



 **TheGreenBow IPsec VPN Client**  
**Guide de Configuration**  
**Windows 2000 Server**

WebSite : <http://www.thegreenbow.com>  
Contact : [support@thegreenbow.com](mailto:support@thegreenbow.com)

## Table of contents

1	Introduction.....	0
1.1	But du document.....	0
1.2	Description de l'environnement réseau.....	0
2	Configuration du serveur Windows 2000 Server.....	0
3	TheGreenBow IPSec VPN Client configuration.....	0
3.1	VPN Client Phase 1 (IKE) Configuration.....	0
3.2	VPN Client Phase 2 (IPSec) Configuration.....	0
4	Ouvrir le tunnel.....	0
5	En cas de problème.....	0
5.1	Un analyseur réseau : ethereal.....	0
5.2	Netdiag.exe.....	0
6	Contacts.....	0

	Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	Doc.version	1.0 – Mai 2004
	VPN version	2.x

# 1 Introduction

## 1.1 But du document

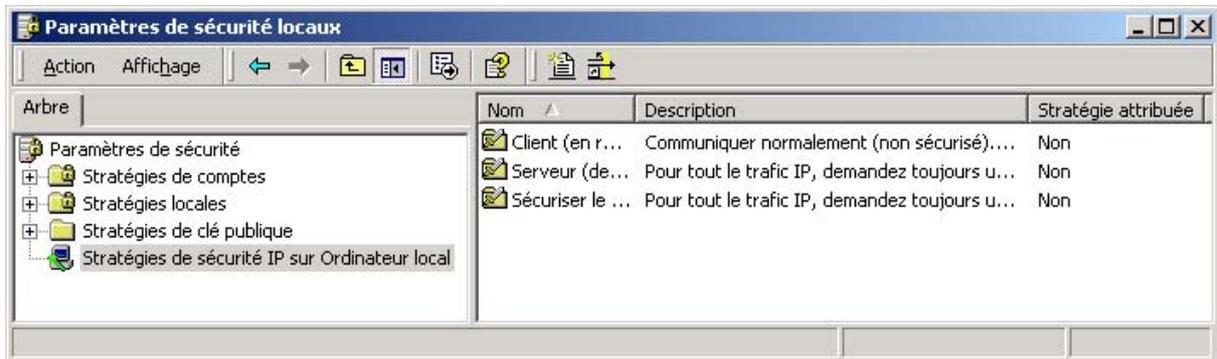
Ce document décrit la configuration du Client IPSec VPN TheGreenBow avec un serveur Windows 2000 Server.

## 1.2 Description de l'environnement réseau

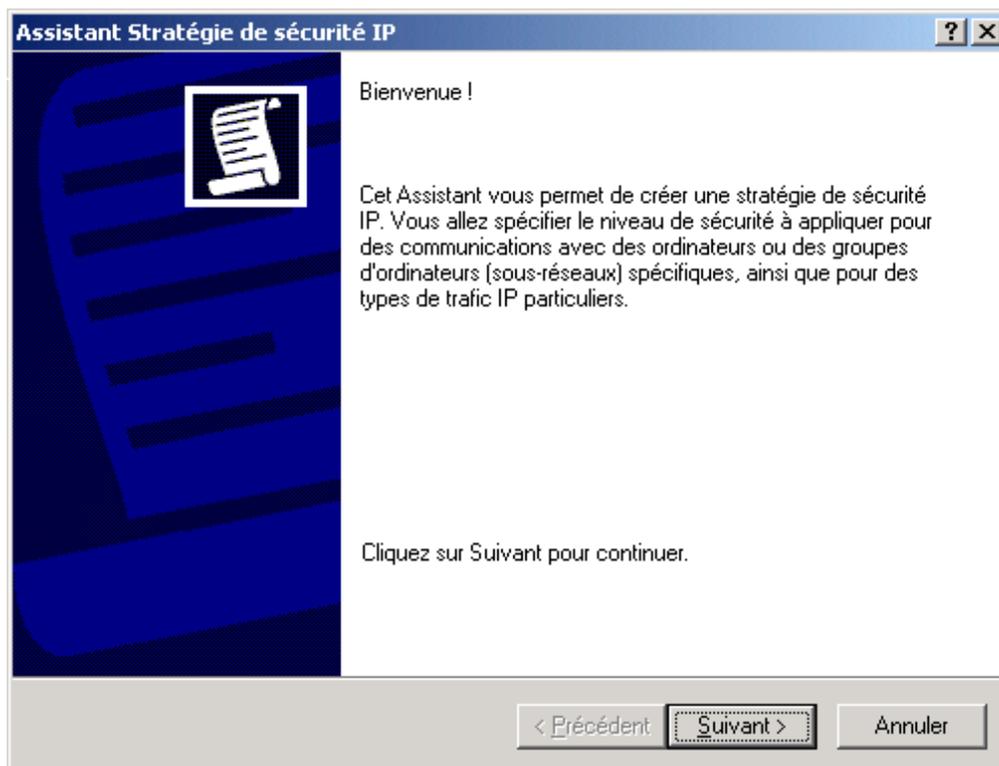
Dans notre document, nous décrivons un exemple de connexion entre le Client IPSec VPN TheGreenBow et un poste sous Windows 2000 Server. Les deux ordinateurs sont dans le même réseau local. Le Client IPSec VPN TheGreenBow a pour adresse IP 192.168.1.3 tandis que le serveur Windows 2000 Server a pour adresse IP 192.168.1.2. Toutes les adresses dans ce document sont données à titre d'exemple.

## 2 Configuration du serveur Windows 2000 Server

- Pour accéder à la configuration IPSec sous Microsoft Windows 2000 Server, cliquez sur Démarrer , Programmes, Outils d'administration, Stratégie de sécurité locale.



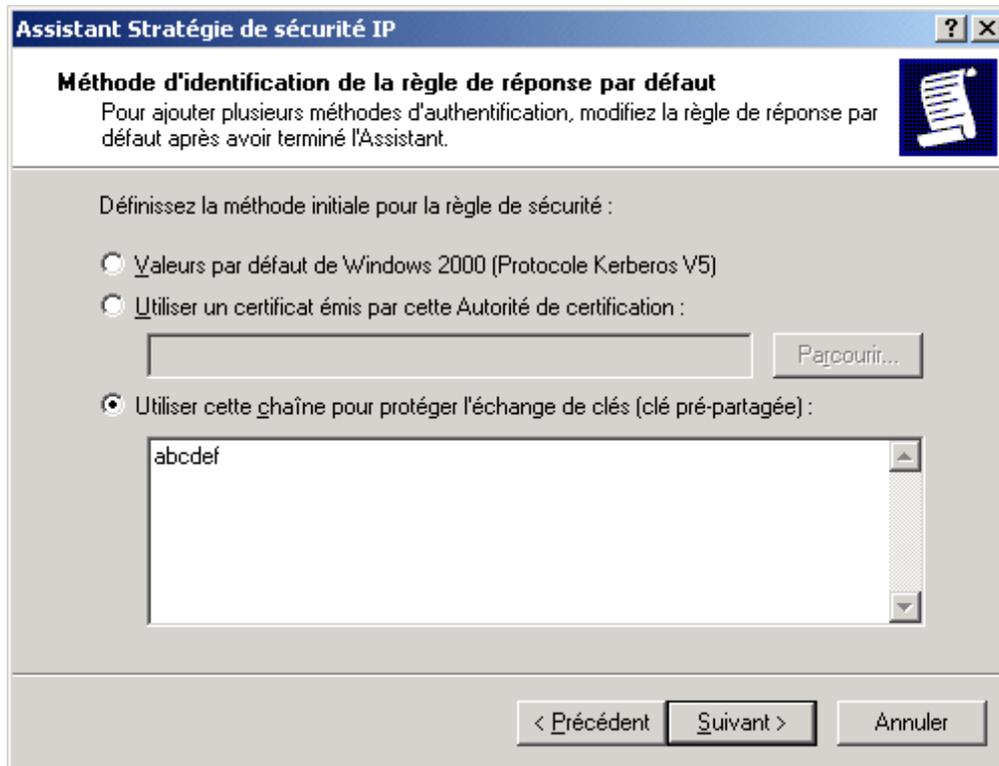
- Cliquez avec le bouton droit de la souris sur « Stratégies de sécurité IP sur Ordinateur local », puis avec le bouton gauche sur « Créer une stratégie de sécurité IP ». L'assistant de configuration de la stratégie de sécurité apparaît. Cliquez sur « Suivant ».



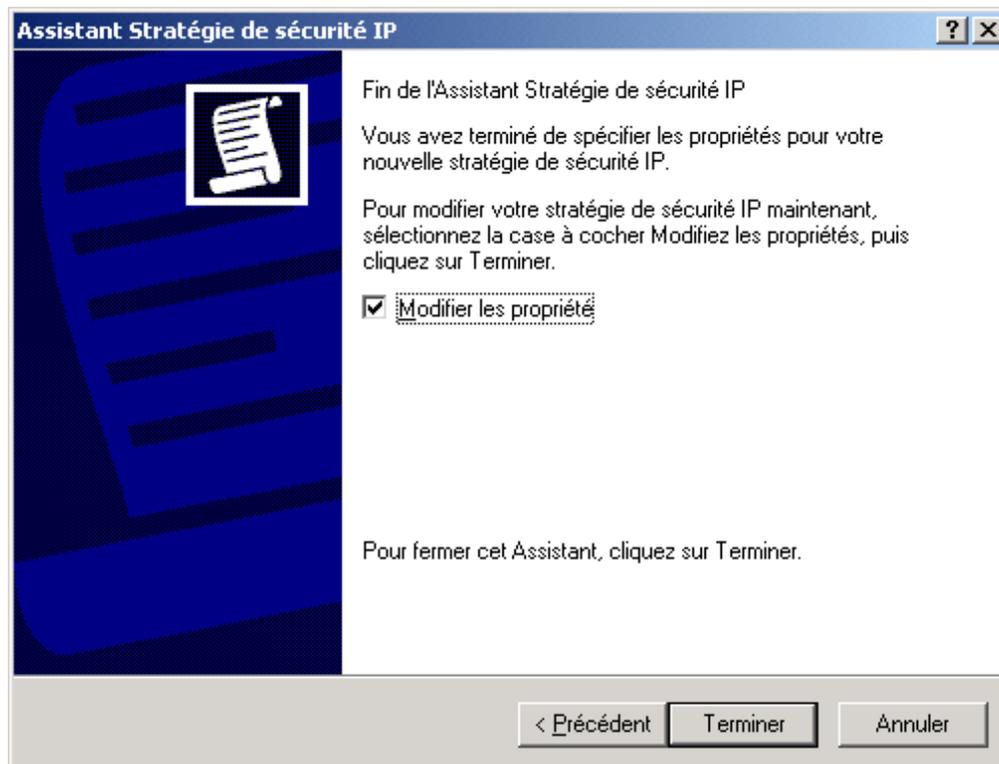
- Donnez un nom à votre règle de sécurité et éventuellement une description. Puis cliquez sur « Suivant ».

- Cliquez sur « Suivant ».

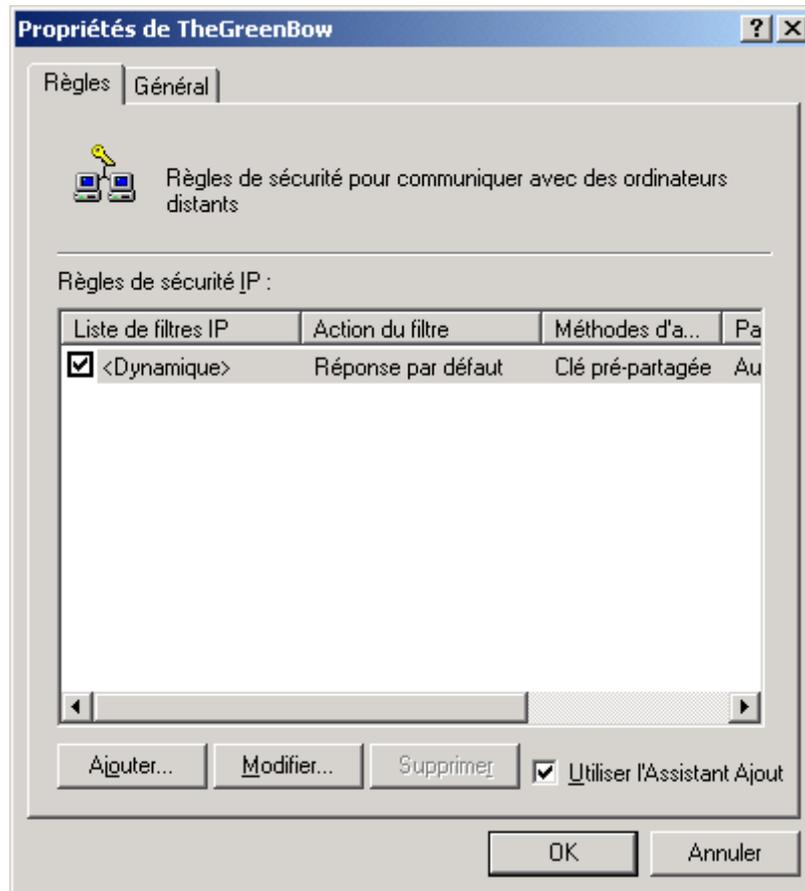
- Cliquez sur « **Utiliser cette chaîne pour protéger l'échange de clés** » et indiquez la clé partagée. Cette valeur sera aussi utilisée par le Client VPN. Puis cliquez sur « **Suivant** ».



