par les autres routeurs de votre réseau local.

RIP Recv Packet Version : choisissez le protocole à utiliser pour la réception des données sur le réseau, à savoir **RIPv1** ou **RIPv2**. La version choisie doit être prise en charge par les autres routeurs de votre réseau local.

Static Routing

Vous préférez parfois utiliser des chemins statiques pour créer votre table de routage au lieu d'utiliser des protocoles de routage dynamique. Les chemins statiques ne consomment pas de ressources UC pour l'échange d'informations de routage avec un routeur homologue. Vous pouvez également utiliser des chemins statiques pour atteindre des routeurs homologues qui ne prennent pas en charge les protocoles de routage dynamique. Les chemins statiques peuvent être utilisés avec des chemins dynamiques. Prenez garde à ne pas introduire de boucles de routage dans le réseau.

Pour configurer le routage statique, vous devez ajouter des entrées de chemins dans la table de routage afin d'indiquer au routeur les destinations IP spécifiques auxquelles transmettre les paquets.

Entrez les données suivantes afin de créer une entrée de chemin statique :

Select Set Number : sélectionnez le numéro d'ensemble (numéro d'entrée de la table de routage) à afficher ou configurer. Si nécessaire, cliquez sur **Delete This Entry** pour supprimer l'entrée.

Destination IP Address : saisissez l'adresse réseau du segment LAN distant. Pour un domaine IP de classe C classique, l'adresse réseau se compose des trois premiers champs de l'adresse IP LAN de destination (le dernier champ doit contenir le chiffre zéro).

Subnet Mask : saisissez le masque de sous-réseau utilisé dans le domaine IP LAN de destination. Pour les domaines IP de classe C, le masque de sous-réseau est **255.255.255.0**.

Gateway : si ce routeur est utilisé pour la connexion du réseau à Internet, l'adresse IP de la passerelle est alors celle du routeur. Si un autre routeur gère les connexions Internet du réseau, entrez l'adresse IP de ce routeur dans ce champ.

Hop Count : cette valeur indique le nombre de nœuds que traverse un paquet de données avant d'atteindre sa destination. Un nœud désigne un périphérique quelconque du réseau, par exemple un commutateur, un ordinateur, etc. La valeur maximale du nombre de sauts est 16.

Show Routing Table : cliquez sur ce bouton pour afficher la table de routage établie à partir des méthodes de routage dynamique ou statique.

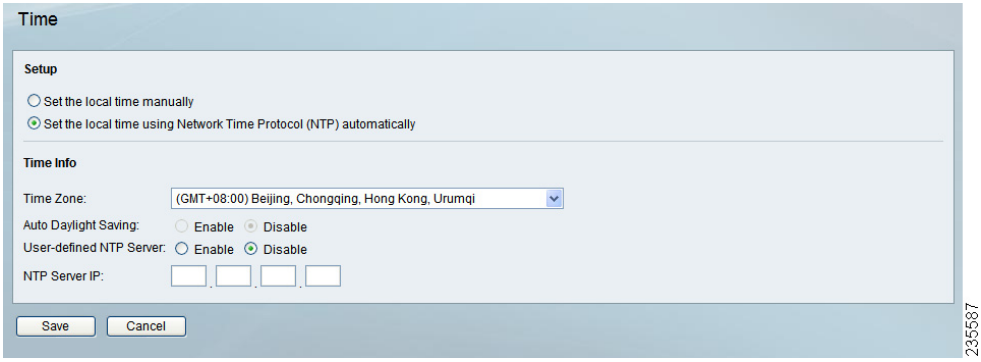
Inter-VLAN Routing

Inter-VLAN Routing : sélectionnez **Enable** pour permettre le routage des paquets entre des VLAN appartenant à différents sous-réseaux. Le paramètre par défaut est **Enable**.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

Setup > Time

Setup > Time



Set the local time manually : si vous souhaitez spécifier manuellement la date et l'heure, cliquez sur cette option, puis sélectionnez la date dans les menus déroulants et entrez l'heure, les minutes et les secondes dans les champs *Time*, au format 24 heures. Par exemple, pour entrer 22h00, indiquez **22** dans le champ des heures, **0** dans celui des minutes et **0** dans celui des secondes.

Set the local time using Network Time Protocol (NTP) automatically : si vous souhaitez utiliser un serveur Network Time Protocol pour définir la date et l'heure, sélectionnez cette option, puis renseignez les champs suivants :

Time Zone : sélectionnez le fuseau horaire de votre région. Votre réglage d'heure sera synchronisé via Internet.

Auto Daylight Saving : si votre région utilise l'heure d'été, sélectionnez l'option **Enable**.

User-defined NTP Server : pour spécifier un serveur NTP défini par l'utilisateur, sélectionnez l'option Enable, puis entrez l'adresse IP de ce serveur dans le champ *NTP Server IP*.

NTP Server IP : si l'option *User-defined NTP Server* est paramétrée sur **Enable**, entrez l'adresse IP du serveur NTP.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

Setup > IP Mode

Setup > IP Mode

IPv4 Only : sélectionnez cette option pour utiliser IPv4 sur Internet et sur le réseau local.

Dual-Stack IP : sélectionnez cette option pour utiliser IPv4 sur Internet et IPv4 et IPv6 sur le réseau local. Les hôtes IPv6 du LAN sont connectés à des îlots IPv6 distants via des tunnels « 6to4 » (conformément à la RFC 3056).

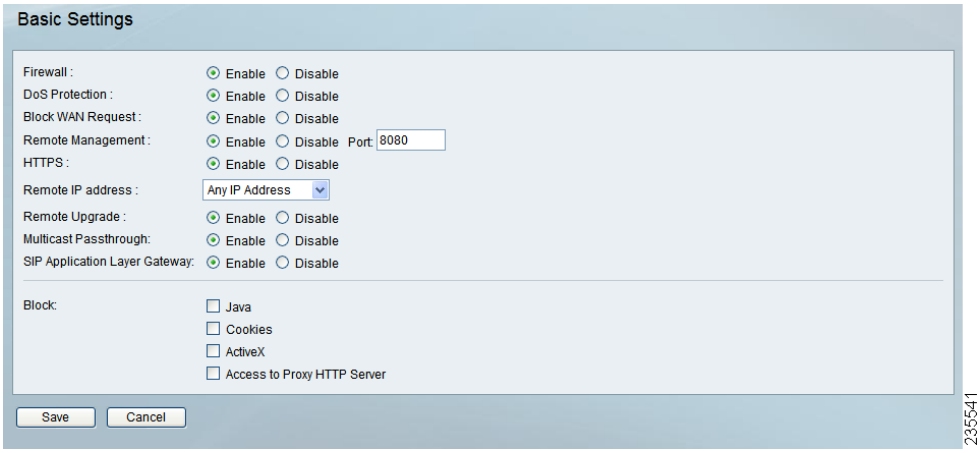
Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

Firewall

Le menu Firewall permet de configurer le routeur afin d'autoriser ou de refuser l'accès à Internet à des utilisateurs internes particuliers. Vous pouvez également configurer le routeur de façon à autoriser ou refuser l'accès aux serveurs internes à des utilisateurs Internet particuliers. Vous avez la possibilité de configurer différents filtres de paquets, applicables à différents utilisateurs aux niveaux interne (LAN) ou externe (WAN), sur la base de leur adresse IP ou de leur numéro de port réseau.

Firewall > Basic Settings

Firewall > Basic Settings



Firewall : lorsque cette fonctionnalité est activée, la fonctionnalité NAT du routeur l'est aussi.

DoS Protection : lorsque cette fonctionnalité est activée, le routeur bloque les attaques par déni de service (DoS). Les attaques de ce type ne visent pas à dérober des données ou à endommager les ordinateurs, mais à surcharger les connexions Internet, de façon à les rendre inutilisables.

Block WAN Request : lorsque cette fonctionnalité est activée, le routeur filtre les demandes anonymes en provenance du WAN.

Remote Management : cette fonctionnalité vous permet d'utiliser un port http ou https pour gérer le routeur à distance. Pour l'activer, sélectionnez **Enable** et entrez le numéro du port dans le champ *Port*, puis configurez les paramètres *HTTPS* et *Remote IP address* situés juste en-dessous.

HTTPS : cette option limite l'accès à l'utilitaire de configuration à partir du WAN aux sessions https uniquement. Une session https utilise le cryptage SSL, ce qui garantit une protection renforcée de la session distante par rapport à http. Le paramètre par défaut est **Enable**.

- **Remote IP address** : sélectionnez la valeur adéquate pour spécifier la ou les adresses IP pouvant accéder au routeur.
- **Any IP Address** : autorise l'accès à partir de toute adresse IP externe.
- **Single IP Address** : autorise l'accès à partir de l'adresse IP saisie dans le champ.
- **IP Range** : autorise l'accès à partir de la plage d'adresses IP saisie dans le champ.
- **Subnet** : autorise l'accès à partir du sous-réseau saisi dans le champ.

Remote Upgrade : cette option vous permet de mettre le routeur à niveau à distance. Pour autoriser la mise à niveau à distance, sélectionnez Enable. La fonctionnalité Remote Management doit être paramétrée sur Enable également. La valeur par défaut est **Disable**.

Multicast Passthrough : si un proxy IGMP est exécuté sur le routeur, activez cette fonctionnalité pour autoriser l'entrée du trafic de multidiffusion IP à partir d'Internet. La valeur par défaut est **Disable**.

SIP Application Layer Gateway : lorsque cette fonctionnalité est activée, l'ALG (Application Layer Gateway, passerelle de couche d'applications) SIP permet aux paquets SIP (Session Initiation Protocol), utilisés pour la voix sur IP, de traverser le pare-feu NAT. Vous pouvez désactiver cette fonctionnalité si le fournisseur de services VoIP utilise d'autres solutions NAT Traversal telles que STUN, TURN et ICE.

Block : cochez les cases en regard des fonctionnalités Web dont vous souhaitez limiter l'utilisation.

- **Java** : Java est un langage de programmation pour sites Web. Si vous bloquez Java, vous risquez de ne pas avoir accès aux sites Internet créés à l'aide de ce langage de programmation.
- **Cookies** : un cookie est un ensemble de données stockées sur l'ordinateur et utilisées par les sites Internet que vous consultez. Il se peut donc que vous ne souhaitiez pas interdire les cookies.
- **ActiveX** : ActiveX est un langage de programmation de sites Web utilisé par Microsoft (Internet Explorer). Si vous bloquez ActiveX, vous risquez de ne pas avoir accès aux sites Internet créés à l'aide de ce langage de

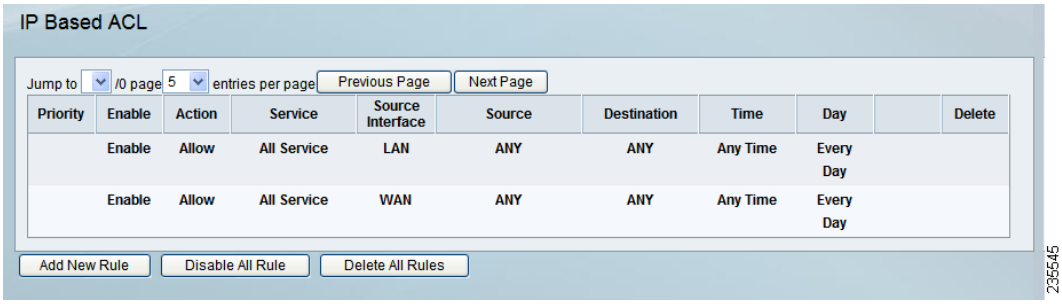
programmation. Le système de mise à jour Windows Update utilise également ActiveX. Par conséquent, les mises à jour Windows ne fonctionnent pas lorsqu'ActiveX est bloqué.

- **Access to Proxy HTTP Server** : si les utilisateurs locaux ont accès aux serveurs proxy WAN, ils pourraient certainement contourner les filtres de contenu du routeur et accéder à des sites Internet bloqués par ce dernier. Cette option permet de bloquer l'accès aux serveurs proxy WAN.

Firewall > IP Based ACL

La fenêtre IP Based ACL vous permet de créer une ACL (Access Control List, liste de contrôle d'accès) contenant jusqu'à 50 règles. Chaque règle de l'ACL autorise ou interdit l'accès au réseau en fonction de divers critères tels que la priorité, le type de service, l'interface, l'adresse IP source, l'adresse IP de destination, le jour de la semaine et la plage horaire.

Firewall > IP Based ACL



Priority : priorité de la règle.

Enable : indique si la règle est activée ou désactivée.

Action : action de la règle, à savoir Allow ou Deny pour autoriser ou interdire.

Service : service(s) au(x)quel(s) s'applique la règle.

Source Interface : interface source, c'est-à-dire WAN, LAN ou ANY (l'un ou l'autre).

Source : adresse IP source. La règle peut s'appliquer à une adresse IP spécifique, à toutes les adresses IP (ANY), à une plage d'adresses IP ou à un sous-réseau IP particulier.

Destination : adresse IP de destination. La règle peut s'appliquer à une adresse IP spécifique, à toutes les adresses IP (ANY), à une plage d'adresses IP ou à un sous-réseau IP particulier.

Time : plage horaire d'application de la règle, qui peut être définie sur Any Time (24 heures) ou en fonction d'une heure de fin et d'une heure de début.

Day : jour(s) de la semaine où la règle est appliquée. La règle peut être appliquée tous les jours (Every Day) ou un ou plusieurs jours spécifiés par l'utilisateur.

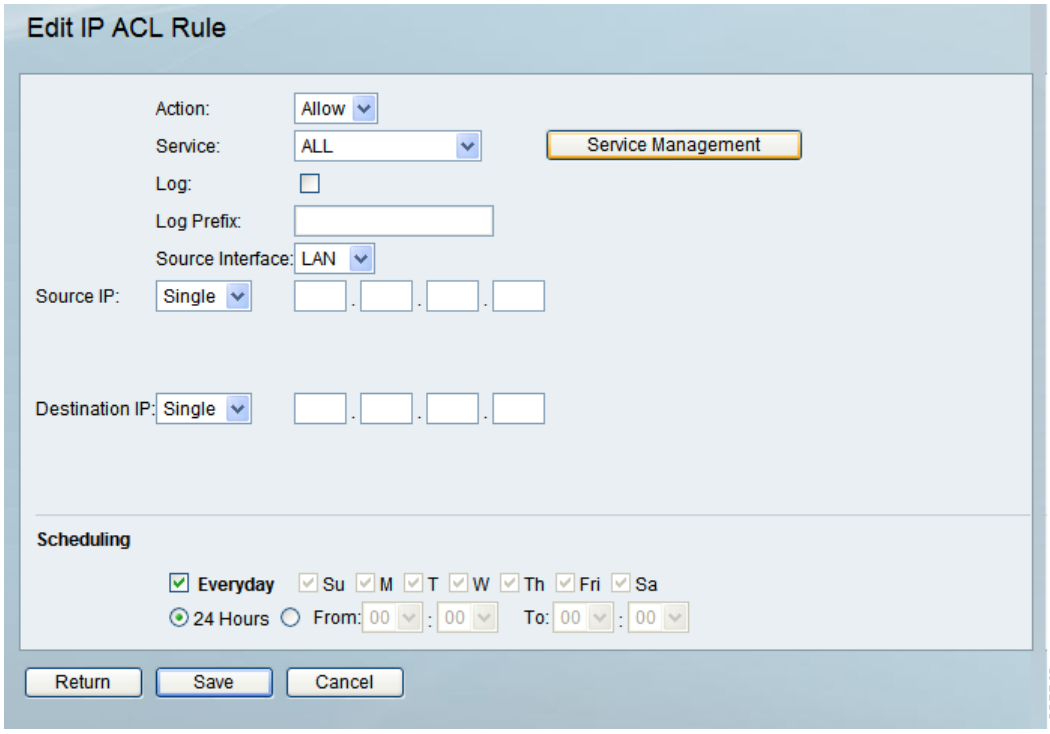
Edit : cliquez sur le bouton **Edit** situé à l'extrémité d'une ligne pour modifier la règle associée.

Delete : cliquez sur le bouton **Delete** situé à l'extrémité d'une ligne pour supprimer la règle associée.

Pour ajouter une règle au tableau des règles de l'ACL, cliquez sur **Add New Rule**. La fenêtre *Edit IP ACL Rule* s'affiche. Ensuite, suivez les instructions indiquées à la section suivante pour créer une nouvelle règle d'ACL. Pour désactiver toutes les règles sans les supprimer, cliquez sur **Disable All Rule**. Pour supprimer toutes les règles du tableau, cliquez sur **Delete All Rules**.

Edit IP ACL Rule

Edit IP ACL Rule



Action : dans le menu déroulant, sélectionnez l'action souhaitée, **Allow** ou **Deny**, pour autoriser ou interdire l'accès.

Service : sélectionnez les types de services auxquels s'applique la règle. Trois possibilités s'offrent à vous : vous pouvez sélectionner un des services prédéfinis dans le menu déroulant, choisir **ALL** pour autoriser ou interdire tous les types de trafic IP ou définir un nouveau service en cliquant sur **Service Management** pour afficher la fenêtre *Service Management*, puis entrer le nom du nouveau service, sélectionner son type (TCP, UDP ou TCP/UDP), saisir les numéros de port de début et de fin, et enfin cliquer sur **Save**. Le nouveau service s'affiche alors dans le menu déroulant de la fenêtre *Edit IP ACL Rule*.

Log : sélectionnez cette option pour consigner dans le journal tout le trafic filtré par cette règle.

Log Prefix : saisissez une chaîne de texte à ajouter en tant que préfixe à chaque événement répondant aux critères de la règle consigné dans le journal.

Source Interface : sélectionnez l'interface source, **WAN**, **LAN** ou **ANY**, dans le menu déroulant.

Source IP : pour appliquer la règle à une adresse IP source particulière, sélectionnez **Single** dans le menu déroulant, puis saisissez cette adresse dans le champ adjacent. Pour appliquer la règle à toutes les adresses IP source, sélectionnez **ANY** dans le menu déroulant. Pour appliquer la règle à une plage d'adresses IP, sélectionnez **Range** et entrez les adresses IP de début et de fin. Pour appliquer la règle à un sous-réseau, sélectionnez **Net** et entrez l'adresse IP ainsi que le masque de sous-réseau.

Destination IP : pour appliquer la règle à une adresse IP de destination particulière, sélectionnez **Single** dans le menu déroulant, puis saisissez cette adresse dans le champ adjacent. Pour appliquer la règle à toutes les adresses IP de destination, sélectionnez **ANY** dans le menu déroulant. Pour appliquer la règle à une plage d'adresses IP, sélectionnez **Range** et entrez les adresses IP de début et de fin. Pour appliquer la règle à un sous-réseau, sélectionnez **Net** et entrez l'adresse IP ainsi que le masque de sous-réseau.

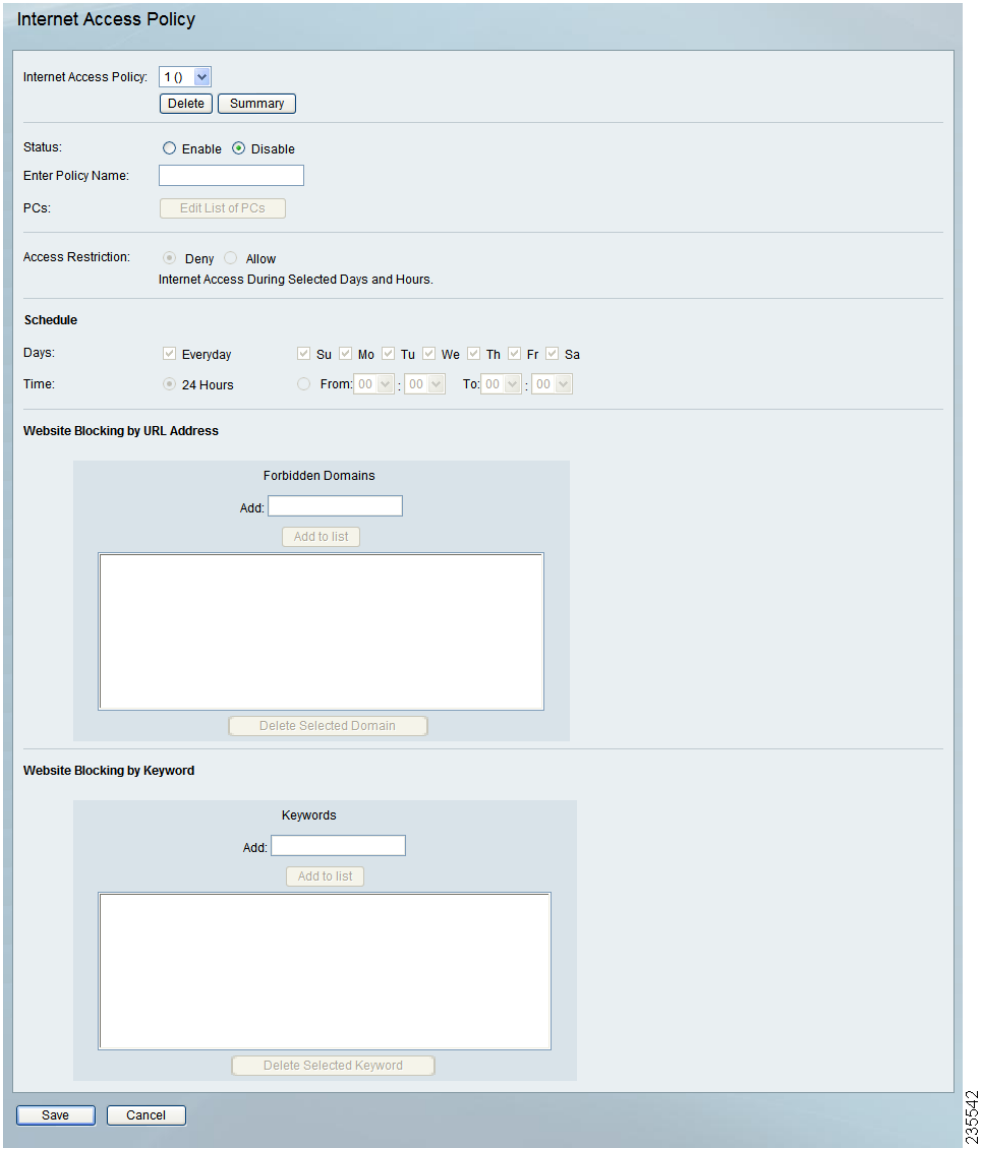
Days : pour faire en sorte que la règle s'applique tous les jours, sélectionnez **Everyday**. Pour que la règle s'applique à certains jours de la semaine uniquement, sélectionnez les jours souhaités.

Time : pour faire en sorte que la règle s'applique toute la journée, sélectionnez **24 Hours**. Pour que la règle s'applique uniquement durant une certaine période de la journée, entrez l'heure de début dans le champ *From* et l'heure de fin dans le champ *To*.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler. Cliquez sur **Return** pour revenir à la fenêtre IP Based ACL.

Firewall > Internet Access Policy

Firewall > Internet Access Policy

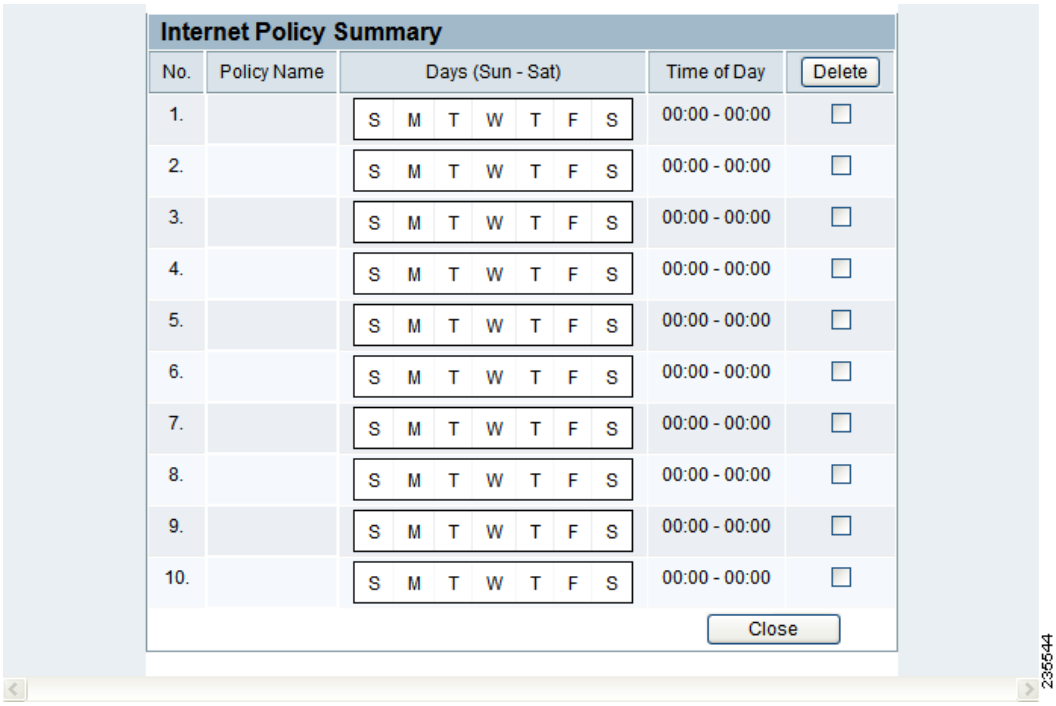


Vous pouvez gérer l'accès à votre réseau en configurant une stratégie. Utilisez les paramètres de cette fenêtre pour définir une stratégie d'accès. Dans le menu déroulant, sélectionnez une stratégie afin d'afficher ses paramètres. Vous pouvez effectuer les opérations suivantes :

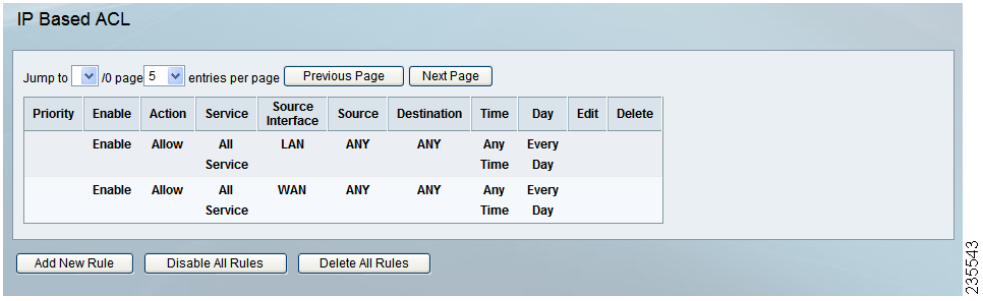
- Créer une stratégie : reportez-vous aux instructions suivantes.
- Supprimer la stratégie active : cliquez sur **Delete**.

- **Afficher toutes les stratégies** : cliquez sur **Summary** pour afficher la fenêtre *Internet Policy Summary*, qui répertorie toutes les stratégies d'accès à Internet. Cette fenêtre indique en outre, pour chaque stratégie, son numéro, son nom ainsi que les jours de la semaine et les heures où elle s'applique, et propose une case à cocher permettant de la supprimer. Pour supprimer une stratégie, cochez la case de la colonne *Delete*, puis cliquez sur **Delete**.
- **Afficher ou modifier les ordinateurs auxquels s'applique la stratégie active** : cliquez sur **Edit List of PCs** afin d'afficher la fenêtre *List of PCs*.

Internet Policy Summary



List of PCs



L'écran *List of PCs* vous permet de définir les ordinateurs concernés en spécifiant leur adresse MAC ou leur adresse IP. Vous pouvez également y saisir une plage d'adresses IP si vous souhaitez appliquer la stratégie à un groupe d'ordinateurs.

Pour créer une stratégie d'accès à Internet, procédez comme suit :

ÉTAPE 1 Sélectionnez le numéro de la stratégie souhaitée dans le menu déroulant *Internet Access Policy*.

ÉTAPE 2 Saisissez le nom de la stratégie dans le champ prévu à cet effet.

ÉTAPE 3 Pour activer cette stratégie, paramétrez l'option *Status* sur **Enable**.

ÉTAPE 4 Cliquez sur **Edit List of PCs** pour sélectionner les ordinateurs auxquels la stratégie doit s'appliquer. L'écran *List of PCs* apparaît. Vous pouvez sélectionner un ordinateur à l'aide de son adresse MAC ou de son adresse IP. Vous pouvez également saisir une plage d'adresses IP si vous souhaitez appliquer cette stratégie à un groupe d'ordinateurs. Après avoir effectué les modifications souhaitées, cliquez sur **Save** pour les appliquer.

ÉTAPE 5 Sélectionnez l'option appropriée, c'est-à-dire **Deny** ou **Allow**, selon que vous souhaitez bloquer ou autoriser l'accès à Internet aux ordinateurs répertoriés dans l'écran *List of PCs*.

ÉTAPE 6 Précisez les jours et les heures pendant lesquels cette stratégie doit s'appliquer. Sélectionnez individuellement les jours où la stratégie doit s'appliquer ou bien sélectionnez **Everyday** pour qu'elle soit valable tous les jours. Entrez une plage horaires (sous forme d'heures et de minutes) au cours de laquelle la stratégie doit être appliquée ou sélectionnez **24 Hours**.

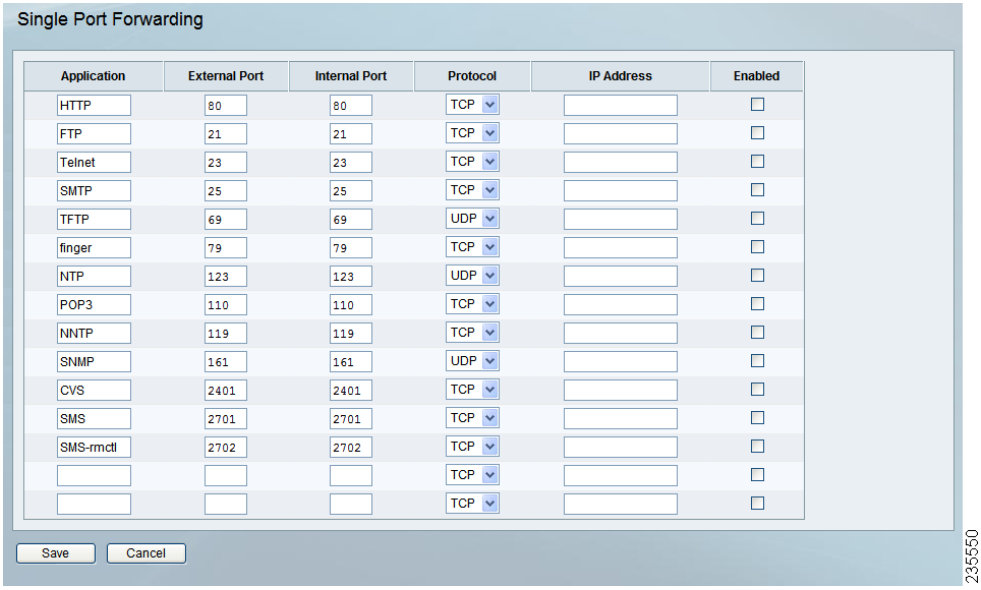
ÉTAPE 7 Pour bloquer l'accès à certains sites Web, utilisez les fonctionnalités **Website Blocking by URL Address** ou **Website Blocking by Keyword**.

- **Website Blocking by URL Address**. Entrez l'URL ou le nom de domaine des sites Web à bloquer.
- **Website Blocking by Keyword**. Entrez les mots clés à bloquer dans les champs correspondants. Si l'un de ces mots clés apparaît dans l'URL d'un site Web, l'accès à ce site sera bloqué. Notez que seule l'URL est analysée, et non pas le contenu de chaque page Web.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

Firewall > Single Port Forwarding

Firewall > Single Port Forwarding



Application : saisissez le nom de l'application à configurer.

External Port : numéro de port utilisé par le serveur ou par l'application Internet. Les utilisateurs Internet doivent se connecter par le biais du port portant ce numéro. Pour obtenir plus d'informations, reportez-vous à la documentation de l'application Internet.

Internal Port numéro de port utilisé par le routeur lors du transfert du trafic Internet à l'ordinateur ou au serveur du LAN. Normalement, ce numéro de port est identique à celui du port externe. S'il est différent, le routeur effectue une « traduction de port », afin que le numéro de port utilisé par les utilisateurs Internet soit différent de celui utilisé par le serveur ou par l'application Internet.

Ainsi, vous pouvez configurer le serveur Web pour qu'il accepte les connexions à la fois sur le port 80 (standard) et sur le port 8080. Activez ensuite le transfert de port et paramétrez le port externe sur 80 et le port interne sur 8080. Avec ce paramétrage, tout trafic en provenance d'Internet et en direction du serveur Web passera par le port 8080, même si les utilisateurs Internet utilisaient auparavant le port standard 80. (Les utilisateurs du LAN local peuvent et doivent se connecter au serveur Web via le port standard 80.)

Protocol : sélectionnez le protocole utilisé pour cette application, c'est-à-dire TCP et/ou UDP.

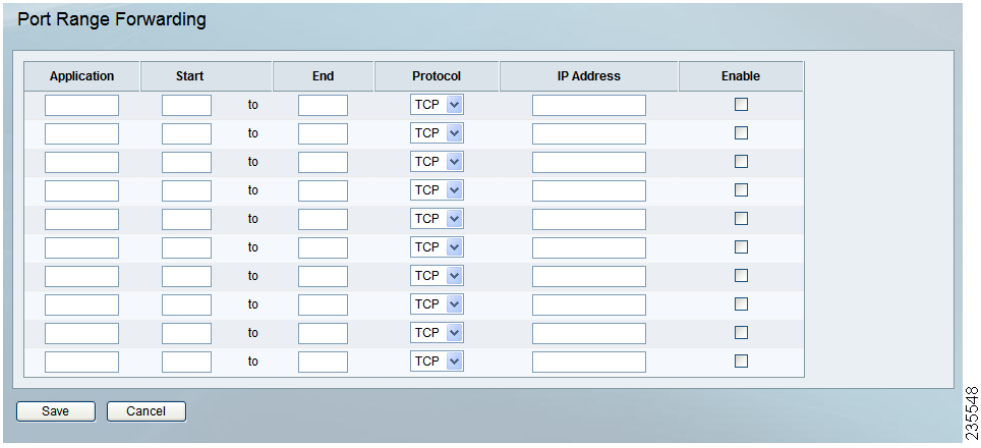
IP Address : pour chaque application, saisissez l'adresse IP de l'ordinateur chargé de l'exécuter.

Enabled : cochez la case **Enabled** pour activer le transfert de port pour l'application concernée.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

Firewall > Port Range Forwarding

Firewall > Port Range Forwarding



Application : saisissez le nom de l'application à configurer.

Start : début de la plage de ports. Spécifiez le début de la plage de numéros de port (ports externes) utilisée par le serveur ou l'application Internet. Pour obtenir plus d'informations, reportez-vous à la documentation de l'application Internet.

End : fin de la page de ports. Spécifiez la fin de la plage de numéros de port (ports externes) utilisée par le serveur ou l'application Internet. Pour obtenir plus d'informations, reportez-vous à la documentation de l'application Internet.

Protocol : sélectionnez le ou les protocoles utilisés pour cette application, c'est-à-dire TCP et/ou UDP.

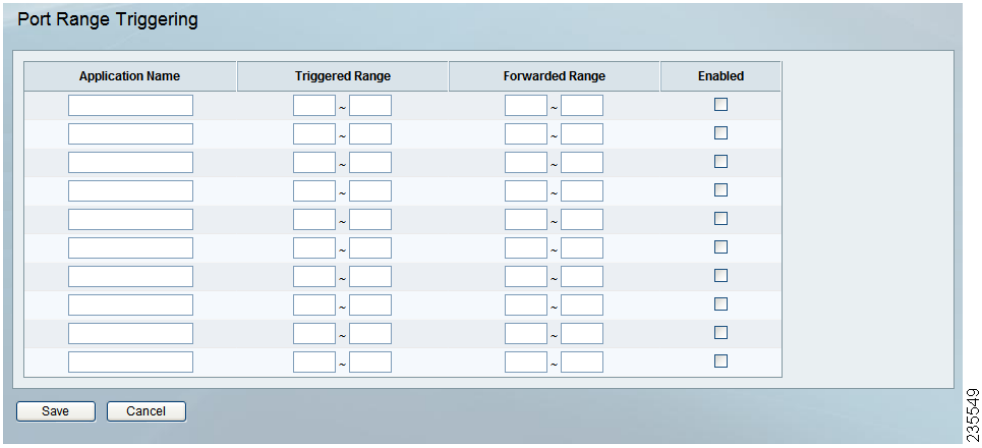
IP Address : pour chaque application, saisissez l'adresse IP de l'ordinateur chargé de l'exécuter.

Enabled : cochez la case **Enabled** pour activer le transfert de plage de ports pour l'application concernée.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

Firewall > Port Range Triggering

Firewall > Port Range Triggering



Application Name : saisissez le nom de l'application à configurer.

Triggered Range : pour chaque application, indiquez la plage de numéros de port déclenchée. Ces ports sont utilisés par le trafic sortant. Pour connaître le ou les numéros de port requis, reportez-vous à la documentation de l'application Internet. Dans le premier champ, saisissez le premier numéro de port de la plage déclenchée. Dans le deuxième champ, saisissez le dernier numéro de port de la plage déclenchée.

Forwarded Range : pour chaque application, indiquez la plage de numéros de port transférée. Ces ports sont utilisés par le trafic entrant. Pour connaître le ou les numéros de port requis, reportez-vous à la documentation de l'application Internet. Dans le premier champ, saisissez le premier numéro de port de la plage transférée. Dans le deuxième champ, saisissez le dernier numéro de port de la plage transférée.

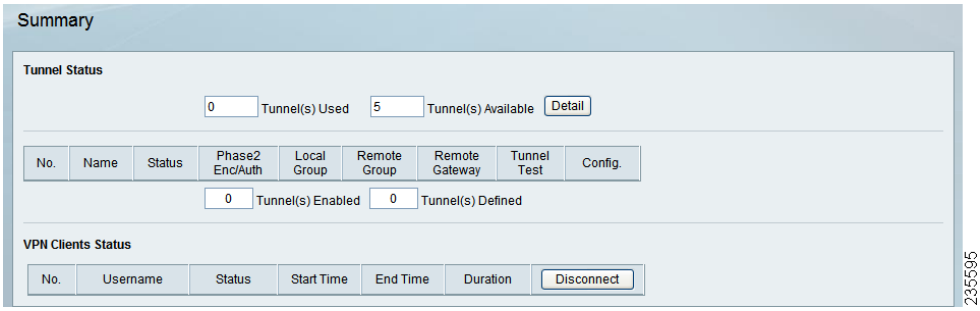
Enabled : cochez la case **Enabled** pour activer le déclenchement de plage de ports pour l'application concernée.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

VPN

VPN > Summary

VPN > Summary



Tunnel(s) Used : affiche le nombre de tunnels utilisés.

Tunnel(s) Available : affiche le nombre de tunnels disponibles.

Detail : cliquez sur le bouton **Detail** pour afficher des informations supplémentaires sur les tunnels.

Tunnel Status

N° Affiche le numéro du tunnel.

Name : indique le nom du tunnel, tel que défini par le champ Tunnel Name de la fenêtre *VPN > IPSec VPN*.

Status : indique l'état du tunnel, à savoir si la connexion est établie (Connected), si elle est en attente (Waiting for Connection), si la résolution du nom d'hôte a échoué (Hostname Resolution Failed) ou si elle est en cours (Resolving Hostname).

Phase2 Enc/Auth. Affiche le type de cryptage de phase 2 (3DES), le type d'authentification (MD5 ou SHA1) et le groupe (768-bit, 1024-bit ou 1536-bit) choisi dans la fenêtre *VPN > IPSec VPN*.

Local Group : affiche l'adresse IP et le sous-réseau du groupe local.

Remote Group : affiche l'adresse IP et le sous-réseau du groupe distant.

Remote Gateway : affiche l'adresse IP de la passerelle distante.

Tunnel Test : cliquez sur **Connect** pour vérifier l'état du tunnel ; le résultat du test est mis à jour dans la colonne *Status*. Si le tunnel est connecté, vous pouvez fermer la connexion VPN IPSec en cliquant sur **Disconnect**.

Config : cliquez sur **Edit** pour modifier les paramètres du tunnel. Cliquez sur **Trash** pour supprimer tous les paramètres du tunnel.

Tunnel(s) Enabled : indique le nombre total de tunnels actuellement activés.

Tunnel(s) Defined : indique le nombre de tunnels actuellement définis. Ce nombre est supérieur à celui indiqué dans le champ *Tunnel(s) Enabled* si des tunnels définis sont désactivés.

VPN Clients Status

No. Affiche le numéro de l'utilisateur compris entre 1 et 5.

Username. Affiche le nom d'utilisateur du client VPN.

Status : affiche l'état de connexion du client VPN.

Start Time : indique les date et heure de début de la session VPN la plus récente du client VPN spécifié.**Start Time** : indique les date et heure de début de la session VPN la plus récente du client VPN spécifié.

End Time : indique les date et heure de fin d'une session VPN si le client VPN s'est déconnecté.

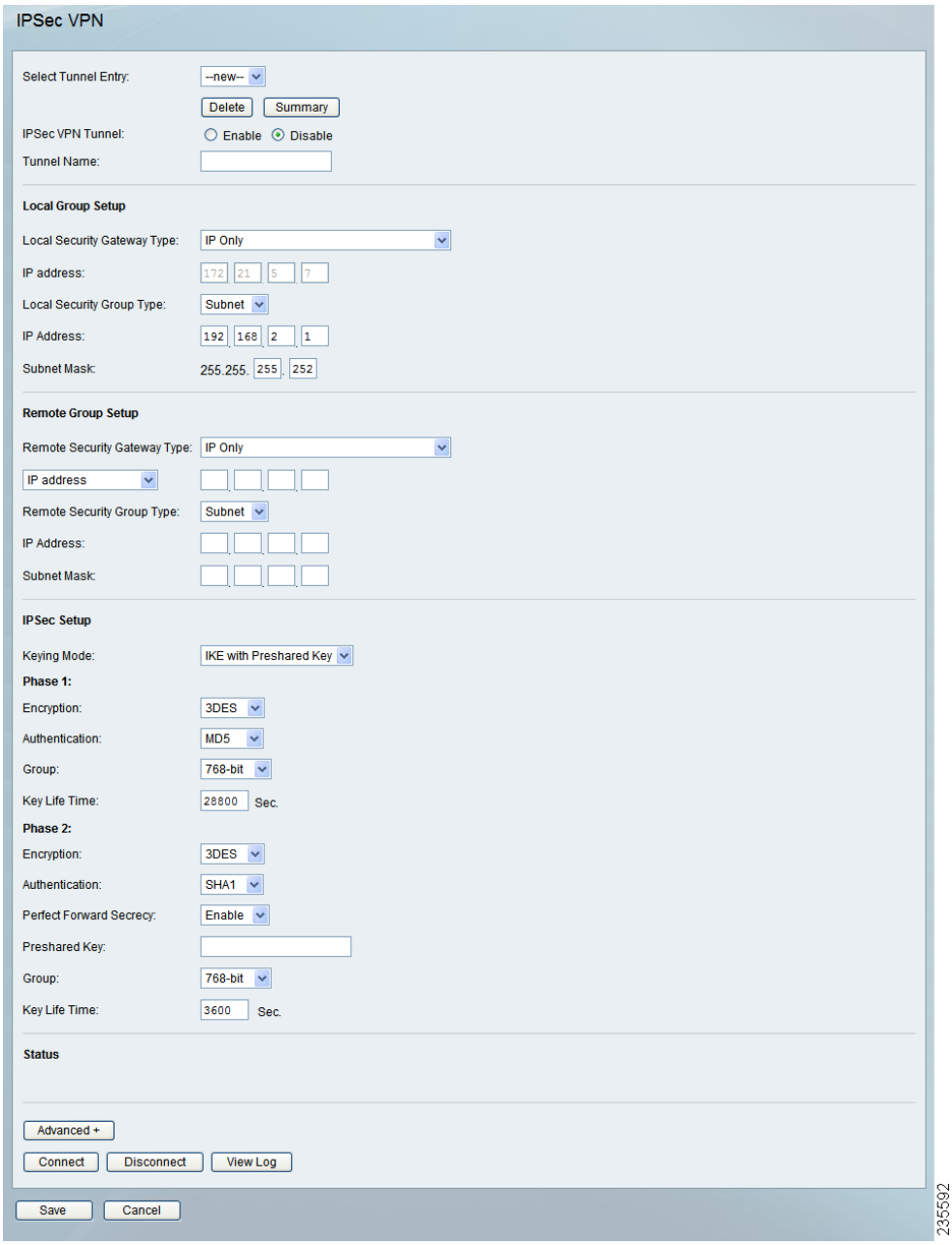
Duration : affiche la durée totale de connexion de la dernière session VPN.

Disconnect : cochez la case *Disconnect* au bout de chaque ligne du tableau VPN Clients Status, puis cliquez sur le bouton **Disconnect** pour fermer une session de client VPN.

VPN > IPsec VPN

Utilisez la fenêtre *VPN > IPSec VPN* pour créer et configurer un tunnel.

VPN > IPsec VPN



Select Tunnel Entry : pour créer un tunnel, sélectionnez **new.** Pour configurer un tunnel existant, sélectionnez-le dans le menu déroulant.

Delete : cliquez sur ce bouton pour supprimer tous les paramètres du tunnel sélectionné.

Summary : cliquez sur ce bouton pour afficher les paramètres et l'état de tous les tunnels activés.

IPSec VPN Tunnel : sélectionnez l'option **Enable** pour activer ce tunnel.

Tunnel Name : saisissez un nom pour ce tunnel, par exemple « Bureau de Lyon ».

Local Group Setup

Local Security Gateway Type : deux paramètres sont disponibles, **IP Only** et **IP + Domain Name (FQDN) Authentication**.

- **IP Only** : si vous sélectionnez ce paramètre, le champ *IP Address* affiche automatiquement l'adresse IP WAN du routeur.
- **IP + Domain Name (FQDN) Authentication** : si vous sélectionnez ce paramètre, le champ *IP Address* affiche automatiquement l'adresse IP WAN et le nom de domaine afin d'accroître la sécurité. Saisissez un nom de domaine arbitraire dans le champ *Domain Name*.

Local Security Group Type : sélectionnez le ou les groupes d'utilisateurs du LAN local, situés derrière le routeur, autorisés à utiliser ce tunnel VPN. Il peut s'agir d'une adresse IP ou d'un sous-réseau. Notez que le paramètre du champ Local Security Group Type doit correspondre à celui du champ Remote Security Group Type de l'autre routeur.

IP Address : saisissez l'adresse IP sur le réseau local.

Subnet Mask : si le champ Local Security Group Type est paramétré sur **Subnet**, saisissez le masque de sous-réseau afin de déterminer les adresses IP sur le réseau local.

Remote Group Setup

Remote Security Gateway Type : sélectionnez **IP Only** ou **IP + Domain Name (FQDN) Authentication**. Le paramètre choisi doit correspondre à celui du champ Local Security Gateway Type du périphérique VPN situé à l'autre extrémité du tunnel.

- **IP Only** : choisissez cette option pour indiquer le périphérique distant pouvant accéder au tunnel. Ensuite, sélectionnez **IP Address** dans le menu déroulant et saisissez l'adresse IP WAN de la passerelle distante dans le champ *IP Address*, ou bien sélectionnez **IP by DNS Resolved** dans le menu

déroulant et saisissez le nom de domaine de la passerelle distante dans le champ *Domain Name*.

- **IP + Domain Name (FQDN) Authentication** : choisissez cette option pour inclure l'adresse IP et un nom de domaine afin d'accroître la sécurité. Saisissez un nom de domaine arbitraire dans le champ *Domain Name*. Ensuite, sélectionnez **IP Address** ou **IP by DNS Resolved** dans le menu déroulant et renseignez le champ qui s'affiche selon l'option choisie, *IP Address* ou *Domain Name*.

Remote Security Group Type : sélectionnez le ou les groupes d'utilisateurs du LAN distant, situés derrière la passerelle distante, autorisés à utiliser ce tunnel VPN. Il peut s'agir d'une adresse IP ou d'un sous-réseau. Notez que le paramètre du champ Remote Security Group Type doit correspondre à celui du champ Local Security Group Type de l'autre routeur.

IP Address : saisissez l'adresse IP sur le réseau distant.

Subnet Mask : si le champ Remote Security Group Type est paramétré sur **Subnet**, saisissez le masque de sous-réseau afin de déterminer les adresses IP sur le réseau distant.

IPSec Setup

Keying Mode : le routeur prend en charge les méthodes de gestion des clés automatique et manuelle. Si vous choisissez la gestion automatique des clés, la négociation des clés pour SA (Security Association) s'effectue via les protocoles IKE (Internet Key Exchange). Si vous sélectionnez la gestion manuelle, aucune négociation de clés n'est nécessaire. La gestion manuelle de clés est utilisée dans les petits environnements statiques ou à des fins de dépannage. Notez que la méthode de gestion des clés doit être identique des deux côtés.

Phase 1

- **Encryption** : la méthode de cryptage détermine la longueur de la clé utilisée pour le cryptage et le décryptage des paquets ESP. Seule la méthode 3DES est prise en charge. Notez que la même méthode de cryptage doit être utilisée des deux côtés.
- **Authentication** : l'authentification détermine la méthode employée pour authentifier les paquets ESP. Vous pouvez sélectionner soit MD5, soit SHA1. Notez que la même méthode d'authentification doit être utilisée des deux côtés (points terminaux VPN).
- **MD5** : algorithme de hachage unidirectionnel produisant une empreinte de 128 bits.

- **SHA1** : algorithme de hachage unidirectionnel produisant une empreinte de 160 bits.
- **Group** : groupe Diffie-Hellman (DH) à utiliser pour l'échange de clés. Sélectionnez le paramètre d'algorithme 768-bit (groupe 1), 1024-bit (groupe 2) ou 1536-bit (groupe 5). Le groupe 5 offre le niveau de sécurité le plus élevé et le groupe 1 le niveau le plus faible.
- **Key Life Time** : indique la durée de validité de la clé générée par IKE. Au terme de cette période, une nouvelle clé est automatiquement renégociée. Saisissez une valeur comprise entre 300 et 100 000 000 millisecondes. La valeur par défaut est **28 800** secondes.

Phase 2

- **Encryption** : la méthode de cryptage détermine la longueur de la clé utilisée pour le cryptage et le décryptage des paquets ESP. Seule la méthode 3DES est prise en charge. Notez que la même méthode de cryptage doit être utilisée des deux côtés.
- **Authentication** : l'authentification détermine la méthode employée pour authentifier les paquets ESP. Vous pouvez sélectionner soit MD5, soit SHA1. Notez que la même méthode d'authentification doit être utilisée des deux côtés (points terminaux VPN).
- **MD5** : algorithme de hachage unidirectionnel produisant une empreinte de 128 bits.
- **SHA1** : algorithme de hachage unidirectionnel produisant une empreinte de 160 bits.
- **Perfect Forward Secrecy** : si la fonctionnalité PFS (Perfect Forward Secrecy, confidentialité de transmission parfaite) est activée, la négociation IKE de phase 2 génère de nouvelles clés pour le cryptage et l'authentification du trafic IP. Notez que cette fonctionnalité doit être sélectionnée des deux côtés.
- **Preshared Key** : IKE utilise ce champ pour authentifier l'homologue IKE distant. Ce champ admet à la fois des caractères et des valeurs hexadécimales (« Mon_@123 » ou « 0x4d795f40313233 », par exemple). Notez que la clé pré-partagée doit être identique des deux côtés.
- **Group** : groupe Diffie-Hellman (DH) à utiliser pour l'échange de clés. Sélectionnez le paramètre d'algorithme 768-bit (groupe 1), 1024-bit (groupe 2) ou 1536-bit (groupe 5). Le groupe 5 offre le niveau de sécurité le plus élevé et le groupe 1 le niveau le plus faible.

- **Key Life Time** : indique la durée de validité de la clé générée par IKE. Au terme de cette période, une nouvelle clé est automatiquement renégociée. Saisissez une valeur comprise entre 300 et 100 000 000 millisecondes. La valeur par défaut est **3 600** secondes.

Status

Status : affiche l'état de connexion du tunnel sélectionné, à savoir Connected ou Disconnected ; selon que la connexion est établie ou non.

Connect : cliquez sur ce bouton pour établir une connexion pour le tunnel VPN actif. Si vous avez apporté des modifications, cliquez sur le bouton **Save** pour les appliquer.

Disconnect : cliquez sur ce bouton pour fermer une connexion pour le tunnel VPN actif.

View Log : cliquez sur ce bouton pour afficher le fichier journal VPN, qui fournit des informations sur chaque tunnel établi.

Advanced : cliquez sur ce bouton pour afficher les paramètres supplémentaires suivants.

Aggressive Mode : spécifie le type d'échange de phase 1, Main mode ou Aggressive mode. Cochez cette case pour sélectionner le mode agressif ou laissez-la décochée (paramètre par défaut) pour sélectionner le mode principal. En mode agressif, deux fois moins de messages qu'en mode principal sont échangés en phase 1 de l'échange SA. Si la sécurité du réseau est prioritaire, sélectionnez Main mode.

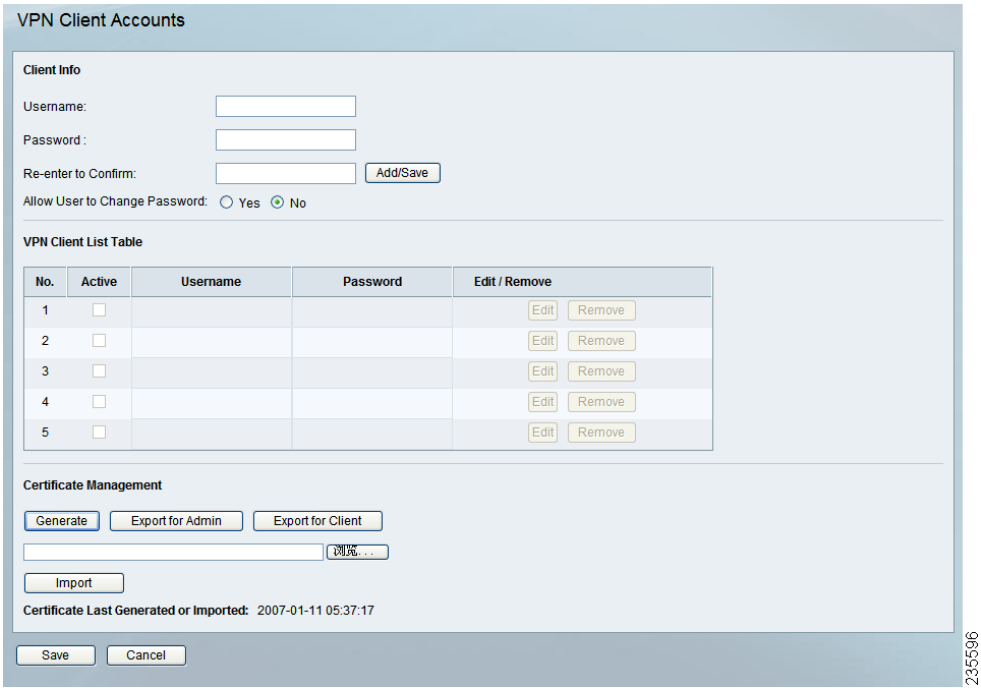
NetBios Broadcasts : cochez cette case pour autoriser le passage du trafic NetBIOS au travers du tunnel VPN. Par défaut, le RVS4000 bloque ces diffusions.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

VPN > VPN Client Accounts

Utilisez cette fenêtre pour gérer les utilisateurs de client VPN. Une fois que vous avez saisi les informations voulues dans la partie supérieure de la fenêtre, les informations relatives aux utilisateurs spécifiés s'affichent dans le tableau. Cette fonctionnalité est disponible avec le client Cisco QuickVPN uniquement. Le routeur prend en charge jusqu'à cinq sessions Cisco QuickVPN simultanées.

VPN > VPN Client Accounts



Username : saisissez le nom d'utilisateur. Celui-ci peut être constitué de n'importe quelle combinaison de caractères du clavier.

Password : saisissez le mot de passe à affecter à cet utilisateur.

Re-enter to Confirm Tapez une seconde fois le mot de passe pour confirmer qu'il a été saisi correctement.

Allow User to Change Password : cette option détermine si l'utilisateur est autorisé ou non à modifier son mot de passe.

VPN Client List Table

No. Affiche le numéro de l'utilisateur.

Active : lorsque cette case est cochée, l'utilisateur désigné peut se connecter ; dans le cas contraire, le compte client VPN est désactivé.

Username : affiche le nom d'utilisateur.

Edit : cliquez sur ce bouton pour modifier le nom d'utilisateur ou le mot de passe.

Remove : cliquez sur ce bouton pour supprimer un compte d'utilisateur.

Certificate Management

Cette section vous permet de gérer le certificat utilisé pour sécuriser la communication entre le routeur et les clients QuickVPN.

Generate : cliquez sur ce bouton pour générer un nouveau certificat destiné à remplacer le certificat existant sur le routeur.

Export for Admin : cliquez sur ce bouton pour exporter le certificat destiné à l'administrateur. Lorsque vous y êtes invité, indiquez l'emplacement où enregistrer le certificat. Le nom de fichier par défaut est « RVS4000_Admin.pem » mais vous pouvez choisir un autre nom. Le certificat destiné à l'administrateur contient la clé privée et doit être stocké dans un emplacement sûr à des fins de sauvegarde. Si vous rétablissez les paramètres de configuration par défaut du routeur, il est possible d'importer et de restaurer ce certificat sur le routeur.

Export for Client : cliquez sur ce bouton pour exporter le certificat destiné au client. Lorsque vous y êtes invité, indiquez l'emplacement où enregistrer le certificat. Le nom de fichier par défaut est « RVS4000_Client.pem » mais vous pouvez choisir un autre nom. Pour que les utilisateurs QuickVPN puissent se connecter en toute sécurité au routeur, ce certificat doit être placé dans le répertoire d'installation du client QuickVPN.

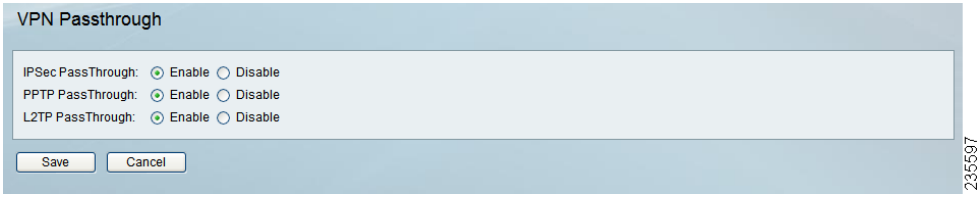
Import : cliquez sur ce bouton pour importer un certificat précédemment enregistré dans un fichier à l'aide des boutons **Export for Admin** ou **Export for Client**. Saisissez le nom du fichier dans le champ ou cliquez sur **Browse** pour localiser le fichier sur l'ordinateur, puis cliquez sur **Import**.

Certificate Last Generated or Imported : affiche la date et l'heure de la dernière génération ou importation d'un certificat.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

VPN > VPN Passthrough

VPN > VPN Passthrough



IPSec PassThrough : IPSec (Internet Protocol Security) désigne une série de protocoles utilisés pour sécuriser l'échange des paquets au niveau de la couche IP. L'option IPSec PassThrough est activée par défaut, pour permettre aux tunnels IPSec de traverser le routeur. Pour la désactiver, sélectionnez **Disable**.

PPTP PassThrough : le protocole PPTP (Point-to-Point Tunneling Protocol) permet de « tunneliser » le protocole PPP (Point-to-Point Protocol) via un réseau IP. L'option PPTP PassThrough est activée par défaut. Pour la désactiver, sélectionnez **Disable**.

L2TP PassThrough : le protocole L2TP (Layer 2 Tunneling Protocol) est la méthode utilisée pour activer des sessions point à point via Internet, au niveau de la couche 2. L'option L2TP PassThrough est activée par défaut. Pour la désactiver, sélectionnez **Disable**.

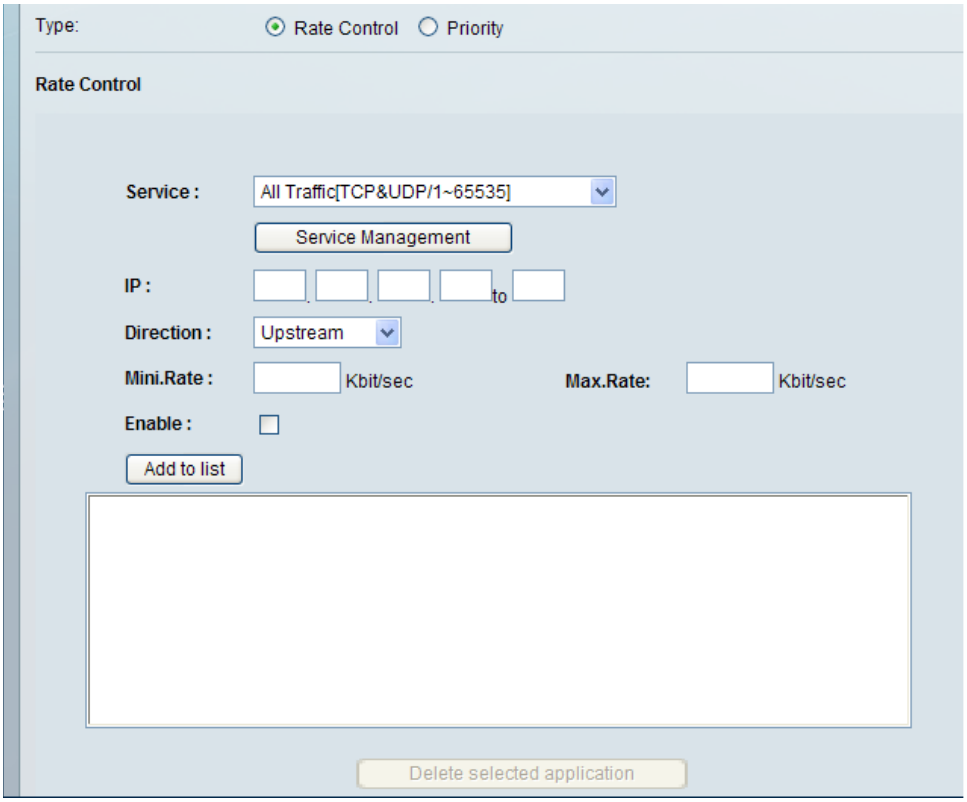
Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

QoS

Vous pouvez utiliser la fenêtre QoS (Quality of Service, qualité de service) pour gérer la bande passante, soit au moyen du contrôle de débit (**Rate Control**), soit en fonction de la priorité (**Priority**). Vous pouvez également configurer le mode de sécurité (Trust Mode) de la qualité de service et les paramètres DSCP.

QoS > Bandwidth Management

QoS > Bandwidth Management—Rate Control



Bande passante

Cette section vous permet de spécifier la bande passante maximale fournie par le FAI sur l'interface WAN, tant en amont qu'en aval.

Bandwidth Management Type

Type : type de gestion de bande passage souhaité, à savoir par contrôle de débit (**Rate Control**) ou selon la priorité (**Priority**, paramètre par défaut). En fonction du paramètre sélectionné, la partie inférieure de la fenêtre affiche soit la section Rate Control, soit la section Priority.

Rate Control

Service : sélectionnez le service dans le menu déroulant. Si la liste ne contient pas le service souhaité, cliquez sur **Service Management** pour l'ajouter.

IP : saisissez l'adresse IP ou la plage d'adresses IP à contrôler. La valeur par défaut, à savoir zéro, inclut toutes les adresses IP internes.

Direction : sélectionnez **Upstream** pour le trafic sortant ou **Downstream** pour le trafic entrant.

Mini. Rate : saisissez le débit minimal de la bande passante garantie.

Max. Rate : saisissez le débit maximal de la bande passante garantie.

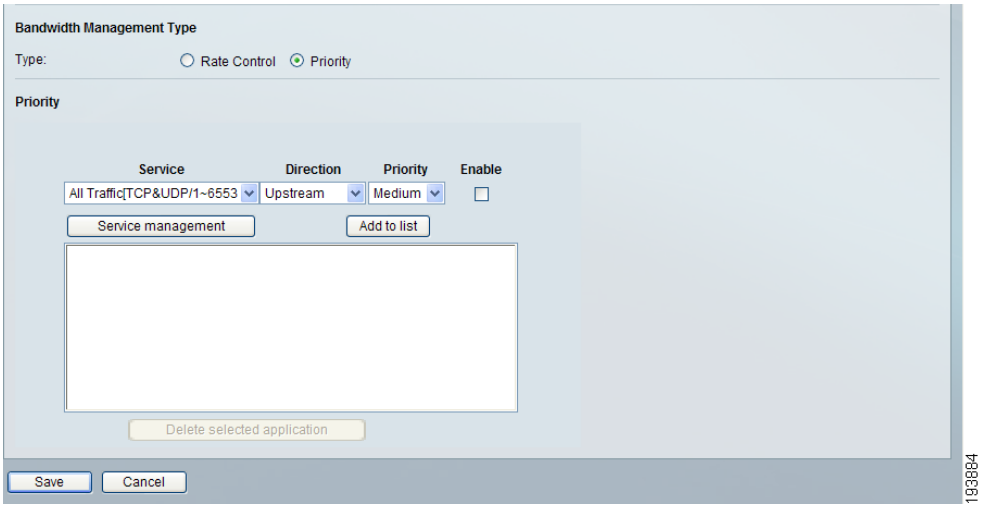
Enable : cochez cette case pour activer cette règle de contrôle de débit.

Add to list : après avoir configuré une règle, cliquez sur ce bouton pour l'ajouter à la liste. Cette liste peut contenir jusqu'à 15 entrées.

Delete selected application : cliquez sur ce bouton pour supprimer une règle de la liste.

Priority

QoS > Bandwidth Management—Priority



Service : sélectionnez le service dans le menu déroulant. Si la liste ne contient pas le service souhaité, cliquez sur **Service Management** pour l'ajouter.

Direction : dans le menu déroulant, sélectionnez **Upstream** pour le trafic sortant ou **Downstream** pour le trafic entrant.

Priority : sélectionnez le paramètre de priorité du service, à savoir (de la priorité la plus élevée à la plus faible) : **High**, **Medium**, **Normal** ou **Low**. Le paramètre par défaut est **Medium** (priorité moyenne).

Enable : cochez cette case pour activer cette règle de priorité.

Add to list : après avoir configuré une règle, cliquez sur ce bouton pour l'ajouter à la liste. Cette liste peut contenir jusqu'à 15 entrées.

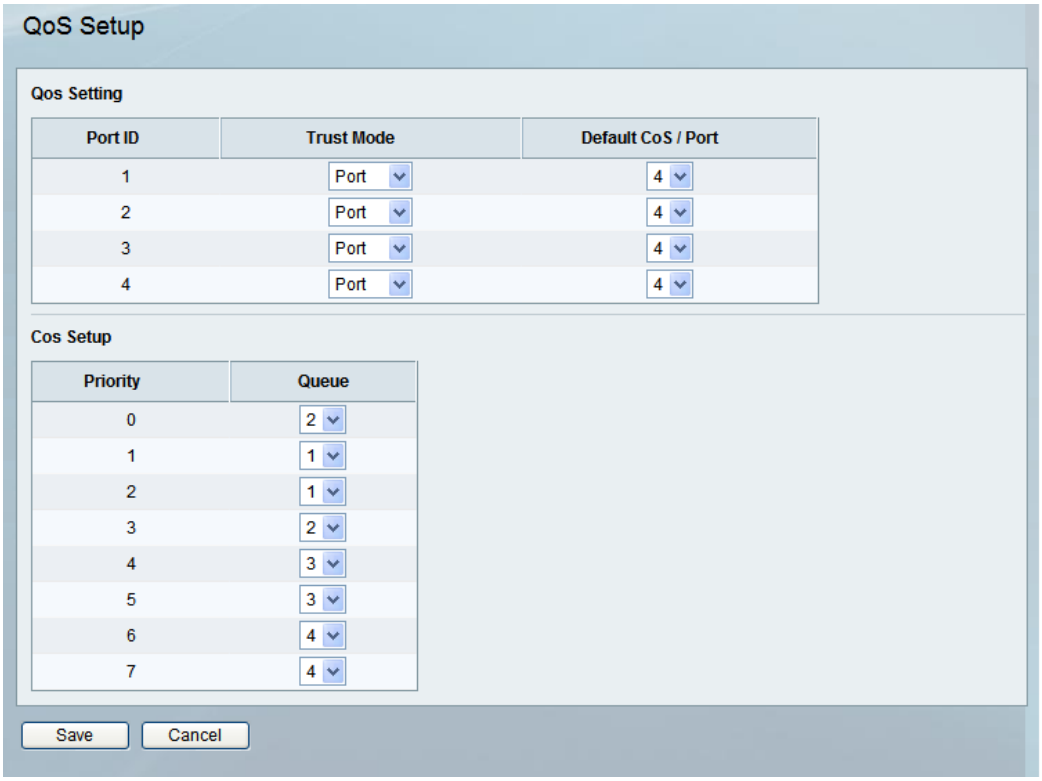
Delete selected application : cliquez sur ce bouton pour supprimer une règle de la liste.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

QoS > QoS Setup

Utilisez la fenêtre *QoS Setup* pour configurer le mode de sécurité de la qualité de service pour chaque port LAN.

QoS > QoS Setup



Port ID : numéro du port LAN.

Trust Mode : sélectionnez le mode de sécurité **Port**, **CoS** ou **DSCP.** Le paramètre par défaut est .**Port**.

Default CoS/Port : si le champ Trust Mode est paramétré sur **Port**, sélectionnez une priorité de port comprise entre **1** et **4** dans le menu déroulant, **4** correspondant à la priorité la plus élevée. Si le champ Trust Mode est paramétré sur **CoS**, sélectionnez une priorité CoS par défaut comprise entre **0** et **7** dans le menu déroulant.

CoS Setup

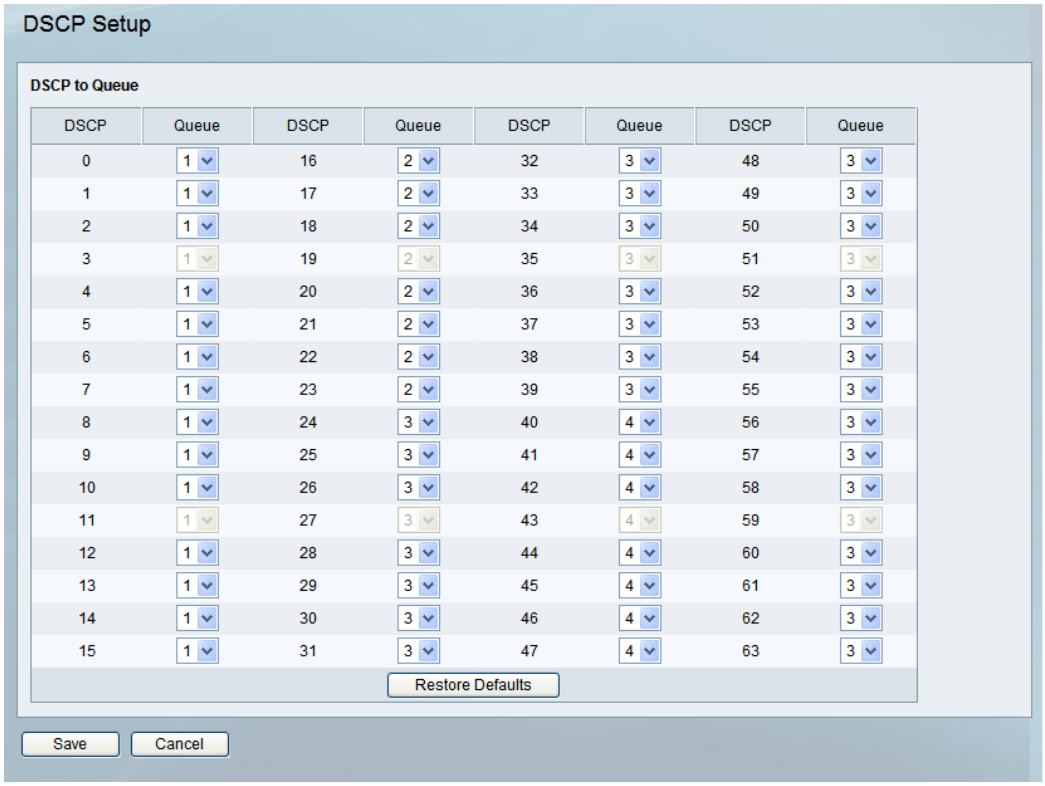
Priority : priorité CoS, comprise entre **0** et **7**.

Queue : sélectionnez la file d'attente de transfert du trafic, comprise entre **1** et **4**, à laquelle la priorité CoS est mappée. La file d'attente **4** possède la priorité la plus élevée.

Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

QoS > DSCP Setup

QoS > DSCP Setup



DSCP : valeur DSCP (Differentiated Services Code Point, code d'accès aux services différenciés) présente dans le paquet entrant.

Queue : sélectionnez la file d'attente de transfert du trafic, comprise entre **1** et **4**, à laquelle la priorité DSCP est mappée. La file d'attente **4** possède la priorité la plus élevée.

Restore Defaults : cliquez sur ce bouton pour rétablir les valeurs DSCP par défaut.

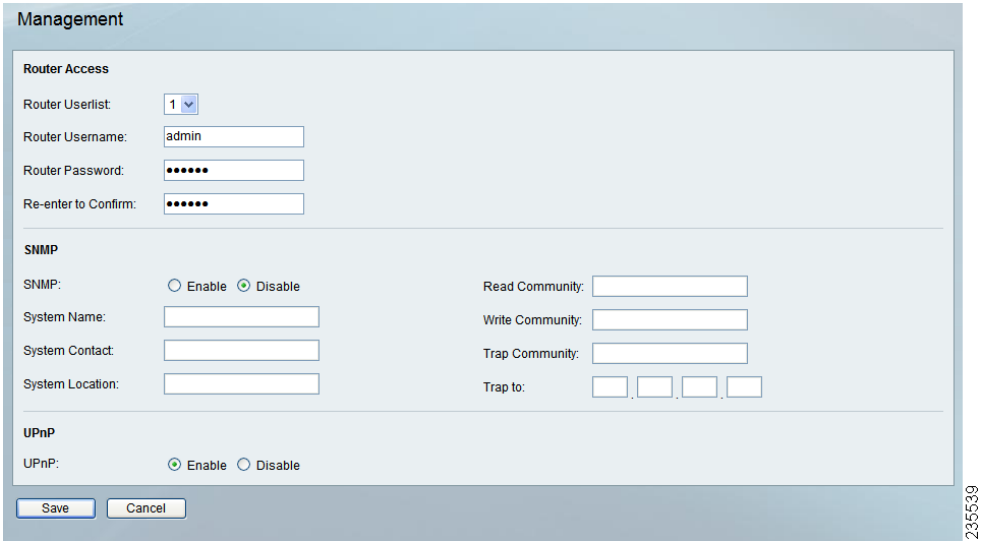
Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

Administration

Utilisez le menu Administration pour configurer les outils et paramètres d'administration système.

Administration > Management

Administration > Management



Router Access

Router Userlist : établissez la liste des utilisateurs du routeur.

Router Username : saisissez le nom d'utilisateur.

Router Password : saisissez le mot de passe.

Re-enter to Confirm : tapez le mot de passe une seconde fois dans ce champ.

SNMP

SNMP : sélectionnez Enable si vous souhaitez utiliser SNMP. Pour utiliser SNMP, vous devez installer un logiciel SNMP sur l'ordinateur.

System Name : saisissez un nom approprié pour désigner ce périphérique. Ce nom sera affiché par le logiciel SNMP.

System Contact : saisissez les informations de contact du système.

System Location : indiquez l'emplacement du système.

Read Community : saisissez le nom de communauté SNMP pour les commandes « Get » SNMP.

Write Community : saisissez le nom de communauté SNMP pour les commandes « Set » SNMP.

Trap Community : saisissez le nom de communauté SNMP pour les commandes « Trap » SNMP.

Trap To : saisissez l'adresse IP du gestionnaire SNMP vers lequel seront envoyés les déroutements. Si vous le souhaitez, ce champ peut rester vide.

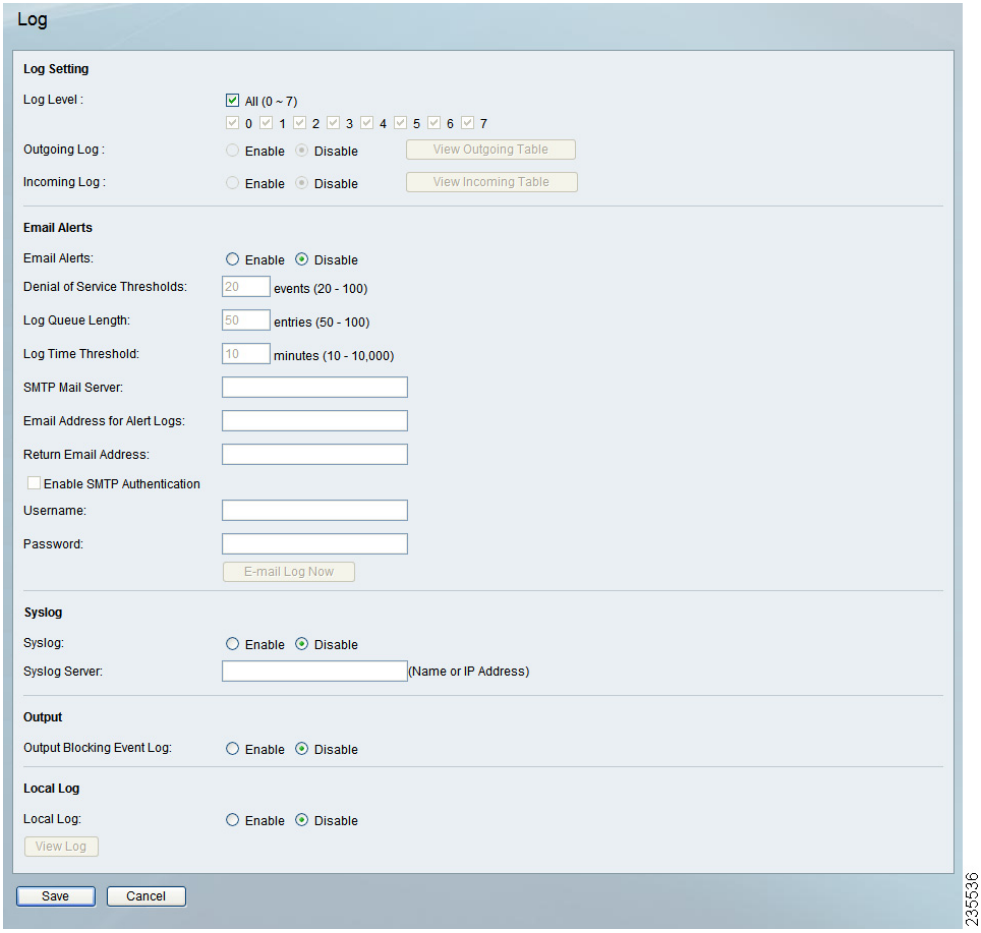
UPnP

Vous pouvez avoir recours à UPnP (Universal Plug and Play) pour configurer des services publics sur le réseau. Lorsque la fonction UPnP est activée, Windows XP peut ajouter ou supprimer des entrées dans le tableau de redirection UPnP. Certains jeux Internet nécessitent l'activation d'UPnP.

UPnP : si vous souhaitez utiliser UPnP, conservez le paramètre par défaut, **Enable**. Sinon, sélectionnez **Disable**.

Administration > Log

Administration > Log



Log Setting

Log Level : sélectionnez le ou les niveaux de consignation dans le journal par le routeur. Le tableau suivant répertorie les niveaux de consignation et leur signification :

Niveaux de consignation

Niveau	Gravité	Description
7	LOG_DEBUG	Message de débogage
6	LOG_INFO	Message d'information uniquement

Niveaux de consignation

Niveau	Gravité	Description
5	LOG_NOTICE	Événement normal mais important
4	LOG_WARNING	Avertissement
3	LOG_ERR	Erreur
2	LOG_CRIT	Conditions primordiales
1	LOG_ALERT	Intervention immédiate requise
0	LOG_EMERG	Système inutilisable

Outgoing Log : sélectionnez **Enable** pour que les événements liés à tous les paquets sortants soient consignés dans le journal. Vous pouvez cliquer sur **View Outgoing Table** pour afficher des informations sur les paquets sortants, notamment les adresses IP source et de destination ainsi que les numéros de service et de port.

Incoming Log : sélectionnez **Enable** pour que les événements liés à tous les paquets entrants soient consignés dans le journal. Vous pouvez cliquer sur **View Incoming Table** pour afficher des informations sur les paquets entrants notamment les adresses IP source et de destination ainsi que les numéros de service et de port.

Email Alerts

Email Alerts : sélectionnez **Enable** pour qu'un e-mail soit envoyé immédiatement en cas de détection d'une attaque par déni de service (DoS). Si vous activez cette fonctionnalité, indiquez les informations d'adresse e-mail requises dans les autres champs concernés de cette section.

Denial of Service Thresholds : saisissez le nombre d'attaques par déni de service devant être bloquées par le pare-feu intégré avant l'envoi d'une alerte par e-mail. La valeur minimale est 20 et la valeur maximale 100.

Log Queue Length : la valeur par défaut est de **50** entrées. Le routeur envoie le journal par e-mail dès qu'il contient plus de 50 entrées.

Log Time Threshold : la valeur par défaut est de **10** minutes. Le routeur envoie le journal par e-mail toutes les 10 minutes.

SMTP Mail Server : saisissez l'adresse (nom de domaine) ou l'adresse IP du serveur SMTP (Simple Mail Transport Protocol) utilisé pour le courrier électronique sortant.

Email Address for Alert Logs : saisissez l'adresse e-mail à laquelle le journal doit être envoyé.