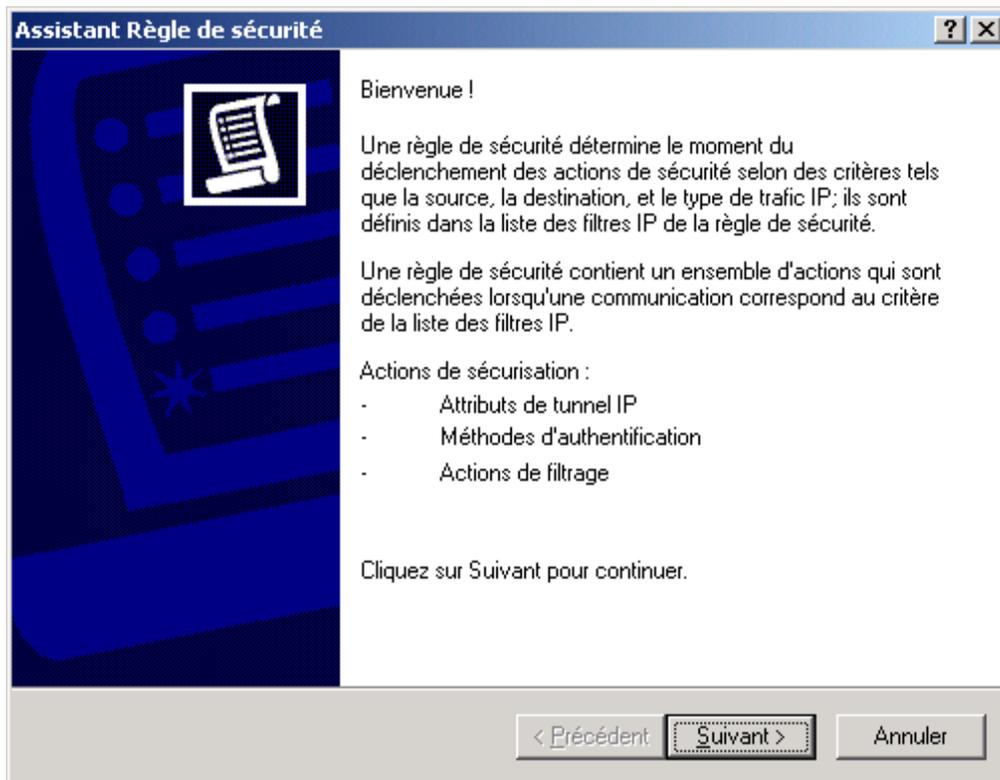
- Pour terminer la création de la stratégie de sécurité, cliquez sur « **Suivant** ».



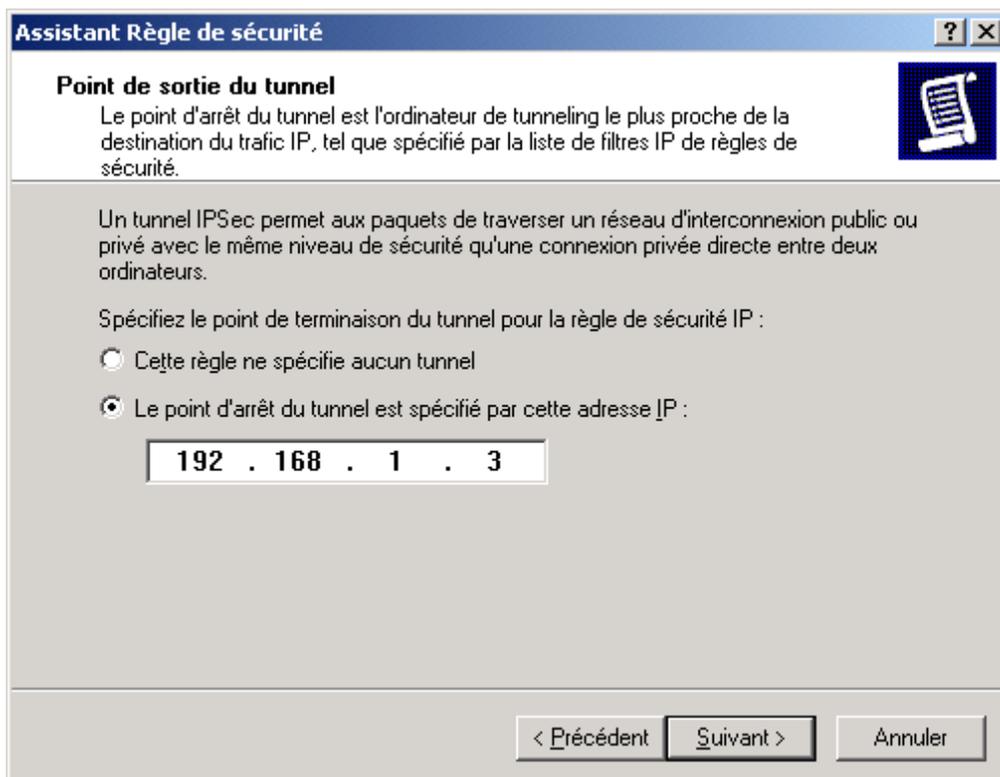
- Décocher la « réponse par défaut » puis cliquez sur « Ajouter ». Nous allons maintenant ajouter une règle de sécurité pour le serveur Windows 2000.



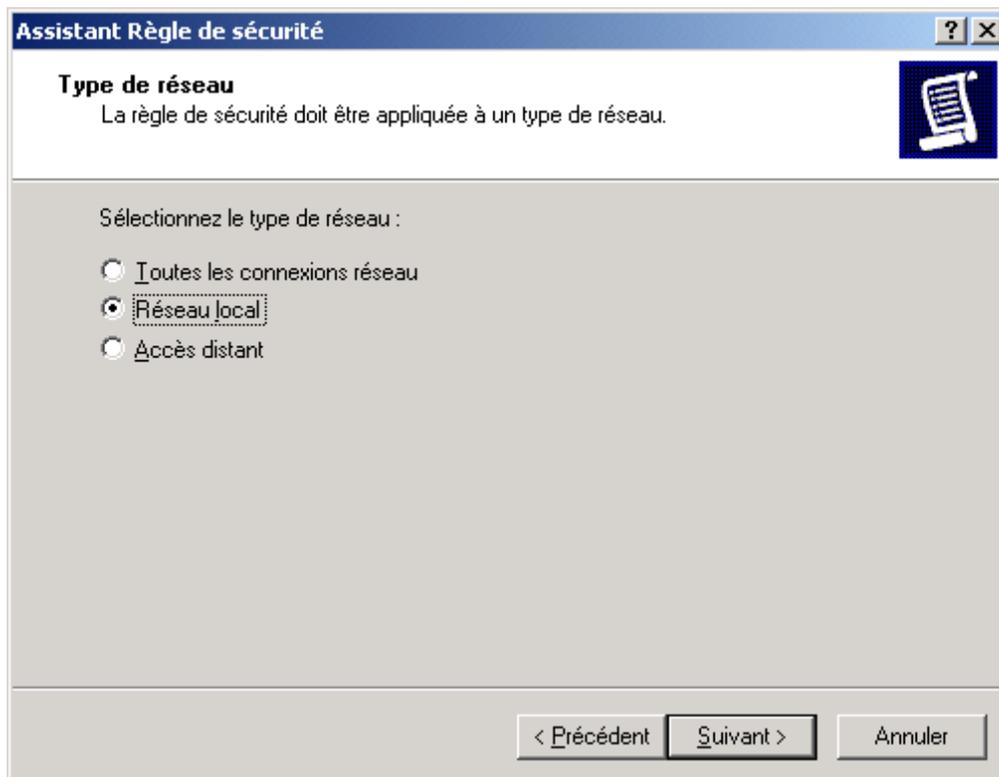
- Cliquez sur « Suivant ».



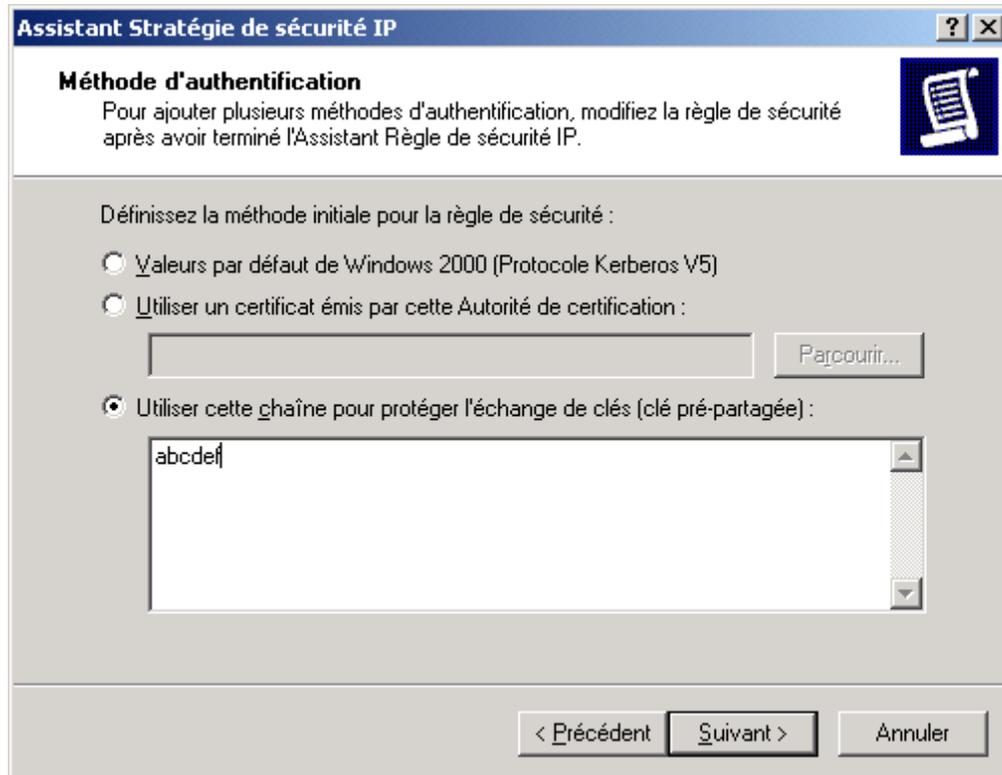
- La règle sécurité décrit un tunnel IPSec entre le serveur Microsoft Windows 2000 et le Client IPSec VPN TheGreenBow. La terminaison du tunnel VPN étant le Client IPSec VPN en 192.168.1.3, tapez cette adresse IP puis cliquez sur « Suivant »



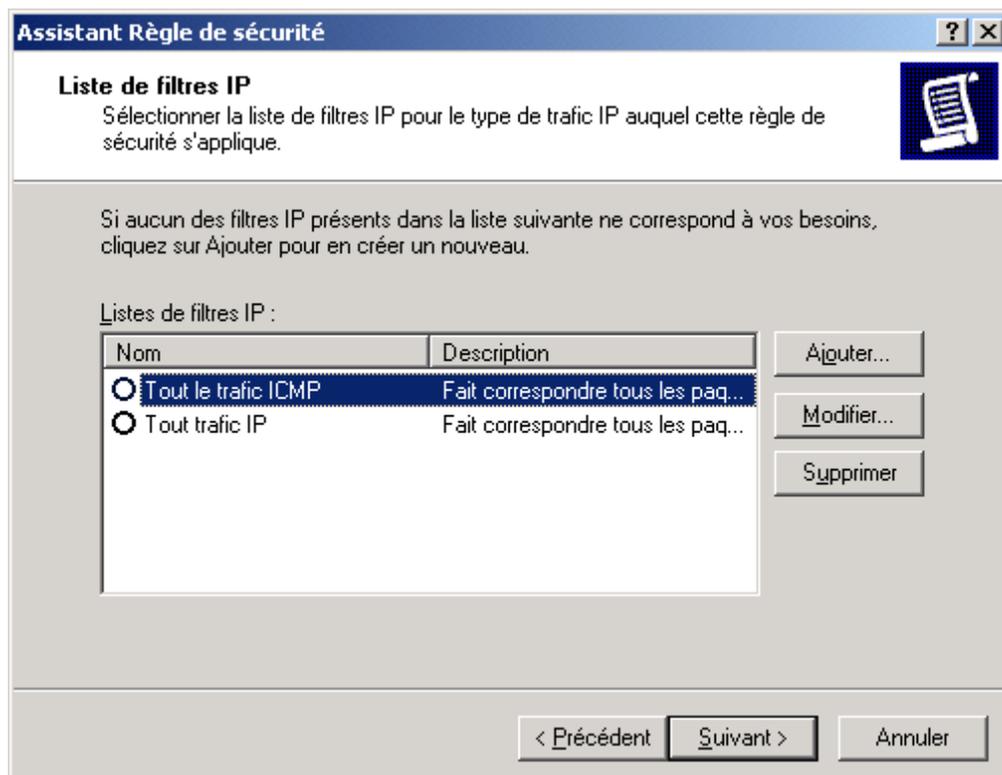
- Dans notre exemple, les ordinateurs sont dans le même réseau local. Cliquez sur « Réseau local » puis sur « Suivant ».



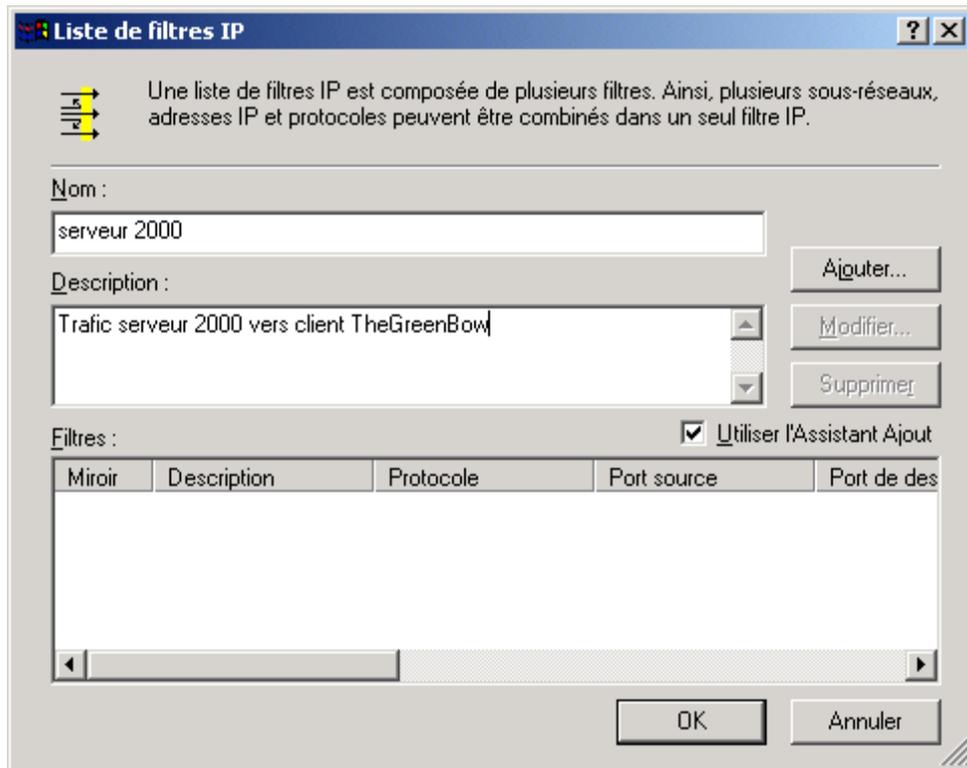
- La communication entre le serveur et le Client IPSec VPN est protégée par une clé partagée. Cliquez sur « **Utiliser cette chaîne pour protéger l'échange de clés** » et indiquez la clé partagée. Cliquez sur « **Suivant** ».



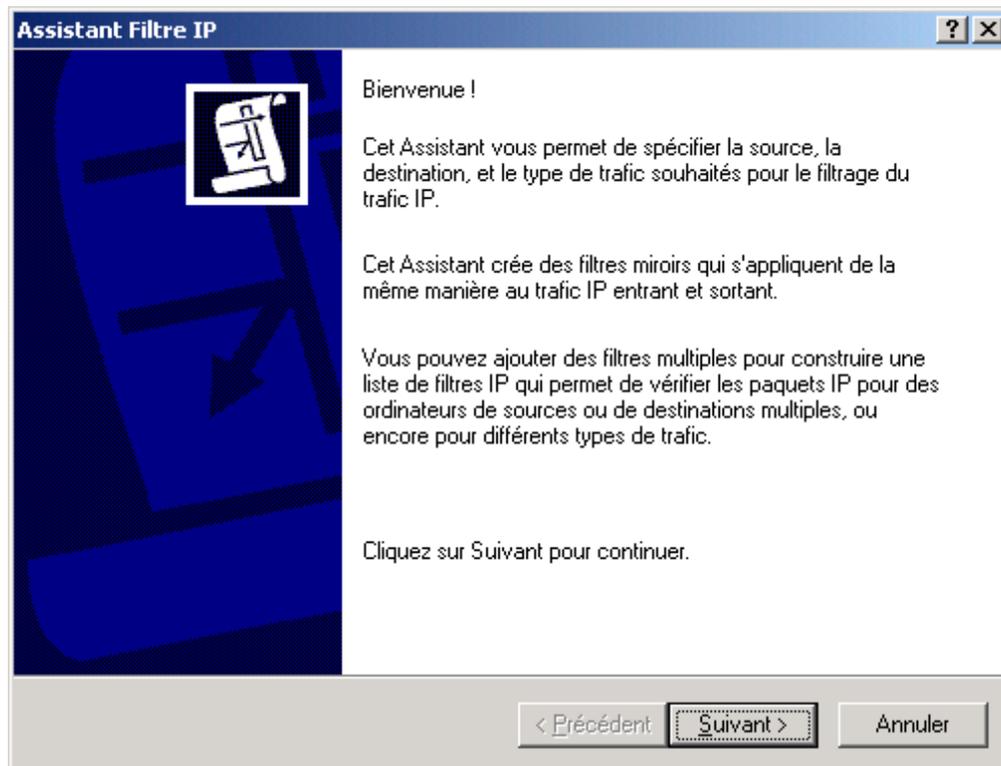
- Il faut maintenant associer une liste de filtre IP à notre règle de sécurité. Cliquez sur « **Ajouter** ».



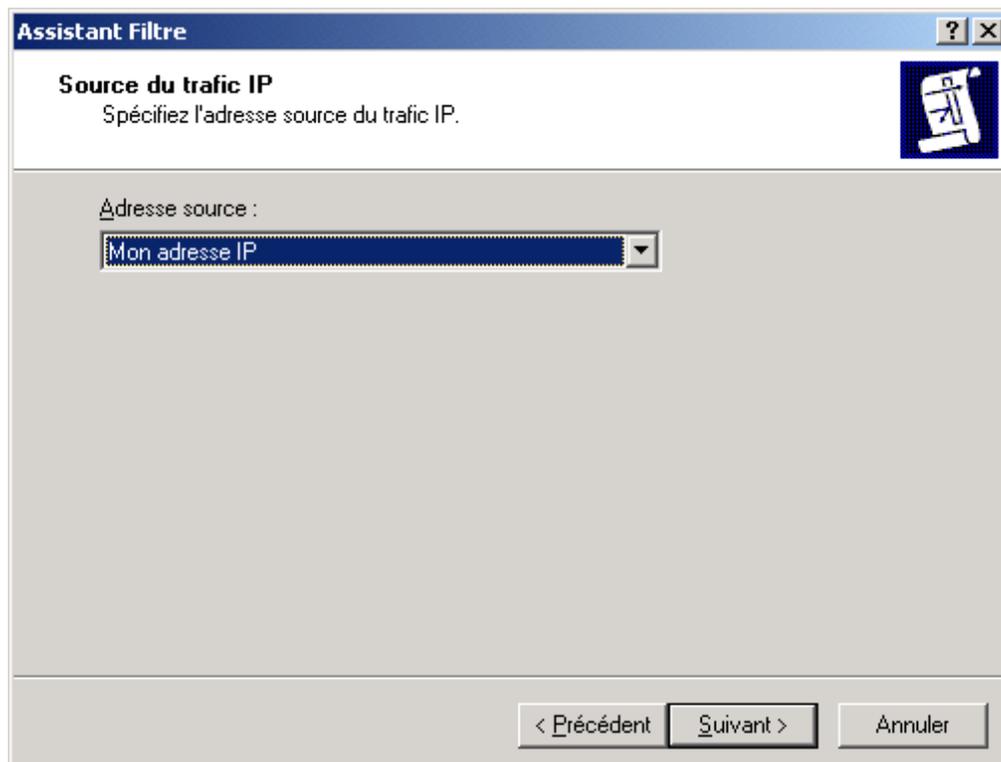
- Donner un nom au filtre IP et éventuellement une description. Puis cliquez sur « Ajouter ».



- L'assistant de configuration apparaît. Cliquez sur « Suivant ».



- Indiquez l'adresse IP du point de départ de la liaison VPN (le serveur Microsoft Windows 2000 Server). Puis cliquez sur « Suivant ».



- Indiquez l'adresse IP du point final de la liaison VPN (le Client IPsec VPN TheGreenBow). Puis cliquez sur « Suivant »

**Assistant Filtre** [?] [X]

**Destination du trafic IP**  
Spécifiez l'adresse de destination du trafic IP.

Adresse de destination :

Adresse IP :

Masque de sous-réseau :

< Précédent    Suivant >    Annuler

- Indiquez le type de protocole puis cliquez sur « Suivant ».

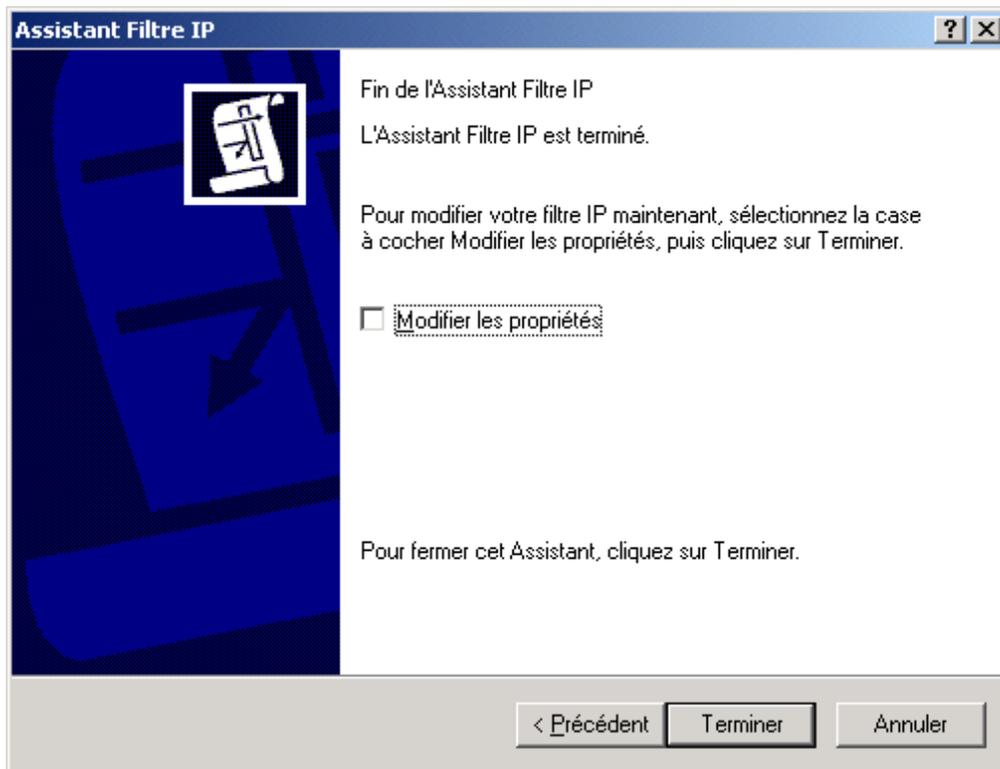
**Assistant Filtre** [?] [X]

**Type de protocole IP**  
Sélectionnez le type de protocole IP. Si ce type prend en charge les ports IP, vous spécifiez aussi le port IP.

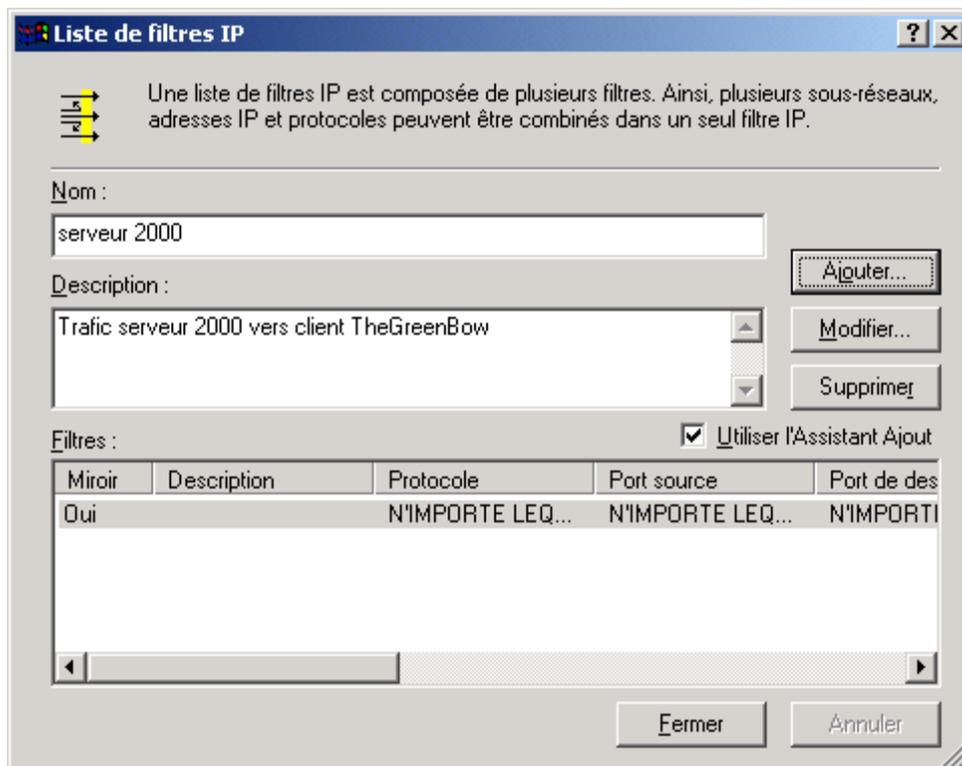
Sélectionnez un type de protocole :

< Précédent    Suivant >    Annuler

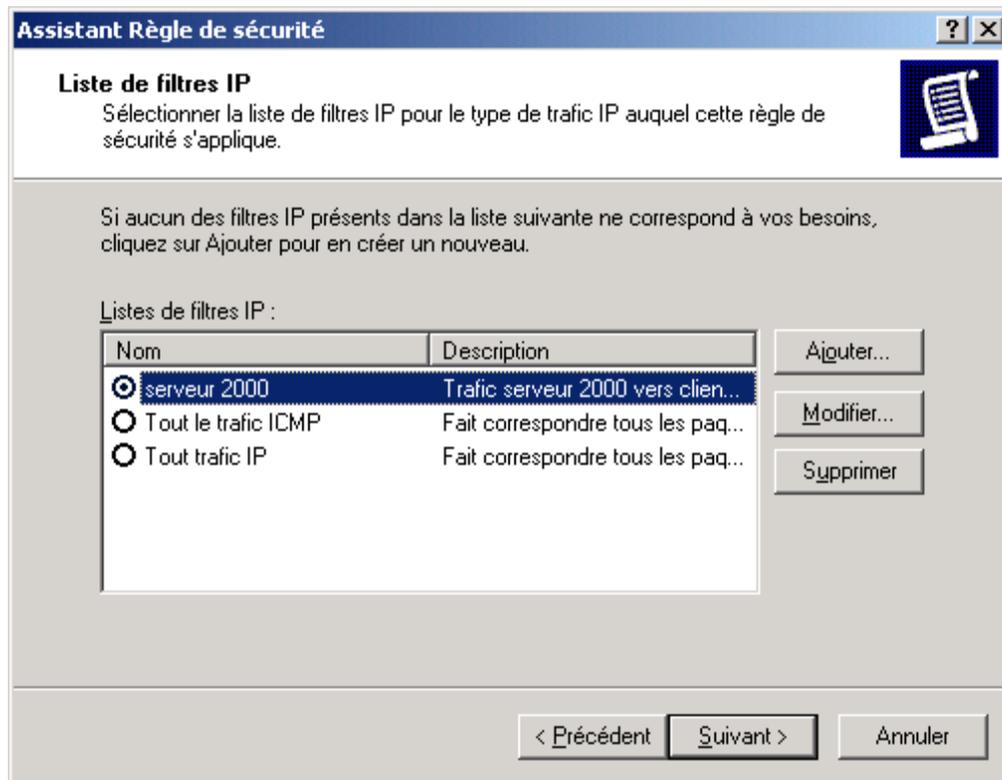
- Cliquez sur « **Suivant** » pour terminer la création du filtre IP.