Return Email Address : il s'agit de l'adresse qui apparaîtra dans le champ De (expéditeur) de l'e-mail.

Enable SMTP Authentication : si le serveur SMTP impose l'authentification, vous pouvez l'activer en cochant cette case. Saisissez ensuite le nom d'utilisateur et le mot de passe.

E-mail Log Now : cliquez sur ce bouton pour envoyer immédiatement le journal par e-mail.

Syslog

Enable : sélectionnez cette option si vous souhaitez utiliser la fonctionnalité Syslog.

Syslog Server : si vous avez sélectionné l'option **Enable**, entrez l'adresse IP du serveur dans ce champ.

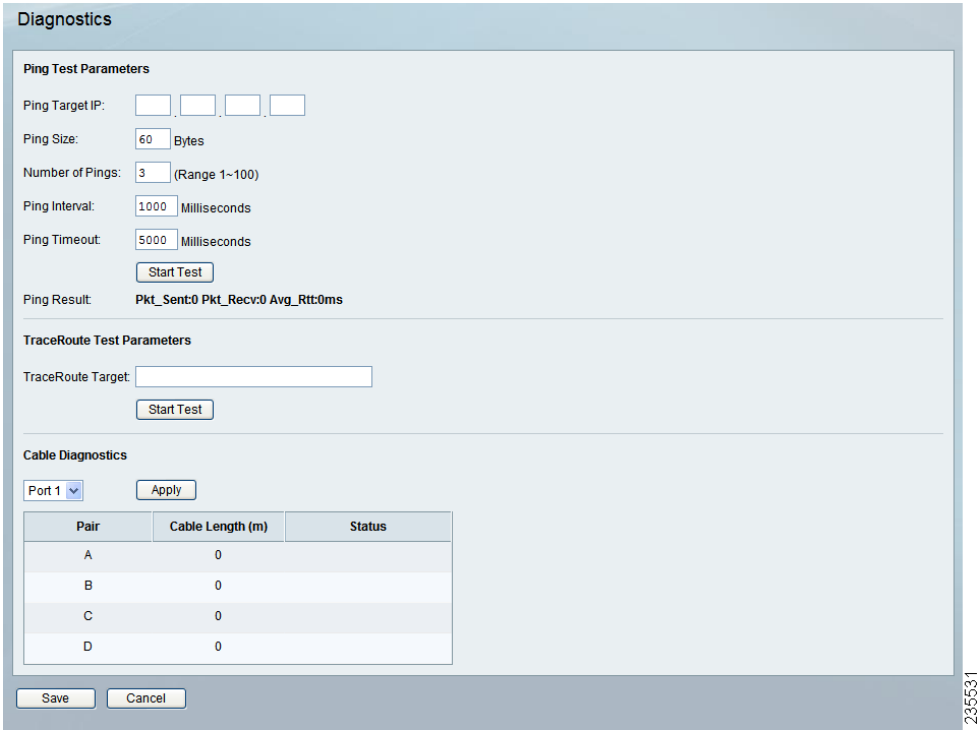
Local Log

Local Log : activez cette option si vous souhaitez afficher un journal de toutes les URL ou adresses IP entrantes et sortantes.

View Log : cliquez sur ce bouton lorsque vous souhaitez afficher le journal. Une nouvelle fenêtre s'ouvre et affiche les données du journal.

Administration > Diagnostics

Administration > Diagnostics



Ping Test Parameters

Ping Target IP : saisissez l'adresse IP ou l'URL pour laquelle effectuer le test Ping.

Ping Size : saisissez la taille du paquet à utiliser.

Number of Pings : saisissez le nombre de requêtes Ping à envoyer au périphérique cible.

Ping Interval : saisissez l'intervalle (en millisecondes) entre les requêtes Ping.

Ping Timeout : saisissez le délai imparti pour la communication Ping (en millisecondes). Si aucune réponse n'est reçue au terme de cette période, on considère que la commande Ping a échoué.

Start Test : cliquez sur ce bouton pour lancer le test. Une nouvelle fenêtre apparaît et affiche les résultats du test.

Ping Result : affiche l'état du test Ping.

TraceRoute Test Parameters

TraceRoute Target : saisissez l'adresse IP cible pour le test TraceRoute.

Start Test : cliquez sur ce bouton pour lancer le test. Une nouvelle fenêtre apparaît et affiche les résultats du test.

Cable Diagnostics

Port : sélectionnez le numéro de port dans le menu déroulant.

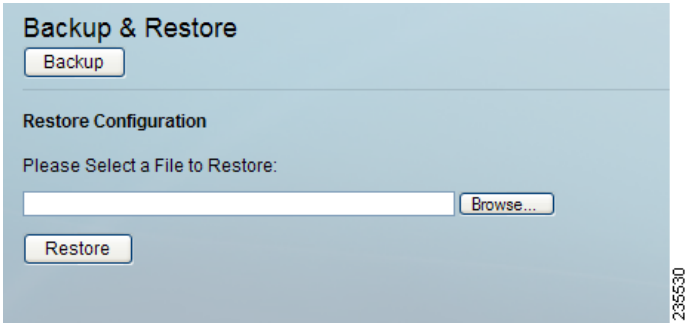
Pair : identifie une paire spécifique (A, B, C ou D) du câble. Chaque câble se compose de 8 broches (4 paires).

Cable Length : affiche la longueur du câble en mètres.

Status : affiche l'état de la paire.

Administration > Backup & Restore

Administration > Backup & Restore



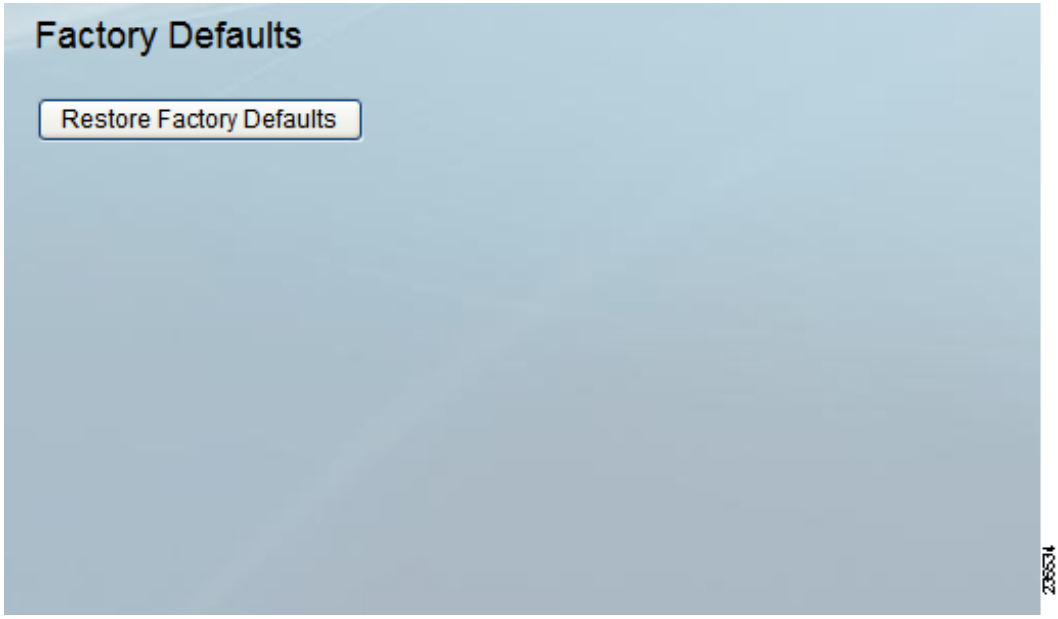
Pour télécharger une copie de la configuration actuelle et enregistrer le fichier sur l'ordinateur, cliquez sur **Backup** afin de lancer le téléchargement.

Restore Configuration

Pour restaurer un fichier de configuration précédemment enregistré sur le routeur, saisissez le nom du fichier dans le champ ou cliquez sur **Browse**, sélectionnez le fichier de configuration et cliquez ensuite sur **Restore** pour télécharger le fichier.

Administration > Factory Defaults

Administration > Factory Defaults



Restore Factory Defaults : cliquez sur ce bouton pour rétablir tous les paramètres de configuration par défaut. Le rétablissement des paramètres par défaut entraîne la perte de tous les paramètres précédemment enregistrés. Lorsque vous cliquez sur ce bouton, une autre fenêtre s'affiche. Cliquez sur **OK** pour continuer. Une autre fenêtre s'affiche pendant le redémarrage du système.

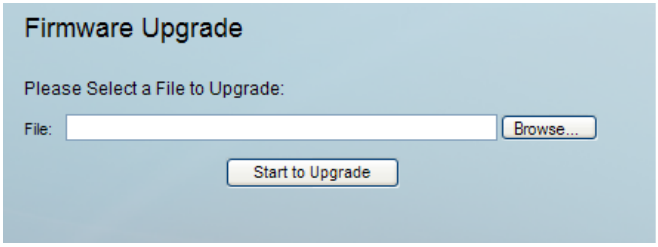
Administration > Reboot

Administration > Reboot

Reboot : cliquez sur ce bouton pour redémarrer le routeur. Le redémarrage du routeur n'entraîne pas la perte des paramètres enregistrés.

Administration > Firmware Upgrade

Administration > Firmware Upgrade

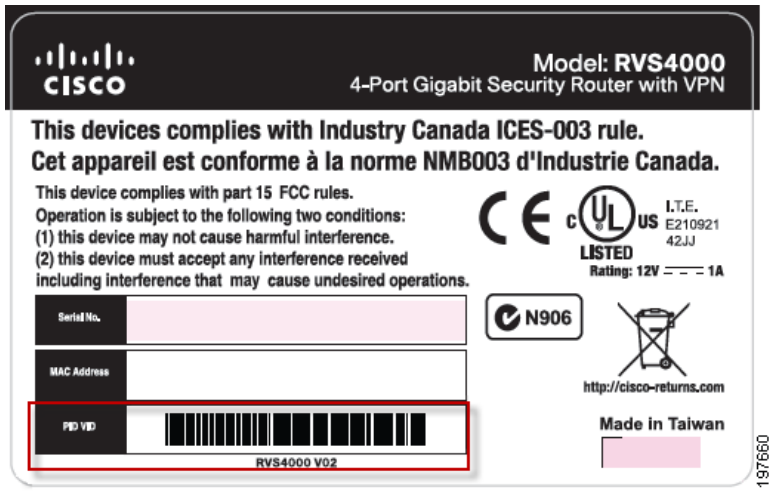


Utilisez cet écran pour mettre le routeur à niveau au moyen du microprogramme disponible sur Cisco.com. Des instructions détaillées vous sont fournies plus loin.

File : tapez le nom du fichier décompressé de mise à niveau du microprogramme ou cliquez sur **Browse** pour le localiser.

Start to Upgrade : après avoir sélectionné le fichier voulu, cliquez sur **Start to Upgrade**, puis suivez les instructions affichées à l'écran pour mettre le microprogramme à niveau.

ÉTAPE 1 Vérifiez la version matérielle du routeur indiquée sur l'étiquette située sur le panneau inférieur. Le numéro PIDVID comprend les caractères V01 (version 1) ou V02 (version 2).



ÉTAPE 2 Pour télécharger le dernier microprogramme du routeur, accédez au site www.cisco.com/go/smallbizfirmware.

ÉTAPE 3 Cliquez sur le lien correspondant à votre routeur.

ÉTAPE 4 Cliquez sur le bouton **Download Firmware**.

ÉTAPE 5 Parcourez les différents écrans pour télécharger le microprogramme le plus récent.

ÉTAPE 6 Décompressez le fichier du microprogramme sur votre ordinateur.

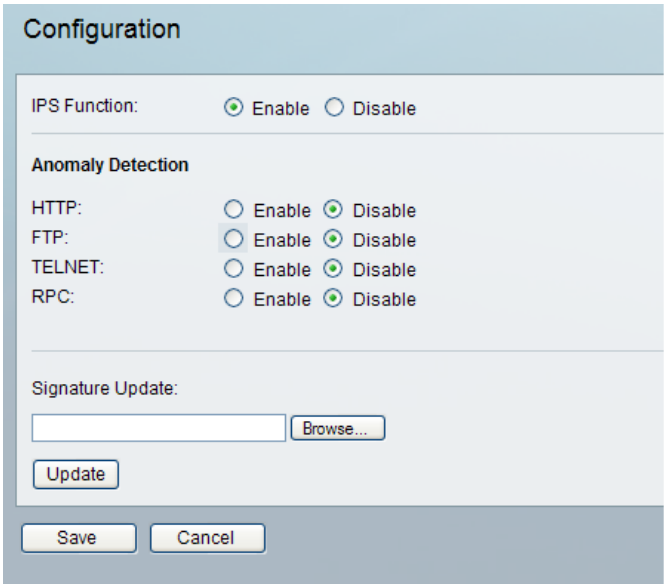
ÉTAPE 7 Dans la page *Administration > Firmware Upgrade*, cliquez sur **Browse** et localisez le fichier.

ÉTAPE 8 Cliquez sur **Start to Upgrade** pour lancer la mise à niveau.

IPS

IPS > Configuration

IPS > Configuration



IPS Function : sélectionnez **Enable** pour activer la fonction IPS (Intrusion Prevention System, système de prévention des intrusions) ou **Disable** pour la désactiver.

Anomaly Detection

HTTP : appariement du trafic HTTP avec les signatures d'attaques Web. Avant l'appariement de formes, le décodeur de requêtes HTTP décode le code UTF-8 (1, 2 et 3 octets) et normalise les URI (en fonction des méthodes d'évasion mentionnées dans le whisker).

FTP : détection des rebonds FTP et des insertions de codes opération Telnet dans le flux de commandes FTP.

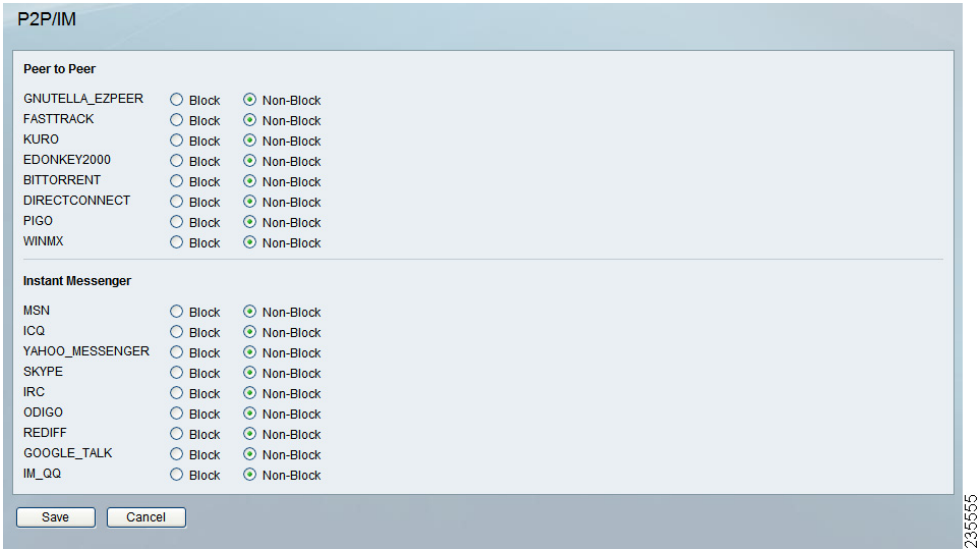
TELNET : normalisation des chaînes de négociation Telnet.

RPC : détection des fragmentations d'enregistrements RPC.

Signature Update : avant de mettre le fichier de signatures à niveau, téléchargez le fichier IPS du routeur sur le site Web de Cisco. Pour télécharger le fichier, accédez au site www.cisco.com/go/software (enregistrement/identifiant de connexion obligatoires) et recherchez RVS4000. Une fois le fichier téléchargé et décompressé, entrez le nom du fichier de signatures IPS dans le champ *Signature Update* ou cliquez sur **Browse** pour le localiser. Cliquez ensuite sur **Update** et suivez les instructions affichées à l'écran.

IPS > P2P/IM

Peer to Peer



Peer to Peer

Il est possible de bloquer (**Block**) ou d'autoriser (**Non-Block**) les applications de partage de fichiers peer-to-peer. Les réseaux préconfigurés de partage de fichiers sont les suivants : GNUTELLA (EZPEER), FASTTRACK, KURO, EDONKEY2000, BITTORRENT, DIRECTCONNECT, PIGO et WINMX.

Instant Messenger

Il est possible de bloquer (**Block**) ou d'autoriser (**Non-Block**) les applications de messagerie instantanée. Les applications préconfigurées de messagerie instantanée sont les suivantes : MSN, ICQ, YAHOO_MESSENGER, SKYPE, IRC, ODIGO, REDIFF, GOOGLE_TALK et IM_QQ.

IPS > Report

Cette fenêtre affiche une représentation graphique du niveau de trafic réseau et des attaques observés au cours des dernières 24 heures.

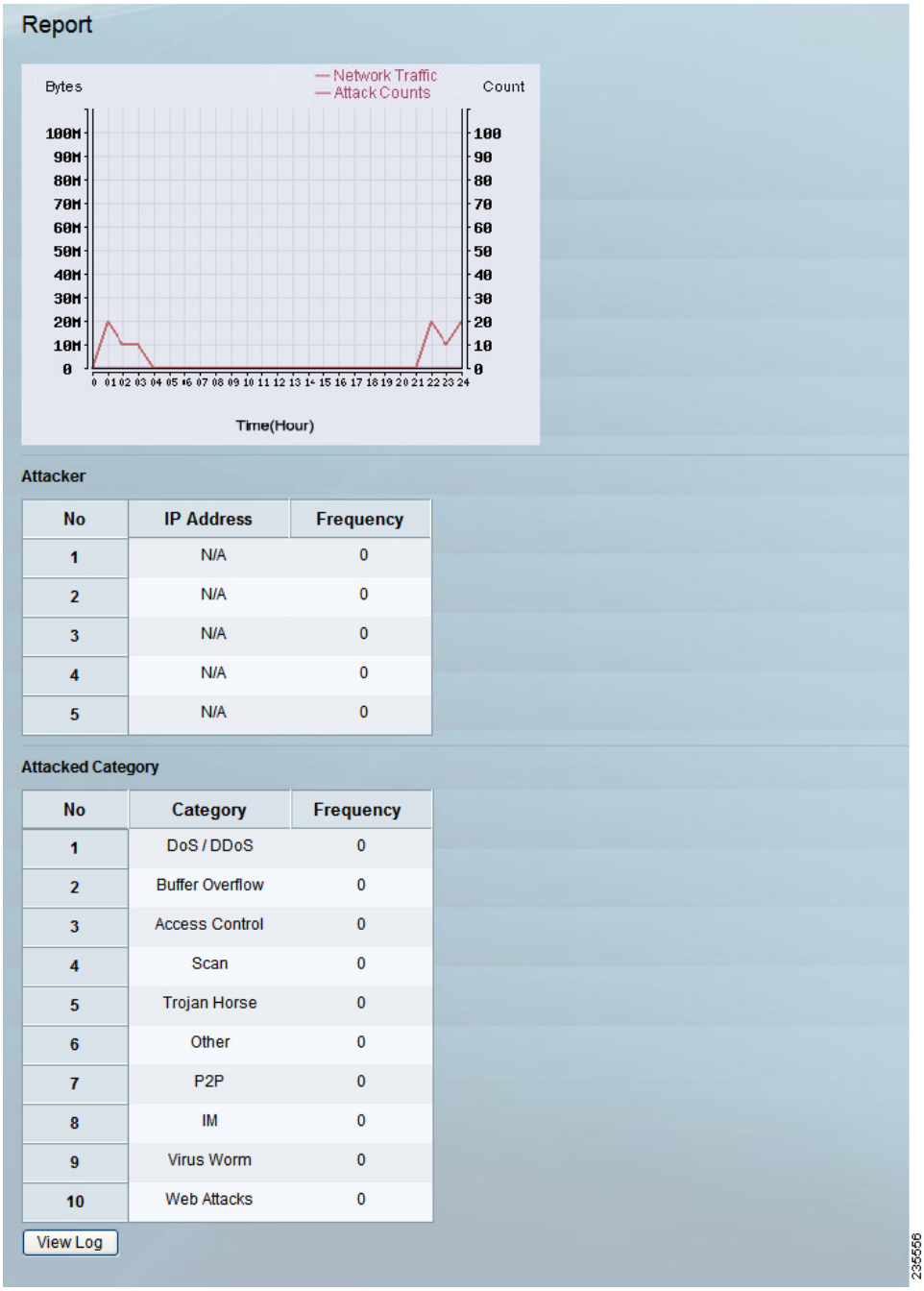
Attacker

Affiche l'adresse IP des auteurs d'attaques et la fréquence (le nombre) des attaques.

Attacked Category

Affiche la catégorie (le type) d'attaque et la fréquence (le nombre) des attaques.

IPS > Report



IPS > Information

IPS > Information

Signature Version : affiche la version des formes de signature du routeur assurant la protection contre les menaces malveillantes.

Last Time Upload : affiche la date de la dernière mise à jour des formes de signature du routeur.

Protect Scope : répertorie les types d'attaques bloquées par la fonctionnalité IPS du routeur.

L2 Switch

L2 Switch > Create VLAN

Les VLAN (Virtual Local-Area Network, réseau local virtuel) sont des sous-groupes logiques de LAN créés via des logiciels plutôt que par la définition d'une solution matérielle. Ils regroupent des postes utilisateur et des périphériques réseau au sein d'un même domaine, indépendamment du segment LAN physique auquel ils sont rattachés. Les réseaux VLAN permettent au trafic réseau de s'écouler plus efficacement dans les sous-groupes. Leur gestion par logiciel réduit le temps nécessaire à la mise en œuvre des modifications réseau.

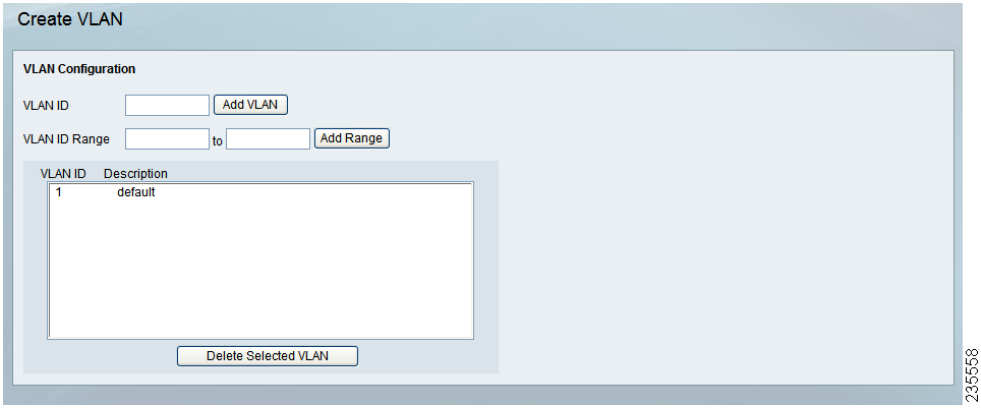
Il n'existe pas de nombre minimal de ports pour les VLAN ; ces derniers peuvent être créés par unité, par périphérique, par pile ou par toute autre combinaison de connexions logiques, puisqu'ils reposent sur des logiciels et ne sont pas définis par des attributs physiques.

Les VLAN fonctionnent au niveau de la couche 2. Dans la mesure où le trafic du VLAN est isolé à l'intérieur de celui-ci, un routeur de couche 3 est nécessaire pour permettre la circulation du trafic entre les VLAN. Les routeurs de couche 3 identifient les segments et effectuent la coordination avec les réseaux VLAN.

Les VLAN sont des domaines de diffusion et multidiffusion. Le trafic de diffusion et multidiffusion n'est acheminé que dans le VLAN dans lequel il est généré.

Le RVS4000 prend en charge jusqu'à quatre VLAN, y compris le VLAN par défaut.

L2 Switch > Create VLAN



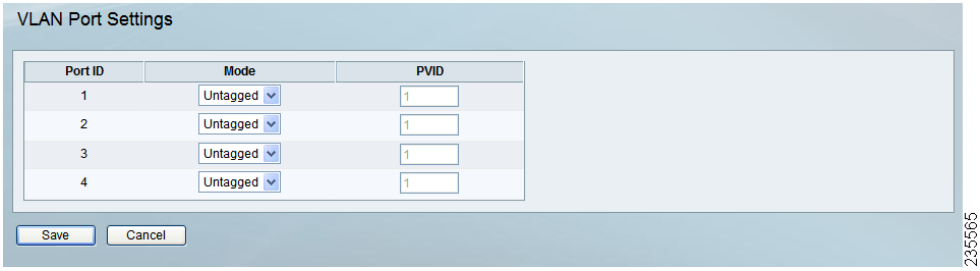
VLAN ID : identifiant du VLAN. Il peut s'agir de tout nombre compris entre 2 et 3290 ou entre 3293 et 4094. (L'identifiant de VLAN 1 est réservé au VLAN par défaut, lequel est utilisé pour les trames non balisées reçues sur l'interface. Les identifiants de VLAN 3291 et 3292 sont eux aussi réservés et ne peuvent être utilisés.) Pour créer un VLAN, saisissez son identifiant et cliquez sur **Add VLAN**.

VLAN ID Range : pour créer plusieurs VLAN à l'aide d'une plage d'identifiants, entrez les identifiants de début et de fin, puis cliquez sur **Add Range**.

Delete Selected VLAN : pour supprimer un VLAN, sélectionnez-le dans la liste des VLAN, puis cliquez sur **Delete Selected VLAN**.

L2 Switch > VLAN Port Settings

L2 Switch > VLAN Port Settings



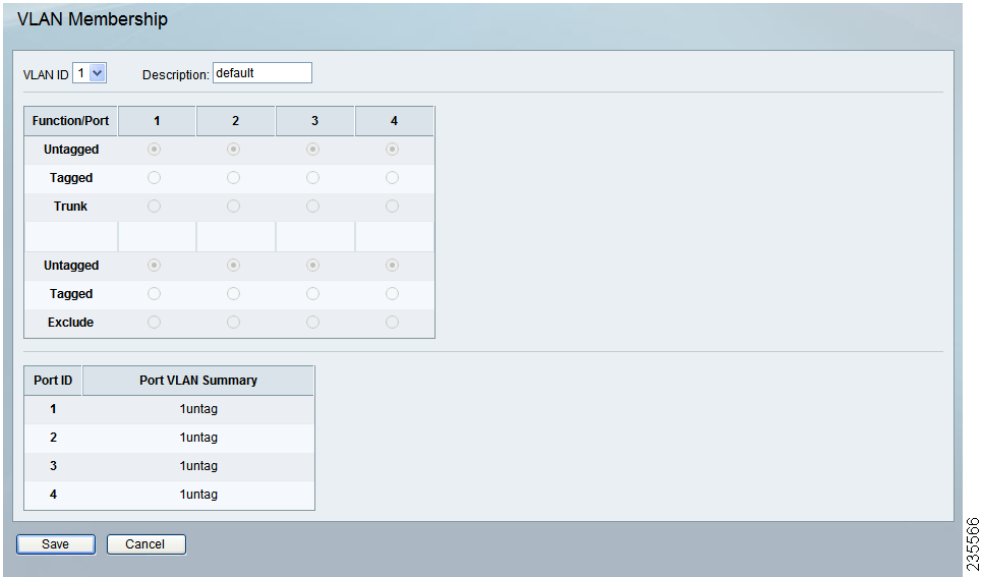
Port ID : affiche le numéro de port, compris entre **1** et **4**.

Mode : sélectionnez le mode du port, **Trunk**, **Untagged** ou **Tagged**. La valeur par défaut est **Untagged**. En mode de liaison (Trunk), les trames entrantes et sortantes peuvent être balisées ou non balisées ; les trames entrantes non balisées sont balisées au moyen du PVID (Port VLAN ID, identifiant VLAN de port) par défaut. En mode non balisé (Untagged), toutes les trames entrantes et sortantes sont non balisées. En mode balisé (Tagged), toutes les trames entrantes et sortantes doivent être balisées ; les trames non balisées sont supprimées.

PVID : identifiant VLAN de port affecté aux trames non balisées reçues sur l'interface. La valeur par défaut est **1**. En mode balisé, le port reçoit uniquement les trames balisées et le port n'a donc pas de PVID.

L2 Switch > VLAN Membership

L2 Switch > VLAN Membership



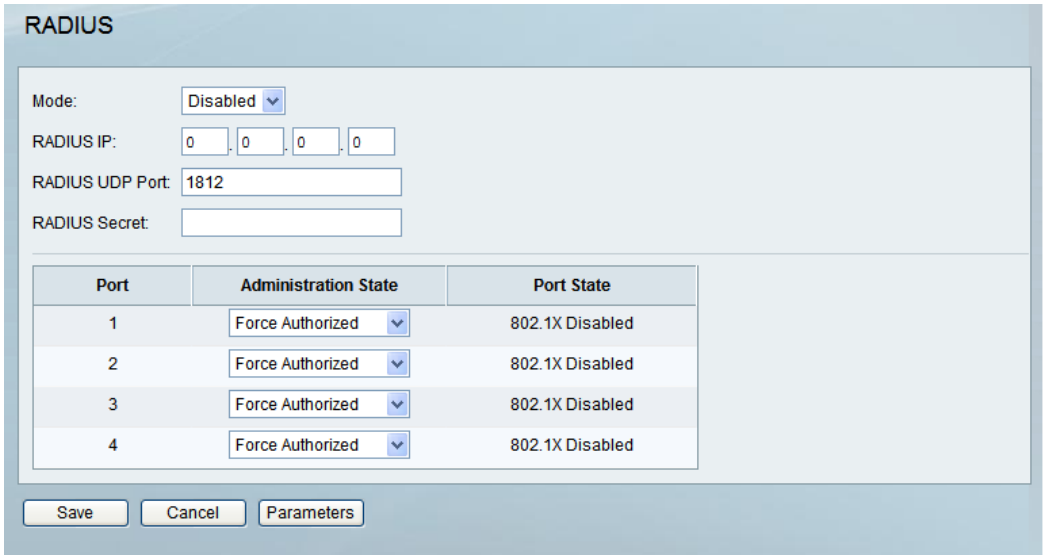
VLAN ID : sélectionnez le VLAN dont vous souhaitez configurer l'appartenance de groupe.

Description : saisissez un nom de groupe VLAN composé de 50 caractères au maximum.

Function/Port : la partie supérieure du tableau indique le mode actuel de chaque port (Untagged, Tagged ou Trunk). Sa partie inférieure permet de définir les ports membres du VLAN sélectionné. La valeur par défaut de chaque port est **Exclude** (le port ne fait pas partie du VLAN). Pour faire en sorte qu'un port appartienne au VLAN, sélectionnez le ou les modes applicables. Par exemple, sélectionnez Untagged si le mode du port est Untagged, Tagged si le mode est Tagged et enfin Tagged ou Untagged si le mode est Trunk.

L2 Switch > RADIUS

L2 Switch > RADIUS



Mode : sélectionnez **Enabled** ou **Disabled** dans le menu déroulant pour activer ou désactiver RADIUS.

RADIUS IP : saisissez l'adresse IP du serveur.

RADIUS UDP Port : saisissez le port UDP. Celui-ci est utilisé pour vérifier l'authentification du serveur RADIUS.

RADIUS Secret : saisissez la chaîne clé utilisée pour l'authentification et le cryptage de toutes les communications RADIUS établies entre le périphérique et le serveur RADIUS. Cette clé doit correspondre à la clé de cryptage du serveur RADIUS. Si aucune valeur propre à l'hôte n'est indiquée, la valeur globale s'applique à chaque hôte.

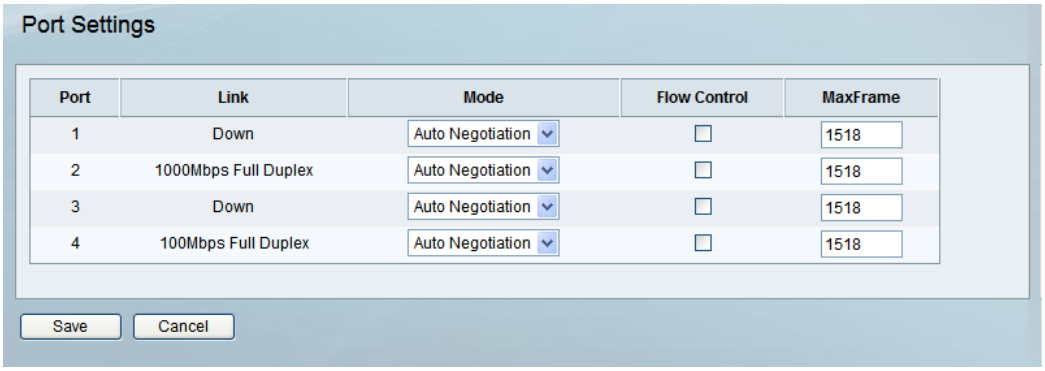
Administration State : indique l'état d'autorisation du port. Les valeurs de champ possibles sont les suivantes :

- **Auto** : l'état du port contrôlé est défini par la méthode d'authentification.
- **Force Authorized** : le port contrôlé est dans l'état d'autorisation forcée (transfert du trafic).
- **Force Unauthorized** : le port contrôlé est dans l'état d'interdiction forcée (élimination du trafic).

Port State : indique l'état du port sélectionné.

L2 Switch > Port Settings

L2 Switch > Port Settings



Port : affiche le numéro de port physique.

Link : affiche le mode duplex et la vitesse du port. **Full Duplex** indique que l'interface prend en charge la transmission entre le périphérique et son partenaire de liaison, dans les deux sens simultanément. **Half Duplex** indique que l'interface prend en charge la transmission entre le périphérique et le client dans un seul sens à la fois

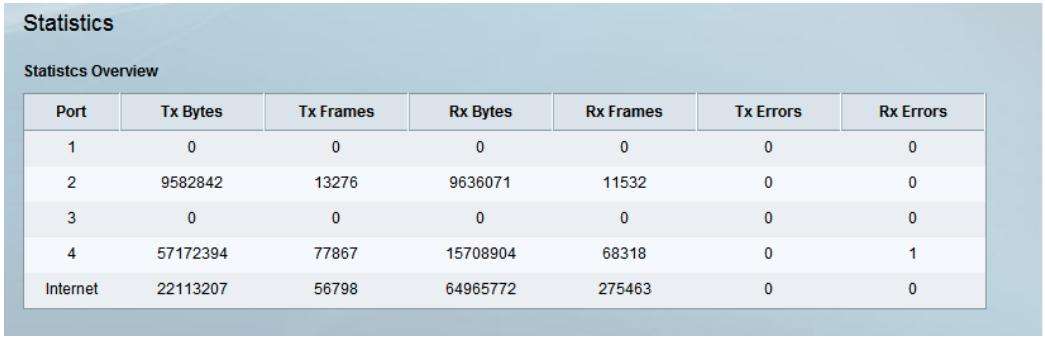
Mode : sélectionnez le mode duplex et la vitesse du port dans le menu déroulant. Vous pouvez également sélectionner **Auto Negotiation**, protocole utilisé entre deux partenaires de liaison et qui permet à un port d'indiquer à son partenaire sa vitesse de transmission, son mode duplex et ses capacités de contrôle de flux.

Flow Control : affiche l'état de contrôle de flux du port. Fonctionne lorsque le port est en mode Full Duplex.

MaxFrame : affiche la taille maximale d'une trame que le port peut recevoir et envoyer.

L2 Switch > Statistics

L2 Switch > Statistics



Statistics Overview

Tx Bytes : affiche le nombre d'octets transmis à partir du port sélectionné.

Tx Frames : affiche le nombre de trames transmises à partir du port sélectionné.

Rx Bytes : affiche le nombre d'octets reçus sur le port sélectionné.

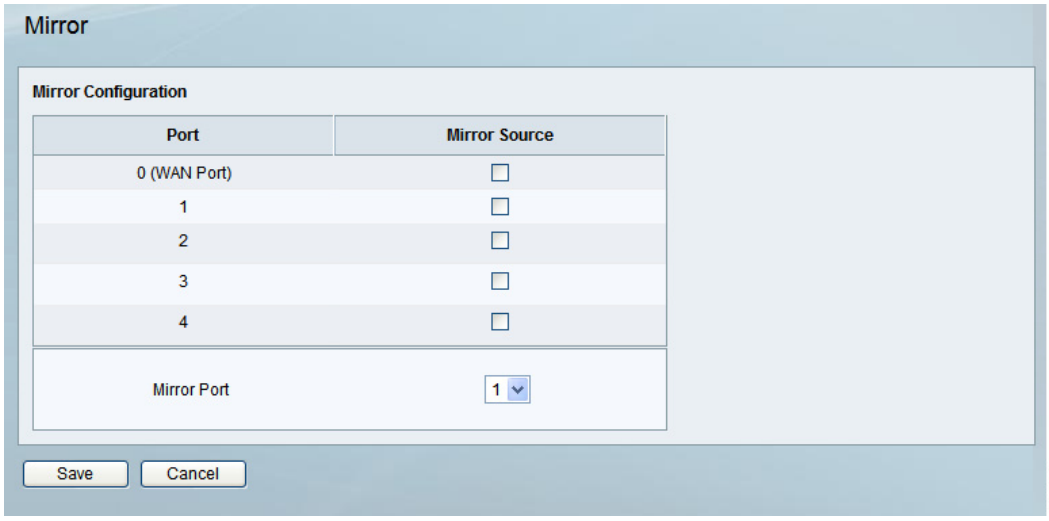
Rx Frames : affiche le nombre de trames reçues sur le port sélectionné.

Tx Errors : affiche le nombre de paquets erronés transmis à partir du port sélectionné.

Rx Errors : affiche le nombre de paquets erronés reçus sur le port sélectionné.

L2 Switch > Mirror

L2 Switch > Mirror

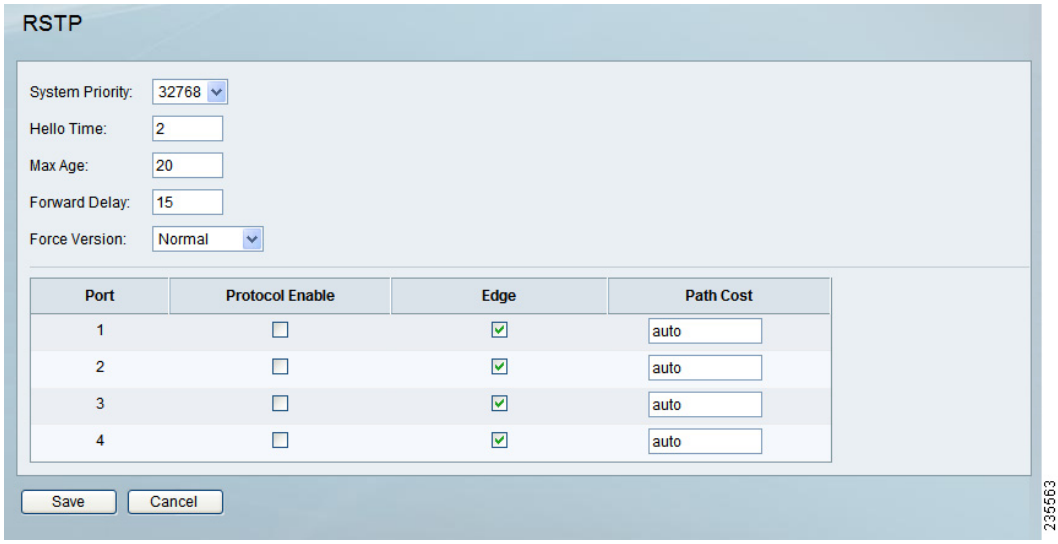


Mirror Source : utilisez cette case à cocher pour activer ou désactiver la mise en miroir du port source pour chaque port du routeur. Pour activer la mise en miroir du port source sur un port, cochez la case en regard de ce port. Pour désactiver la mise en miroir du port source sur un port, laissez sa case décochée. La case est **décochée** par défaut.

Mirror Port : sélectionnez le numéro de port de destination miroir dans le menu déroulant.

L2 Switch > RSTP

L2 Switch > RSTP



Le protocole RSTP (Rapid Spanning Tree Protocol) prévient les boucles au sein du réseau et, par une reconfiguration dynamique, détermine les liens physiques d'un commutateur qui doivent transmettre les trames.

System Priority : saisissez la priorité système comprise entre 0 et 61 440 par incréments de 4 096. Les valeurs admises sont 0, 4 096, 8 192, 12 288, 16 384, 20 480, 24 576, 28 672, 32 768, 40 960, 45 056, 49 152, 53 248, 57 344 et 61 440. Plus la priorité système est faible, plus le routeur a des chances de se situer à la racine de l'arborescence. La valeur par défaut est **32 768**.

Hello Time : saisissez un temps d'attente compris entre 1 et 10. La valeur par défaut est **2**.

Max Age : saisissez une durée maximale comprise entre 6 et 40. La valeur par défaut est **20**.

Forward Delay : saisissez un délai de transition compris entre 4 et 30. La valeur par défaut est **15**.

Force Version : version de protocole par défaut à utiliser. Sélectionnez **Normal** (utiliser RSTP) ou **Compatible** (compatible avec le protocole STP de version antérieure). La valeur par défaut est **Normal**.

Protocol Enable : cochez cette case pour activer RSTP sur le port associé. Par défaut, cette case est décochée (**RSTP désactivé**).

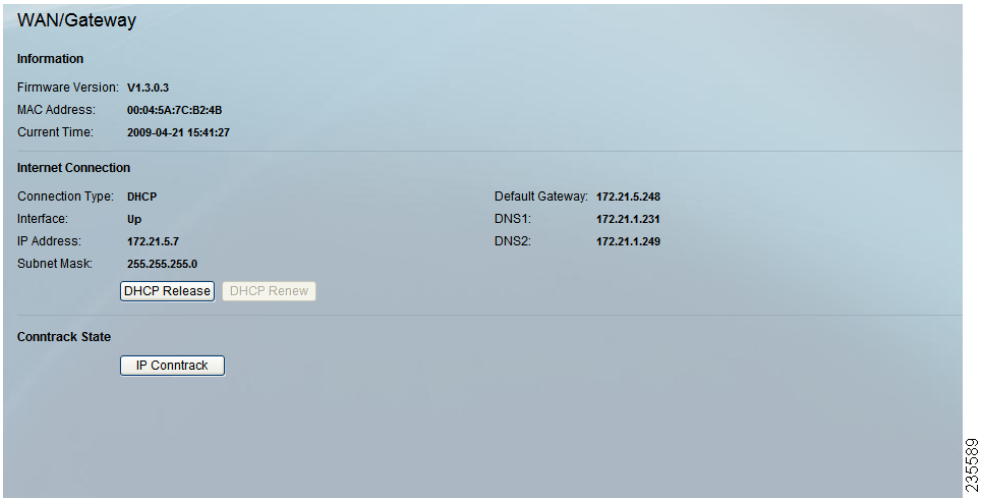
Edge : cochez cette case pour indiquer que le port associé est un port de périphérie (station terminale). Décochez la case pour spécifier qu'il s'agit d'une liaison (pont) vers un autre périphérique STP. Par défaut, la case est cochée (**port de périphérie**).

Path Cost : côut du chemin RSTP pour les ports désignés. Entrez un nombre compris entre 1 et 200 000 000, ou tapez le mot **auto** (coût de chemin généré automatiquement). La valeur par défaut est **auto**.

Status

Status > Gateway

Status > Gateway



Firmware Version : affiche le numéro de version du microprogramme actuel de la passerelle.

MAC Address : affiche l'adresse MAC de la passerelle, telle qu'elle est vue par votre FAI.

Current Time : affiche les date et heure, en fonction du fuseau horaire sélectionné dans le menu Setup.

Internet Connection

Connection Type : affiche le type de connexion.

Interface : affiche l'interface Internet de la passerelle.

IP Address : affiche l'adresse IP Internet de la passerelle.

Subnet Mask : affiche le masque de sous-réseau correspondant à l'adresse IP précédemment spécifiée.

Default Gateway : indique l'adresse IP de la passerelle de votre FAI.

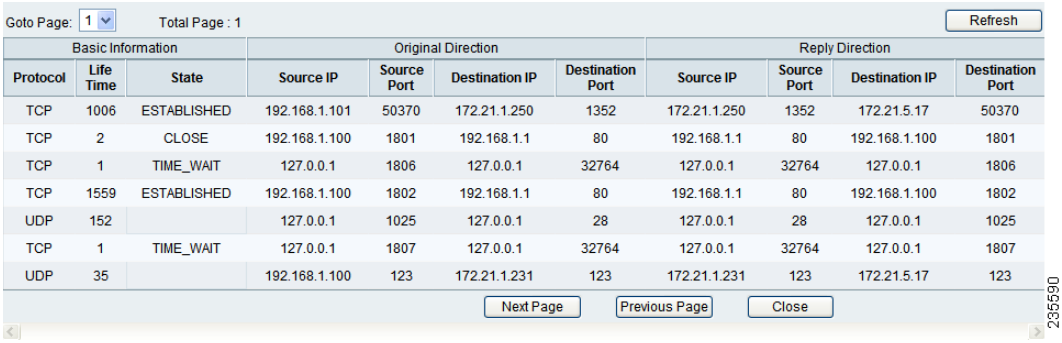
DNS 1-2 : indique les adresses IP des serveurs DNS (Domain Name System) actuellement utilisés par la passerelle.

IP Conntrack : cliquez sur ce bouton pour afficher la fenêtre *IP Conntrack*.

IP Conntrack

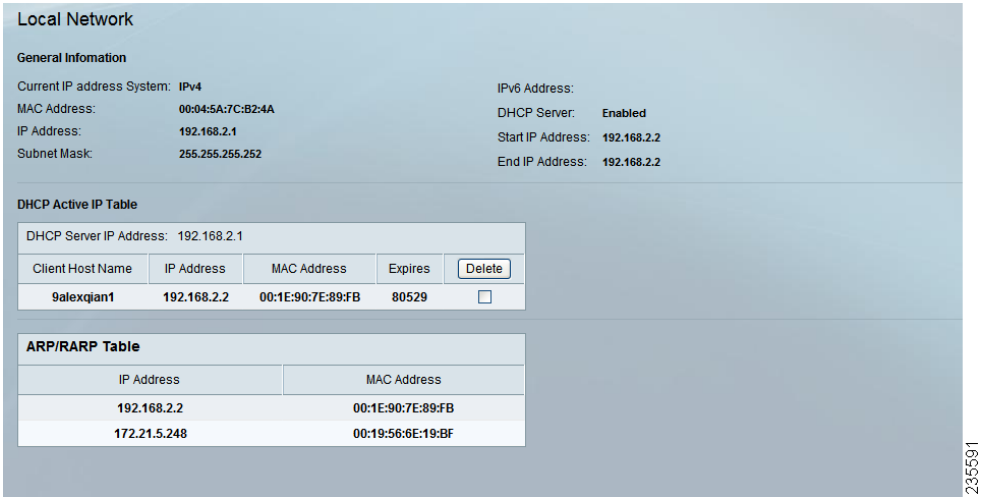
La fenêtre *IP Conntrack (Connection Tracking)* affiche des informations sur les connexions TCP/UDP, notamment les paires adresses IP-numéros de port source et destination (appelées paires de connecteurs), les types de protocoles (TCP/UDP/ICMP), l'état de la connexion et les délais d'expiration. Pour afficher plus d'informations, cliquez sur **Next Page** ou sur **Previous Page**, ou sélectionnez le numéro de la page dans le menu déroulant *Go to Page*. Pour afficher des informations à jour, cliquez sur **Refresh**. Cliquez sur **Close** pour revenir à la fenêtre *Status > Gateway*.

Status > Gateway > IP Conntrack



Status > Local Network

Status > Local Network



Current IP address System : affiche le système actif.

MAC Address : adresse MAC du routeur, du point de vue du réseau Ethernet local.

IP Address : adresse IP Internet.

Subnet Mask : masque de sous-réseau correspondant à l'adresse IP précédemment spécifiée.

IPv6 Address : adresse IP IPv6, le cas échéant.

DHCP Server : état de la fonction serveur DHCP du routeur.

Start IP Address : première adresse de la plage d'adresses IP utilisée par le serveur DHCP.

End IP Address : dernière adresse de la plage d'adresses IP utilisée par le serveur DHCP.

DHCP Client Table : cliquez sur ce bouton pour ouvrir une fenêtre qui affiche les ordinateurs utilisant le routeur en tant que serveur DHCP. La fenêtre *DHCP Client Table* affiche tous les clients DHCP (ordinateurs et autres périphériques réseau) ainsi que les informations suivantes à leur sujet : nom du client, interfaces, adresses IP et MAC, et délai avant expiration de l'adresse IP qui lui est attribuée.

ARP/RARP Client Table : cliquez sur ce bouton pour ouvrir une fenêtre qui affiche les ordinateurs utilisant le routeur en tant que serveur ARP/RARP. La fenêtre *ARP/RARP Table* affiche tous les clients ARP/RARP (ordinateurs et autres périphériques réseau) ainsi que les informations suivantes à leur sujet : adresses IP et MAC.

6

Utilisation de l'assistant d'installation de VPN

Ce chapitre explique comment utiliser l'assistant d'installation de VPN. Il comprend les sections suivantes :

Assistant d'installation de VPN

Vous pouvez désormais configurer de manière simple et rapide un tunnel VPN passerelle à passerelle entre deux routeurs VPN à l'aide de l'assistant d'installation de VPN. Cet assistant fonctionne avec les ordinateurs équipés de Microsoft Windows 2000, XP et Vista. Ce document explique comment exécuter l'assistant d'installation de VPN.

Avant de commencer

L'assistant d'installation de VPN fonctionne avec les routeurs suivants :

- Routeur de sécurité Gigabit 4 ports avec VPN Cisco RVS4000
- Routeur de sécurité Gigabit sans fil N 4 ports avec VPN Cisco WRVS4400N v1.1
- Routeur de sécurité Gigabit sans fil N 4 ports avec VPN Cisco WRVS4400N v2

Suivez ces instructions pour configurer les données requises à l'aide de l'interface Web d'administration. Pour obtenir des instructions sur l'interface Web d'administration, reportez-vous au guide d'administration de votre routeur.

ÉTAPE 1 Cliquez sur **Firewall > Basic Settings**.

ÉTAPE 2 Activez la gestion à distance et entrez **8 080** dans le champ Port. Notez que vous ne pouvez entrer aucune autre valeur si vous souhaitez utiliser l'assistant VPN. Assurez-vous également que l'option HTTPS est sélectionnée.

ÉTAPE 3 Cliquez sur **Save**.

ÉTAPE 4 Cliquez sur **VPN > Summary** et assurez-vous que le nombre de tunnels disponibles (**Tunnel(s) available**) n'est pas égal à zéro.

ÉTAPE 5 Vérifiez que les adresses IP LAN des routeurs avec VPN appartiennent à des sous-réseaux différents pour que la connexion VPN fonctionne.

REMARQUE L'assistant d'installation de VPN part du principe que le routeur VPN n'est équipé d'aucun pare-feu/périphérique NAT.

Exécution de l'assistant d'installation de VPN

ÉTAPE 1 Accédez à l'assistant d'installation de l'une des deux manières suivantes :

- Si vous possédez un CD-ROM d'installation pour RVS4000, WRVS4400N v1.1 ou WRVS4400N v2, insérez-le dans le lecteur de CD-ROM.
- Téléchargez l'assistant d'installation de VPN à partir du site d'assistance Cisco pour votre routeur.

ÉTAPE 2 Dans le menu Start, cliquez sur **Run**. Dans le champ affiché, saisissez : **D:\VPN Setup Wizard.exe**

ÉTAPE 3 Dans la fenêtre de bienvenue, cliquez sur **Start**.

Fenêtre de bienvenue

ÉTAPE4 Lisez les informations relatives à l'assistant, puis cliquez sur **Next** pour continuer.

Fenêtre d'information

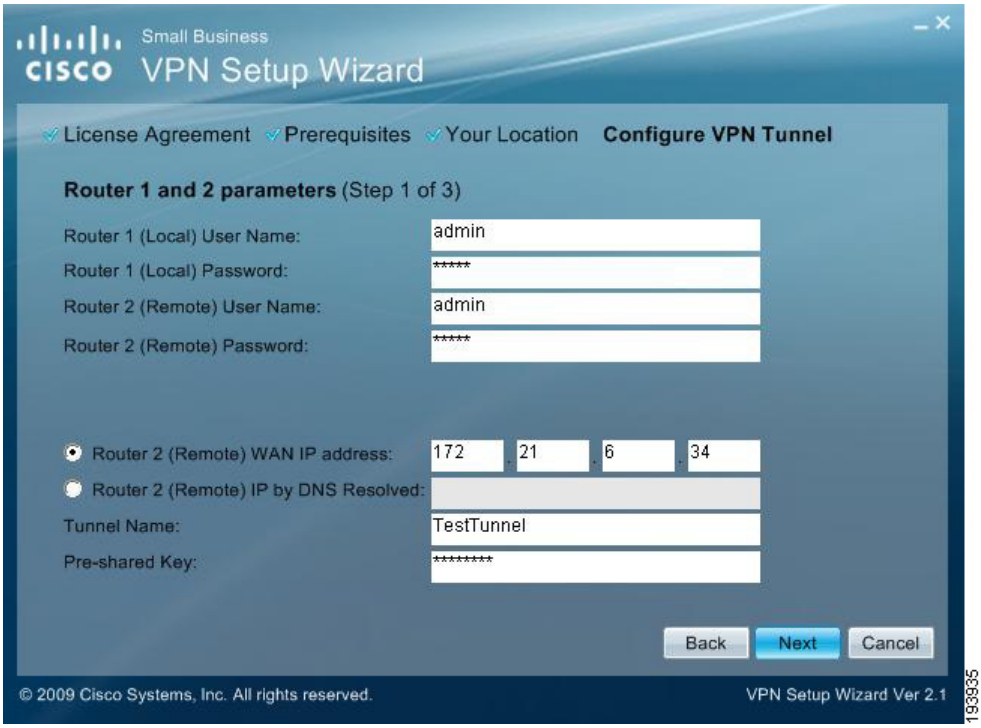
ÉTAPE 5 Choisissez une méthode pour créer la connexion VPN :

- Si votre PC est connecté localement à l'un des deux routeurs, choisissez **Build VPN connection from Local LAN port of one router**, cliquez sur **Next**, puis continuez à suivre les instructions.
- Si votre PC est connecté à distance aux routeurs, choisissez **Build VPN connection from Internet remotely**, puis reportez-vous à la section **« Création de votre connexion VPN à distance », page 110** pour lire les instructions relatives à ce type d'installation.

Création de la connexion VPN à distance

ÉTAPE6 Saisissez les données requises dans la fenêtre de configuration du tunnel VPN, puis cliquez sur **Next** pour continuer.

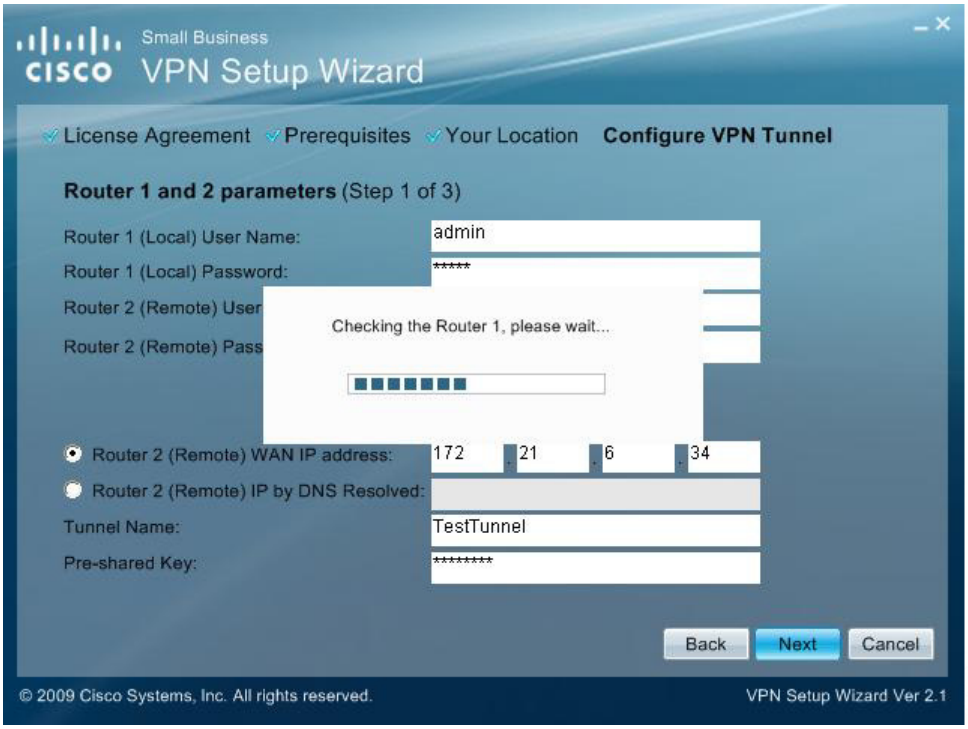
Configuration du tunnel VPN



- **Router 1 User Name** : saisissez le nom d'utilisateur du routeur 1.
- **Router 1 Password** : saisissez le mot de passe du routeur 1.
- **Router 2 User Name** : saisissez le nom d'utilisateur du routeur 2.
- **Router 2 Password** : saisissez le mot de passe du routeur 2.
- **Tunnel Name** : saisissez un nom pour ce tunnel.
- **Pre-shared Key** : la fonction IKE utilise le champ de clé pré-partagée pour authentifier l'homologue IKE distant. Dans ce champ, vous pouvez utiliser à la fois des caractères et des valeurs hexadécimales (« Mon_@123 » ou « 0x4d795f40313233 », par exemple). Notez que la clé pré-partagée doit être identique des deux côtés.
- **Router 2 WAN IP address** : saisissez l'adresse IP WAN du routeur 2.
- **Router 2 IP by DNS Resolved** : saisissez le nom de domaine DDNS du routeur 2 s'il n'a pas d'adresse IP statique pour la connexion Internet.

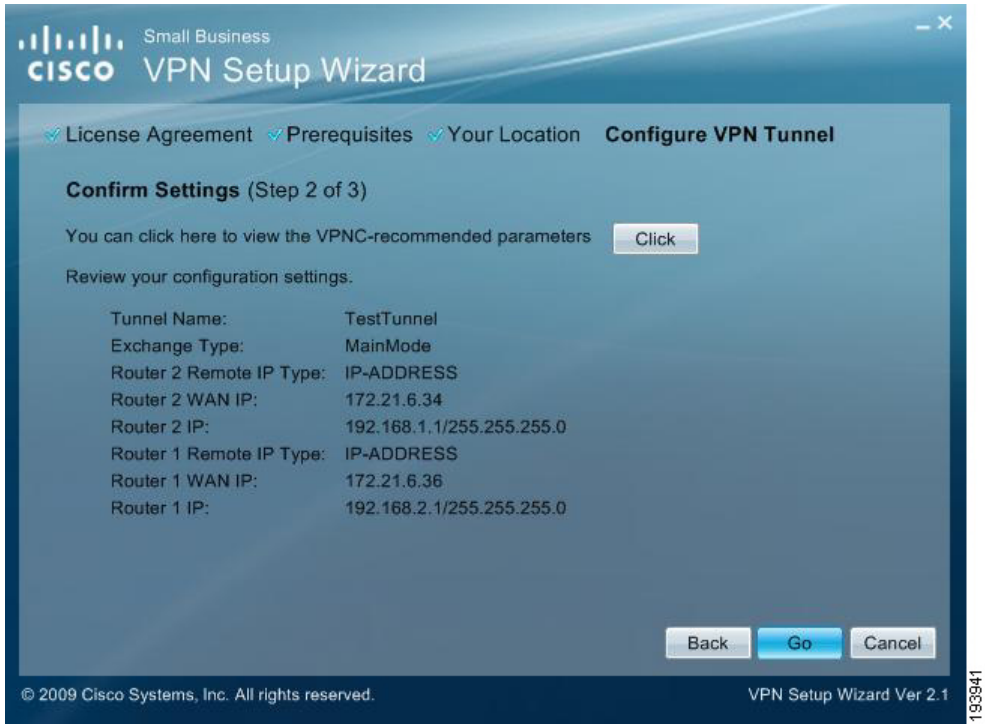
La configuration du routeur est vérifiée.

Vérification de la configuration du routeur



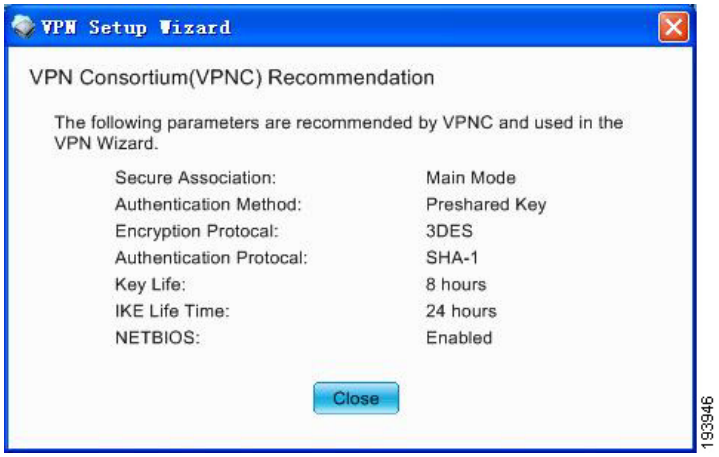
ÉTAPE7 Lorsque la fenêtre de récapitulatif s'affiche, utilisez le bouton **Click** pour faire apparaître la fenêtre du récapitulatif VPNC.

Fenêtre de récapitulatif



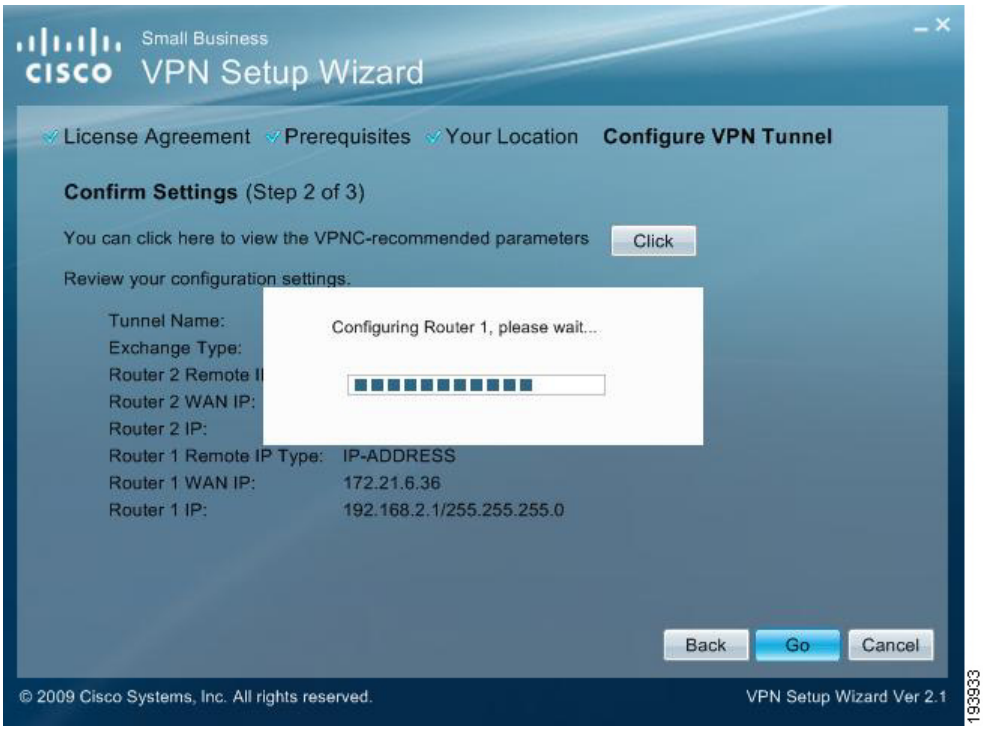
ÉTAPE 8 Vérifiez les paramètres, si nécessaire. Lorsque vous avez terminé, cliquez sur **Close** pour continuer.

Fenêtre du récapitulatif VPNC



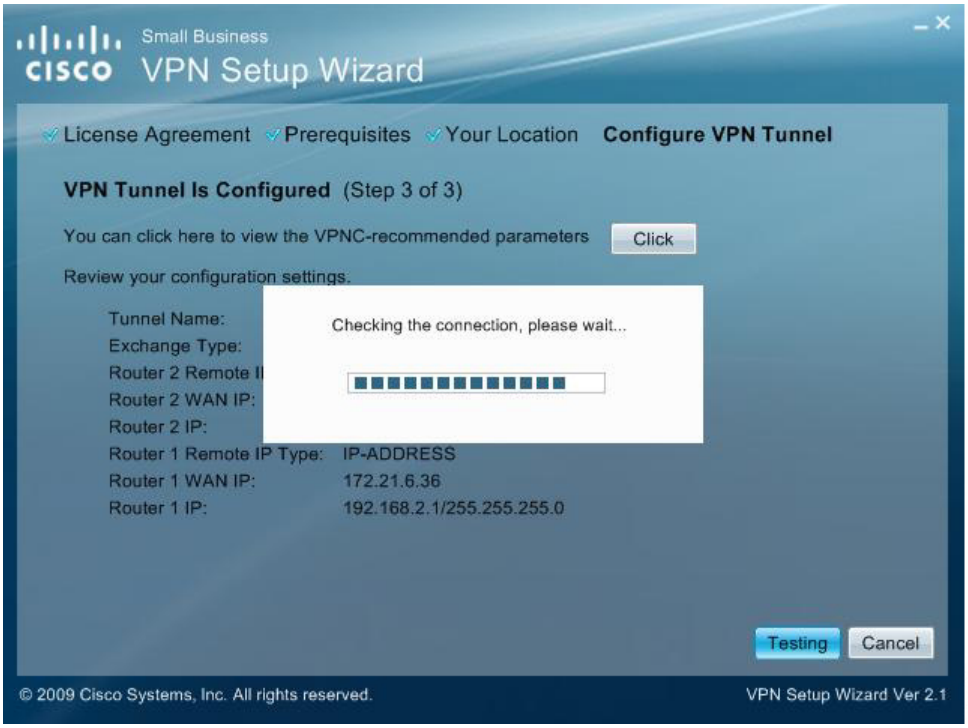
ÉTAPE 9 Dans la fenêtre de récapitulatif, si toutes vos entrées apparaissent correctement, cliquez sur **Go**. Sinon, cliquez sur **Back** pour revenir en arrière et apporter vos modifications.

Configuration du routeur



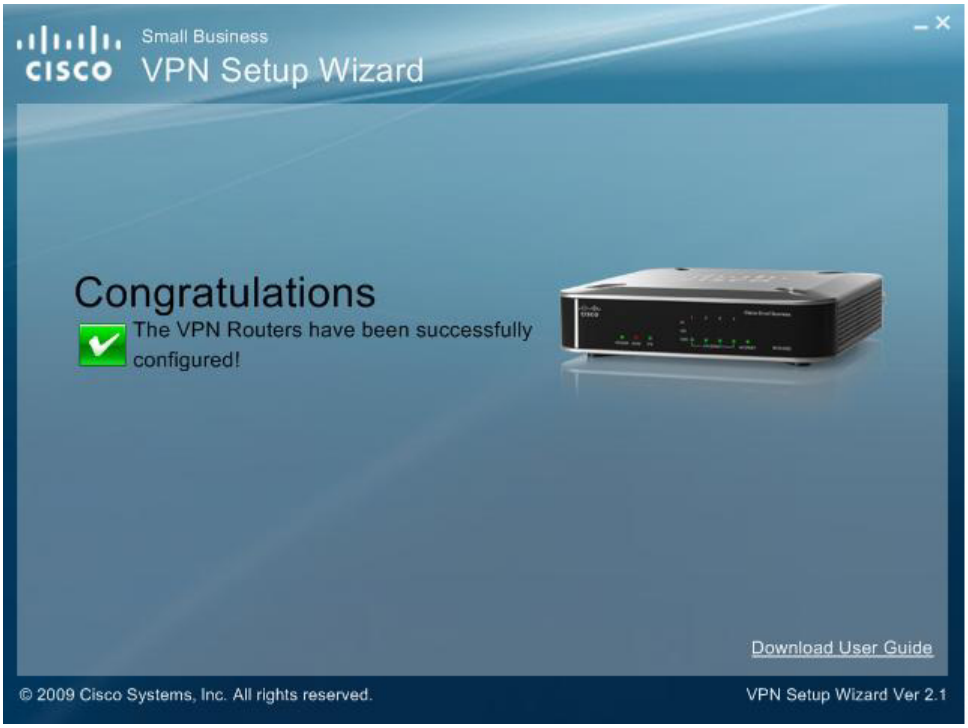
ÉTAPE 10 Cliquez sur **Testing** pour vérifier que les connexions ont été correctement établies.

Test de la connexion



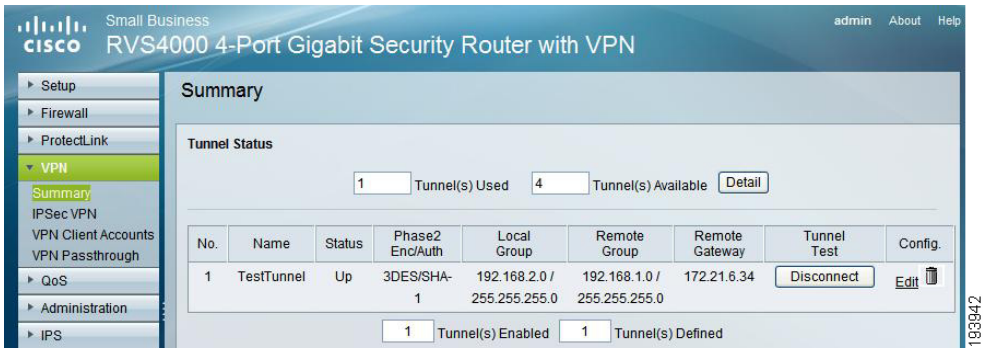
ÉTAPE 11 Lorsque le test est terminé, cliquez sur **Exit** pour quitter l'assistant.

Quittez l'assistant.



Félicitations ! L'installation est maintenant terminée. Vous pouvez maintenant vous connecter à l'interface Web d'administration pour voir les résultats.

Résultats du test



Création de votre connexion VPN à distance

Cette procédure fait suite à l'Étape 5, page 103. Utilisez-la pour créer votre connexion VPN à partir d'un PC distant.

ÉTAPE 1 Choisissez **Build VPN connection from Internet remotely**. Cliquez sur **Next** pour continuer.

Création de la connexion VPN à distance

ÉTAPE 2 Saisissez les données requises dans la fenêtre Configure VPN Tunnel, puis cliquez sur **Next** pour continuer.

Fenêtre de configuration du tunnel VPN

- **Router 1 User Name** : saisissez le nom d'utilisateur du routeur 1.
- **Router 1 Password** : saisissez le mot de passe du routeur 1.
- **Router 2 User Name** : saisissez le nom d'utilisateur du routeur 2.
- **Router 2 Password** : saisissez le mot de passe du routeur 2.
- **Tunnel Name** : saisissez un nom pour ce tunnel.
- **Pre-shared Key** : la fonction IKE utilise le champ de clé pré-partagée pour authentifier l'homologue IKE distant. Dans ce champ, vous pouvez utiliser à la fois des caractères et des valeurs hexadécimales (« Mon_@123 » ou « 0x4d795f40313233 », par exemple). Notez que la clé pré-partagée doit être identique des deux côtés.
- **Router 1 WAN IP address** : saisissez l'adresse IP WAN du routeur 1.
- **Router 1 IP by DNS Resolved** : saisissez le nom de domaine DDNS du routeur 1 s'il n'a pas d'adresse IP statique pour la connexion Internet.
- **Router 2 WAN IP address** : saisissez l'adresse IP WAN du routeur 2.

- **Router 2 IP by DNS Resolved** : saisissez le nom de domaine DDNS du routeur 2 s'il n'a pas d'adresse IP statique pour la connexion Internet.

ÉTAPE 3 La configuration du routeur est vérifiée.

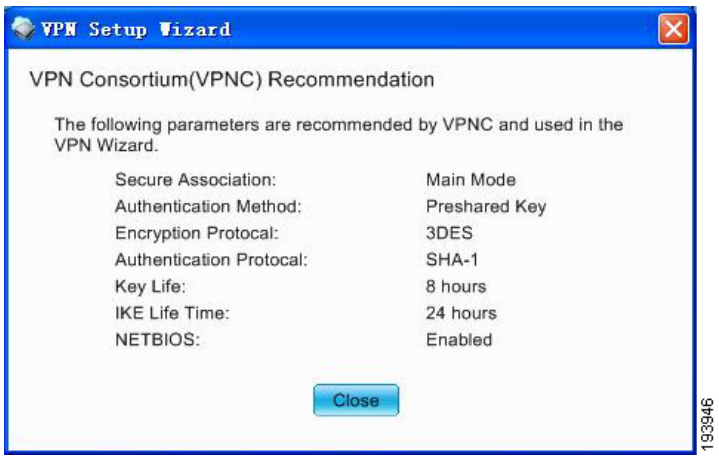
Vérification de la configuration du routeur

ÉTAPE 4 La fenêtre de récapitulatif s'affiche. Utilisez le bouton **Click** pour afficher la fenêtre du récapitulatif VPNC.

Fenêtre de récapitulatif

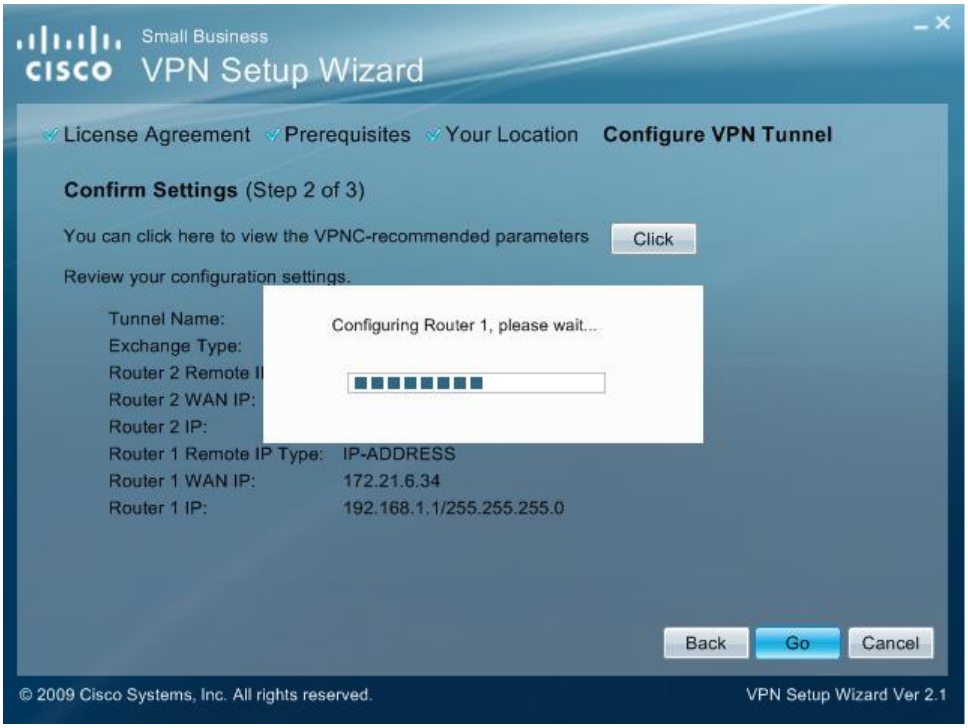
ÉTAPE 5 La fenêtre du récapitulatif VPNC affiche les paramètres conformes aux normes de l'industrie. Lorsque vous avez terminé, cliquez sur **Close** pour continuer.

Fenêtre du récapitulatif VPNC



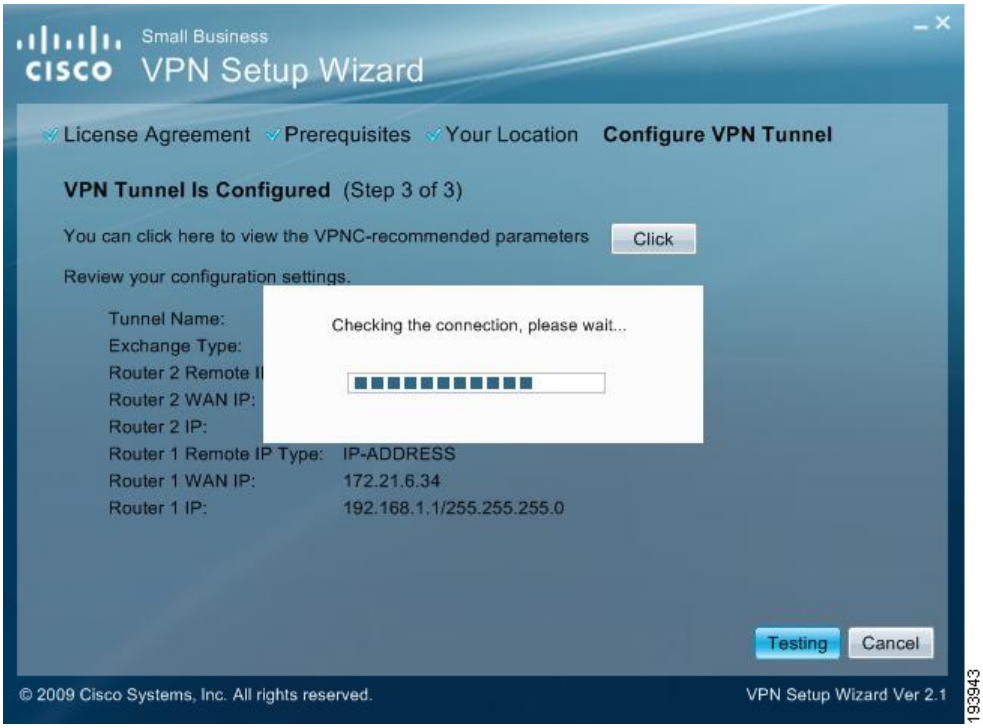
ÉTAPE 6 Dans la fenêtre de récapitulatif, si toutes vos entrées apparaissent correctement, cliquez sur **Go**. Sinon, cliquez sur **Back** pour revenir en arrière et apporter vos modifications.

Configuration du routeur

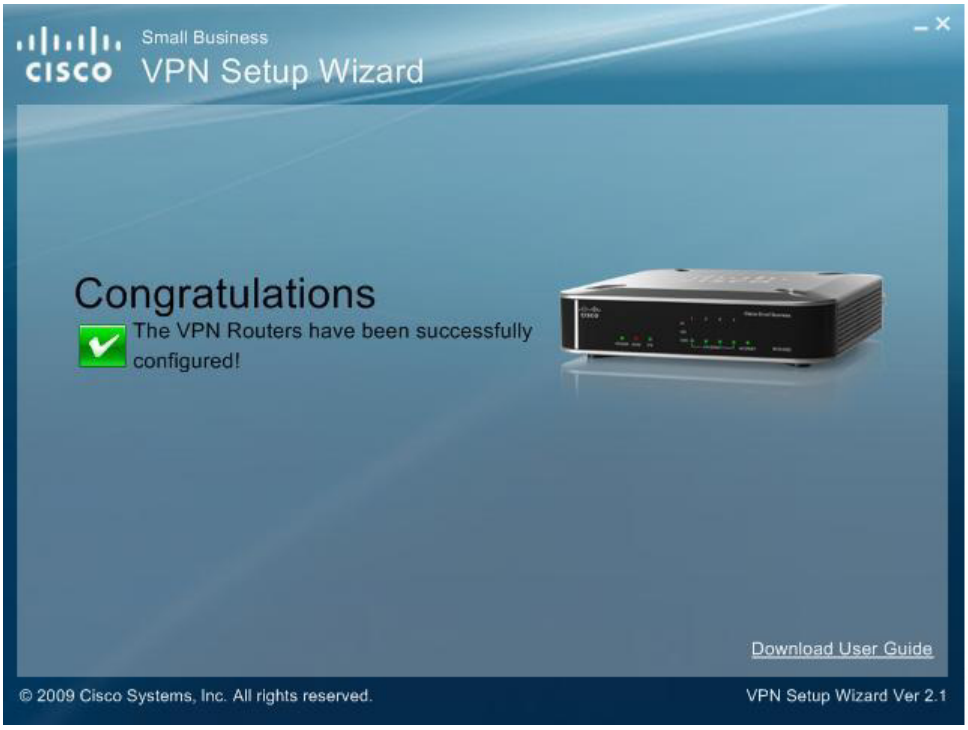


ÉTAPE 7 Cliquez sur **Testing** pour vérifier que les connexions ont été correctement établies.

Test de la connexion

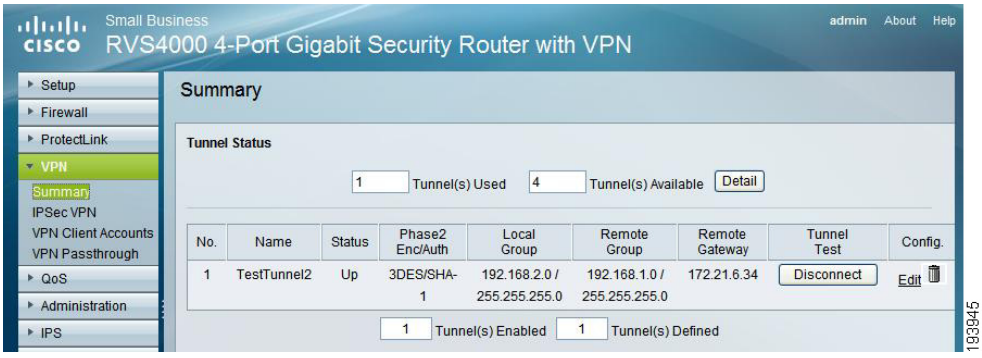


ÉTAPE 8 Lorsque le test est terminé, cliquez sur **Exit** pour quitter l'assistant.



Félicitations ! L'installation est maintenant terminée. Vous pouvez maintenant vous connecter à l'interface Web d'administration pour voir les résultats.