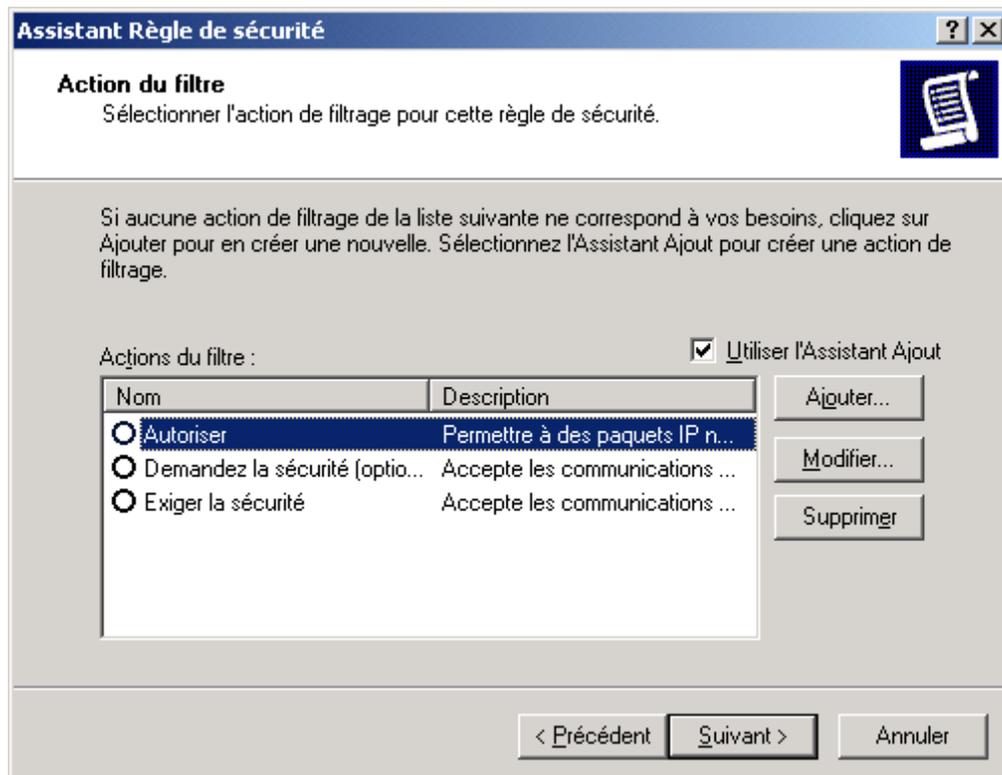
- Le filtre IP a été ajouté. Cliquez sur « **Fermer** »



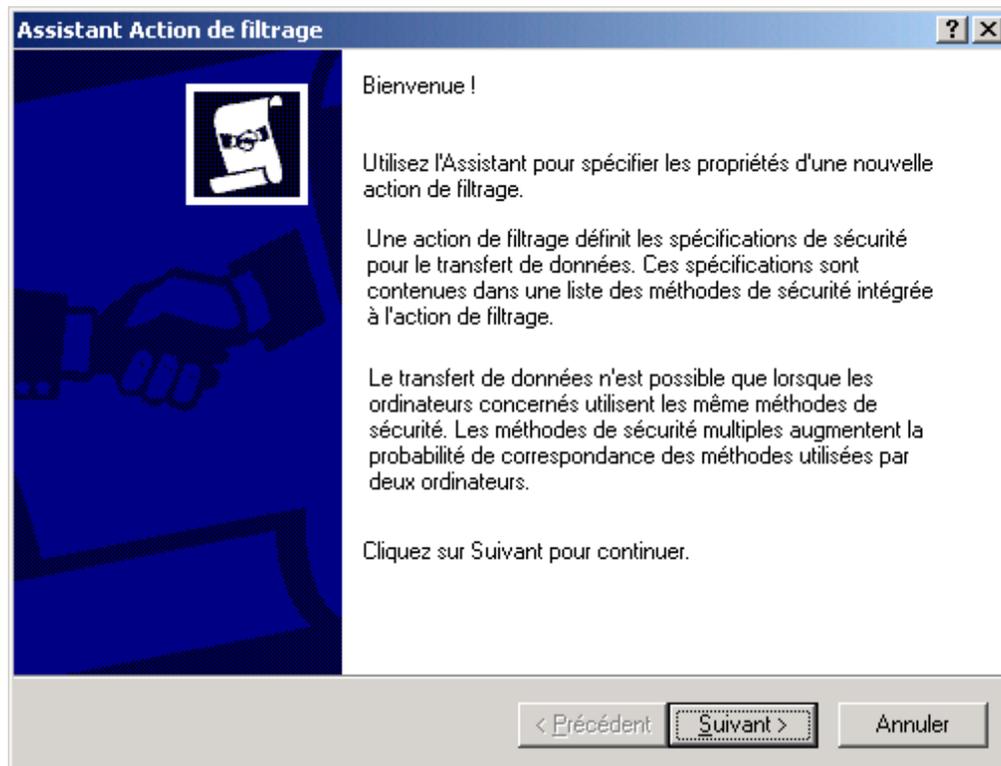
- Sélectionner dans la liste le filtre IP que vous venez de créer, puis cliquez sur « Suivant ».



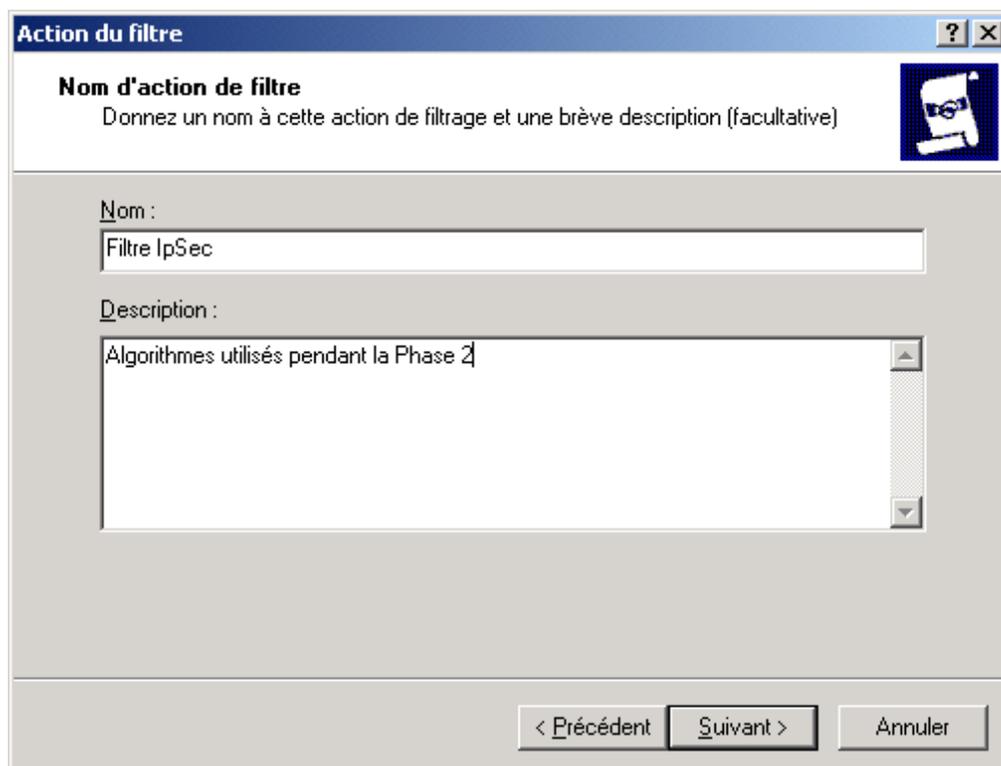
- Il faut associer une action de filtre à la règle de sécurité. Cliquez sur « Ajouter ».



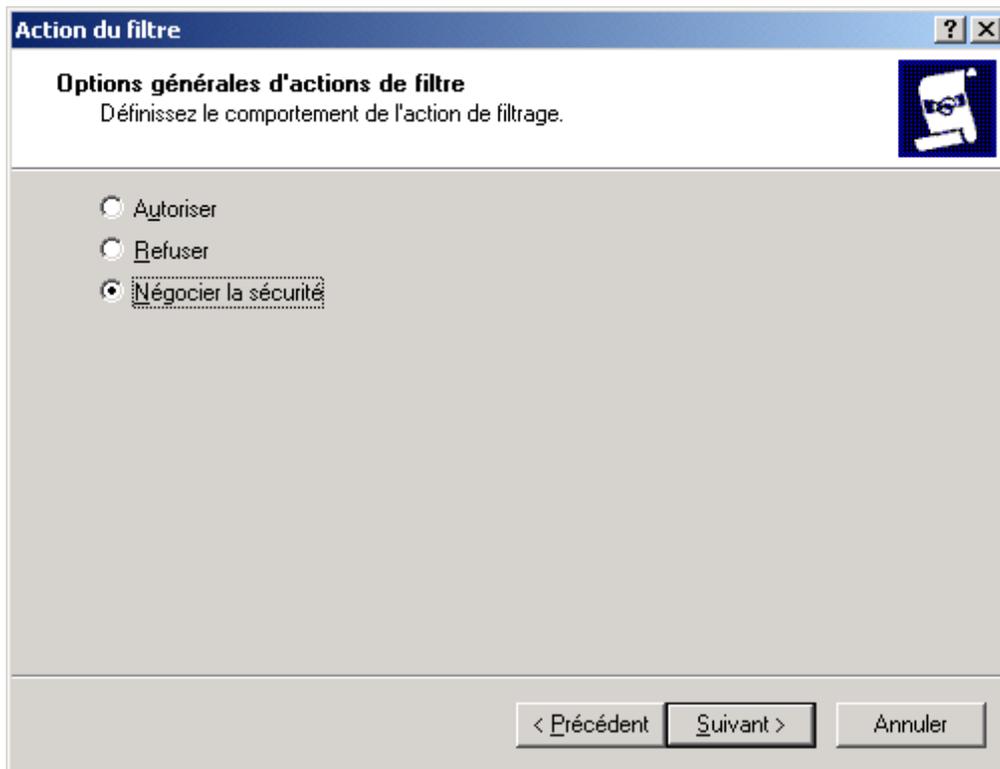
- Cliquez sur « Suivant ».



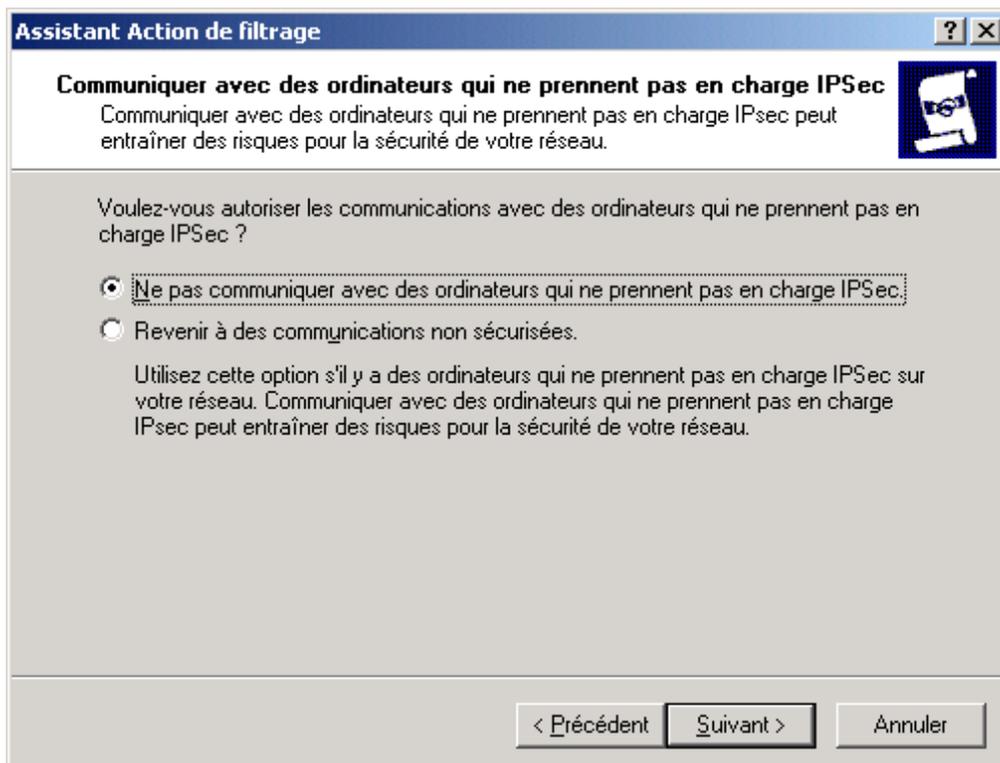
- Donner un nom à l'action du filtre puis cliquez sur « Suivant ».



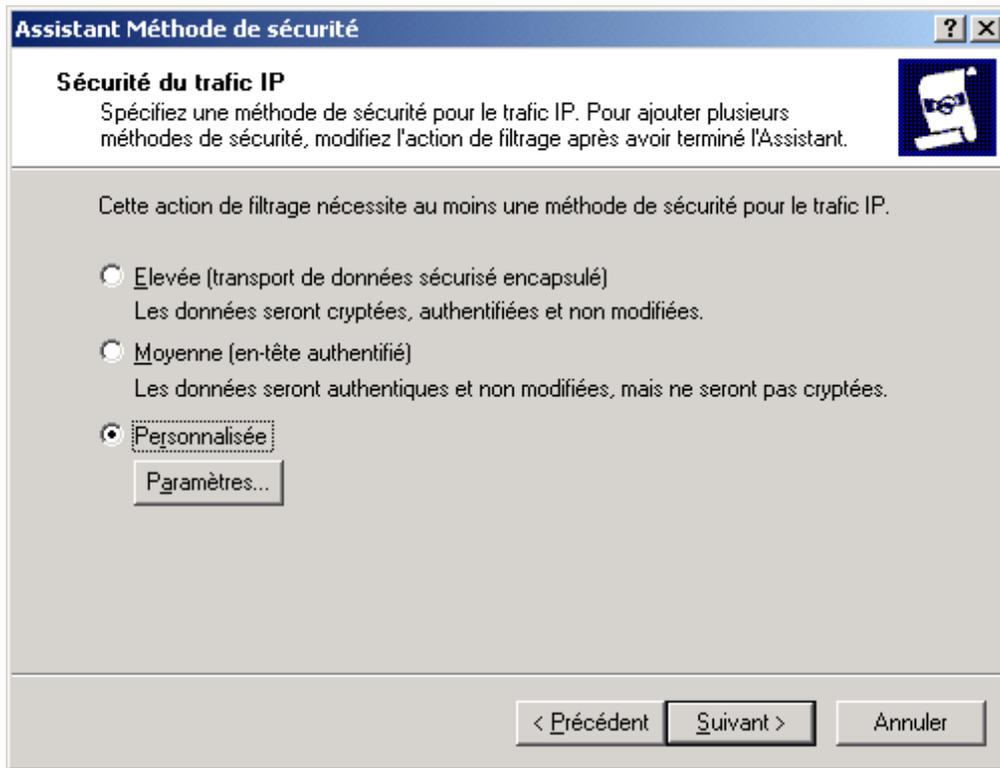
- Cliquez sur « **Négocier la sécurité** » puis sur « **Suivant** ».