Affichage des résultats du test



A

Dépannage

Cette annexe propose des solutions aux problèmes susceptibles de se produire lors de l'installation et de l'utilisation du routeur. Les explications ci-dessous vous aideront à résoudre les problèmes que vous rencontrez. Si vous ne trouvez pas de réponse dans cette section, visitez le site Web de Cisco à l'adresse suivante : www.cisco.com.

Je dois définir une adresse IP statique sur un ordinateur.

Par défaut, le routeur, à l'aide du serveur DHCP qu'il contient, affecte des adresses IP comprises entre 192.168.1.100 et 192.168.1.149. Les adresses IP statiques que vous-même définissez doivent être comprises entre 192.168.1.2 et 192.168.1.99 ou entre 192.168.1.150 et 192.168.1.254. Chaque ordinateur ou périphérique réseau utilisant le protocole TCP/IP doit posséder une adresse unique afin de s'identifier sur ce réseau. Si son adresse IP n'est pas unique sur le réseau, Windows génère un message d'erreur indiquant un conflit d'adresses IP. Pour attribuer une adresse IP statique à un ordinateur, procédez comme suit :

Windows 2000

ÉTAPE 1 Cliquez sur **Démarrer**, **Paramètres** et **Panneau de configuration**. Cliquez deux fois sur **Connexions réseau et accès à distance**.

ÉTAPE 2 Cliquez à l'aide du bouton droit de la souris sur la **Connexion au réseau local** associée à l'adaptateur Ethernet que vous utilisez, puis sélectionnez **Propriétés**.

ÉTAPE 3 Dans la zone *Les composants sélectionnés sont utilisés par cette connexion*, sélectionnez **Protocole Internet (TCP/IP)**, puis cliquez sur **Propriétés**. Sélectionnez l'option **Utiliser l'adresse IP suivante**.

ÉTAPE 4 Saisissez une adresse IP unique qui n'est utilisée par aucun autre ordinateur du réseau connecté au routeur. Utilisez impérativement une adresse IP comprise entre 192.168.1.2 et 192.168.1.99 ou entre 192.168.1.151 et 192.168.1.254.

ÉTAPE 5 Saisissez le masque de sous-réseau **255.255.255.0**.

ÉTAPE 6 Indiquez la passerelle par défaut : **192.168.1.1** (adresse IP par défaut du routeur).

ÉTAPE 7 Sélectionnez **Utiliser l'adresse de serveur DNS suivante**, puis spécifiez le serveur DNS préféré et le serveur DNS auxiliaire (informations fournies par votre FAI). Contactez votre FAI ou consultez son site Web pour vous procurer ces informations.

ÉTAPE 8 Cliquez sur **OK** dans la fenêtre *Propriétés de Protocole Internet (TCP/IP)*, puis de nouveau sur **OK** dans la fenêtre *Propriétés de Connexion au réseau local*.

ÉTAPE 9 Redémarrez l'ordinateur si vous y êtes invité.

Windows XP

ÉTAPE 1 Cliquez sur **Démarrer**, puis sur **Panneau de configuration**.

ÉTAPE 2 Cliquez sur l'icône **Connexions réseau et Internet**, puis sur l'icône **Connexions réseau**.

ÉTAPE 3 Cliquez avec le bouton droit de la souris sur la **connexion au réseau local** associée à votre adaptateur Ethernet, puis cliquez sur **Propriétés**.

ÉTAPE 4 Dans la zone *Cette connexion utilise les éléments suivants*, sélectionnez **Protocole Internet (TCP/IP)**. Cliquez sur **Propriétés**.

ÉTAPE 5 Choisissez **Utiliser l'adresse IP suivante** et indiquez une adresse IP unique (non utilisée par un autre ordinateur sur le réseau connecté au routeur). Utilisez impérativement une adresse IP comprise entre 192.168.1.2 et 192.168.1.99 ou entre 192.168.1.151 et 192.168.1.254.

ÉTAPE 6 Saisissez le masque de sous-réseau **255.255.255.0**.

ÉTAPE 7 Indiquez la passerelle par défaut : **192.168.1.1** (adresse IP par défaut du routeur).

ÉTAPE 8 Sélectionnez **Utiliser l'adresse de serveur DNS suivante**, puis spécifiez le serveur DNS préféré et le serveur DNS auxiliaire (informations fournies par votre FAI). Contactez votre FAI ou consultez son site Web pour vous procurer ces informations.

ÉTAPE 9 Cliquez sur le bouton **OK** dans la fenêtre *Propriétés de Protocole Internet (TCP/IP)*. Cliquez sur le bouton **OK** dans la fenêtre *Propriétés de Connexion au réseau local*.

Je souhaite tester ma connexion Internet.

ÉTAPE 1 Vérifiez vos paramètres TCP/IP.

Windows 2000

a. Cliquez sur **Démarrer**, **Paramètres** et **Panneau de configuration**. Cliquez deux fois sur **Connexions réseau et accès à distance**.

b. Cliquez à l'aide du bouton droit de la souris sur la **Connexion au réseau local** associée à l'adaptateur Ethernet que vous utilisez, puis sélectionnez **Propriétés**.

c. Dans la zone *Les composants sélectionnés sont utilisés par cette connexion*, sélectionnez **Protocole Internet (TCP/IP)**, puis cliquez sur **Propriétés**. Vérifiez que les options **Obtenir une adresse IP automatiquement** et **Obtenir les adresses des serveurs DNS automatiquement** sont sélectionnées.

d. Cliquez sur **OK** dans la fenêtre *Propriétés de Protocole Internet (TCP/IP)*, puis de nouveau sur **OK** dans la fenêtre *Propriétés de Connexion au réseau local*.

e. Redémarrez l'ordinateur si vous y êtes invité.

Windows XP

Ces instructions sont données pour l'interface par défaut de Windows XP. Si vous utilisez l'interface Classique (où les icônes et les menus se présentent comme dans les versions précédentes de Windows), suivez les instructions fournies pour Windows 2000.

a. Cliquez sur **Démarrer**, puis sur **Panneau de configuration**.

b. Cliquez sur l'icône **Connexions réseau et Internet**, puis sur l'icône **Connexions réseau**.

c. Cliquez avec le bouton droit de la souris sur la **connexion au réseau local** associée à votre adaptateur Ethernet, puis cliquez sur **Propriétés**.

d. Dans la zone *Cette connexion utilise les éléments suivants*, sélectionnez **Protocole Internet (TCP/IP)** et cliquez sur **Propriétés**. Vérifiez que les options **Obtenir une adresse IP automatiquement** et **Obtenir les adresses des serveurs DNS automatiquement** sont sélectionnées.

ÉTAPE 2 Ouvrez une invite de commande.

a. Windows 98 et Millenium : cliquez sur **Démarrer**, puis sur **Exécuter**. Dans le champ *Ouvrir*, saisissez **command**. Appuyez sur **Entrée** ou cliquez sur **OK**.

b. Windows 2000 et XP : cliquez sur **Démarrer**, puis sur **Exécuter**. Dans le champ *Ouvrir*, saisissez **cmd**. Appuyez sur **Entrée** ou cliquez sur **OK**.

ÉTAPE 3 À l'invite de commande, tapez **ping 192.168.1.2** et appuyez sur **Entrée**.

- Si vous obtenez une réponse, cela signifie que l'ordinateur communique avec le routeur.
- Si vous n'obtenez PAS de réponse, vérifiez le câble et assurez-vous que l'option **Obtenir une adresse IP automatiquement** est sélectionnée dans les paramètres TCP/IP de votre adaptateur Ethernet.

ÉTAPE 4 À l'invite de commande, tapez **ping** suivi de votre adresse IP Internet, puis appuyez sur **Entrée**. L'adresse IP Internet apparaît désormais dans l'utilitaire de configuration du routeur. Par exemple, si votre adresse IP Internet est 1.2.3.4, vous devez saisir la commande **ping 1.2.3.4**, puis appuyer sur la touche **Entrée**.

- Si vous obtenez une réponse, cela signifie que l'ordinateur est connecté au routeur.
- Si vous n'obtenez PAS de réponse, essayez d'appliquer la commande ping à partir d'un autre ordinateur pour vérifier que l'ordinateur d'origine n'est pas la source du problème.

ÉTAPE 5 À l'invite de commande, tapez **ping www.cisco.com**, puis appuyez sur **Entrée**.

- Si vous obtenez une réponse, cela signifie que l'ordinateur est connecté à Internet. Si vous ne parvenez pas à ouvrir une page Web, exécutez la commande ping à partir d'un autre ordinateur pour vérifier que l'ordinateur d'origine n'est pas la source du problème.
- Si vous n'obtenez PAS de réponse, le problème est peut-être lié à la connexion. Essayez d'exécuter la commande ping sur un autre ordinateur pour vérifier que l'ordinateur d'origine n'est pas la source du problème.

Je n'obtiens aucune adresse IP sur Internet par le biais de ma connexion Internet.

ÉTAPE 1 Reportez-vous à la section **« Je souhaite tester ma connexion Internet. », page 119** ci-dessus pour vérifier votre connexion.

ÉTAPE 2 Si vous devez cloner l'adresse MAC de votre adaptateur Ethernet sur le routeur, reportez-vous à la section MAC Address Clone du **Chapitre 5, « Configuration du routeur »**.

ÉTAPE 3 Vérifiez que vous utilisez les paramètres Internet appropriés. Contactez votre FAI pour savoir si votre connexion Internet est de type DHCP, Adresse IP statique ou PPPoE (souvent adopté par les utilisateurs DSL). Pour obtenir plus d'informations sur les paramètres du type de connexion Internet, reportez-vous à la section sur la configuration de base du routeur du **Chapitre 5, « Configuration du routeur »**.

ÉTAPE 4 Vérifiez que vous utilisez le câble approprié. Assurez-vous que la DEL Internet est allumée et fixe.

ÉTAPE 5 Assurez-vous que le câble de votre modem câble ou DSL est connecté au port Internet du routeur. Vérifiez que la page Status de l'utilitaire de configuration du routeur indique une adresse IP valide fournie par votre FAI.

ÉTAPE 6 Mettez l'ordinateur, le routeur et le modem câble/DSL hors tension. Patientez 30 secondes, puis mettez le routeur, le modem câble/DSL et l'ordinateur sous tension. Vérifiez dans l'utilitaire de configuration du routeur (**System > Summary**) que vous obtenez une adresse IP.

Je ne parviens pas à accéder à la fenêtre Setup de l'utilitaire de configuration du routeur.

ÉTAPE 1 Pour vérifier que votre ordinateur est correctement connecté au routeur, reportez-vous à la section **« Je souhaite tester ma connexion Internet. », page 119**.

ÉTAPE 2 Vérifiez que votre ordinateur dispose d'une adresse IP, d'un masque de sous-réseau, d'une passerelle et d'un DNS.

ÉTAPE 3 Définissez une adresse IP statique sur votre système ; reportez-vous à la section **« Je dois définir une adresse IP statique sur un ordinateur. », page 117** ci-dessus.

ÉTAPE 4 Reportez-vous à la section **« Je dois supprimer les paramètres de proxy ou la fenêtre de connexion à distance (pour les utilisateurs PPPoE). », page 125**.

Je ne parviens pas à faire fonctionner mon réseau privé virtuel (VPN) via le routeur.

Accédez à l'interface Web du routeur en spécifiant **http://192.168.1.1** ou l'adresse IP du routeur, puis choisissez **VPN > VPN Pass Through**. Vérifiez que les options IPSec passthrough et/ou PPTP passthrough sont activées.

Les VPN qui utilisent l'authentification IPSec et le protocole ESP (Encapsulation Security Payload, également appelé protocole 50) fonctionnent correctement. Au moins une session IPSec fonctionne via le routeur ; toutefois, des sessions IPSec simultanées sont possibles, en fonction des spécificités de vos VPN.

Les réseaux VPN qui utilisent IPSec et le protocole AH (Authentication Header, également appelé protocole 51) sont incompatibles avec le routeur. AH est parfois limité par des incompatibilités avec la norme NAT.

Modifiez l'adresse IP du routeur en indiquant un autre sous-réseau, afin d'éviter tout conflit entre l'adresse IP VPN et votre adresse IP locale. Par exemple, si votre serveur VPN attribue l'adresse IP 192.168.1.X (X étant un chiffre compris entre 1 et 254) et que votre adresse IP LAN locale est 192.168.1.X (X étant le même chiffre que celui utilisé dans l'adresse IP VPN), le routeur aura des difficultés à acheminer les informations vers la bonne destination. Si vous modifiez l'adresse IP du routeur en lui affectant l'adresse 192.168.2.1, le problème devrait être résolu. Modifiez l'adresse IP du routeur via le menu Setup de l'utilitaire de configuration. Si vous avez attribué une adresse IP statique à un ordinateur ou périphérique du réseau, vous devez remplacer son adresse IP par 192.168.2.*Y* (*Y* étant un chiffre compris entre 1 et 254). Veuillez noter que chaque adresse IP doit être unique sur le réseau.

Votre VPN peut exiger que les paquets du port 500/UDP soient envoyés à l'ordinateur connecté au serveur IPSec.

Pour obtenir plus d'informations, visitez le site Web de Cisco à l'adresse suivante : www.cisco.com.

J'ai besoin de configurer un serveur derrière mon routeur.

Pour utiliser un serveur en tant que serveur de messagerie, serveur Web ou FTP, vous devez connaître les numéros de port utilisés. Par exemple, le port 80 (HTTP) est utilisé pour le Web, le port 21 (FTP) pour le FTP et les ports 25 (SMTP sortant) et 110 (POP3 entrant) pour le serveur de messagerie. Pour obtenir plus d'informations, reportez-vous à la documentation fournie avec le serveur que vous avez installé. Pour configurer le transfert de port via l'utilitaire de configuration du routeur, procédez comme suit. Vous devrez configurer le serveur Web, le serveur ftp et le serveur de messagerie.

ÉTAPE 1 Accédez à l'utilitaire de configuration du routeur en spécifiant **http://192.168.1.1** ou l'adresse IP du routeur. Choisissez **Firewall > Single Port Forwarding**.

ÉTAPE 2 Sélectionnez le service dans la colonne *Application*.

ÉTAPE 3 Entrez l'adresse IP du serveur auquel les utilisateurs d'Internet doivent accéder. Par exemple, si l'adresse IP de l'adaptateur Ethernet du serveur Web est 192.168.1.100, saisissez 100 dans le champ. Cochez ensuite la case Enable pour l'entrée saisie. Examinez les exemples suivants :

Application	Début et fin	Protocole	Adresse IP	Activé
HTTP	80 à 80	Les deux	192.168.1.100	X
FTP	21 à 21	TCP	192.168.1.101	X
SMTP (sortant)	25 à 25	Les deux	192.168.1.102	X
POP3 (entrant)	110 à 110	Les deux	192.168.1.102	X

ÉTAPE4 Configurez autant d'entrées que nécessaire.

ÉTAPE 5 Une fois la configuration terminée, cliquez sur **Save**.

Je dois configurer une solution d'hébergement de jeux en ligne ou utiliser d'autres applications Internet.

Si vous souhaitez jouer à des jeux en ligne ou utiliser des applications Internet, sachez que la plupart fonctionneront sans qu'il ne soit nécessaire de réaliser un transfert de port ou un hébergement DMZ. Mais il se peut que vous souhaitiez héberger un jeu en ligne ou une application Internet. Dans ce cas, vous devrez configurer le routeur de sorte qu'il transmette les données ou les paquets entrants à un ordinateur spécifique. Cela s'applique également aux applications Internet que vous utilisez. Pour connaître les services de ports à utiliser, le plus simple est de consulter le site Web du jeu en ligne ou de l'application que vous souhaitez utiliser. Pour configurer l'hébergement d'un jeu en ligne ou utiliser une application Internet spécifique, procédez comme suit :

ÉTAPE 1 Accédez à l'utilitaire de configuration du routeur en spécifiant **http://192.168.1.1** ou l'adresse IP du routeur. Choisissez **Firewall > Single Port Forwarding**.

ÉTAPE 2 Sélectionnez le service dans la colonne *Application*.

ÉTAPE 3 Entrez l'adresse IP du serveur auquel les utilisateurs d'Internet doivent accéder. Par exemple, si l'adresse IP de l'adaptateur Ethernet du serveur Web est 192.168.1.100, saisissez 100 dans le champ. Cochez ensuite la case **Enable** pour l'entrée saisie. Examinez les exemples suivants :

Application	Début et fin	Protocole	Adresse IP	Activé
UT	7 777 à 27 900	Les deux	192.168.1.100	X
Halflife	27 015 à 27 015	Les deux	192.168.1.105	X
PC Anywhere	5 631 à 5 631	UDP	192.168.1.102	X
VPN IPSEC	500 à 500	UDP	192.168.1.100	X

ÉTAPE 4 Configurez autant d'entrées que nécessaire.

ÉTAPE 5 Une fois la configuration terminée, cliquez sur **Save**.

Je ne parviens pas à faire fonctionner correctement un jeu Internet, un serveur ou une application.

Si vous rencontrez des difficultés pour faire fonctionner correctement un jeu Internet, un serveur ou une application, utilisez une zone d'hébergement DMZ (DeMilitarized Zone : zone démilitarisée) afin d'exposer votre ordinateur à Internet. Cette option est utile lorsqu'une application requiert un nombre de ports trop important ou lorsque vous ne savez pas quels services de ports utiliser. Assurez-vous que toutes les entrées de transfert sont désactivées si vous souhaitez utiliser l'hébergement DMZ. Le transfert a en effet priorité sur l'hébergement DMZ. En d'autres termes, les données qui parviennent au routeur sont d'abord vérifiées par les paramètres de transfert. Si le numéro du port d'entrée des données n'est pas soumis au transfert de port, le routeur transmet alors les données à l'ordinateur ou au périphérique réseau défini pour l'hébergement DMZ.

ÉTAPE 1 Accédez à l'utilitaire de configuration du routeur en spécifiant **http://192.168.1.1** ou l'adresse IP du routeur. Choisissez **Firewall > Single Port Forwarding**.

ÉTAPE 2 Désactivez les entrées que vous avez saisies pour le transfert.

ÉTAPE 3 Choisissez **Setup > DMZ**.

ÉTAPE 4 Entrez l'adresse IP de l'adaptateur Ethernet de l'ordinateur à exposer à Internet. Cela permet à cet ordinateur d'ignorer la sécurité NAT.

ÉTAPE 5 Sélectionnez **Enable** pour activer l'hébergement DMZ.

ÉTAPE 6 Une fois la configuration terminée, cliquez sur **Save**.

J'ai oublié mon mot de passe ou l'invite de mot de passe s'affiche systématiquement lors de l'enregistrement des paramètres du routeur.

Rétablissez les valeurs par défaut du routeur : pour cela, appuyez sur le bouton RESET pendant dix secondes, puis relâchez-le. Si le système vous demande toujours votre mot de passe lors de l'enregistrement des paramètres, procédez comme suit :

ÉTAPE 1 Accédez à l'interface Web du routeur en spécifiant http://192.168.1.1 ou l'adresse IP du routeur.

ÉTAPE 2 Pour vous connecter, indiquez le mot de passe par défaut : **admin**.

ÉTAPE 3 Dans l'arborescence, cliquez sur **Administration > Management**.

ÉTAPE 4 Indiquez un nouveau mot de passe dans le champ **Router Password**.

ÉTAPE 5 Confirmez le nouveau mot de passe dans le champ **Re-enter to Confirm**.

ÉTAPE 6 Cliquez sur **Save**.

Je dois supprimer les paramètres de proxy ou la fenêtre de connexion à distance (pour les utilisateurs PPPoE).

Si vous disposez de paramètres de proxy, vous devez les désactiver sur votre ordinateur. Le routeur servant de passerelle pour la connexion Internet, l'ordinateur n'a pas besoin des paramètres de proxy pour accéder à Internet. Pour vérifier que les paramètres de proxy sont désactivés et que le navigateur que vous utilisez est défini pour une connexion directe au réseau local (LAN), procédez comme suit :

Dans Internet Explorer, cliquez sur **Outils**, **Options Internet**, puis sur l'onglet **Connexions**. Vérifiez que l'option **Ne jamais établir de connexion** est activée. Dans Netscape Navigator, cliquez sur **Edition** > **Préférences** > **Avancé** > **Proxies**. Vérifiez que l'option **Connexion directe à Internet** est activée. Pour obtenir plus d'informations, reportez-vous à la documentation de votre navigateur.

Pour recommencer, je dois rétablir les paramètres d'usine par défaut du routeur.

Maintenez le bouton RESET enfoncé pendant 30 secondes, puis relâchez-le. Les valeurs définies par défaut en usine pour le mot de passe, le transfert et d'autres paramètres sont rétablies. En d'autres termes, le routeur revient à sa configuration initiale.

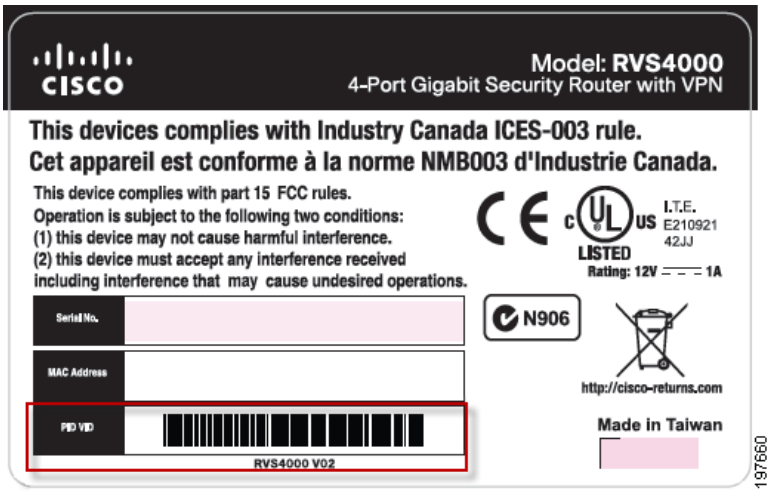
Je dois mettre le micrologiciel à niveau.

Suivez les instructions indiquées à la section **Administration > Firmware Upgrade, page 82**.

La mise à niveau du micrologiciel a échoué.

La mise à niveau peut avoir échoué pour diverses raisons. Vous pouvez tenter à nouveau l'opération en suivant les instructions indiquées à la section **Administration > Firmware Upgrade, page 82**. Vous pouvez également, si vous disposez d'un équipement de version 1, utiliser la procédure « de secours » ci-dessous.

REMARQUE Pour déterminer la version de votre matériel, consultez le code PIDVID indiqué sur l'étiquette située sous le routeur.



ÉTAPE 1 Si votre routeur est de version matérielle 1, rendez-vous à l'adresse suivante : www.cisco.com/go/software.

ÉTAPE 2 Dans la zone de recherche, indiquez : **RVS4000**

ÉTAPE 3 Dans les résultats de la recherche, choisissez Download Software for Cisco RVS4000 4-port Gigabit Security Router - VPN.

Lorsque vous y êtes invité, indiquez votre nom d'utilisateur et votre mot de passe Cisco.com. Si vous ne disposez pas d'informations de connexion sur Cisco.com, vous pouvez vous inscrire en tant que nouvel utilisateur.

ÉTAPE 4 Cliquez sur le lien **Router Firmware Rescue Utility**.

ÉTAPE 5 Enregistrez le fichier zip sur votre ordinateur.

ÉTAPE 6 Extrayez le fichier **setup.exe** du fichier zip, puis lancez **setup.exe** pour installer l'utilitaire sur votre ordinateur.

ÉTAPE 7 Débranchez les câbles réseau de **tous** les ports LAN et WAN du routeur, **à l'exception** du câble réseau connecté à l'ordinateur sur lequel l'utilitaire de mise à niveau du micrologiciel est installé.

ÉTAPE8 Double-cliquez sur l'icône **RVS4000 Upgrade Utility** se trouvant sur votre bureau ou lancez l'utilitaire en choisissant **Démarrer > Tous les programmes > Cisco Small Business RVS4000**.

ÉTAPE 9 Suivez les instructions indiquées à l'écran pour procéder à la mise à niveau.

Le protocole PPPoE de mon service DSL se déconnecte sans cesse.

En réalité, PPPoE n'est pas une connexion dédiée ou permanente. Certains FAI DSL déconnectent le service après une période d'inactivité, comme c'est le cas pour une connexion à Internet via la ligne téléphonique. Une option de configuration permet de maintenir la connexion. Si cela ne fonctionne pas, vous devrez régulièrement rétablir la connexion.

ÉTAPE 1 Pour vous connecter au routeur, ouvrez votre navigateur Web, puis saisissez **http://192.168.1.1** ou l'adresse IP du routeur.

ÉTAPE 2 Indiquez le mot de passe s'il vous est demandé (le mot de passe par défaut est **admin**).

ÉTAPE 3 Dans le menu **Setup > WAN**, sélectionnez l'option **Keep Alive** et paramétrez *Redial Period* sur **20** (secondes).

ÉTAPE 4 Cliquez sur **Save**.

Si la connexion est à nouveau interrompue, effectuez les étapes 1 à 2 pour la rétablir.

Je ne parviens pas à accéder à mon courrier électronique, à Internet ou à mon VPN, ou je reçois des données corrompues d'Internet.

Il se peut que le paramètre Maximum Transmission Unit (MTU) doive être ajusté. Par défaut, ce paramètre est fixé à 1500. Pour la plupart des utilisateurs DSL, il est fortement recommandé d'utiliser une valeur MTU de 1492. En cas de difficultés, procédez comme suit :

ÉTAPE 1 Pour vous connecter au routeur, ouvrez votre navigateur Web, puis saisissez **http://192.168.1.1** ou l'adresse IP du routeur.

ÉTAPE 2 Indiquez le mot de passe s'il vous est demandé (le mot de passe par défaut est **admin**).

ÉTAPE 3 Accédez au menu **Setup > WAN**.

ÉTAPE 4 Trouvez l'option MTU, puis sélectionnez **Manual**. Dans le champ *Size*, saisissez **1 492**.

ÉTAPE5 Cliquez sur **Save** pour poursuivre.

ÉTAPE6 Si vous rencontrez toujours des difficultés, essayez différentes valeurs de taille. Essayez les valeurs de la liste suivante (une valeur à la fois et dans l'ordre indiqué) jusqu'à ce que le problème soit résolu :

1 462
1 400
1 362
1 300

J'ai besoin d'utiliser le déclenchement de port.

La fonction de déclenchement de port examine les services de port sortants utilisés et déclenche l'ouverture d'un port spécifique par le routeur, en fonction du port utilisé par une application Internet. Procédez comme suit :

ÉTAPE 1 Pour vous connecter au routeur, ouvrez votre navigateur Web, puis saisissez **http://192.168.1.1** ou l'adresse IP du routeur.

ÉTAPE 2 Indiquez le mot de passe s'il vous est demandé (le mot de passe par défaut est **admin**).

ÉTAPE 3 Cliquez sur **Firewall > Port Range Triggering**.

ÉTAPE 4 Saisissez le nom que vous souhaitez donner à l'application dans le champ Application Name.

ÉTAPE 5 Entrez les ports de début et de fin de la plage de ports déclenchée. Si nécessaire, demandez à votre fournisseur d'accès Internet des informations sur les services de port sortants utilisés.

ÉTAPE 6 Entrez les ports de début et de fin de la plage de ports transférée. Si nécessaire, demandez à votre fournisseur d'accès Internet des informations sur les services de port entrants requis par l'application Internet.

ÉTAPE 7 Cochez la case **Enabled** pour l'entrée saisie.

ÉTAPE 8 Une fois la configuration terminée, cliquez sur **Save**.

Lorsque je spécifie une adresse URL ou IP, j'obtiens une erreur liée à l'expiration du délai et je suis invité à recommencer.

- Utilisez d'autres ordinateurs pour vérifier que le problème n'est pas lié à l'ordinateur utilisé. Si les autres ordinateurs fonctionnent correctement, assurez-vous que les paramètres IP de votre station de travail sont corrects (adresse IP, masque de sous-réseau, modem routeur par défaut et adresse DNS). Redémarrez l'ordinateur présentant un problème.
- Si les ordinateurs sont correctement configurés, mais ne fonctionnent toujours pas, vérifiez le routeur. Vérifiez qu'il est connecté et sous tension. Connectez-vous au routeur et vérifiez ses paramètres. Si vous ne parvenez pas à établir la connexion, vérifiez le réseau local (LAN) et la connexion de l'alimentation.
- Si le routeur est configuré correctement, vérifiez le fonctionnement de votre connexion Internet (modem câble/DSL, etc.). Vous pouvez passer outre le routeur pour vérifier la connexion directe.
- Configurez manuellement le protocole TCP/IP à l'aide d'une adresse DNS fournie par votre FAI.

- Assurez-vous que le navigateur est configuré pour une connexion directe et que les connexions à distance sont désactivées. Dans Internet Explorer, cliquez sur **Outils**, **Options Internet**, puis sur l'onglet **Connexions**. Vérifiez que la case **Ne jamais établir de connexion** est cochée. Dans Netscape Navigator, cliquez sur **Edition**, **Préférences**, **Avancé** et **Proxies**. Vérifiez que l'option **Connexion directe à Internet** est activée.

J'essaie d'accéder à l'utilitaire de configuration du routeur, mais je ne vois pas apparaître la fenêtre de connexion. C'est le message « 404 Interdit » qui s'affiche.

Si vous utilisez Internet Explorer, suivez la procédure ci-après jusqu'à voir apparaître la fenêtre de connexion de l'utilitaire de configuration (la démarche est similaire avec Netscape Navigator) :

ÉTAPE 1 Cliquez sur **Fichier**. Assurez-vous que l'option **Travailler hors connexion** n'est PAS activée.

ÉTAPE 2 Appuyez sur **CTRL + F5**. Ce type d'actualisation forcée contraint Internet Explorer à charger les nouvelles pages Web et non les pages mises en cache.

ÉTAPE 3 Cliquez sur **Outils**. Cliquez sur **Options Internet**. Cliquez sur l'onglet **Sécurité**. Cliquez sur le bouton **Niveau par défaut**. Assurez-vous que le niveau de sécurité choisi est Moyen ou inférieur. Cliquez sur le bouton **OK**.

Un tunnel QuickVPN est connecté à mon RVS4000 mais je ne parviens pas à voir les ordinateurs du réseau distant avec Internet Explorer.

Les tunnels QuickVPN ne prennent pas en charge la diffusion NetBIOS. Pour accéder aux ordinateurs ou aux lecteurs partagés sur le réseau distant, il est recommandé d'utiliser l'adresse IP pour identifier la ressource.

Je dispose d'un tunnel VPN IPSec passerelle à passerelle connecté entre deux routeurs RVS4000. Les utilisateurs de chacun des réseaux ne parviennent pas à voir les ordinateurs du réseau distant avec Internet Explorer.

Le routeur RVS4000 prend en charge la diffusion NetBIOS via un tunnel VPN IPSec passerelle à passerelle. L'administrateur doit néanmoins activer cette fonctionnalité dans la section Advanced de la fenêtre *VPN > IPSec VPN*.

Foire aux questions

Quel est le nombre maximal d'adresses IP prises en charge par le routeur ?

Le routeur peut prendre en charge jusqu'à 253 adresses IP.

La fonctionnalité d'intercommunication IPSec est-elle prise en charge par le routeur ?

Oui, activez-la ou désactivez-la dans l'onglet *VPN > VPN Pass Through*.

Où le routeur est-il installé sur le réseau ?

Dans un environnement standard, le routeur est installé entre le modem câble/DSL et le réseau local (LAN). Connectez le routeur au port ETHERNET du modem câble/DSL.

Le routeur prend-il en charge les protocoles IPX ou AppleTalk ?

Non. TCP/IP est le seul protocole standard pour Internet et est devenu la norme internationale de communication. Les protocoles IPX (protocole de communication NetWare utilisé uniquement pour acheminer des messages d'un nœud à un autre) et AppleTalk (protocole de communication utilisé sur les réseaux Apple et Macintosh) peuvent être adoptés pour des connexions de LAN à LAN, mais ne peuvent être utilisés pour relier Internet à un LAN.

Qu'est-ce que la technologie NAT (Network Address Translation) et quelle est sa fonction ?

La technologie NAT (Network Address Translation) permet de convertir plusieurs adresses IP d'un réseau local privé en une adresse IP publique diffusée sur Internet. Cela renforce la sécurité car l'adresse d'un ordinateur connecté au réseau local (LAN) privé n'est jamais transmise sur Internet. Qui plus est, la technologie NAT permet d'utiliser le routeur via des comptes Internet bon marché, notamment des modems câble ou DSL, lorsque vous disposez d'une seule adresse TCP/IP fournie par votre FAI. L'utilisateur peut disposer de plusieurs adresses privées derrière cette adresse unique fournie par le FAI.

Le routeur prend-il en charge d'autres systèmes d'exploitation que Windows 98, Windows Millenium, Windows 2000 et Windows XP ?

Oui, mais Cisco ne propose à l'heure actuelle aucun service de support technique couvrant l'installation, la configuration et le dépannage de ces systèmes d'exploitation.

Le routeur prend-il en charge l'envoi de fichier avec ICQ ?

Oui. Toutefois, vous devrez peut-être modifier les paramètres de connexion ICQ si votre ordinateur se trouve derrière un pare-feu. Pour obtenir plus d'instructions, reportez-vous à la documentation sur ICQ ou au site d'assistance en ligne.

J'ai configuré un serveur Unreal Tournament (UT), mais les autres utilisateurs du LAN ne peuvent pas y accéder. Que dois-je faire ?

Si vous avez configuré un serveur Unreal Tournament, vous devez créer une adresse IP statique pour chaque ordinateur du réseau local et transférer les ports 7777, 7778, 7779, 7780, 7781 et 27900 vers l'adresse IP du serveur. Vous pouvez également utiliser une plage de transfert des ports 7777 à 27900. Si vous souhaitez utiliser l'UT Server Admin, transférez un autre port (le port 8080 fonctionne bien en général mais sert à l'administration à distance ; il se peut que vous deviez le désactiver) puis, dans la section [UWeb.WebServer] du fichier server.ini, paramétrez ListenPort sur 8080 (doit correspondre au port mappé ci-dessus) et ServerName sur l'IP attribuée au routeur par votre FAI.

Plusieurs joueurs sur le LAN peuvent-ils accéder à un même serveur de jeux et jouer simultanément par le biais d'une seule et même adresse IP publique ?

Cela dépend du jeu en réseau ou du serveur de jeux que vous utilisez. Par exemple, Unreal Tournament prend en charge les connexions multiples avec une seule adresse IP publique.

Comment puis-je faire fonctionner le jeu *Half-Life: Team Fortress* avec le routeur ?

Le port client par défaut pour Half-Life est 27005. La mention « +clientport 2700x » doit être ajoutée à la ligne de commande de raccourci HL sur les ordinateurs de votre LAN, x correspondant à 6, 7, 8 et ainsi de suite. Plusieurs ordinateurs peuvent ainsi être connectés au même serveur. Problème : la version 1.0.1.6 ne permet pas à plusieurs ordinateurs dotés d'une même clé CD de se connecter simultanément, même s'il s'agit du même LAN (ce qui n'est pas le cas avec la version 1.0.1.3). En matière d'hébergement de jeux, il n'est pas nécessaire que le serveur HL soit dans la zone démilitarisée (DMZ). Transférez simplement le port 27015 vers l'adresse IP locale du serveur.

Comment bloquer des éléments endommagés téléchargés depuis un site FTP ?

Si vous importez des fichiers endommagés lors du téléchargement d'un composant via votre client FTP, essayez d'utiliser un autre programme FTP.

La page Web se bloque, les fichiers téléchargés sont endommagés et des caractères illisibles apparaissent à l'écran. Que dois-je faire ?

Modifiez les propriétés de votre adaptateur Ethernet : remplacez le mode Auto Detect par 10 Mbps/Half Duplex.

ÉTAPE 1 Sur un ordinateur Windows, cliquez sur **Démarrer**, **Panneau de configuration**, puis **Système**.

ÉTAPE 2 **Cliquez sur l'onglet Matériel**, puis cliquez sur Gestionnaire de périphériques.

ÉTAPE 3 Cliquez sur le signe plus placé à côté de la mention **Cartes réseau** pour développer la liste des cartes.

ÉTAPE 4 Cliquez avec le bouton droit de la souris sur votre carte de réseau, puis cliquez sur **Propriétés**.

ÉTAPE 5 Cliquez sur l'onglet **Avancé**.

ÉTAPE 6 Dans la liste **Propriété**, cliquez sur **Link Speed/Duplex mode**. Dans la liste **Valeur**, choisissez **10 Mbps/Half Duplex**.

ÉTAPE 7 Assurez-vous que votre paramètre de proxy est désactivé dans le navigateur.

Dans Internet Explorer, cliquez sur **Outils**, **Options Internet**, puis sur l'onglet **Connexions**. Vérifiez que la case **Ne jamais établir de connexion** est cochée. Dans Netscape Navigator, cliquez sur **Edition** > **Préférences** > **Avancé** > **Proxies**. Vérifiez que l'option **Connexion directe à Internet** est activée. Pour obtenir plus d'informations, reportez-vous à la documentation de votre navigateur.

Si tout le reste échoue au cours de l'installation, que puis-je faire ?

Réinitialisez le routeur en maintenant le bouton RESET enfoncé pendant dix secondes. Réinitialisez votre modem câble ou DSL en le mettant hors tension, puis sous tension. Téléchargez et installez la dernière version du micrologiciel disponible sur le site Web de Cisco, à l'adresse suivante : www.cisco.com.

Comment être informé de la disponibilité des nouvelles mises à niveau du micrologiciel du routeur ?

Toutes les mises à niveau des micrologiciels Cisco sont mises à disposition sur www.cisco.com, où vous pouvez les télécharger gratuitement. Le micrologiciel du routeur peut être mis à niveau à l'aide de l'utilitaire de configuration. Si la connexion Internet du routeur fonctionne correctement, il est inutile de télécharger une version plus récente du micrologiciel, à moins que cette version ne contienne des nouvelles fonctionnalités que vous souhaitez utiliser. Le téléchargement d'une

version plus récente du micrologiciel du routeur n'améliore pas la qualité ou la vitesse de votre connexion Internet et risque de nuire à sa stabilité actuelle.

Le routeur fonctionne-t-il dans un environnement Macintosh ?

Oui, mais vous ne pouvez accéder aux pages de configuration du routeur qu'à partir des versions Internet Explorer 5.0 ou Netscape Navigator 5.0 (ou supérieures) pour Macintosh.

Je ne parviens pas à afficher l'écran de configuration Web du routeur. Que puis-je faire ?

Vous devrez peut-être supprimer les paramètres proxy dans votre navigateur Internet. Vous pouvez également supprimer les paramètres de connexion à distance de votre navigateur. Consultez la documentation relative à votre navigateur. Assurez-vous que le navigateur est configuré pour une connexion directe et que les connexions à distance sont désactivées. Dans Internet Explorer, cliquez sur **Outils**, **Options Internet**, puis sur l'onglet **Connexions**. Vérifiez que la case **Ne jamais établir de connexion** est cochée. Dans Netscape Navigator, cliquez sur **Edition** > **Préférences** > **Avancé** > **Proxies**. Vérifiez que l'option **Connexion directe à Internet** est activée.

Qu'est-ce que l'hébergement DMZ ?

Une zone démilitarisée (DeMilitarized Zone) permet à une adresse IP (ordinateur) d'être visible sur Internet. Certaines applications nécessitent l'ouverture de plusieurs ports TCP/IP. Il est recommandé de configurer votre ordinateur avec une adresse IP statique si vous souhaitez utiliser l'hébergement DMZ.

Si l'hébergement DMZ est utilisé, l'utilisateur exposé partage-t-il l'adresse IP publique avec le routeur ?

Non.

Est-ce que le routeur transmet les paquets PPTP ou achemine de manière directe les sessions PPTP ?

Le routeur permet la transmission des paquets PPTP.

Le routeur est-il compatible avec différentes plates-formes ?

Toute plate-forme prenant en charge Ethernet et TCP/IP est compatible avec le routeur.

Combien de ports est-il possible de transférer simultanément ?

En théorie, le routeur peut établir jusqu'à 2 048 sessions simultanées, mais vous pouvez transférer seulement 30 plages de ports.

Le routeur peut-il remplacer un modem ? Le routeur contient-il un modem câble ou DSL ?

Non, cette version du routeur doit fonctionner en association avec un modem câble ou DSL.

Quels sont les modems compatibles avec le routeur ?

Le routeur est compatible avec la quasi-totalité des modems câble ou DSL prenant en charge Ethernet.

Comment puis-je savoir si je dispose d'une adresse IP statique ou DHCP ?

Pour le savoir, contactez votre FAI.

Comment utiliser le logiciel mIRC avec le routeur ?

Dans le menu **Firewall > SIngle Port Forwarding**, donnez la valeur 113 au transfert de port pour l'ordinateur sur lequel vous utilisez mIRC.

B

Utilisation de Cisco QuickVPN pour Windows 2000, XP ou Vista

Présentation

Cette annexe explique comment installer et utiliser le logiciel Cisco QuickVPN téléchargeable sur le site www.cisco.com. QuickVPN fonctionne sur les ordinateurs équipés de Windows 2000, XP, Vista ou Windows 7. (Les ordinateurs exécutant d'autres systèmes d'exploitation doivent utiliser des logiciels VPN tiers.) La version 1.2.5 ou ultérieure de QuickVPN Client est requise sous Windows Vista. Windows 7 requiert la version 1.4.0.5 ou ultérieure.

Cette annexe comprend les sections suivantes :

Avant de commencer

Le logiciel QuickVPN fonctionne uniquement avec un routeur de sécurité Cisco Gigabit 4 ports avec VPN configuré de manière à accepter une connexion QuickVPN. Pour configurer les paramètres de client VPN du routeur, procédez comme suit :

ÉTAPE 1 Cliquez sur **VPN > VPN Client Accounts**.

ÉTAPE 2 Saisissez le nom d'utilisateur dans le champ *Username*.

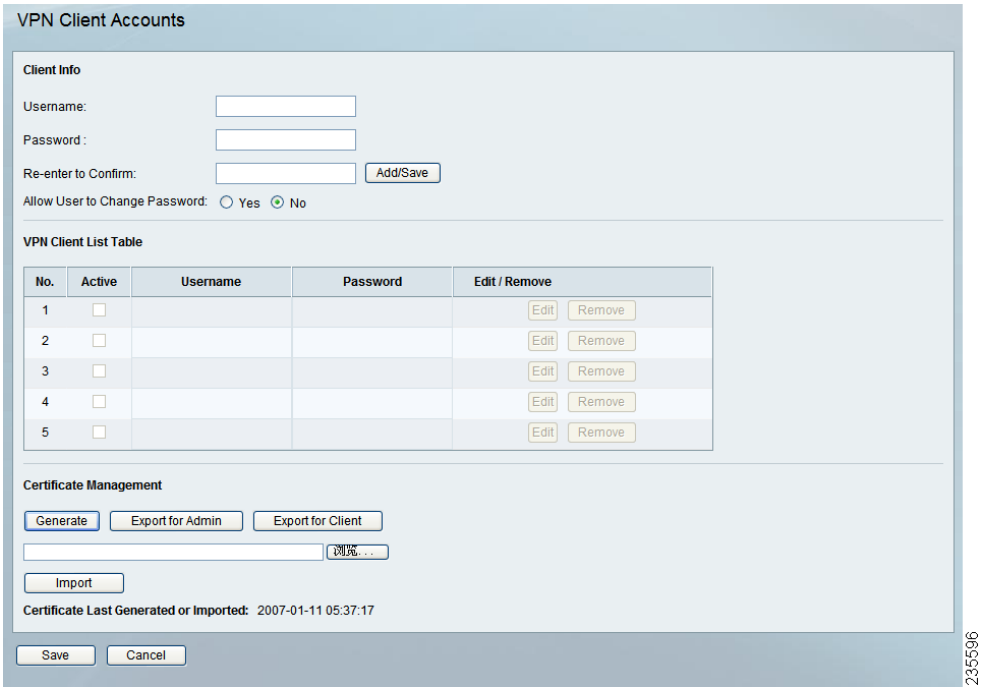
ÉTAPE 3 Saisissez une première fois le mot de passe dans le champ *Password*, puis une seconde fois dans le champ *Re-enter to confirm*.

ÉTAPE 4 Cliquez sur **Add/Save**.

ÉTAPE 5 Cochez la case d'option **Active** pour le client VPN n° 1.

ÉTAPE 6 Cliquez sur **Save**.

Fenêtre VPN Client Accounts



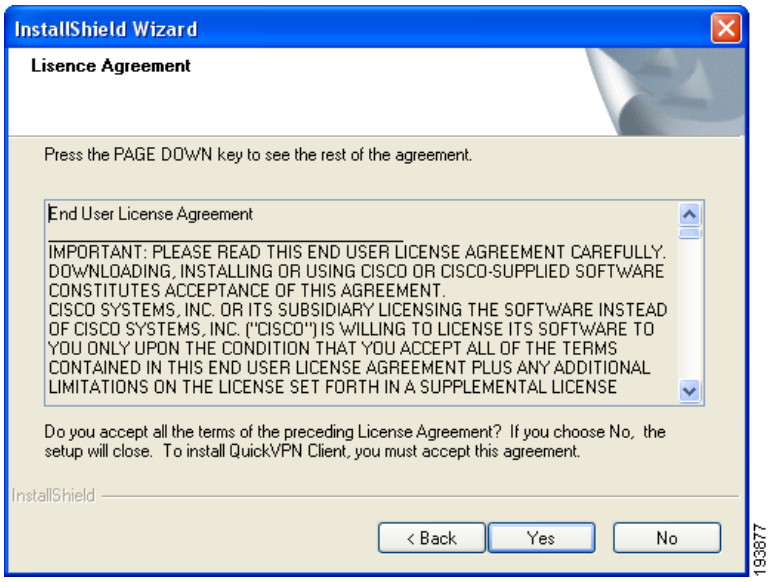
Installation du logiciel Cisco QuickVPN

Installation à partir du CD-ROM

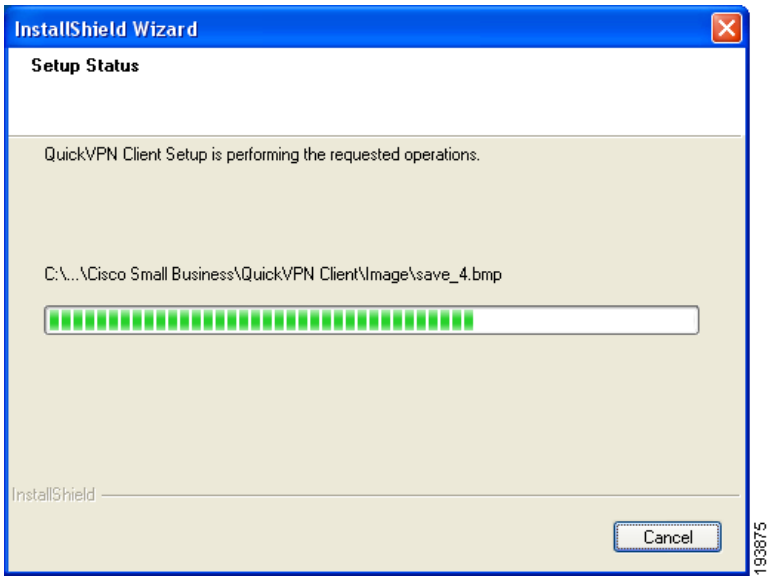
ÉTAPE 1 Insérez le CD-ROM RVS4000 dans le lecteur de CD-ROM. Dans le menu **Start**, cliquez sur **Run**. Dans le champ prévu à cet effet, entrez **D:\VPN_Client.exe** (si **D**·est la lettre du lecteur de CD-ROM).

ÉTAPE 2 La fenêtre contenant l'accord de licence s'affiche. Cliquez sur **Yes** pour accepter le contrat. Les fichiers appropriés sont alors copiés sur votre ordinateur.

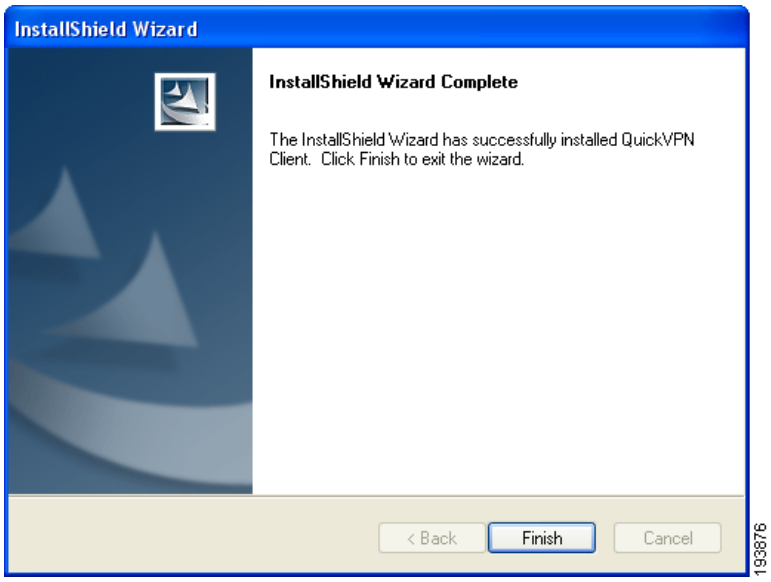
Contrat de licence



Copie des fichiers



Installation des fichiers terminée



ÉTAPE 3 Cliquez sur **Finished** pour terminer l'installation. Passez à la section, **« Utilisation du logiciel Cisco QuickVPN », page 140**.

Téléchargement et installation à partir d'Internet

ÉTAPE 1 Suivez le lien de téléchargement de microprogrammes indiqué à l'**Annexe F, « Pour en savoir plus ».**

ÉTAPE 2 Sur la page accessible via ce lien, cliquez sur **Download Software**.

ÉTAPE 3 Dans le menu, sélectionnez **Cisco Small Business Routers > RVS4000**.

ÉTAPE 4 Sélectionnez **QuickVPN Utility**.

ÉTAPE 5 Enregistrez le fichier zip sur votre ordinateur, puis extrayez le fichier .exe.

ÉTAPE 6 Double-cliquez sur le fichier .exe et suivez les instructions affichées à l'écran. Passez à la section suivante, **« Utilisation du logiciel Cisco QuickVPN », page 140**.

Utilisation du logiciel Cisco QuickVPN

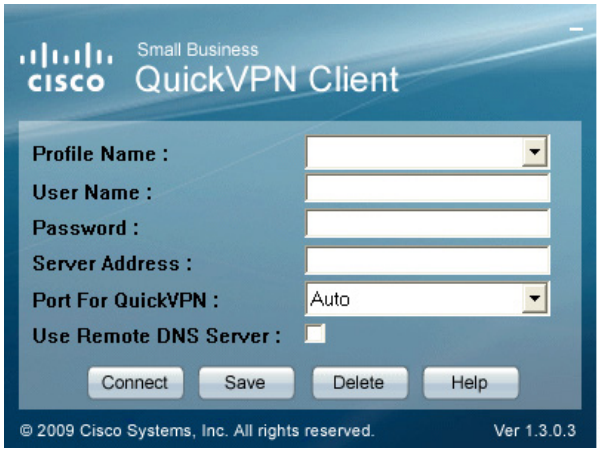
ÉTAPE 1 Double-cliquez sur l'icône du logiciel Cisco QuickVPN, sur votre bureau ou dans la barre d'état système.

QuickVPN Desktop Icon

QuickVPN Tray Icon—
No Connection

ÉTAPE 2 La fenêtre de connexion QuickVPN s'affiche. Dans le champ *Profile Name*, saisissez un nom pour votre profil. Dans les champs *User Name* et *Password*, saisissez le nom d'utilisateur et le mot de passe qui vous ont été attribués. Dans le champ *Server Address*, saisissez l'adresse IP ou le nom de domaine du routeur de sécurité Cisco Gigabit 4 ports avec VPN. Dans le champ *Port For QuickVPN*, saisissez le numéro de port que le client QuickVPN utilisera pour communiquer avec le routeur VPN distant ou conservez la valeur par défaut **Auto**.

Connexion QuickVPN



Pour enregistrer ce profil, cliquez sur **Save**. (Si vous devez créer un tunnel vers plusieurs sites, vous pouvez créer plusieurs profils ; notez cependant qu'un seul tunnel peut être actif à la fois.) Pour supprimer ce profil, cliquez sur **Delete**. Pour obtenir des informations, cliquez sur **Help**.

ÉTAPE 3 Pour établir la connexion QuickVPN, cliquez sur **Connect**. La progression de la connexion est affichée : *connexion*, *provisionnement*, *activation de la stratégie* et *vérification du réseau*.

ÉTAPE 4 Une fois que la connexion QuickVPN est établie, l'icône de la barre QuickVPN devient verte et la fenêtre d'état du QuickVPN s'affiche. La fenêtre comprend l'adresse IP de l'extrémité distante du tunnel VPN, la date et l'heure de l'établissement du tunnel VPN, ainsi que la durée totale d'activité de ce dernier.

QuickVPN Tray Icon—Connection

État du QuickVPN

Pour désactiver le tunnel VPN, cliquez sur **Disconnect**. Pour modifier votre mot de passe, cliquez sur **Change Password**. Pour obtenir des informations, cliquez sur **Help**.

ÉTAPE 5 Si vous avez cliqué sur **Change Password** et que vous êtes autorisé à modifier votre propre mot de passe, la fenêtre *Connect Virtual Private Connection* s'affiche. Entrez votre mot de passe dans le champ *Old Password*. Saisissez votre nouveau mot de passe dans le champ *New Password*. Saisissez-le à nouveau dans le champ *Confirm New Password*. Cliquez sur **OK**, pour enregistrer votre nouveau mot de passe. Cliquez sur **Cancel**, pour annuler vos modifications. Pour obtenir des informations, cliquez sur **Help**.

Connexion de la Connexion privée virtuelle

REMARQUE Vous ne pouvez modifier votre mot de passe que si votre administrateur système vous a accordé les droits correspondants.

Distribution de certificats aux utilisateurs de QuickVPN

Suivez cette procédure pour exporter à partir du RVS4000 un certificat destiné aux utilisateurs de QuickVPN et installer ce certificat sur leur ordinateur.

ÉTAPE 1 Pour créer un certificat, procédez comme suit :

a. Connectez-vous à l'utilitaire de configuration.

b. Sélectionnez **VPN > VPN Client Accounts**.

c. Cliquez sur **Generate** pour créer un nouveau certificat.

d. Cliquez sur **Export for Client** et enregistrez le certificat en tant que fichier **.PEM**.

ÉTAPE 2 Distribuez le certificat à tous les utilisateurs de QuickVPN.

ÉTAPE 3 Chaque utilisateur de QuickVPN doit alors installer le certificat de la manière suivante :

a. Enregistrez le certificat dans le répertoire sous lequel est installé le client QuickVPN. Par exemple :
C:\Program Files\Cisco\QuickVPN Client

b. Lancez le client QuickVPN et spécifiez le nom d'utilisateur, le mot de passe et l'adresse du serveur (adresse IP ou nom de domaine).

c. Cliquez sur **Connect**.

Pour obtenir plus d'informations sur la gestion des certificats, reportez-vous à la section **« VPN > VPN Client Accounts », page 66** du **Chapitre 5, « Configuration du routeur ».**

C

Configuration d'IPSec avec un ordinateur exécutant Windows 2000 ou XP

Cette annexe explique comment configurer IPSec avec un ordinateur exécutant Windows 2000 ou Windows XP. Reportez-vous aux rubriques suivantes :

Introduction

La présente annexe décrit la procédure à suivre pour créer un tunnel IPSec sécurisé en utilisant des clés pré-partagées pour relier un réseau privé à l'intérieur du routeur et un ordinateur exécutant Windows 2000 ou XP. Les informations relatives à la configuration du serveur Windows 2000 sont disponibles sur le site Web de Microsoft :

Microsoft KB Q252735—Comment configurer le tunneling IPSec dans Windows 2000 :
http://support.microsoft.com/support/kb/articles/Q252/7/35.asp

Microsoft KB Q257225—Résolution des problèmes IPSec dans Microsoft Windows 2000 Server :
http://support.microsoft.com/support/kb/articles/Q257/2/25.asp

REMARQUE

- Notez toutes les modifications que vous effectuez. Ces modifications seront identiques dans l'application « secpol » de Windows et dans l'utilitaire de configuration du routeur.
- Il se peut que le bouton présent à l'écran diffère de celui indiqué dans les instructions. cliquez sur le bouton approprié de votre écran, **OK** ou **Fermer**.

Environnement

Les adresses IP et les autres éléments spécifiques mentionnés dans cette annexe sont des exemples.

Windows 2000 ou Windows XP

Adresse IP : 140.111.1.2 <= L'adresse IP est fournie par le FAI de l'utilisateur (exemple uniquement).

Masque de sous-réseau : 255.255.255.0

RVS4000

Adresse IP WAN : 140.111.1.1 <= L'adresse IP est fournie par le FAI de l'utilisateur (exemple uniquement).

Masque de sous-réseau : 255.255.255.0

Adresse IP LAN : 192.168.1.1

Masque de sous-réseau : 255.255.255.0

Comment établir un tunnel IPSec sécurisé ?

L'établissement d'un tunnel IPSec sécurisé est une opération en cinq étapes, décrites dans la procédure suivante :

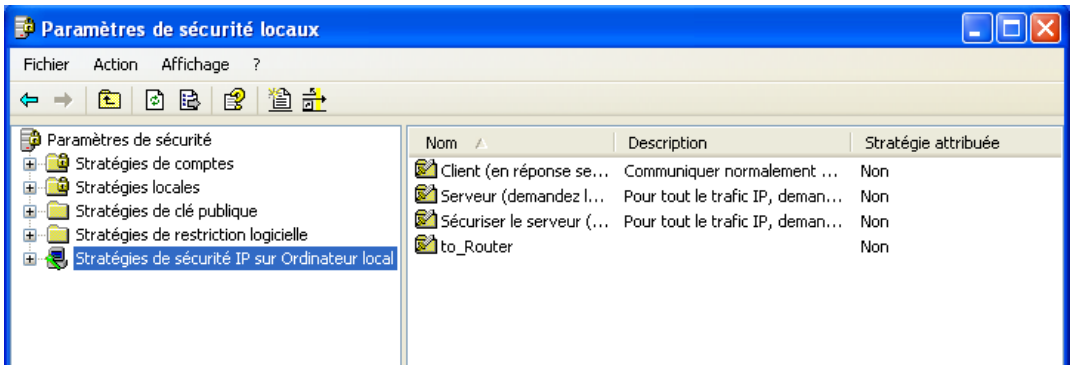
- Étape 1 : création d'une stratégie IPSec
- Étape 2 : création des listes de filtres
- Étape 3 : configuration des règles de tunnel individuelles
- Étape 4 : attribution d'une nouvelle stratégie IPSec
- Étape 5 : création d'un tunnel à l'aide de l'utilitaire Web

Établissement d'un tunnel IPSec sécurisé

ÉTAPE1 Création d'une stratégie IPSec

a. Cliquez sur le bouton **Démarrer**, sélectionnez **Exécuter**, puis saisissez **secpol.msc** dans le champ *Ouvrir*. La fenêtre *Paramètres de sécurité locaux* s'affiche.

Paramètres de sécurité locaux



b. A l'aide du bouton droit de la souris, cliquez sur **Stratégies de sécurité IP sur Ordinateur local** (Windows XP) ou **Stratégies de sécurité IP sur Ordinateur local** (Windows 2000), puis cliquez sur **Créer une stratégie de sécurité IP**.

c. Cliquez sur le bouton **Suivant**, puis entrez un nom pour la stratégie (par exemple, to_Router). Cliquez ensuite sur **Suivant**.

d. Décochez la case **Activer la règle de réponse par défaut**, puis cliquez sur **Suivant**.

e. Cliquez sur **Terminer**, en vous assurant que l'option **Modifier** est sélectionnée.

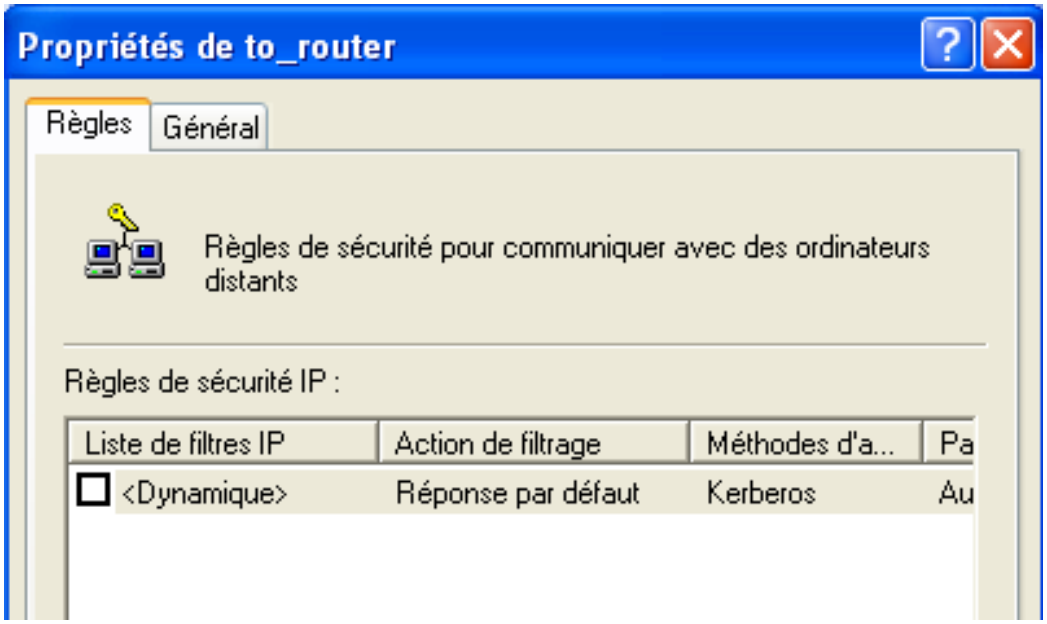
ÉTAPE 2 Création des listes de filtres

REMARQUE Dans cette section, le terme « win » désigne à la fois Windows 2000 et Windows XP.

Liste de filtres 1 : win->Router

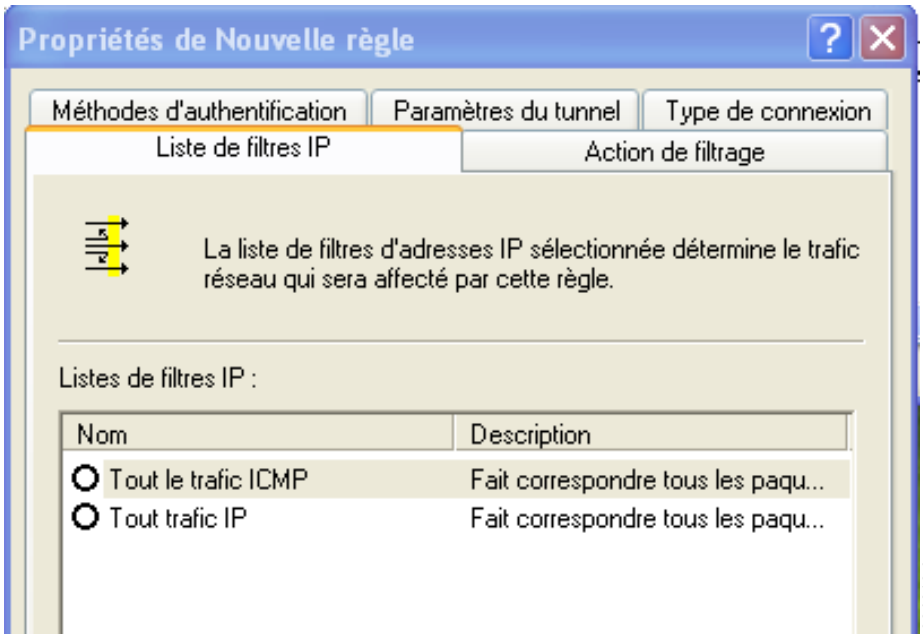
a. Dans la fenêtre Propriétés de Nouvelle règle, vérifiez que l'onglet **Règles** est sélectionné. Décochez la case **Utiliser l'Assistant Ajout**, puis cliquez sur **Ajouter** pour créer une nouvelle règle.

Onglet Règles



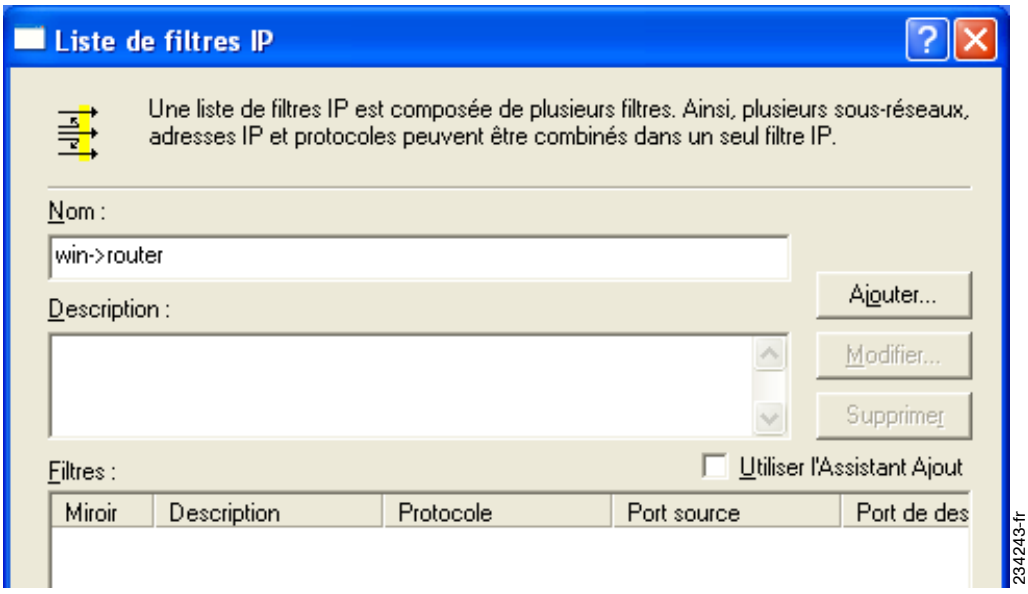
b. Assurez-vous que l'onglet **Liste de filtres IP** est sélectionné. Cliquez sur **Ajouter.**

Onglet Liste de filtres IP



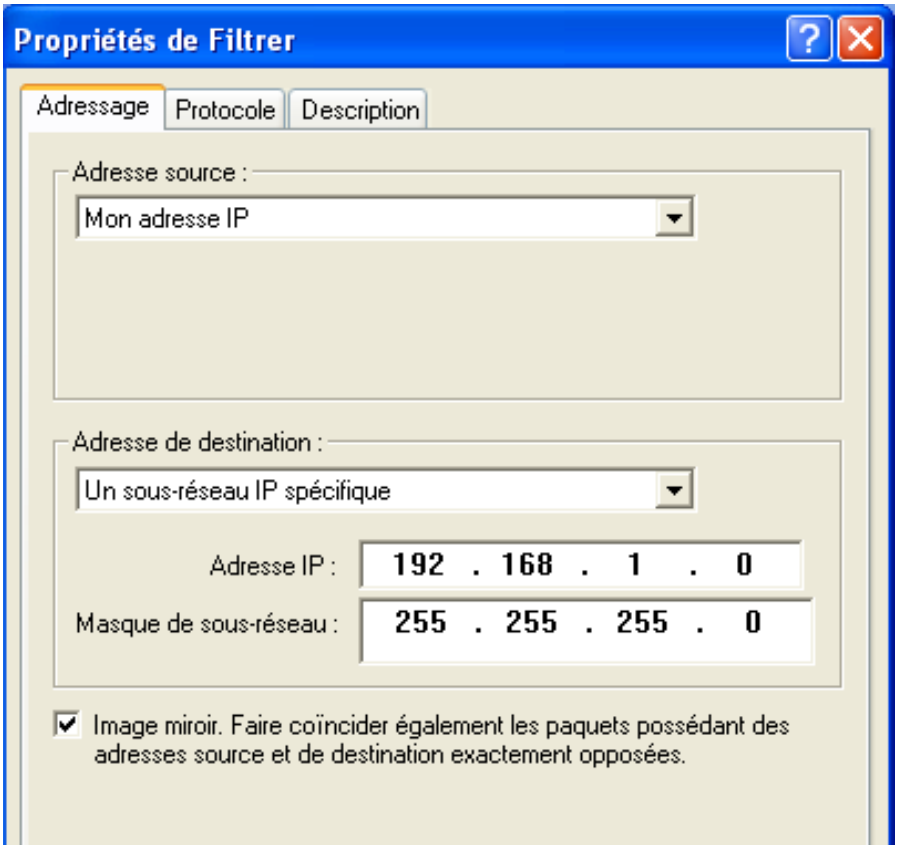
c. La fenêtre *Liste de filtres IP* doit s'afficher. Entrez le nom souhaité pour la liste de filtres (win->Router, par exemple) et décochez la case **Utiliser l'Assistant Ajout**. Cliquez ensuite sur **Ajouter**.

Liste de filtres IP



d. La fenêtre *Propriétés de filtre* s'affiche. Sélectionnez l'onglet **Adressage**.

Propriétés de filtre



Dans le champ *Adresse source*, sélectionnez **Mon adresse IP**. Dans le champ *Adresse destination*, sélectionnez **Un sous-réseau IP spécifique**, et entrez l'adresse IP **192.168.1.0** et le masque de sous-réseau **255.255.255.0**. (Il s'agit des paramètres par défaut du routeur. Si vous avez modifié ces paramètres, entrez les nouvelles valeurs dans ces champs.)

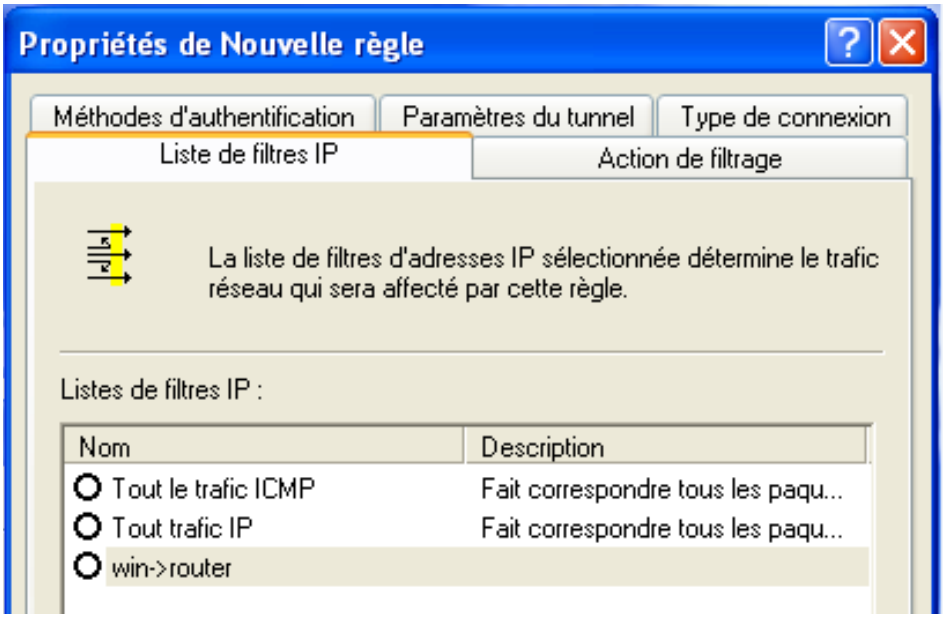
e. Si vous souhaitez entrer une description de votre filtre, cliquez sur l'onglet **Description** et saisissez votre description.

f. Cliquez sur **OK**. Cliquez ensuite sur **OK** ou **Fermer** dans la fenêtre *Liste de filtres IP*.

Liste de filtres 2 : Router=>win

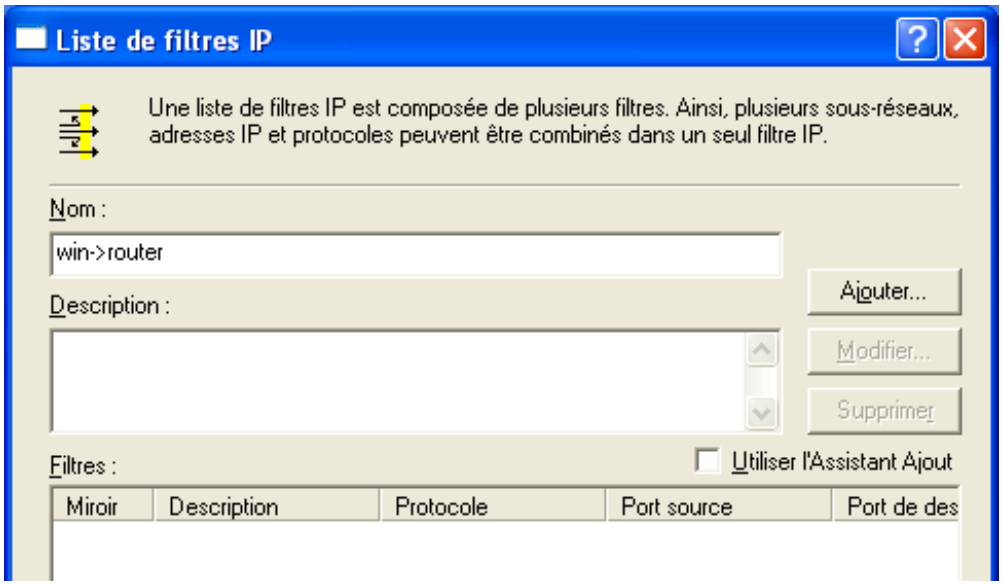
g. La fenêtre *Propriétés de Nouvelle règle* s'affiche. Sélectionnez l'onglet **Liste de filtres IP** et assurez-vous que **win -> Router** apparaît en surbrillance. Cliquez ensuite sur **Ajouter**.

Propriétés de Nouvelle règle



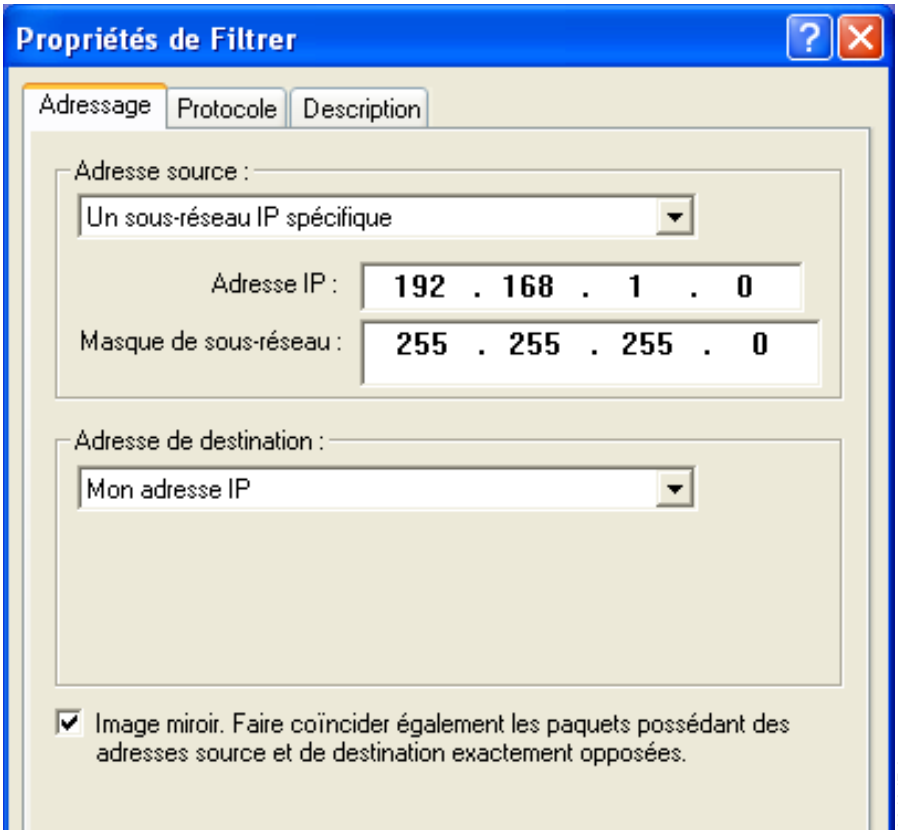
h. La fenêtre *Liste de filtres IP* doit s'afficher. Saisissez le nom souhaité pour la liste de filtres (**Router->win**, par exemple) et décochez la case **Utiliser l'Assistant Ajout**. Cliquez sur **Ajouter.**

Liste de filtres IP



i. La fenêtre *Propriétés de filtre* s'affiche. Sélectionnez l'onglet **Adressage**. Dans le champ **Adresse source**, sélectionnez **Un sous-réseau IP spécifique**, et entrez l'adresse IP **192.168.1.0** et le masque de sous-réseau **255.255.255.0**. Si vous avez modifié les paramètres par défaut, entrez vos nouvelles valeurs. Dans le champ *Adresse de destination*, sélectionnez **Mon adresse IP**.

Propriétés de filtre

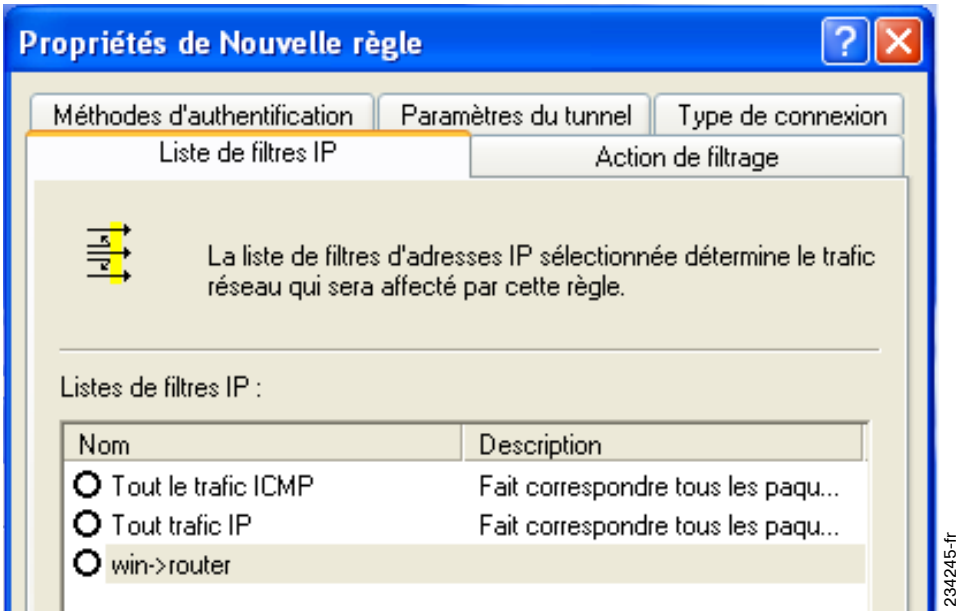


j. Si vous souhaitez entrer une description de votre filtre, cliquez sur l'onglet **Description** et saisissez votre description.

k. Cliquez sur **OK** ou **Fermer**.

La fenêtre *Propriétés de Nouvelle règle* s'affiche avec l'onglet **Liste de filtres IP** sélectionné. La fenêtre contient les listes pour **Router->win** et **win->Router**.

Propriétés de Nouvelle règle



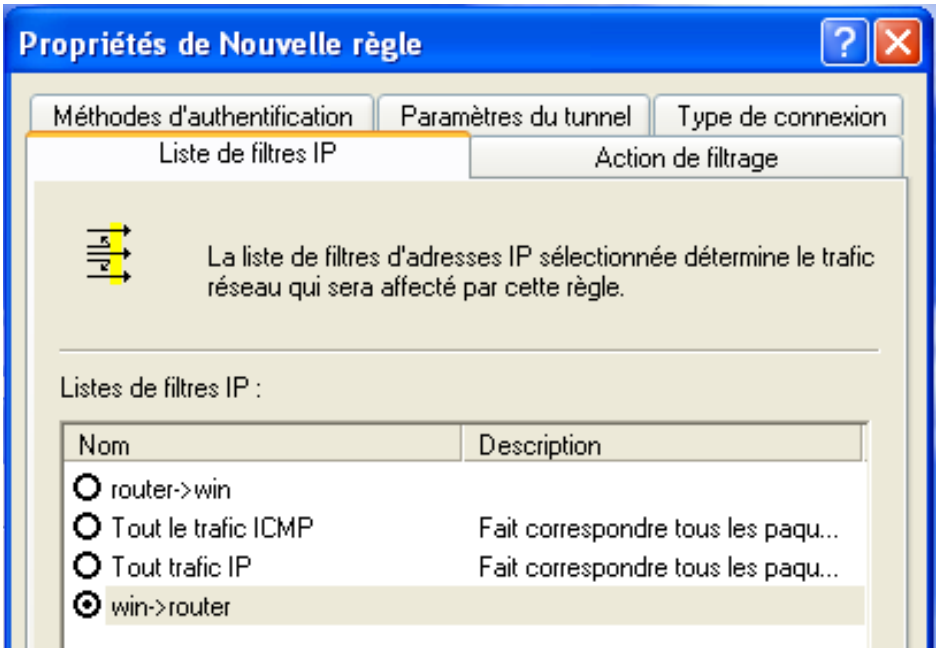
l. Cliquez sur **OK** (Windows XP) ou **Fermer** (Windows 2000) dans la fenêtre *Liste de filtres IP*.