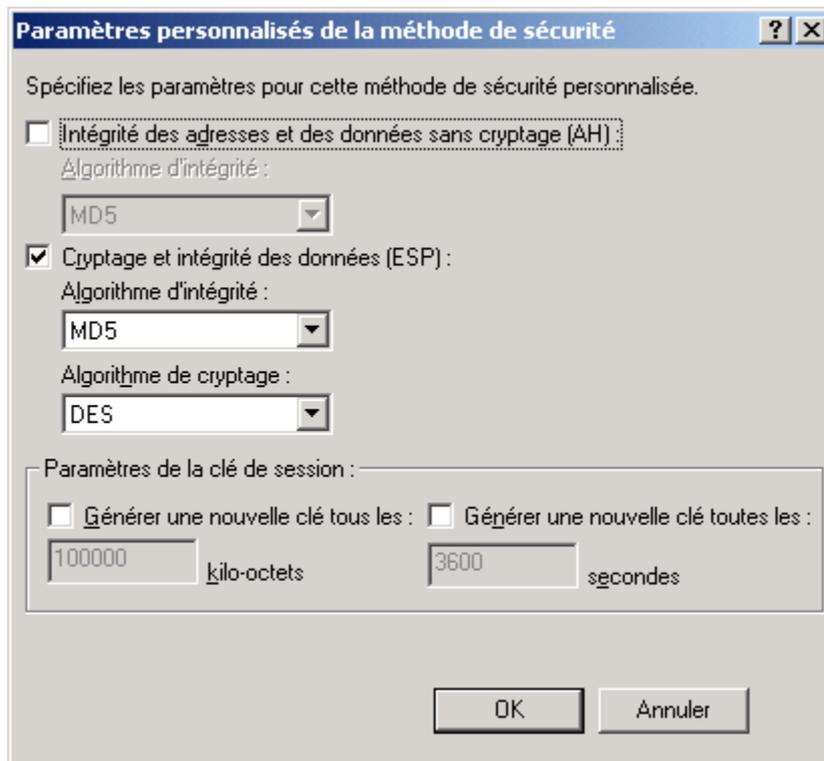
- Cliquez sur « **Ne pas communiquer avec des ordinateurs qui ne prennent pas en charge Ipsec** » si vous souhaitez que toute communication VPN entre le serveur et le Client IPsec VPN TheGreenBow soit sécurisée. Puis cliquez sur « **Suivant** ».



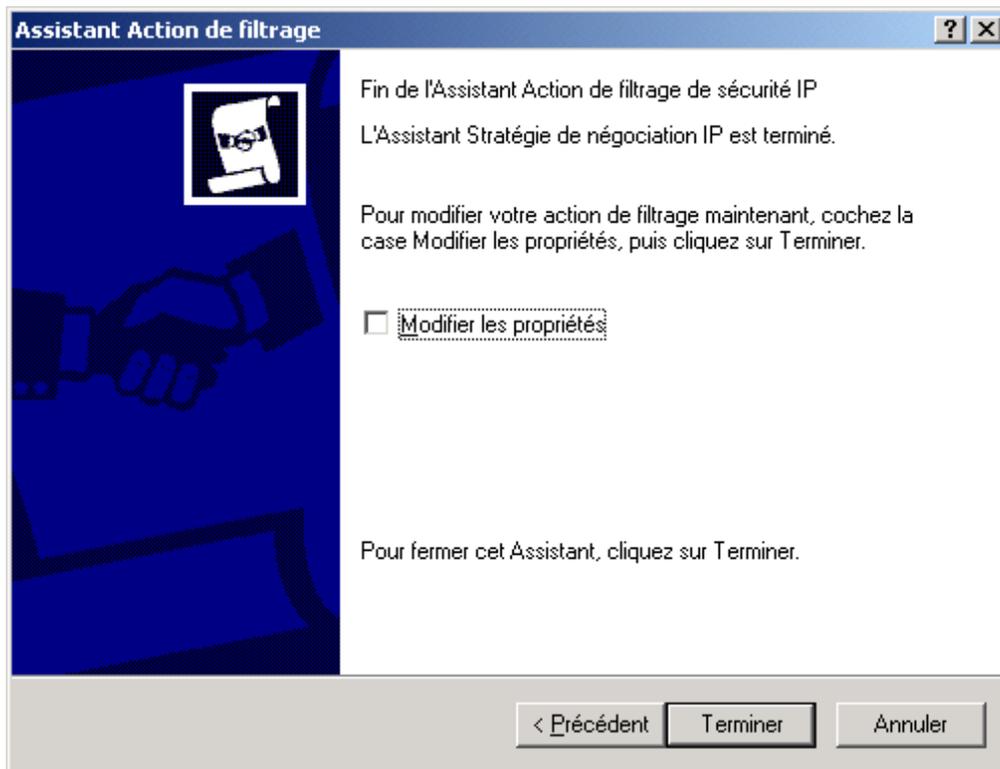
- Sélectionnez « Personnalisée » puis cliquez sur « Paramètres ».



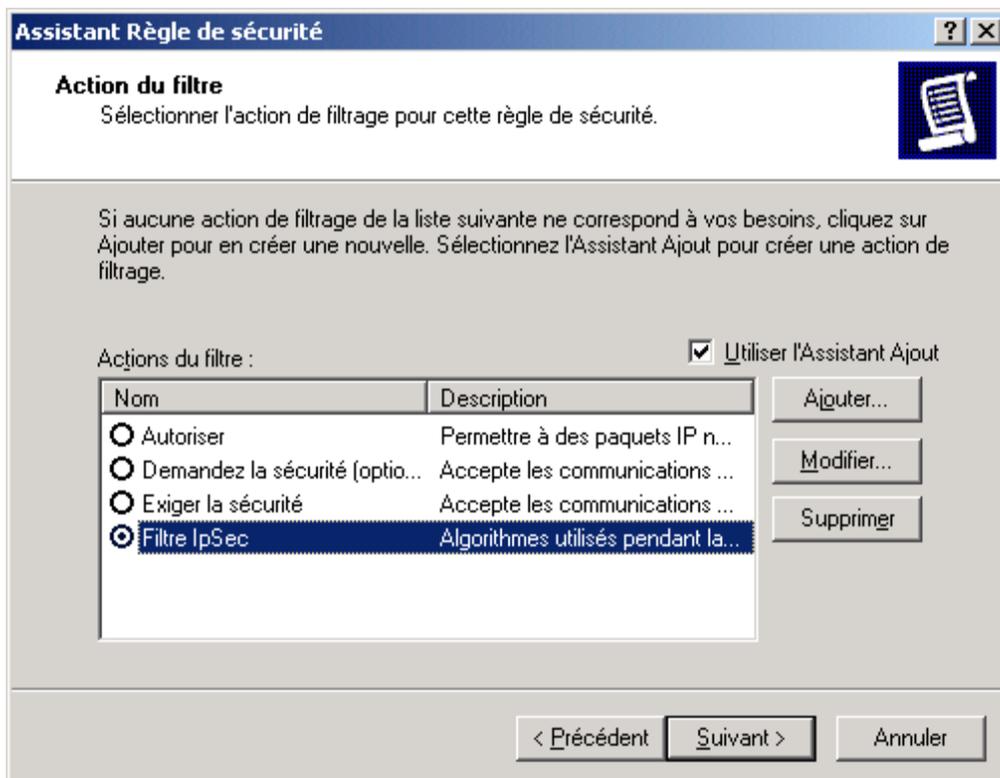
- Dans notre exemple, nous utiliserons du MD5 et du DES en ESP. Cliquez sur « OK », puis sur « Suivant ».



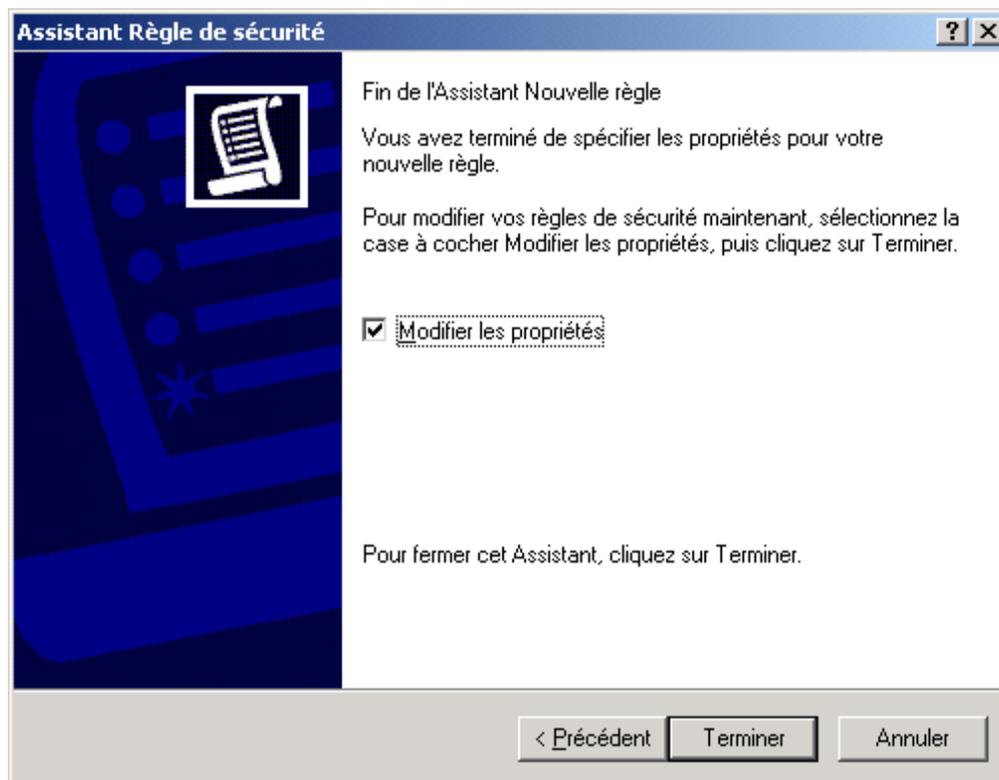
- Pour terminer la configuration de l'action du filtre cliquez sur « Terminer ».



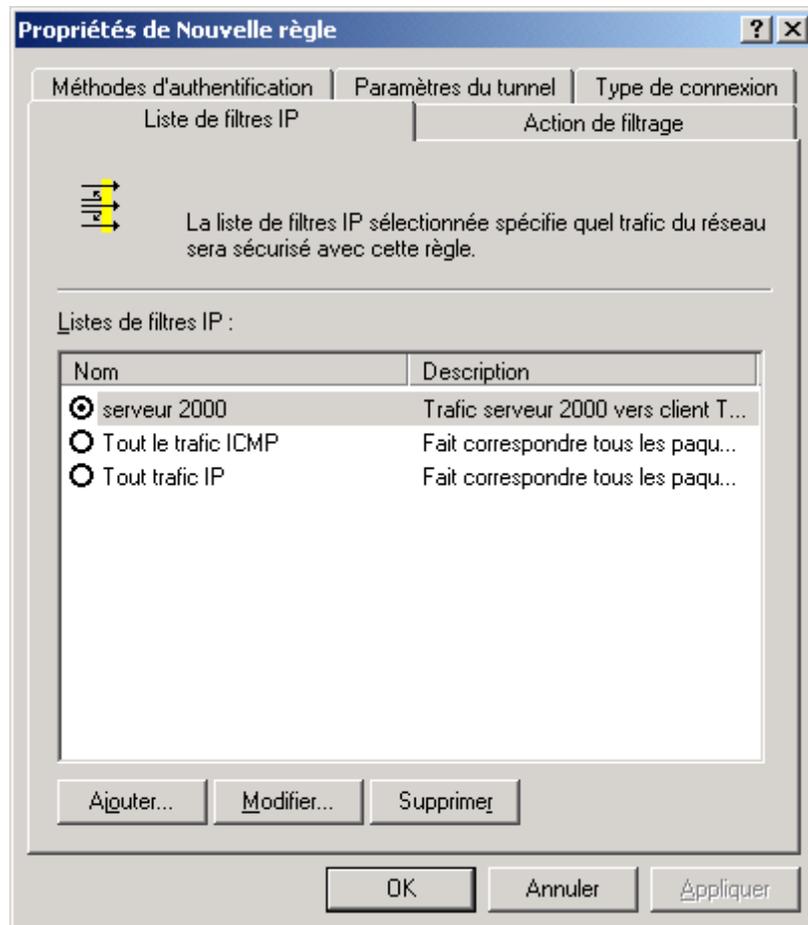
- La nouvelle action du filtre IP apparaît dans la liste d'action de filtre. Cliquez sur « Suivant ».



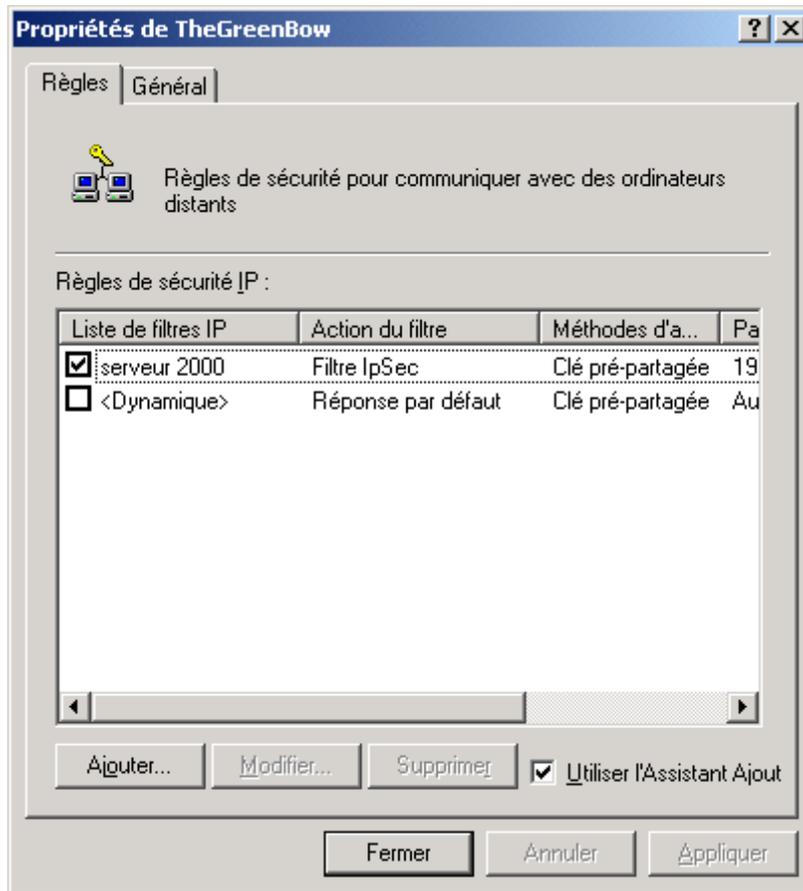
- Cliquez sur « Terminer ».



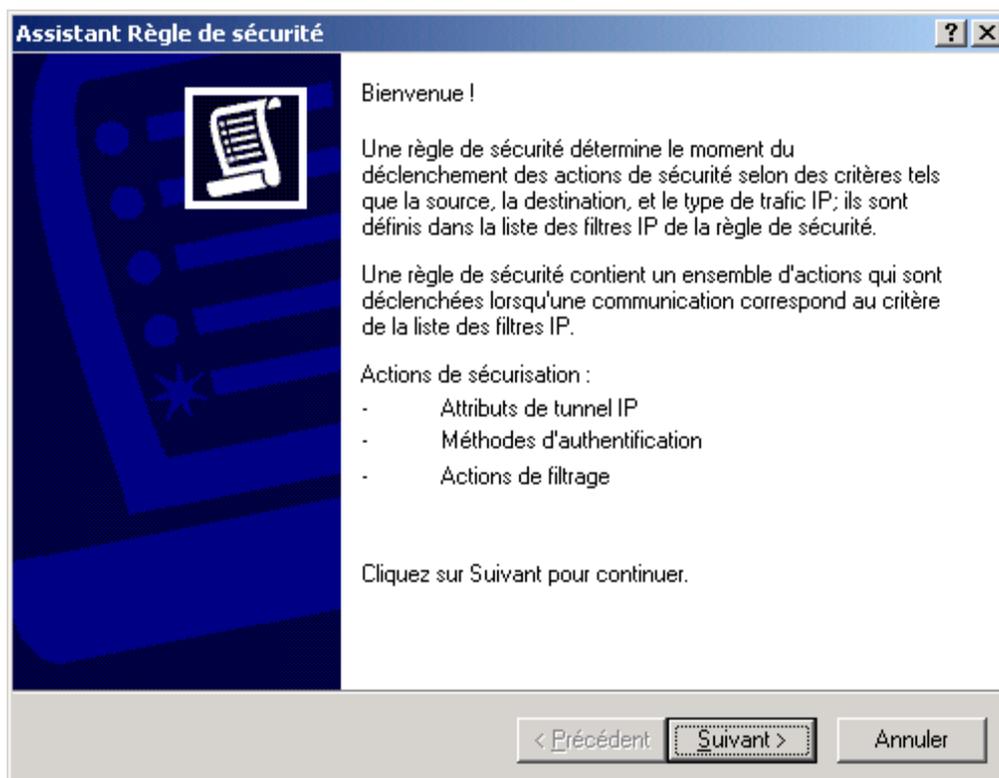
- Le filtre IP que nous venons de créer apparaît dans la liste des filtres IP. Cliquez sur « Fermer » pour terminer la création de la première règle de sécurité.



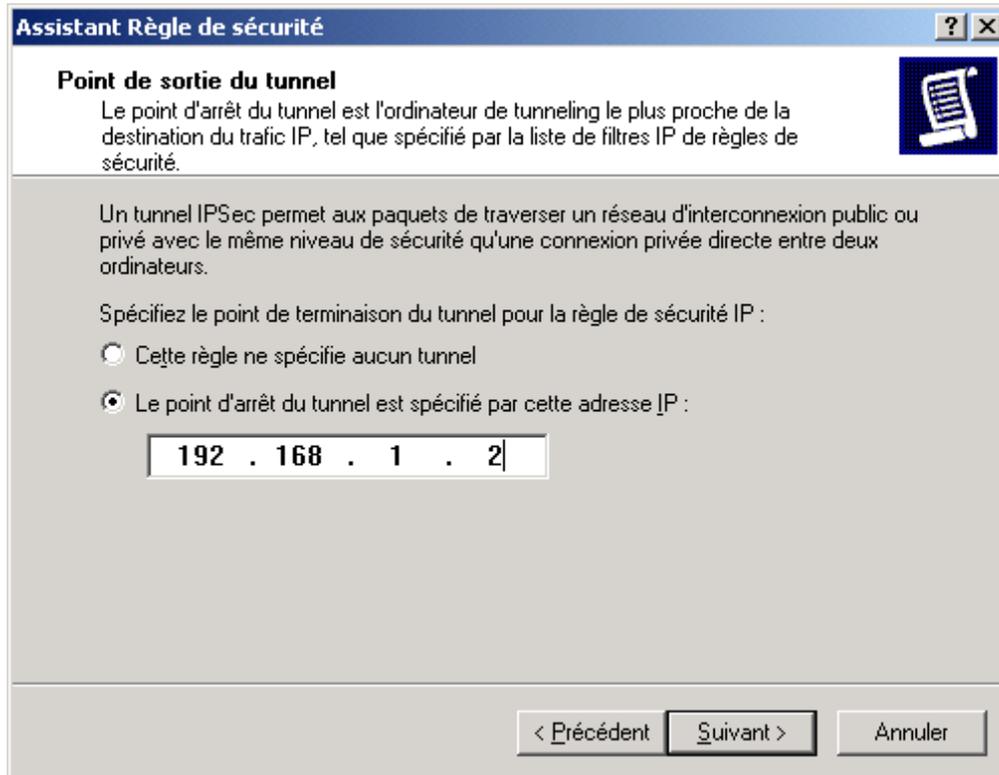
- Nous allons en créer une seconde règle de sécurité qui gèrera les communications du Client IPsec VPN TheGreenBow vers le serveur Microsoft Windows 2000 Server. Cliquez sur « **Ajouter** »



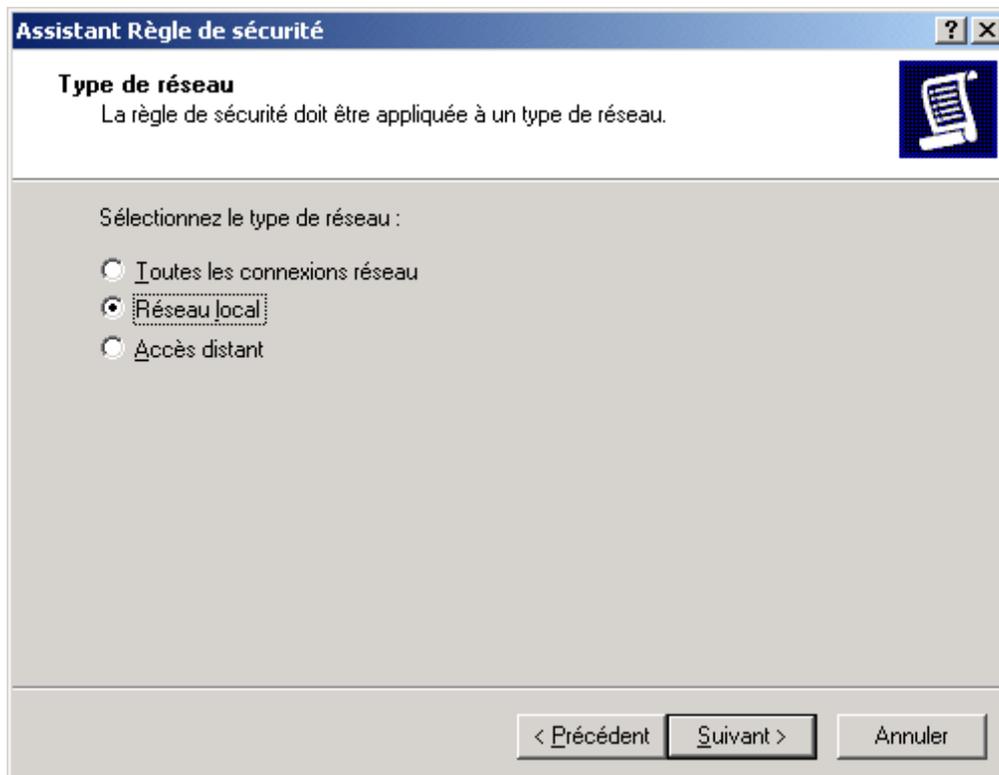
- Cliquez sur « **Suivant** ».



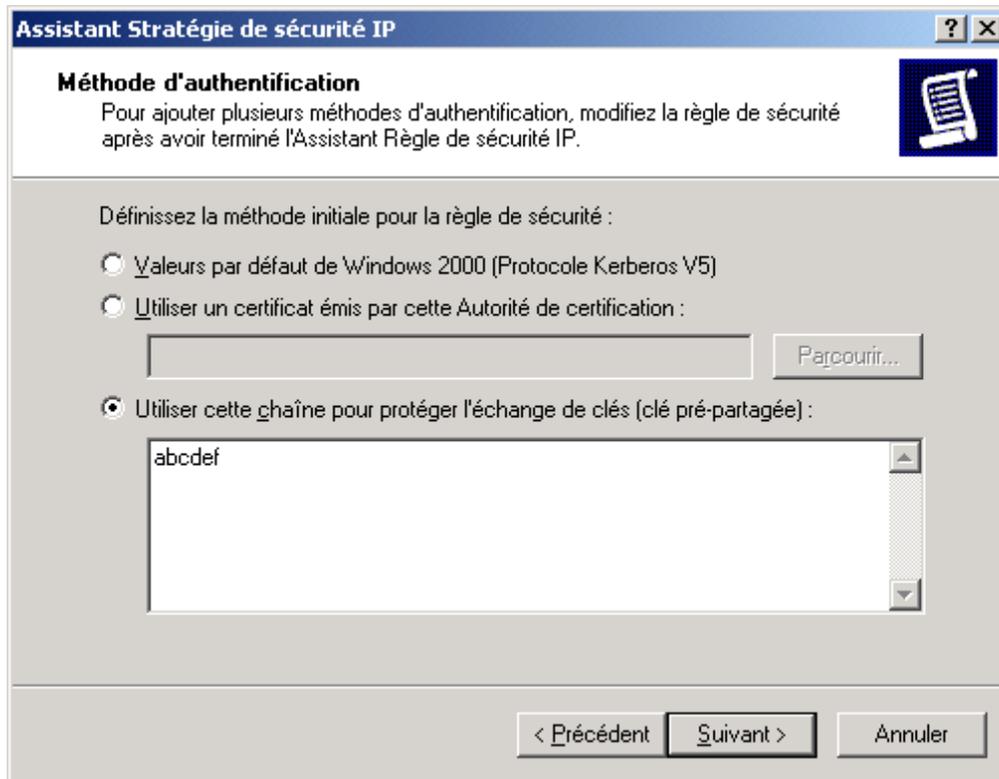
- Indiquez l'adresse IP du point final du tunnel VPN (ici le serveur Microsoft Windows 2000 Server) puis cliquez sur « Suivant ».



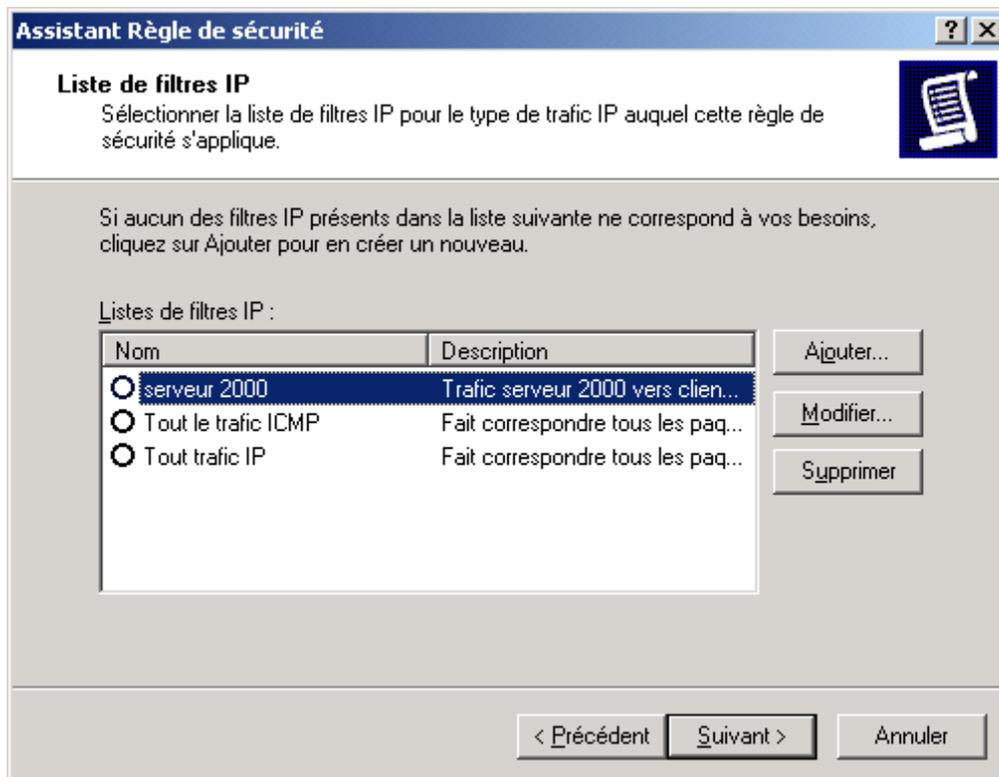
- Dans notre exemple, les ordinateurs sont dans le même réseau local. Cliquez sur « Réseau local » puis sur « Suivant ».