ÉTAPE 3 Configuration des règles de tunnel individuelles

Tunnel 1 : win->Router

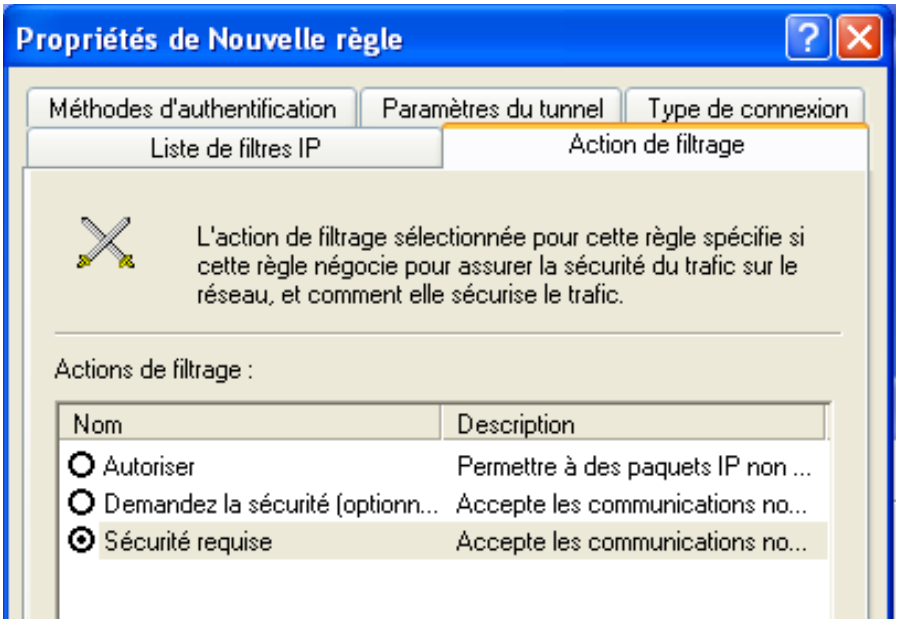
a. Dans l'onglet **Liste de filtres IP**, sélectionnez la liste **win->Router**.

Onglet Liste de filtres IP



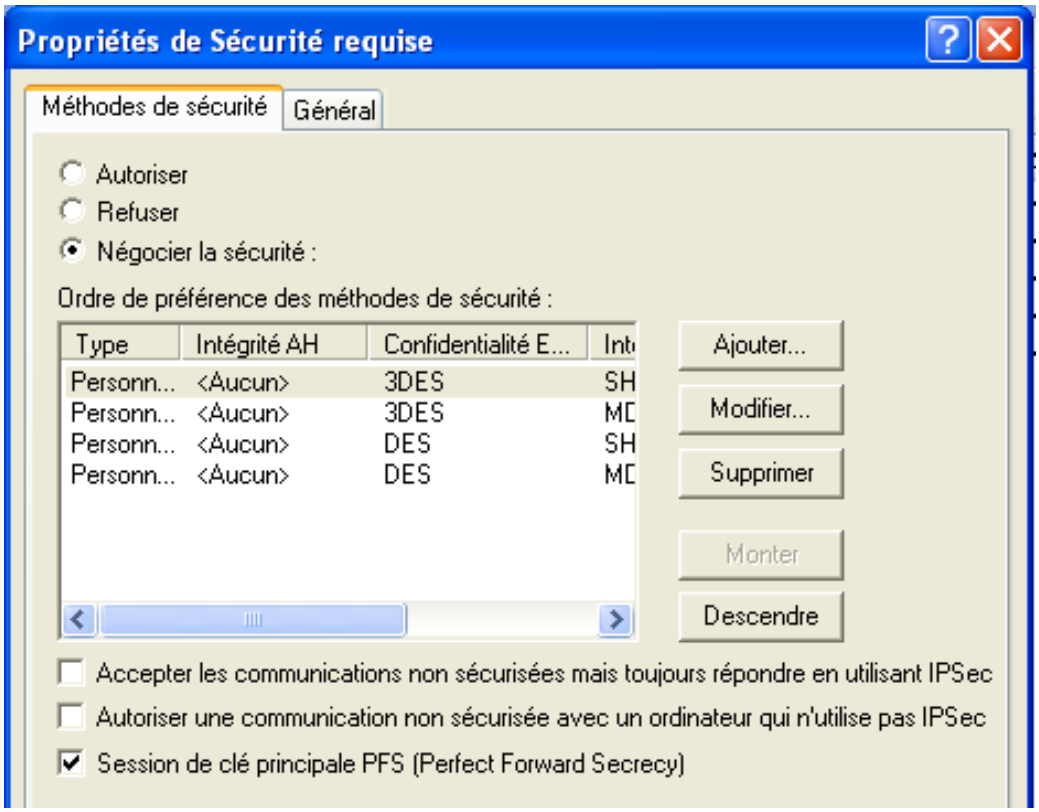
b. Cliquez sur l'onglet *Action de filtrage*, puis sur la case d'option **Demander la sécurité**. Cliquez ensuite sur **Modifier**.

Onglet Action de filtrage



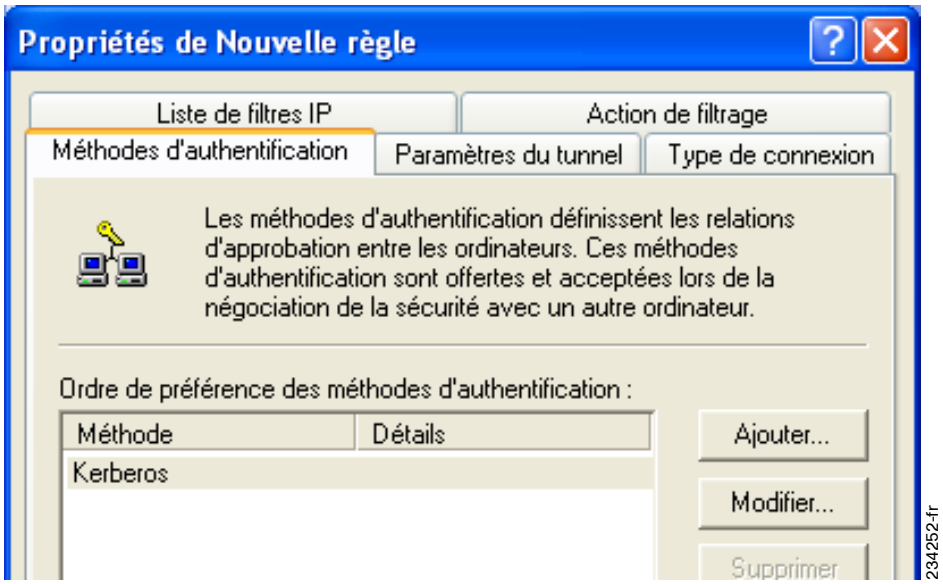
c. Dans l'onglet *Méthodes de sécurité*, vérifiez que l'option **Négocier la sécurité** est activée, puis décochez la case **Accepter les communications non sécurisées, mais toujours répondre en utilisant IPSec**. Sélectionnez **Session de clé principale PFS**, puis cliquez sur le bouton **OK**.

Onglet Méthodes de sécurité



d. Sélectionnez l'onglet **Méthodes d'authentification**, puis cliquez sur **Modifier**.

Onglet Méthode d'authentification

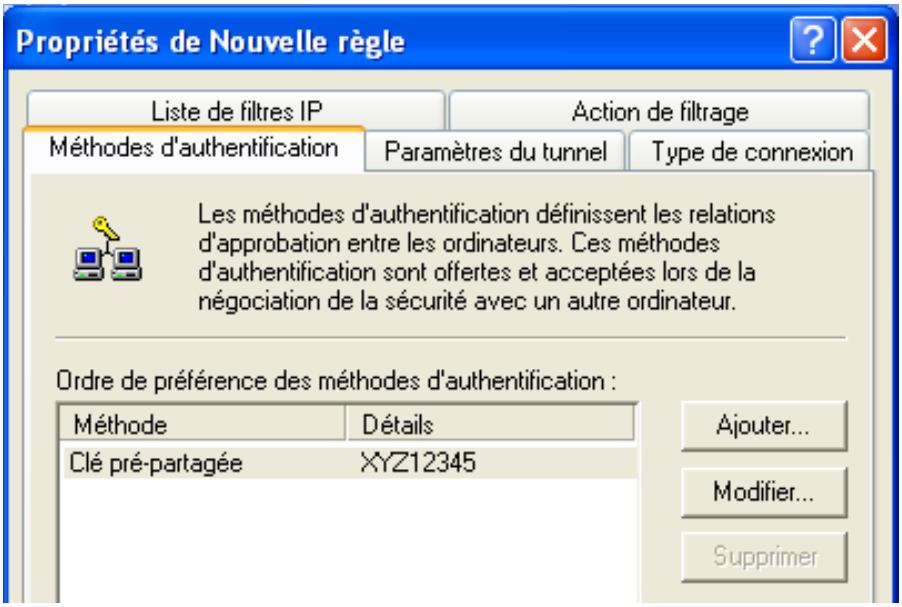


e. Remplacer la méthode d'authentification par **Utiliser cette chaîne pour protéger l'échange de clés (clé pré-partagée)**, puis saisissez la chaîne de clé pré-partagée, telle que XYZ12345. Cliquez sur **OK**.

Clé pré-partagée

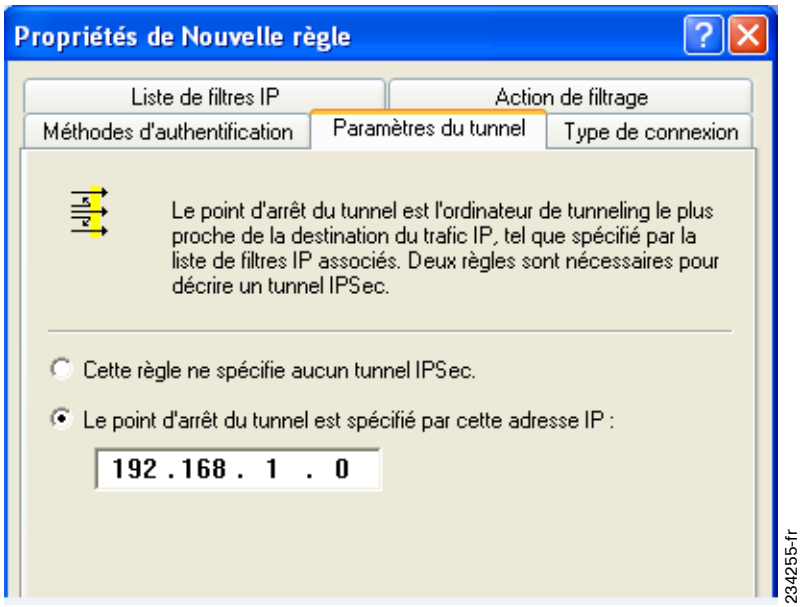
f. Cette nouvelle clé pré-partagée s'affiche. Cliquez sur le bouton **Appliquer** pour continuer si elle s'affiche sur votre écran, sinon passez à l'étape suivante.

Nouvelle clé pré-partagée



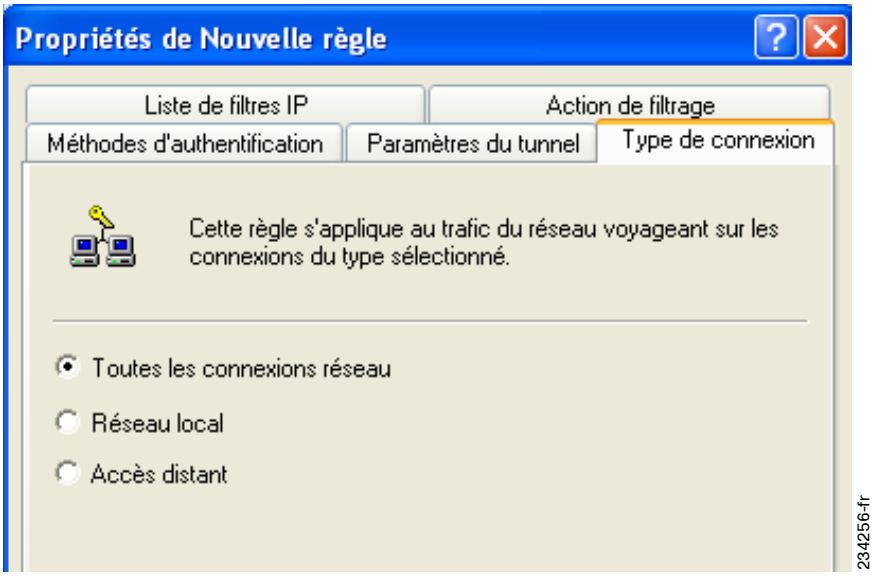
g. Sélectionnez l'onglet **Paramètres du tunnel** et cliquez sur la case d'option **Le point d'arrêt du tunnel est spécifié par cette adresse IP**. Entrez ensuite l'adresse IP WAN du routeur.

Onglet Paramètres du tunnel



h. Sélectionnez l'onglet **Type de connexion**, puis cliquez sur **Toutes les connexions réseau**. Cliquez ensuite sur **OK** ou **Fermer** pour terminer cette règle.

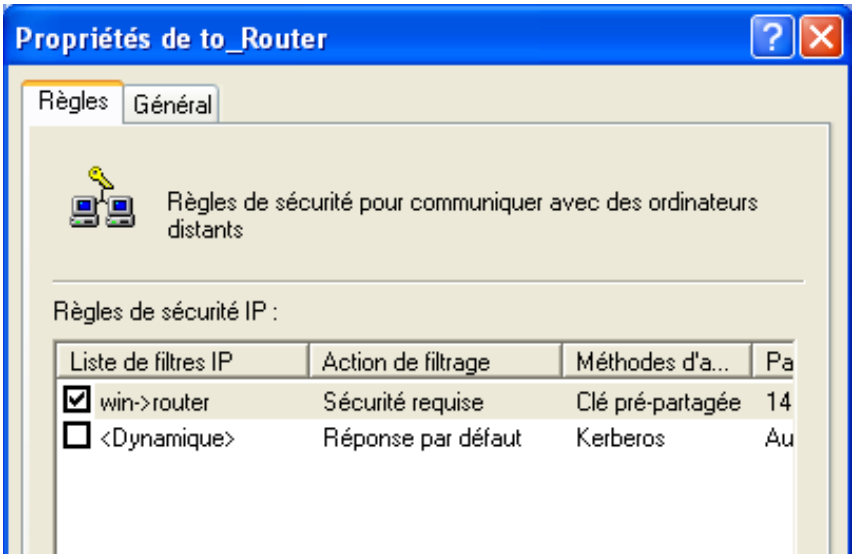
Onglet Type de connexion



Tunnel 2 : Router->win

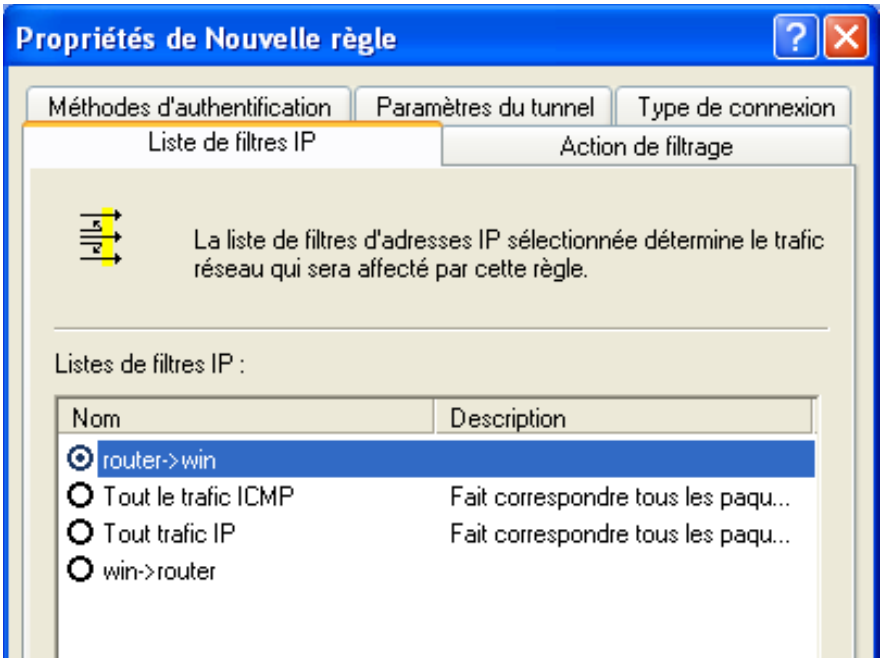
i. Dans la fenêtre Propriétés de Nouvelle règle, assurez-vous que l'option **win -> Router** est sélectionnée et décochez la case **Utiliser l'Assistant Ajout**. Cliquez ensuite sur **Ajouter** pour créer le second filtre IP.

Fenêtre Propriétés



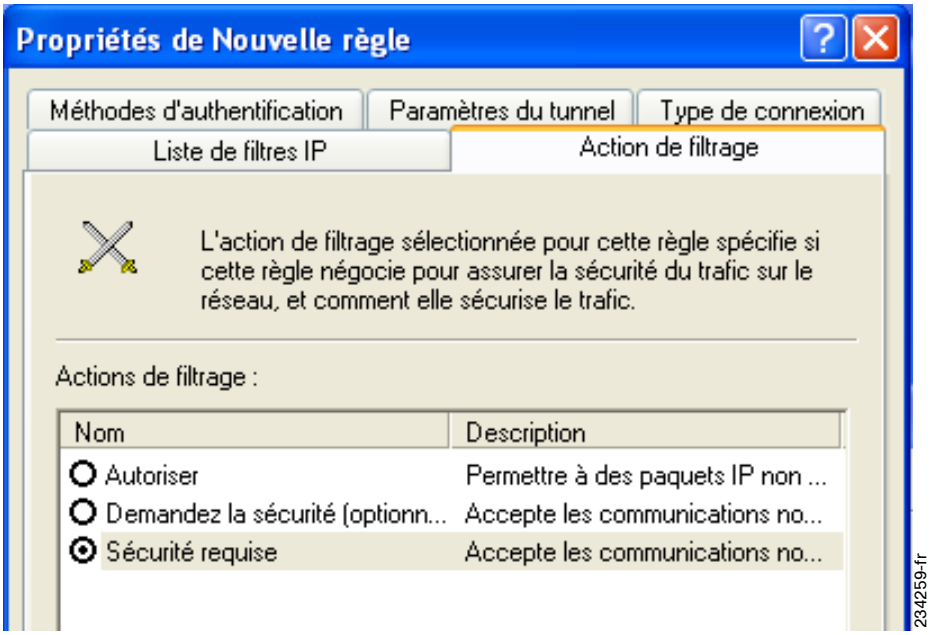
j. Dans l'onglet **Liste de filtres IP**, cliquez sur la liste de filtres **Router->win**.

Onglet Liste de filtres IP



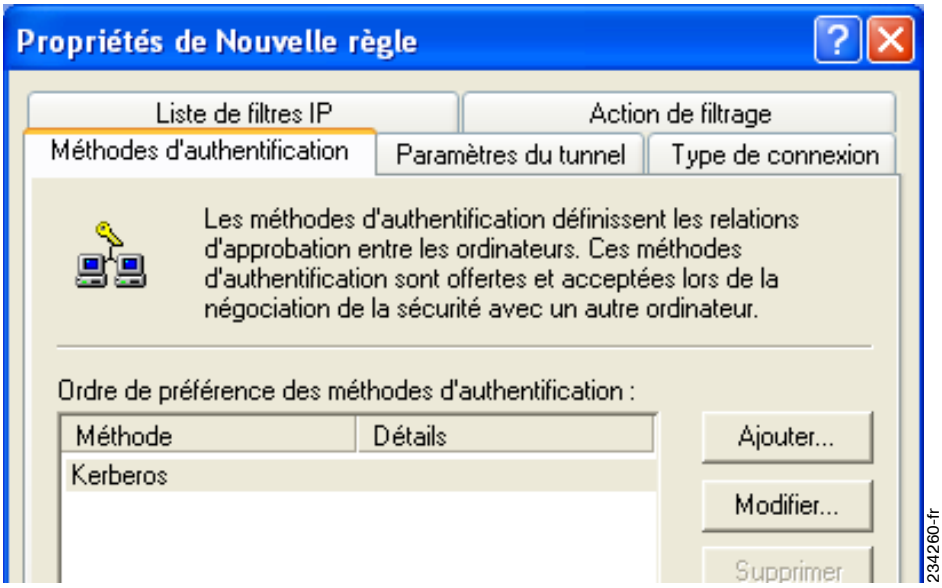
k. Cliquez sur l'onglet **Action de filtrage**, puis sur la case d'option **Demander la sécurité**. Cliquez ensuite sur **Modifier**. Dans l'onglet **Méthodes de sécurité**, vérifiez que l'option **Négocier la sécurité** est activée, puis décochez la case **Accepter les communications non sécurisées, mais toujours répondre en utilisant IPSec**. Sélectionnez **Session de clé principale PFS**, puis cliquez sur le bouton **OK**.

Onglet Action de filtrage



l. Cliquez sur l'onglet **Méthodes d'authentification** et vérifiez que la méthode d'authentification **Kerberos** est sélectionnée. Cliquez ensuite sur **Modifier**.

Onglet Méthode d'authentification



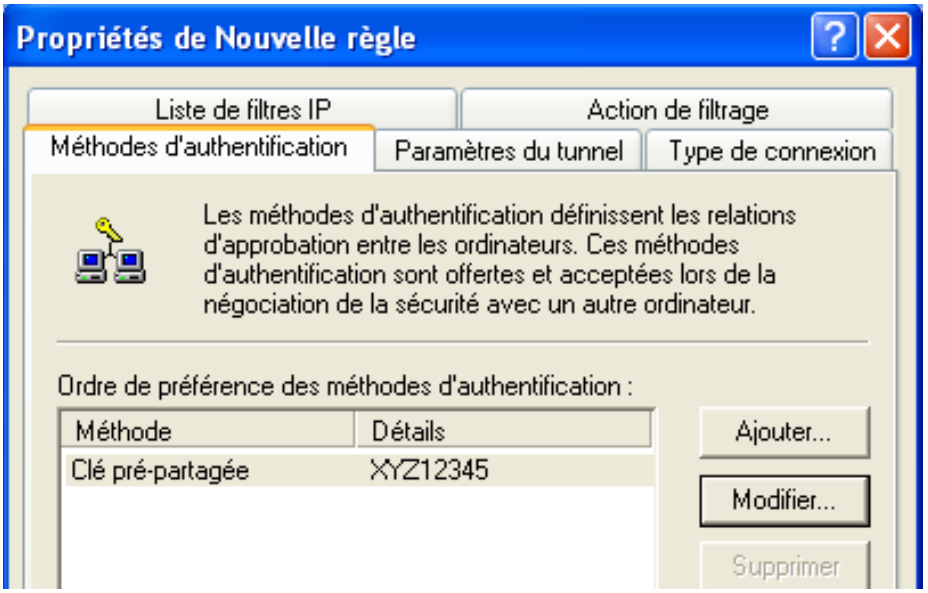
m. Remplacer la méthode d'authentification par **Utiliser cette chaîne pour protéger l'échange de clés (clé pré-partagée)**, puis saisissez la chaîne de clé

pré-partagée, telle que XYZ12345. (Il s'agit d'un exemple de chaîne de clé. Votre clé doit être unique et facile à mémoriser.) Cliquez ensuite sur le bouton **OK**.

Clé pré-partagée

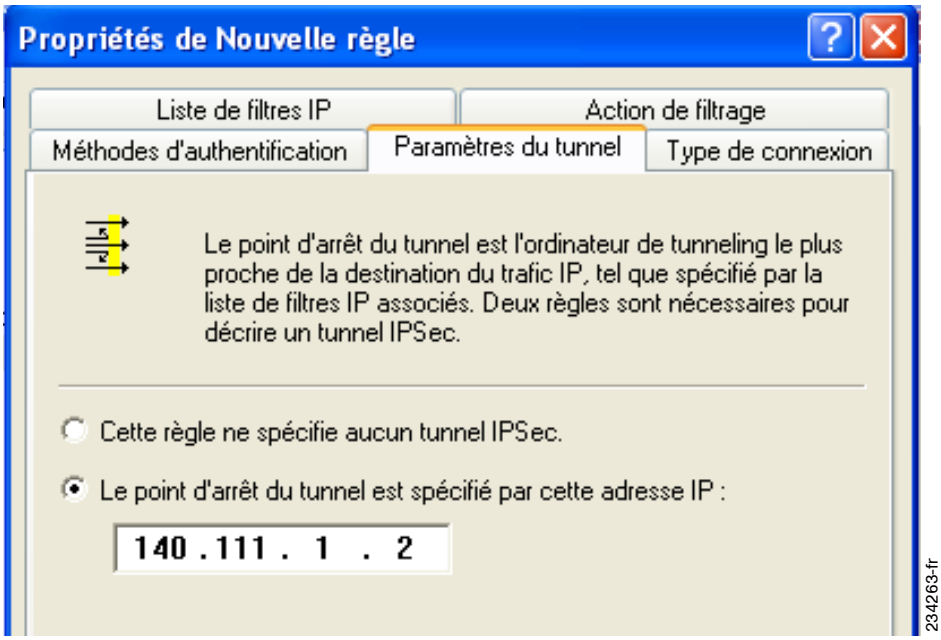
n. Cette nouvelle clé pré-partagée s'affiche. Cliquez sur le bouton **Appliquer** pour continuer si elle s'affiche sur votre écran, sinon passez à l'étape suivante.

Nouvelle clé pré-partagée



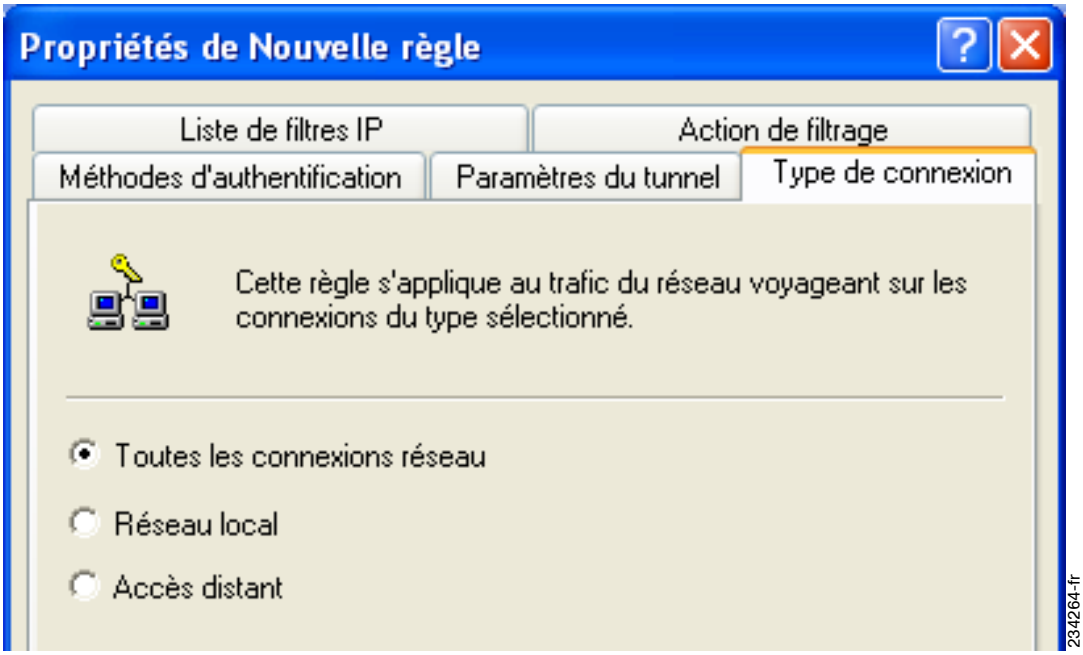
o. Cliquez sur l'onglet **Paramètres du tunnel**. Sélectionnez la case d'option **Le point d'arrêt du tunnel est spécifié par cette adresse IP**, puis entrez l'adresse IP de l'ordinateur exécutant Windows 2000/XP.

Onglet Paramètres du tunnel



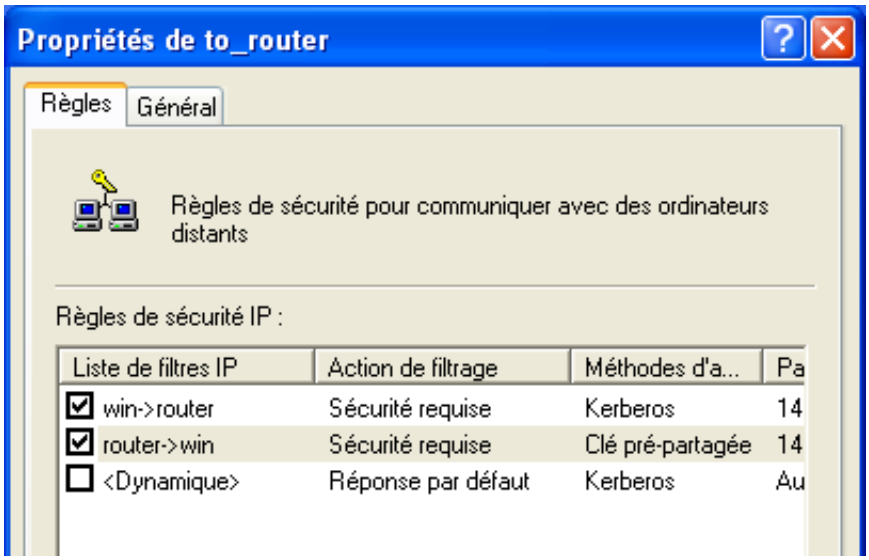
p. Sélectionnez l'onglet **Type de connexion**, puis cliquez sur **Toutes les connexions réseau**. Cliquez ensuite sur **OK** ou **Fermer** pour terminer.

Onglet Type de connexion



q. Dans l'onglet **Règles**, cliquez sur le bouton **OK** ou **Fermer** pour revenir à la fenêtre affichant les règles de sécurité.

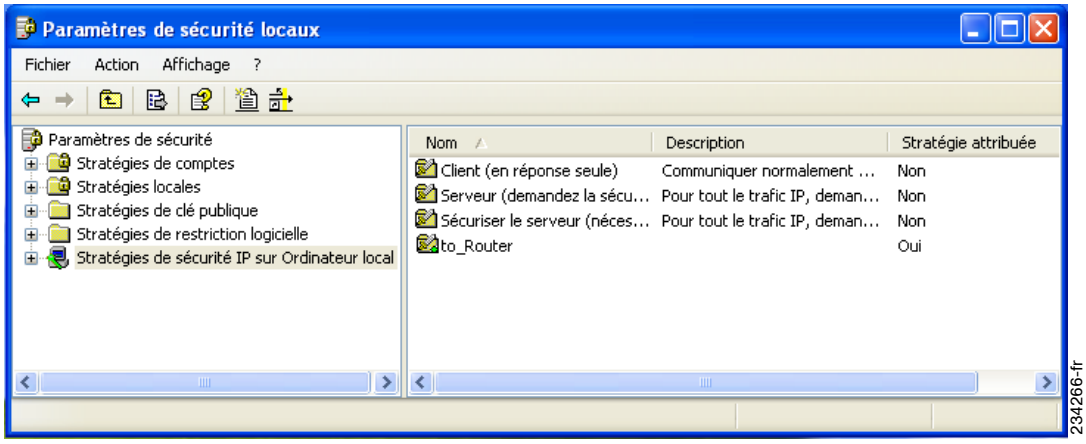
Onglet Règles



ÉTAPE 4 Attribution d'une nouvelle stratégie IPSec

Dans la fenêtre *Stratégies de sécurité IP sur Ordinateur local*, cliquez avec le bouton droit de la souris sur **to_Router**, puis cliquez sur **Attribuer**. Une flèche verte apparaît sur l'icône du dossier.

Ordinateur local



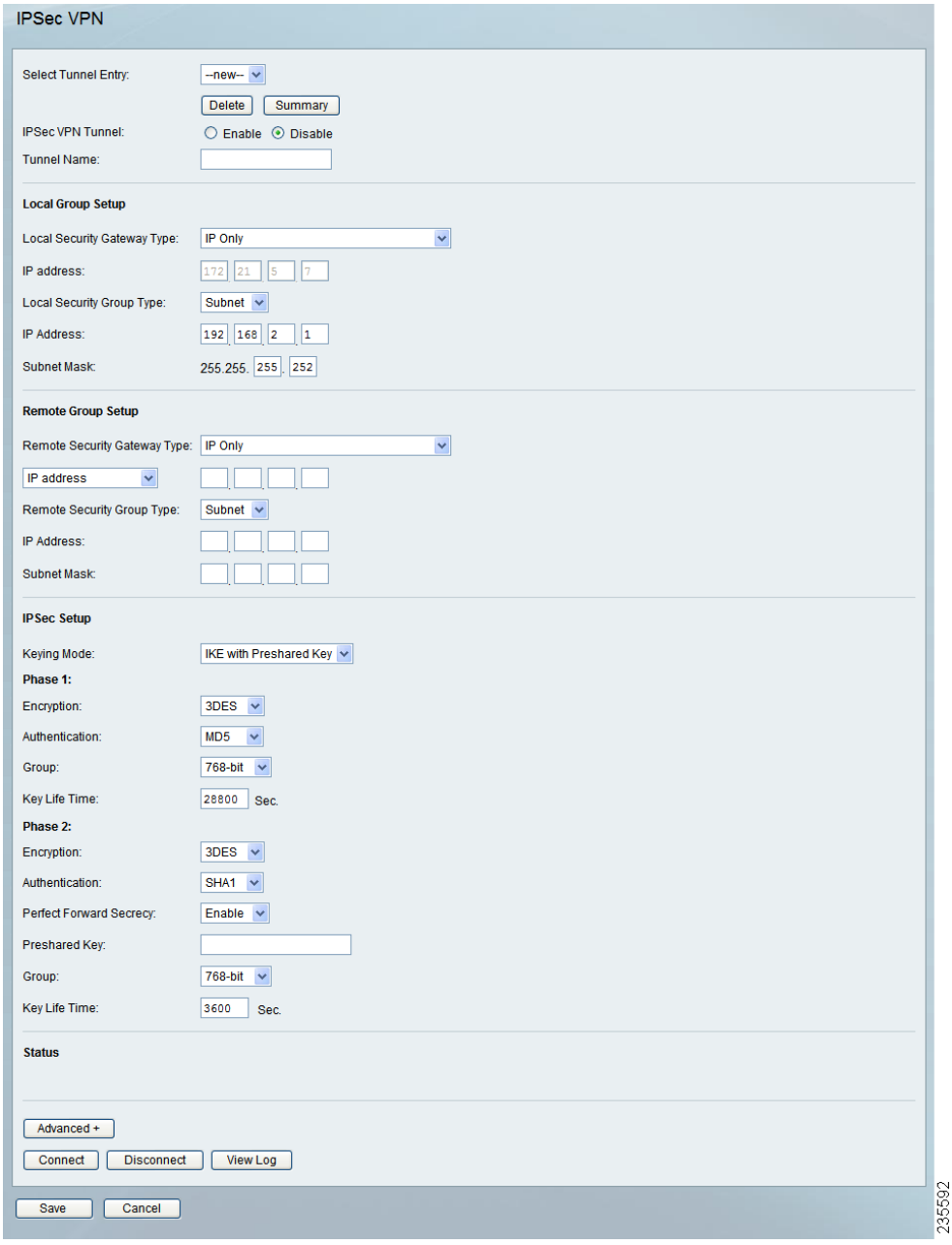
ÉTAPE 5 Création d'un tunnel à l'aide de l'utilitaire de configuration Web

a. Ouvrez votre navigateur Web et entrez **192.168.1.1** dans le champ *Adresse*. Appuyez sur **Entrée**.

b. Lorsque les champs *User name* et *Password* apparaissent, saisissez **admin** comme nom d'utilisateur et mot de passe par défaut. Appuyez sur **Entrée**.

c. Cliquez sur **VPN > IPSec VPN**.

VPN > IPsec VPN



d. Sélectionnez le tunnel que vous voulez créer dans la liste déroulante *Select Tunnel Entry*. Cliquez ensuite sur **Enable**. Entrez le nom du tunnel dans le champ *Tunnel Name*. Ceci vous permet d'identifier les divers tunnels et il n'est donc pas nécessaire que ce nom corresponde au nom utilisé à l'autre bout du tunnel.

e. Entrez l'adresse IP et le masque de sous-réseau du routeur VPN local dans les champs de la section *Local Group Setup*. Pour permettre l'accès à l'ensemble du sous-réseau IP, entrez **0** pour le dernier ensemble d'adresses IP (par exemple, 192.168.1.0).

f. Entrez l'adresse IP et le masque de sous-réseau du périphérique VPN à l'autre extrémité du tunnel (la passerelle VPN distante ou le périphérique VPN distant avec laquelle/lequel vous voulez communiquer) dans les champs *Remote Group Setup*.

g. Sélectionnez l'un des deux types d'authentification : **MD5** ou **SHA1** (SHA1 étant recommandé car cette option garantit un niveau de protection plus élevé). Comme pour le cryptage, vous pouvez sélectionner l'un de ces deux paramètres, mais le même type d'authentification doit être utilisé par le périphérique VPN à l'autre bout du tunnel. L'authentification peut également être désactivée des deux côtés du tunnel, à l'aide de l'option **Disable**.

h. Dans la liste **Keying Mode**, choisissez **IKE with Preshared Key**. Saisissez une suite de chiffres ou de lettres dans le champ **Pre-Shared Key**. Activez aussi l'option **Perfect Forward Secrecy**, pour faire en sorte que l'échange de clé initial et les proprositions IKE soient sécurisés.

i. Cliquez sur **Save** pour enregistrer vos modifications.

Votre tunnel est maintenant défini.

D

Tunnel VPN passerelle à passerelle

Présentation

Cette annexe présente, à l'aide d'un exemple, la procédure à suivre pour configurer un tunnel VPN IPSec entre deux routeurs VPN. Deux ordinateurs sont utilisés pour tester la réponse du tunnel. Elle comprend les sections suivantes :

Avant de commencer

Vous devez disposer des équipements suivants :

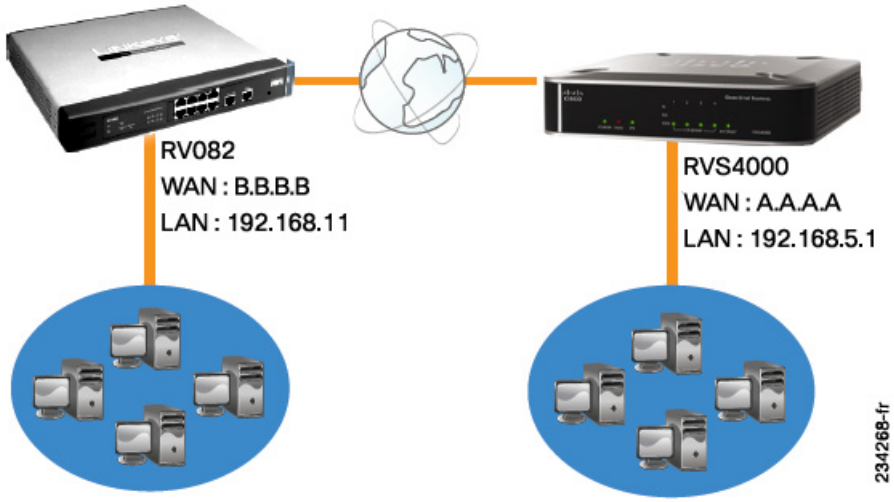
- Deux ordinateurs de bureau exécutant Windows (chaque ordinateur sera connecté à un routeur VPN)
- Deux routeurs VPN (routeur de sécurité Gigabit 4 ports avec VPN, modèle RVS4000, et routeur VPN 10/100 8 ports, modèle RV082) connectés à Internet

Vous pouvez déployer n'importe quel routeur VPN, comme le routeur VPN 10/100 16, 8 ou 4 ports (modèles RV016, RV082 ou RV042) ; néanmoins, cet exemple est basé sur le modèle RV082.

Configuration lorsque la passerelle distante utilise une adresse IP statique

Dans cet exemple, il est supposé que la passerelle distante utilise une adresse IP statique. Si la passerelle distante utilise une adresse IP dynamique, reportez-vous à **« Configuration lorsque la passerelle distante utilise une adresse IP dynamique », page 176**.

Tunnel VPN IPSec de passerelle à passerelle, la passerelle distante utilisant une adresse IP statique



REMARQUE Chaque ordinateur doit être équipé d'un adaptateur réseau.

ÉTAPE1 Configuration du RVS4000.

Suivez ces instructions pour le premier routeur VPN, appelé RVS4000. L'autre routeur VPN est appelé RV082.

a. Lancez le navigateur Web pour un ordinateur en réseau, appelé Ordinateur 1.

b. Accédez à l'utilitaire de configuration du RVS4000. (Pour obtenir plus de détails, reportez-vous au **Chapitre 5, « Configuration du routeur »**.)

c. Cliquez sur **VPN > IPSec VPN**.