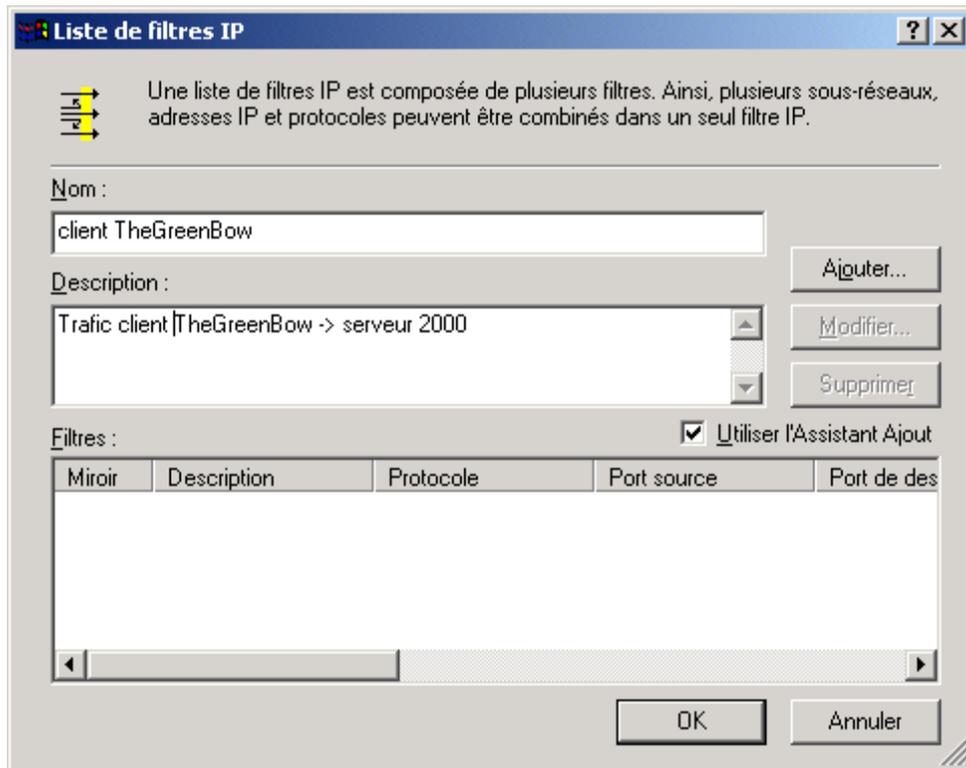
- La communication entre le serveur et le Client IPSec VPN est protégée par une clé partagée. Cliquez sur « **Utiliser cette chaîne pour protéger l'échange de clés** » et indiquez la clé partagée. Cliquez sur « **Suivant** ».



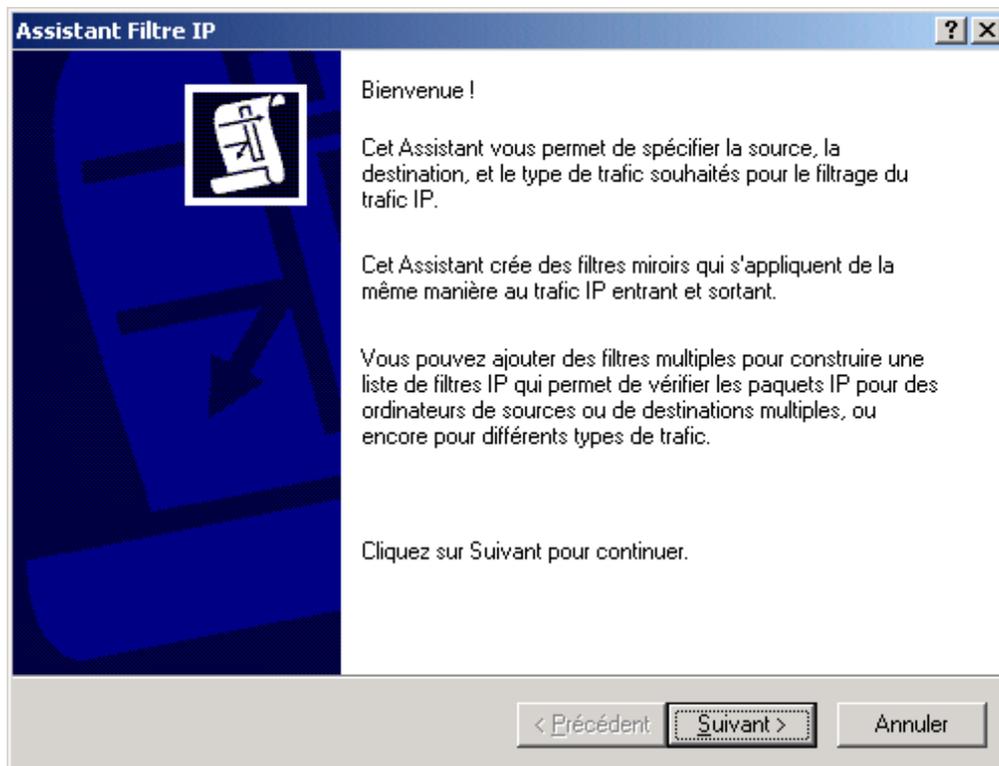
- Cliquez sur « **Ajouter** » pour insérer un filtre IP spécifique à notre nouvelle règle de sécurité.



- Nommez le nouveau filtre IP puis cliquez sur « Ajouter ».



- Cliquez sur « Suivant ».



- Sélectionnez « **Une adresse IP spécifique** » et tapez l'adresse IP du Client IPsec VPN TheGreenBow. Puis cliquez sur « **Suivant** ».

**Assistant Filtre** [?] [X]

**Source du trafic IP**  
Spécifiez l'adresse source du trafic IP.

Adresse source :

Adresse IP :

Masque de sous-réseau :

< Précédent    Suivant >    Annuler

- Sélectionner « **Mon adresse IP** » comme adresse de destination du trafic IP, puis cliquez sur « **Suivant** ».

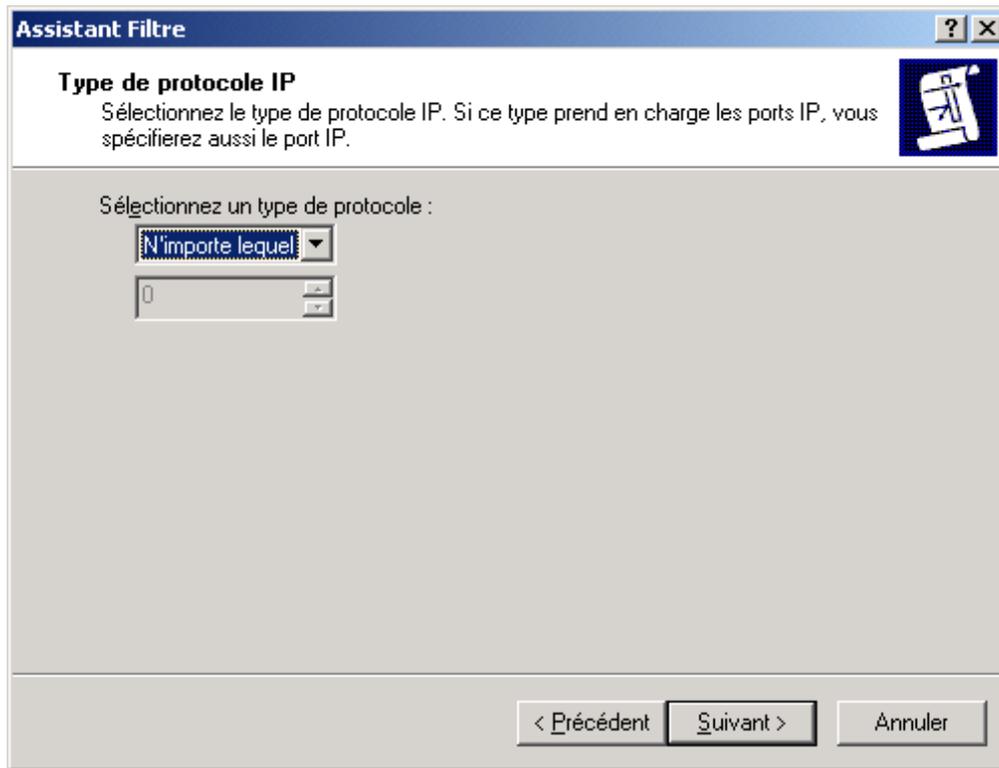
**Assistant Filtre** [?] [X]

**Destination du trafic IP**  
Spécifiez l'adresse de destination du trafic IP.

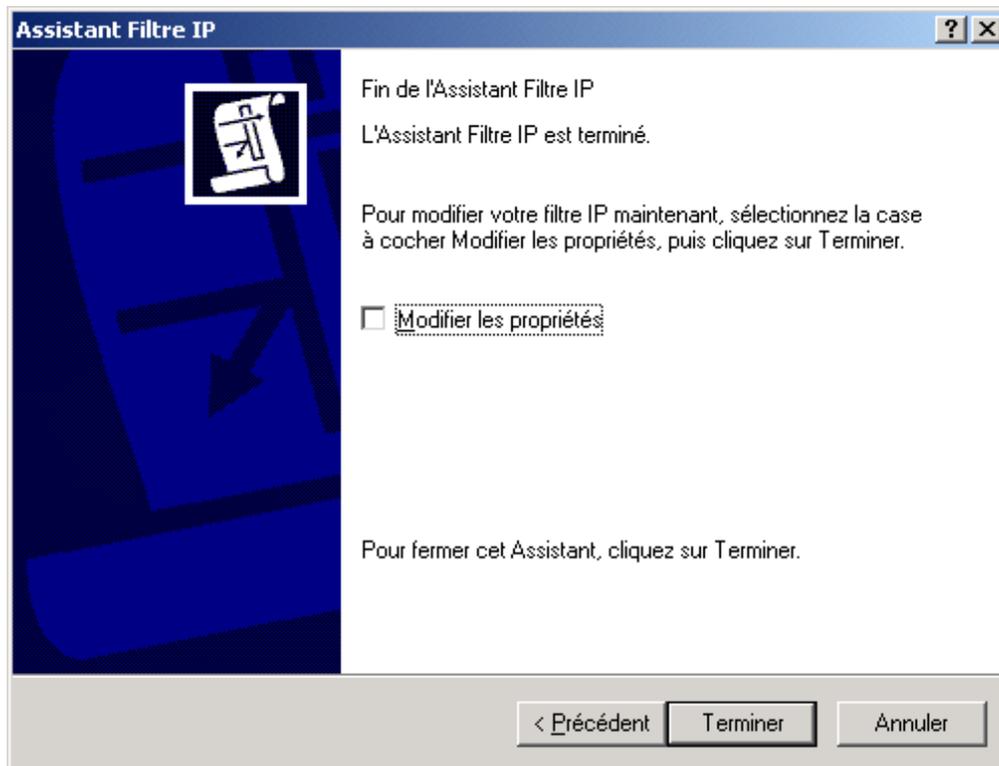
Adresse de destination :

< Précédent    Suivant >    Annuler

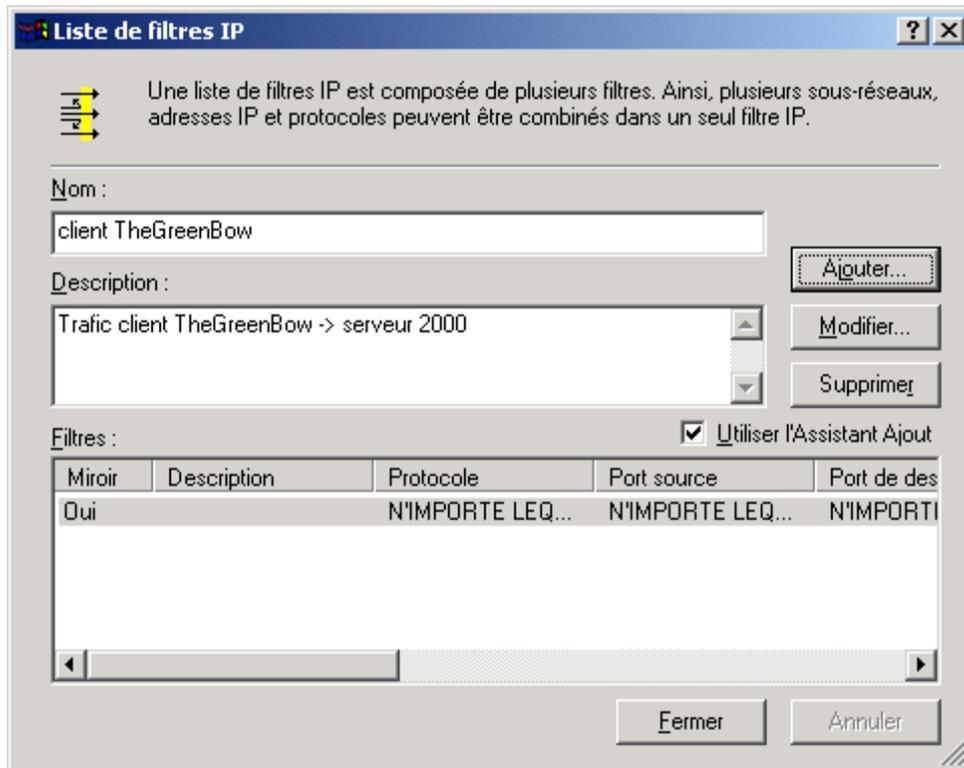
- Indiquez le type de Protocole IP puis cliquez sur « Suivant ».