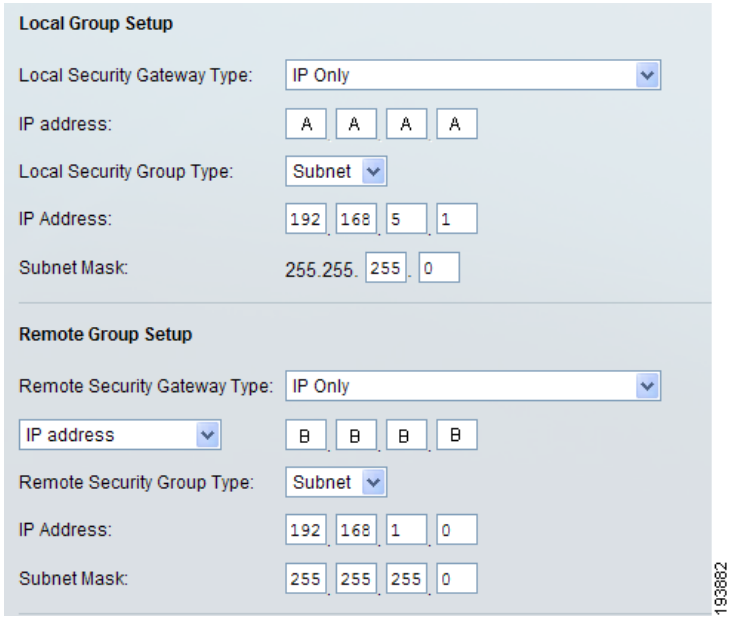
d. Saisissez un nom dans le champ *Tunnel Name*.

e. Pour le paramètre IPSec VPN Tunnel, sélectionnez **Enable**.

f. L'adresse IP WAN (A.A.A.A) du RVS4000 sera automatiquement détectée.

Pour Local Security Group Type, sélectionnez **Subnet**. Saisissez les paramètres du réseau local du RVS4000 dans les champs *IP Address* et *Subnet Mask*.

Paramètres VPN IPSec du RVS4000



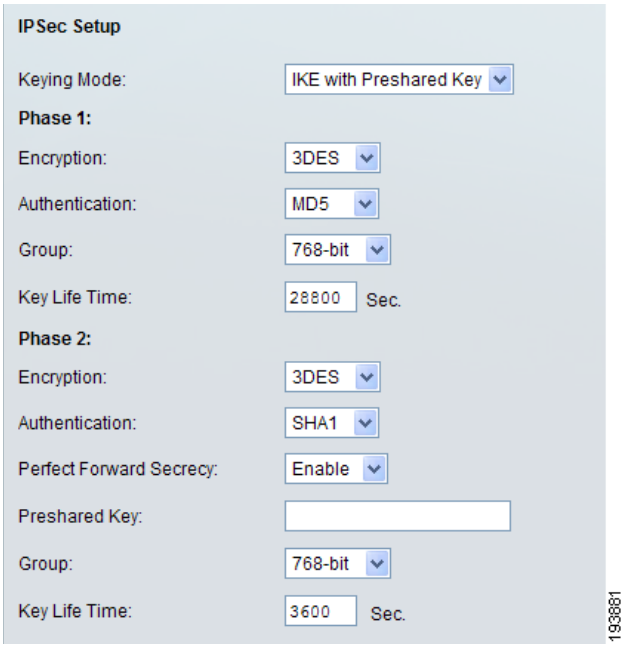
g. Pour Remote Security Gateway Type, sélectionnez **IP address**. Entrez l'adresse IP WAN du RV082 dans le champ *IP Address*.

h. Pour Remote Security Group Type, sélectionnez **Subnet**. Saisissez les paramètres du réseau local du RV082 dans les champs *IP Address* et *Subnet Mask*.

i. Dans la section IPSec Setup, sélectionnez les paramètres appropriés pour le cryptage, l'authentification et d'autres options essentielles de gestion.

j. Dans le champ *Preshared Key*, saisissez une chaîne pour la clé pré-partagée, par exemple 13572468.

Paramètres de configuration IPSec du RVS4000



k. Pour afficher des paramètres plus détaillés, cliquez sur **Advanced Settings**. Sinon, cliquez sur **Save** et passez à l'étape suivante pour configurer le RV082.

ÉTAPE 2 Configuration du RV082.

Les instructions sont similaires pour le RV082.

a. Lancez le navigateur Web pour un ordinateur en réseau, appelé Ordinateur 2.

b. Accédez à l'utilitaire de configuration du RV082. (Pour obtenir plus de détails, reportez-vous au guide d'administration du RV082.)

c. Cliquez sur l'onglet **IPSec VPN**.

d. Cliquez sur l'onglet **Gateway to Gateway**.

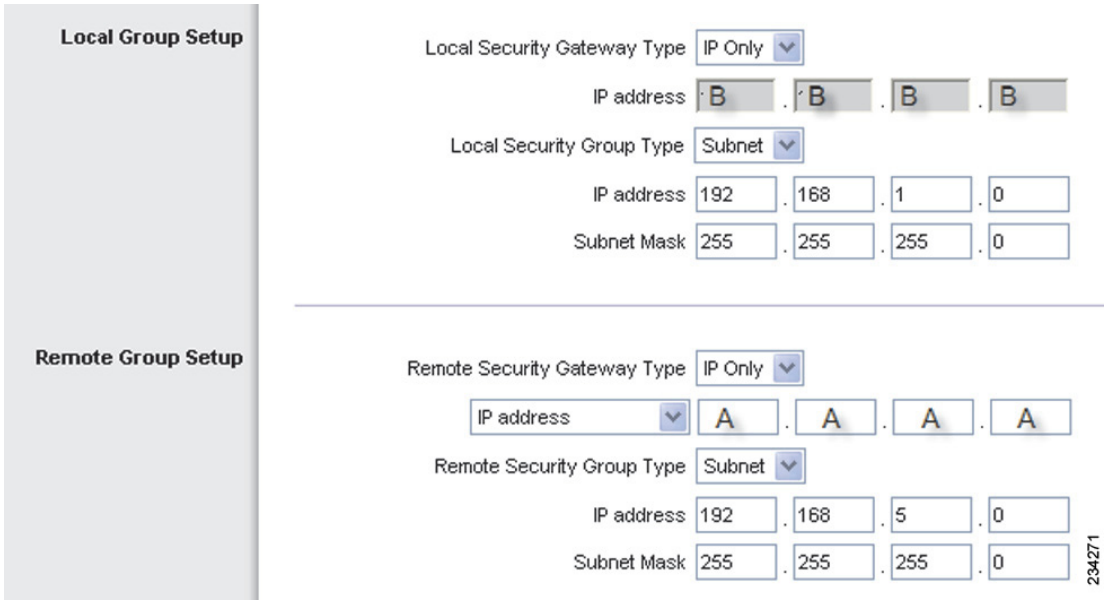
e. Saisissez un nom dans le champ *Tunnel Name*.

f. Pour le paramètre VPN Tunnel, sélectionnez **Enable**.

g. L'adresse IP WAN (B.B.B.B) du RV082 sera automatiquement détectée.

Pour Local Security Group Type, sélectionnez **Subnet**. Saisissez les paramètres du réseau local du RV082 dans les champs *IP Address* et *Subnet Mask*.

Paramètres VPN du RV082



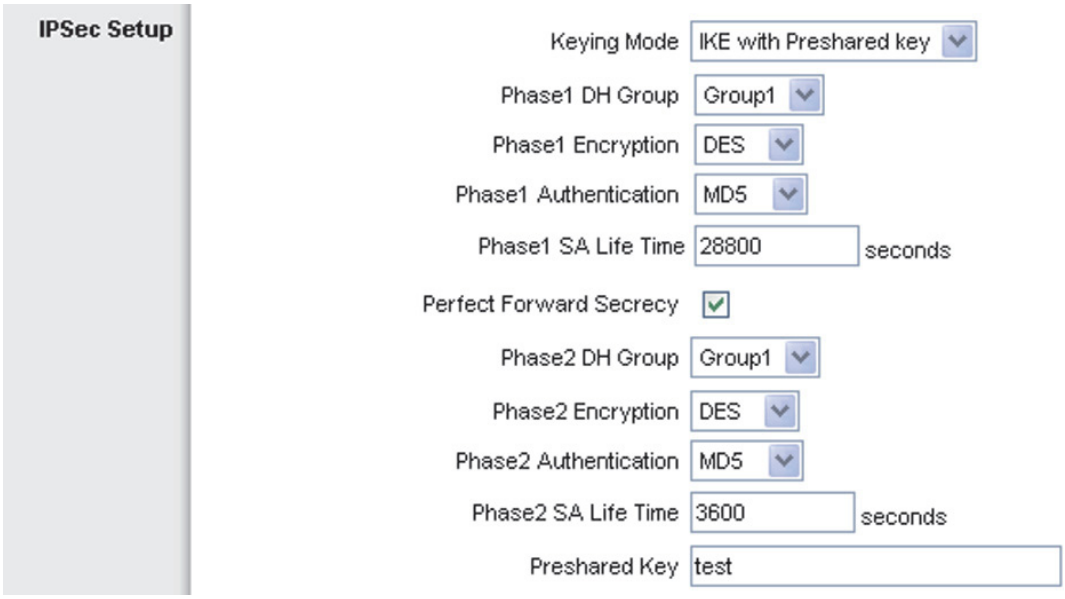
h. Pour Remote Security Gateway Type, sélectionnez **IP address**. Entrez l'adresse IP WAN du RVS4000 dans le champ *IP Address*.

i. Pour Remote Security Group Type, sélectionnez **Subnet**. Saisissez les paramètres du réseau local du RVS4000 dans les champs *IP Address* et *Subnet Mask*.

j. Dans la section IPSec Setup, sélectionnez les paramètres appropriés pour le cryptage, l'authentification et d'autres options essentielles de gestion. (Ils doivent correspondre aux paramètres du RVS4000.)

k. Dans le champ *Preshared Key*, saisissez une chaîne pour la clé pré-partagée, par exemple 13572468.

Paramètres de configuration IPSec du RV082



1. Pour afficher des paramètres plus détaillés, cliquez sur **Advanced Settings**. Sinon, cliquez sur **Save**.

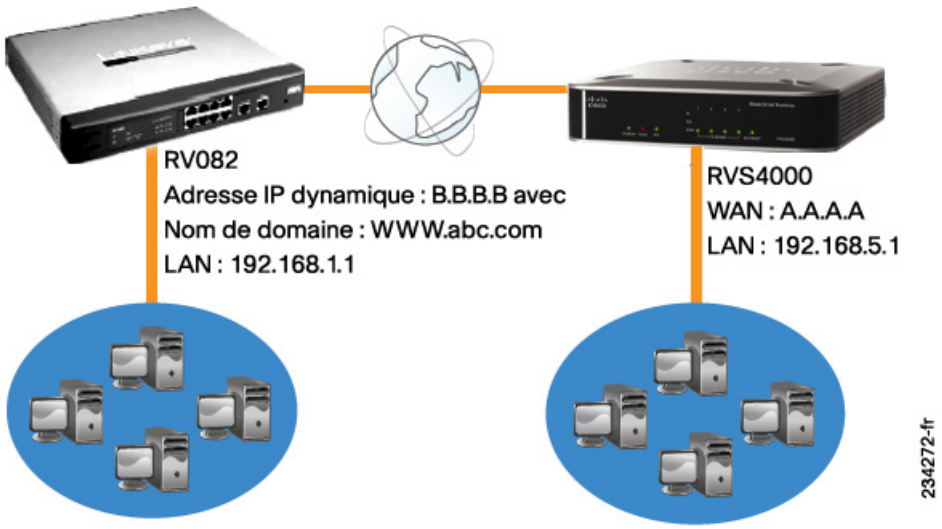
ÉTAPE 3 Configuration de l'Ordinateur 1 et de l'Ordinateur 2.

Vérifiez que l'Ordinateur 1 et l'Ordinateur 2 peuvent exécuter une commande ping l'un sur l'autre (reportez-vous à l'aide de Windows pour obtenir plus d'informations). Si les ordinateurs sont en mesure d'exécuter l'un sur l'autre une commande ping, vous avez l'assurance que le tunnel VPN est configuré correctement.

Configuration lorsque la passerelle distante utilise une adresse IP dynamique

Dans cet exemple, il est supposé que la passerelle distante utilise une adresse IP dynamique. Si la passerelle distante utilise une adresse IP statique, reportez-vous à **« Configuration lorsque la passerelle distante utilise une adresse IP statique », page 171**.

Tunnel VPN IPSec de passerelle à passerelle, la passerelle distante utilisant une adresse IP dynamique



REMARQUE Chaque ordinateur doit être équipé d'un adaptateur réseau.

ÉTAPE 1 Configuration du RVS4000.

Suivez ces instructions pour le premier routeur VPN, appelé RVS4000. L'autre routeur VPN est appelé RV082.

a. Lancez le navigateur Web pour un ordinateur en réseau, appelé Ordinateur 1.

b. Accédez à l'utilitaire de configuration du RVS4000. (Pour obtenir plus de détails, reportez-vous au **Chapitre 5, « Configuration du routeur »**.)

c. Cliquez sur **VPN > IPSec VPN**.

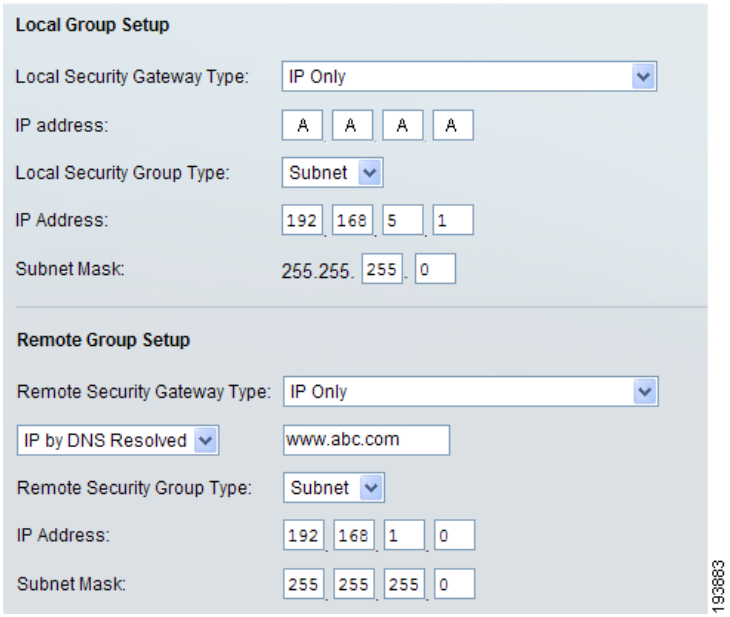
d. Saisissez un nom dans le champ *Tunnel Name*.

e. Pour le paramètre IPSec VPN Tunnel, sélectionnez **Enable**.

f. L'adresse IP WAN (A.A.A.A) du RVS4000 sera automatiquement détectée.

Pour Local Security Group Type, sélectionnez **Subnet**. Saisissez les paramètres du réseau local du RVS4000 dans les champs *IP Address* et *Subnet Mask*.

Paramètres VPN IPSec du RVS4000



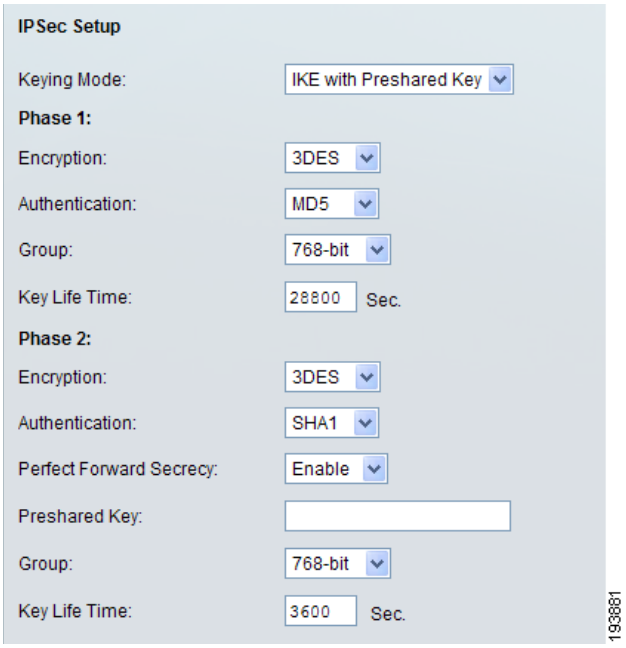
g. Pour Remote Security Gateway Type, sélectionnez **IP by DNS Resolved**. Saisissez le nom de domaine du RV082 dans le champ prévu à cet effet.

h. Pour Remote Security Group Type, sélectionnez **Subnet**. Saisissez les paramètres du réseau local du RV082 dans les champs *IP Address* et *Subnet Mask*.

i. Dans la section IPSec Setup, sélectionnez les paramètres appropriés pour le cryptage, l'authentification et d'autres options essentielles de gestion.

j. Dans le champ *Preshared Key*, saisissez une chaîne pour cette clé. Par exemple, 13572468.

Paramètres de configuration IPSec du RVS4000



k. Pour afficher des paramètres plus détaillés, cliquez sur **Advanced Settings**. Sinon, cliquez sur **Save** et passez à l'étape suivante, « Configuration du RV082 ».

ÉTAPE 2 Configuration du RV082.

Les instructions sont similaires pour le RV082.

a. Lancez le navigateur Web pour un ordinateur en réseau, appelé Ordinateur 2.

b. Accédez à l'utilitaire de configuration du RV082. (Pour obtenir plus de détails, reportez-vous au guide d'administration du RV082.)

c. Cliquez sur l'onglet **IPSec VPN**.

d. Cliquez sur l'onglet **Gateway to Gateway**.

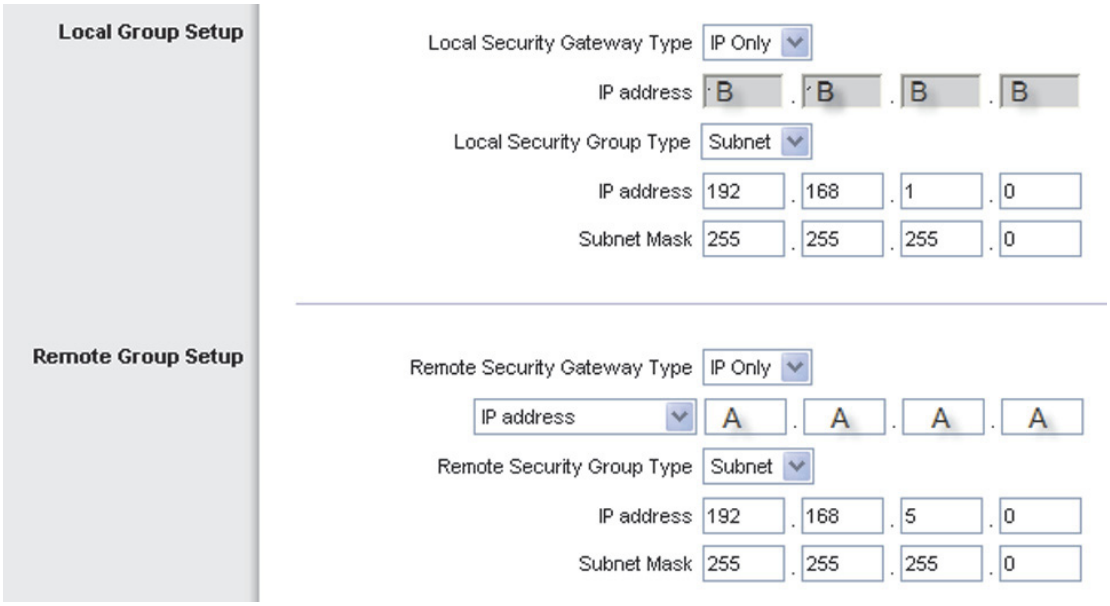
e. Saisissez un nom dans le champ *Tunnel Name*.

f. Pour le paramètre VPN Tunnel, sélectionnez **Enable**.

g. L'adresse IP WAN (B.B.B.B) du RV082 sera automatiquement détectée.

Pour Local Security Group Type, sélectionnez **Subnet**. Saisissez les paramètres du réseau local du RV082 dans les champs *IP Address* et *Subnet Mask*.

Paramètres VPN du RV082



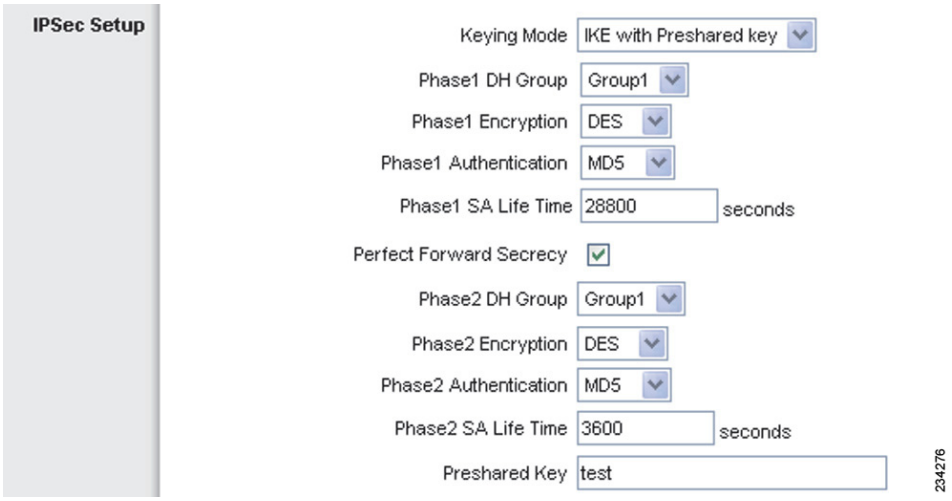
h. Pour Remote Security Gateway Type, sélectionnez **IP address**. Entrez l'adresse IP WAN du RVS4000 dans le champ *IP Address*.

i. Pour Remote Security Group Type, sélectionnez **Subnet**. Saisissez les paramètres du réseau local du RVS4000 dans les champs *IP Address* et *Subnet Mask*.

j. Dans la section IPSec Setup, sélectionnez les paramètres appropriés pour le cryptage, l'authentification et d'autres options essentielles de gestion. (Ils doivent correspondre aux paramètres du RVS4000.)

k. Dans le champ *Preshared Key*, saisissez une chaîne pour la clé pré-partagée, par exemple 13572468.

Paramètres de configuration IPSec du RV082



l. Pour afficher des paramètres plus détaillés, cliquez sur **Advanced Settings**. Sinon, cliquez sur **Save**.

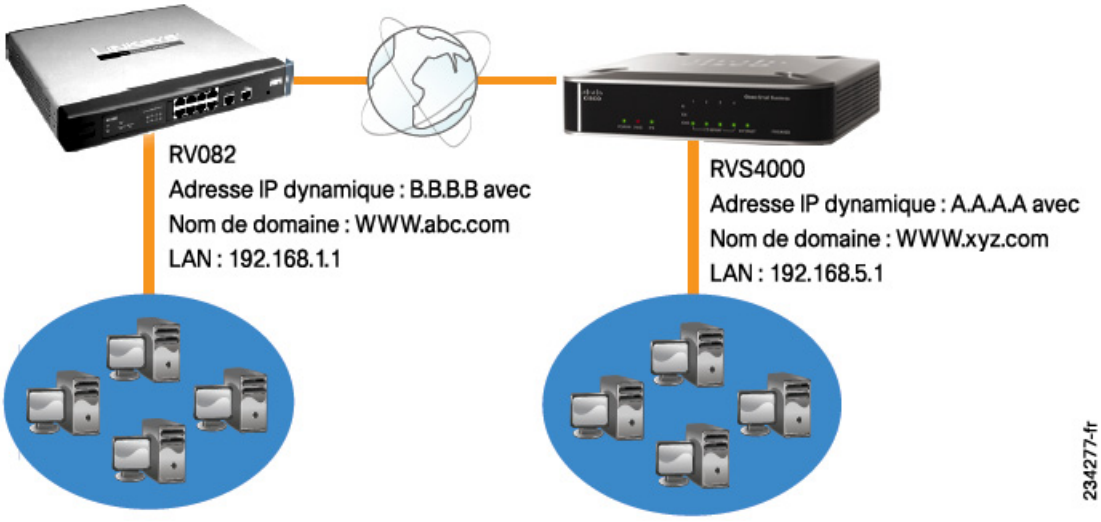
ÉTAPE 3 Configuration de l'Ordinateur 1 et de l'Ordinateur 2.

Vérifiez que l'Ordinateur 1 et l'Ordinateur 2 peuvent exécuter une commande ping l'un sur l'autre (reportez-vous à l'aide de Windows pour obtenir plus d'informations). Si les ordinateurs sont en mesure d'exécuter l'un sur l'autre une commande ping, vous avez l'assurance que le tunnel VPN est configuré correctement.

Configuration lorsque les deux passerelles utilisent une adresse IP dynamique

Dans cet exemple, il est supposé que les deux passerelles utilisent une adresse IP dynamique. Si la passerelle distante est la seule à utiliser une adresse IP dynamique, reportez-vous à **« Configuration lorsque la passerelle distante utilise une adresse IP dynamique », page 176**.

Tunnel VPN IPSec de passerelle à passerelle, les deux passerelles utilisant une adresse IP dynamique



REMARQUE Chaque ordinateur doit être équipé d'un adaptateur réseau.

ÉTAPE 1 Configuration du RVS4000.

Suivez ces instructions pour le premier routeur VPN, appelé RVS4000. L'autre routeur VPN est appelé RV082.

a. Lancez le navigateur Web pour un ordinateur en réseau, appelé Ordinateur 1.

b. Accédez à l'utilitaire de configuration du RVS4000. (Pour obtenir plus de détails, reportez-vous au **Chapitre 5, « Configuration du routeur »**.)

c. Cliquez sur **VPN > IPSec VPN**.

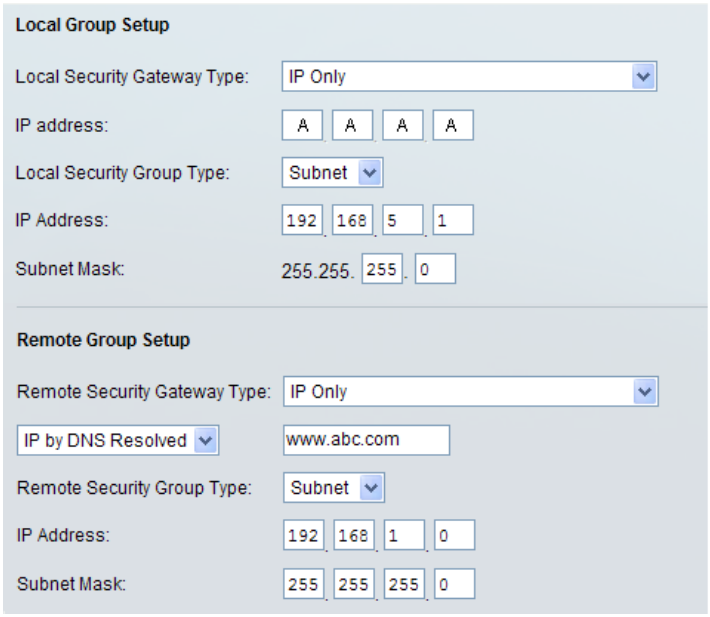
d. Saisissez un nom dans le champ *Tunnel Name*.

e. Pour le paramètre IPSec VPN Tunnel, sélectionnez **Enable**.

f. L'adresse IP WAN (A.A.A.A) du RVS4000 sera automatiquement détectée.

Pour Local Security Group Type, sélectionnez **Subnet**. Saisissez les paramètres du réseau local du RVS4000 dans les champs *IP Address* et *Subnet Mask*.

Paramètres VPN IPSec du RVS4000



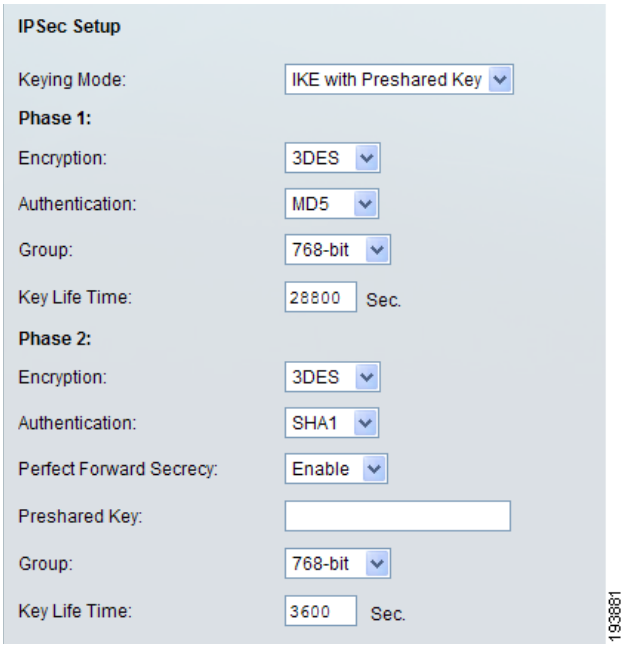
g. Pour Remote Security Gateway Type, sélectionnez **IP by DNS Resolved**. Saisissez le nom de domaine du RV082 dans le champ prévu à cet effet.

h. Pour Remote Security Group Type, sélectionnez **Subnet**. Saisissez les paramètres du réseau local du RV082 dans les champs *IP Address* et *Subnet Mask*.

i. Dans la section IPSec Setup, sélectionnez les paramètres appropriés pour le cryptage, l'authentification et d'autres options essentielles de gestion.

j. Dans le champ *Preshared Key*, saisissez une chaîne pour la clé pré-partagée, par exemple 13572468.

Paramètres de configuration IPSec du RVS4000



k. Pour afficher des paramètres plus détaillés, cliquez sur **Advanced Settings**. Sinon, cliquez sur **Save** et passez à l'étape suivante, « Configuration du RV082 ».

ÉTAPE 2 Configuration du RV082.

Les instructions sont similaires pour le RV082.

a. Lancez le navigateur Web pour un ordinateur en réseau, appelé Ordinateur 2.

b. Accédez à l'utilitaire de configuration du RV082. (Pour obtenir plus de détails, reportez-vous au guide d'administration du RV082.)

c. Cliquez sur l'onglet **IPSec VPN**.

d. Cliquez sur l'onglet **Gateway to Gateway**.

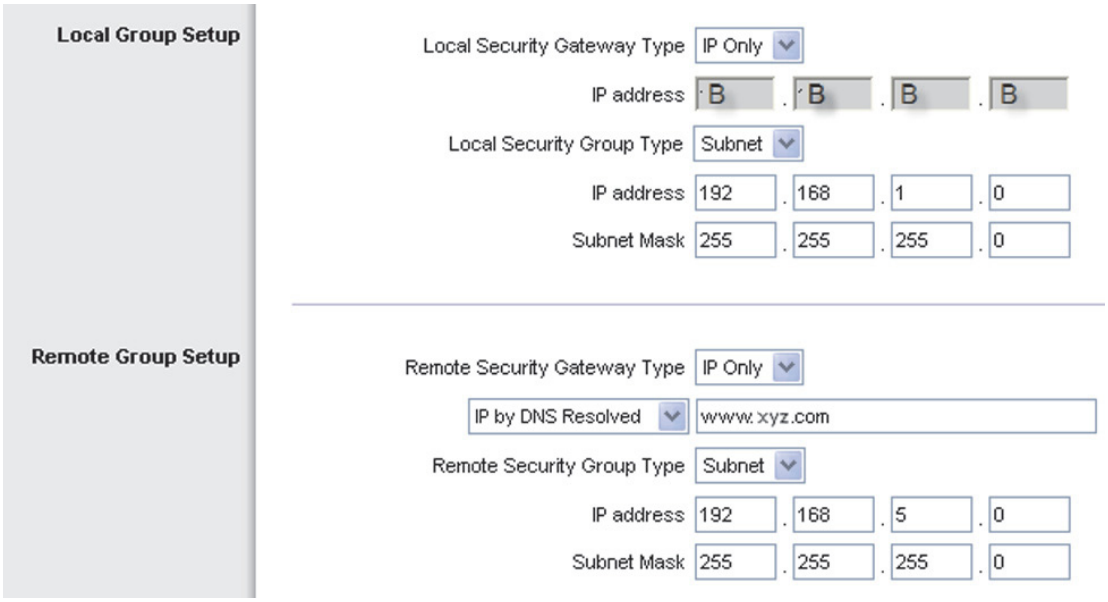
e. Saisissez un nom dans le champ *Tunnel Name*.

f. Pour le paramètre VPN Tunnel, sélectionnez **Enable**.

g. L'adresse IP WAN (B.B.B.B) du RV082 sera automatiquement détectée.

Pour Local Security Group Type, sélectionnez **Subnet**. Saisissez les paramètres du réseau local du RV082 dans les champs *IP Address* et *Subnet Mask*.

Paramètres VPN du RV082



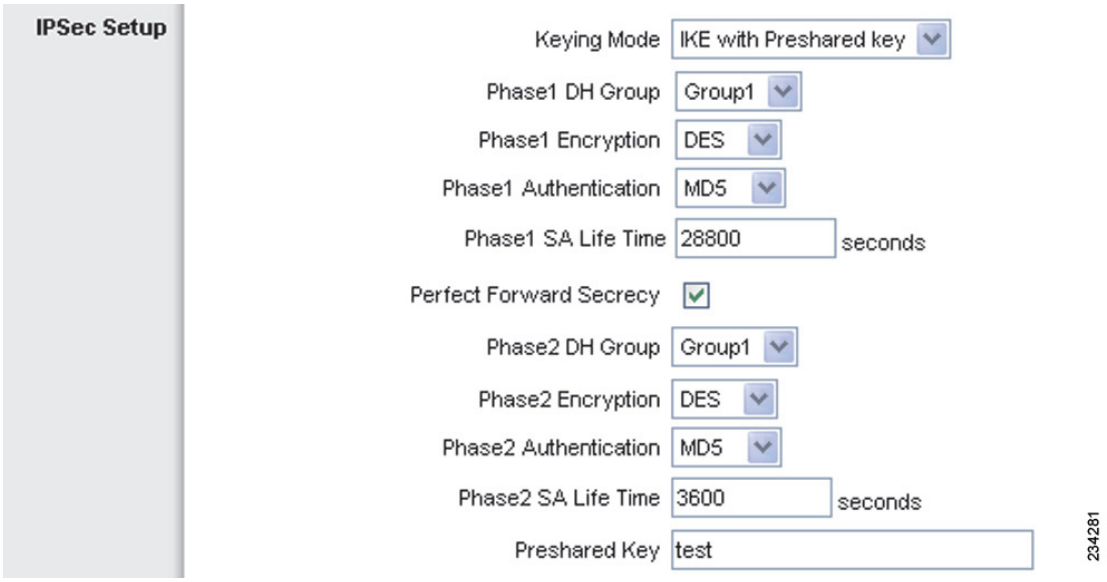
h. Pour Remote Security Gateway Type, sélectionnez **IP by DNS Resolved**. Saisissez le nom de domaine du RVS4000 dans le champ prévu à cet effet.

i. Pour Remote Security Group Type, sélectionnez **Subnet**. Saisissez les paramètres du réseau local du RVS4000 dans les champs *IP Address* et *Subnet Mask*.

j. Dans la section IPSec Setup, sélectionnez les paramètres appropriés pour le cryptage, l'authentification et d'autres options essentielles de gestion. (Ils doivent correspondre aux paramètres du RVS4000.)

k. Dans le champ *Preshared Key*, saisissez une chaîne pour la clé pré-partagée, par exemple 13572468.

Paramètres de configuration IPSec du RV082



l. Pour afficher des paramètres plus détaillés, cliquez sur **Advanced Settings**. Sinon, cliquez sur **Save**.

ÉTAPE 3 Configuration de l'Ordinateur 1 et de l'Ordinateur 2.

Vérifiez que l'Ordinateur 1 et l'Ordinateur 2 peuvent exécuter une commande ping l'un sur l'autre (reportez-vous à l'aide de Windows pour obtenir plus d'informations). Si les ordinateurs sont en mesure d'exécuter l'un sur l'autre une commande ping, vous avez l'assurance que le tunnel VPN est configuré correctement.

E

Spécifications

Cette annexe décrit les spécifications du routeur de sécurité Gigabit 4 ports avec VPN Cisco RVS4000.

Spécifications

Modèle	RVS4000
Normes	IEEE802.3, 802.3u, 802.1X, RFC791 (protocole IP), RFC2460, IPv4 (RFC791), IPv6 (RFC2460), RIPv1 (RFC1058), RIPv2 (RFC1723)
Ports	ETHERNET, POWER
Boutons	RESET
Type de câblage	UTP Catégorie 5e ou ultérieure
DEL	POWER, DIAG, IPS, ETHERNET (1 à 4), INTERNET
Système d'exploitation	Linux

Performances

Débit du NAT	800 Mbit/s lorsque IPS est désactivée

Installation/Configuration

Interface utilisateur Web	Interface utilisateur Web intégrée pour une configuration facile par navigateur (HTTP/HTTPS)

Gestion

Version SNMP	SNMP versions 1, 2c
Consignation des événements	Locale, syslog, alertes e-mail
Firmware Upgrade	Disponibilité des microprogrammes par navigateur Web
Diagnostics	Flash, RAM

Fonctionnalités de sécurité

Contrôle d'accès	Capacité de liste de contrôle d'accès : basée sur MAC et sur IP
Pare-feu	Pare-feu SPI (Stateful Packet Inspection)
Filtrage du contenu	Blocage de l'URL statique ou du mot de passe (compris), filtrage dynamique via le service de sécurité Trend Micro™ ProtectLink™ Gateway (en option)
Système de prévention des intrusions (IPS)	Détection par balayage IP, détection d'une anomalie dans l'application (HTTP, FTP, Telnet, RCP), contrôle P2P, contrôle de la messagerie instantanée, normalisation des protocoles de niveaux 3 et 4 (IP, TCP, UDP, ICMP), correspondance des signatures de niveau 7.
Gestion sécurisée	HTTPS, nom d'utilisateur/mot de passe
802.1X	Authentification RADIUS basée sur les ports (EAP-MD5, EAP-PEAP)

Qualité de service

Basée sur le service	La gestion de bande passante basée sur le service prend en charge la priorité et le contrôle du débit
Types de hiérarchisation	802.1p, DSCP et basée sur les ports
Files d'attente	4 files d'attente

Réseau

DHCP	Serveur DHCP, client DHCP, agent de relais DHCP
DNS	Relais DNS, DNS dynamique (DynDNS, TZO)
NAT	PAT, NAPT
DMZ	Logiciel configurable sur tout type de configuration de port LAN, DHCPv6, ICMPv6
IPv6	Double pile IPv4 et IPv6, 6to4, configuration automatique des adresses sans état
DHCP statique	Le serveur DHCP prend en charge une adresse IP statique basée sur une adresse MAC

VPN

	5 tunnels QuickVPN pour l'accès client à distance ; 5 tunnels passerelle à passerelle IPSec pour la connectivité des bureaux distants ; Cryptage 3DES ; Authentification MD5/SHA1 ; NAT-T IPSec ; Passthrough VPN pour les protocoles PPTP, L2TP et IPSec

Routage

	Routage statique et routage Inter-VLAN RIP v1, v2

Couche 2

VLAN	VLAN basés sur les marquages 802.1Q et sur les ports
Nombre de VLAN	Prend en charge 4 VLAN 802.1Q (ID VLAN comprise entre 1 et 4 094)
Mise en miroir des ports	L'un des cinq ports WAN/LAN peut être mis en miroir sur un port LAN sélectionné
RSTP	Prend charge le protocole RSTP (Rapid Spanning Tree Protocol) pour une détection multiplex et une reconfiguration plus rapide

Environnement

Dimensions	170 mm x 41 mm x 170 mm
L x H x P	(6,69 po x 1,61 po x 6,69 po)
Poids unitaire	0,38 kg (0,84 lb)
Alimentation	12 V 1 A
Certification	FCC Classe B, CE, ICES-003
Température de fonctionnement	De 0 à 40 °C (de 32 à 104 °F)
Température de stockage	De –20 à 70 °C (de –4 à 158 °F)
Humidité de fonctionnement	De 10 à 85 % sans condensation
Humidité de stockage	De 5 à 90 % sans condensation

Les caractéristiques peuvent être modifiées sans préavis.

F

Pour en savoir plus

Cisco propose un vaste choix de ressources qui vous aident, ainsi que vos clients, à profiter pleinement de tous les avantages du routeur de sécurité Gigabit 4 ports avec VPN Cisco RVS4000.

Ressources sur les produits

Assistance technique	
Communauté d'assistance Cisco Small Business	www.cisco.com/go/smallbizsupport
Assistance technique et documentation en ligne	www.cisco.com/go/smallbizhelp
Coordonnées de l'assistance téléphonique	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Téléchargement de micrologiciels Cisco Small Business	www.cisco.com/go/smallbizfirmware Des logiciels supplémentaires pour le routeur RVS4000 sont disponibles dans l'espace de téléchargement du site Cisco.com, à l'adresse www.cisco.com/go/software (inscription/connexion requise).
Documentation sur les produits	
Routeurs Cisco Small Business : ressources	www.cisco.com/go/smallbizrouters

Cisco Small Business	
Site Cisco Partner Central pour les PME (identifiant de connexion partenaire obligatoire)	www.cisco.com/web/partners/sell/smb
Accueil Cisco Small Business	www.cisco.com/smb

Documentation associée

Concernant la configuration matérielle du routeur Cisco RVS4000, reportez-vous au document *Cisco Small Business Model RVS4000 4-Port Gigabit Security Router with VPN Quick Start Guide*.

Pour obtenir des informations relatives à la conformité et à la sécurité de l'équipement, reportez-vous au document *Regulatory Compliance and Safety Information for the Cisco Wired and Wireless Routers and Access Point Devices (EMC Class B Devices)*.