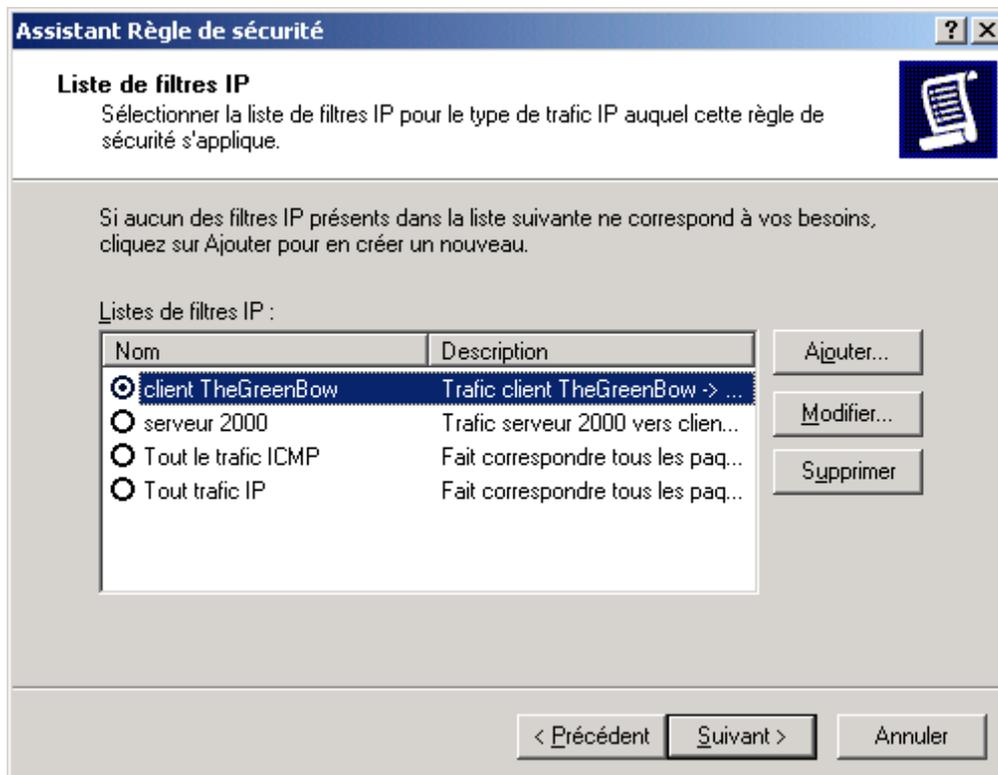
- Cliquez sur « Terminer »



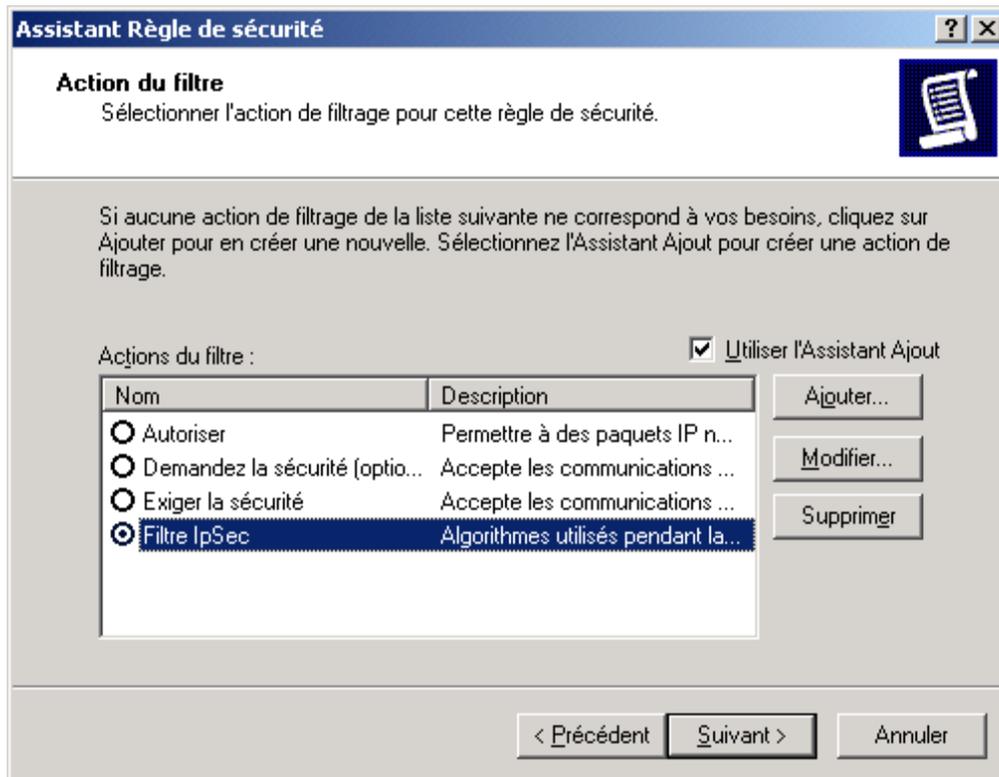
- Cliquez sur « Fermer ».



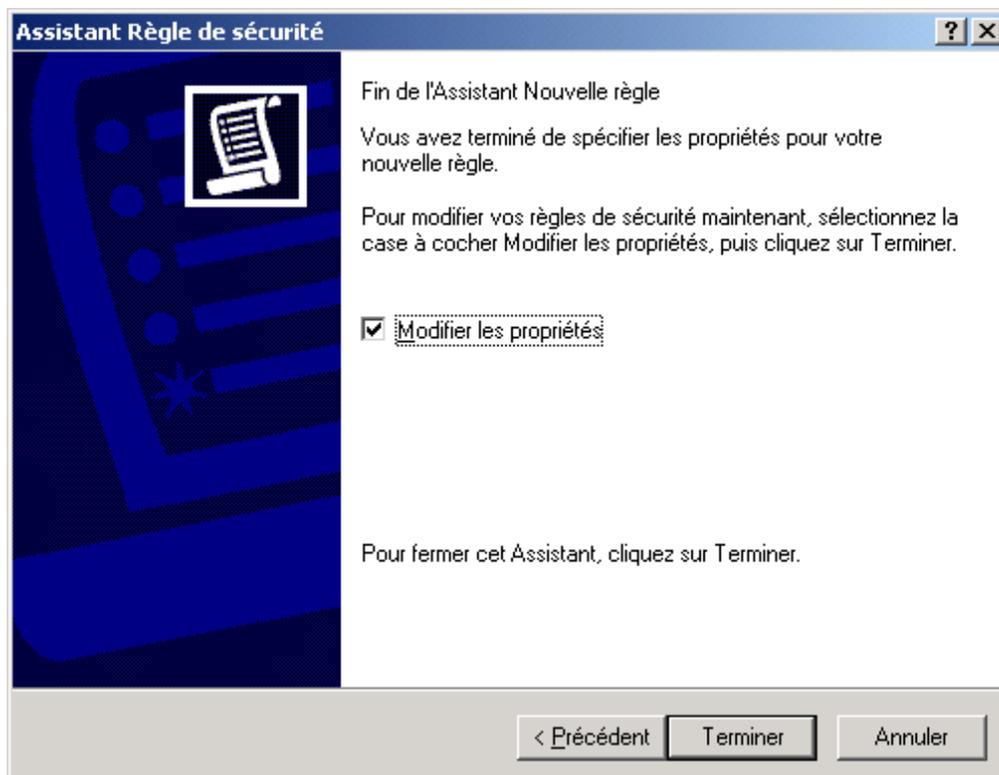
- Sélectionnez le filtre IP « Client TheGreenBow » puis cliquez sur « Suivant ».



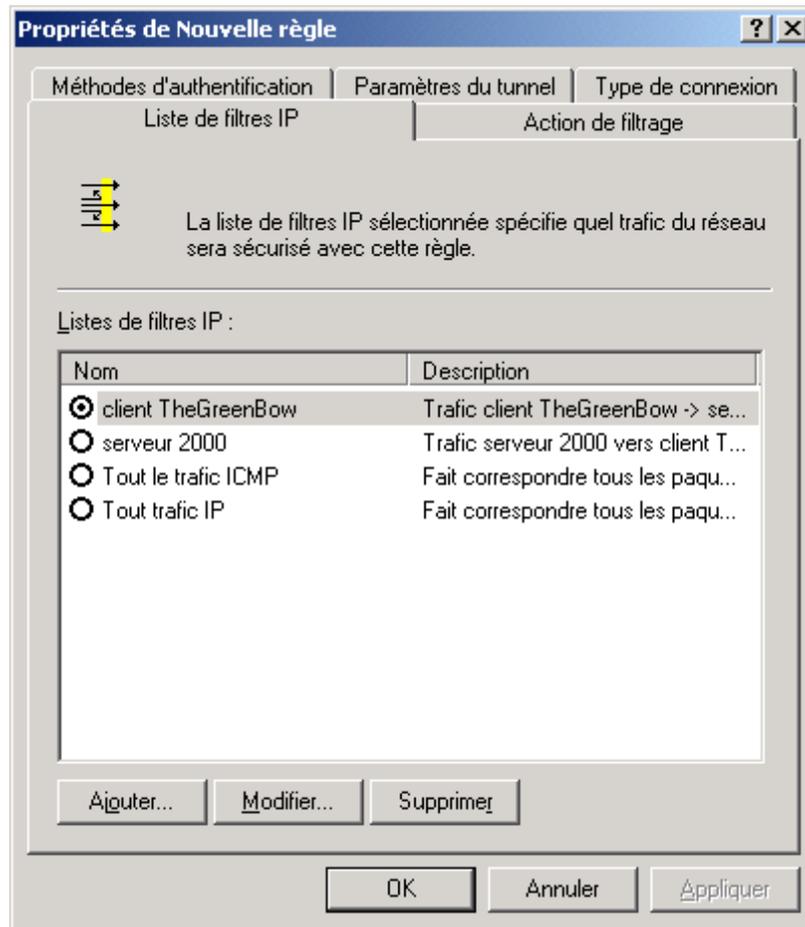
- Sélectionnez l'action de filtre « **Filtre IPSec** » puis cliquez sur « **Suivant** ».



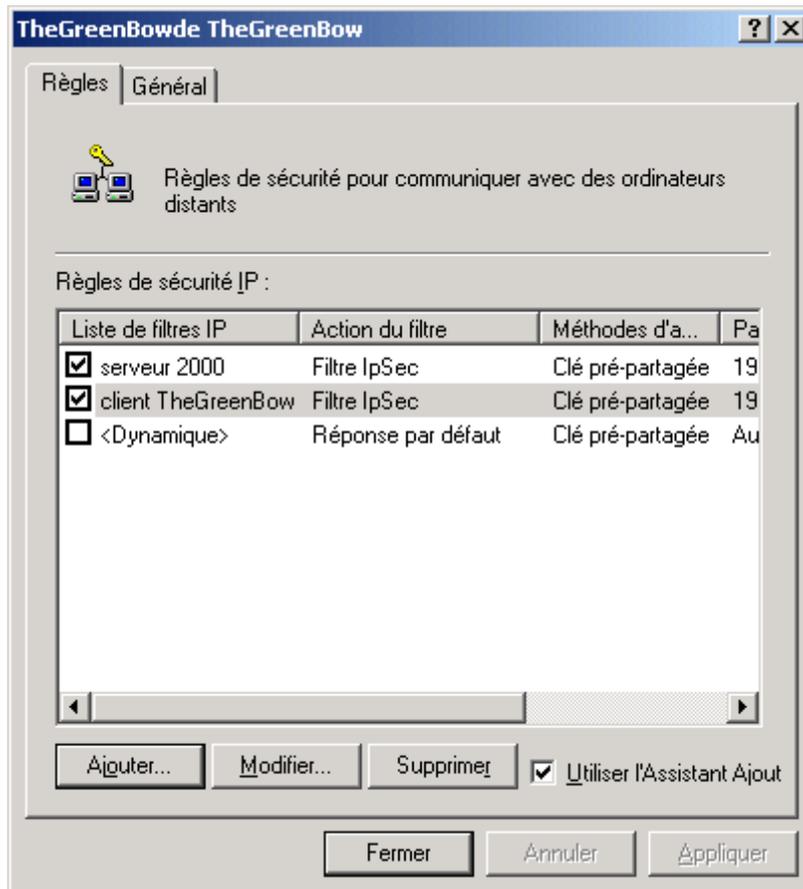
- Cliquez sur « **Terminer** ».



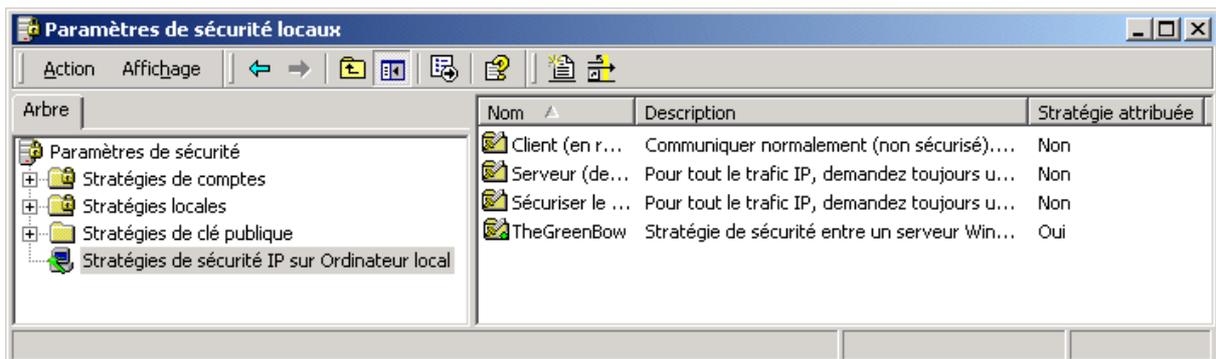
- Sélectionnez « Client TheGreenBow » dans l'onglet « Liste de filtres IP » puis cliquez sur « OK ».



- Cliquez sur l'onglet « Fermer ».



- Pour activer la nouvelle stratégie de sécurité, cliquez avec le bouton droit de la souris sur la stratégie « TheGreenBow », puis cliquez avec le bouton gauche sur « Attribuer ». Un point vert sur le coin inférieur droit apparaît sur l'icône « TheGreenBow ».



### 3 TheGreenBow IPsec VPN Client configuration

#### 3.1 VPN Client Phase 1 (IKE) Configuration

Dans le champ « **Interface** », vous pouvez sélectionner une étoile (« \* ») si le client reçoit une adresse IP dynamique de son FAI par exemple.

Dans le champ « **Adresse distante** », entrez l'adresse IP du serveur.

The screenshot shows the 'Authentification' configuration window. The 'Adresse distante' field is highlighted with an arrow pointing to a text box that says: 'L'adresse de la passerelle distante est soit son adresse IP soit son adresse DNS.' The two password fields for 'Clé Partagée' and 'Confirmer' are also highlighted with arrows pointing to the text 'abcdef'.

Configuration Phase 1

### 3.2 VPN Client Phase 2 (IPSec) Configuration

Dans cette fenêtre, vous définissez la configuration VPN IPSec.

Le champ « **Adresse Locale** » est l'adresse IP virtuelle du client au sein du réseau.

The screenshot shows the 'Configuration IPSec' window in TheGreenBow VPN Client. The window title is 'TheGreenBow VPN Client'. The menu bar includes 'Fichier', 'Configuration', and 'Outils ?'. The main area is titled 'Configuration IPSec' and contains the following fields and options:

- Nom (Phase 2): CnxVpn1
- Adresse locale: 192 . 168 . 1 . 3
- Adresse distante: 192 . 168 . 1 . 2
- Masque réseau:  0 . 0 . 0 . 0
- ESP section:
  - Chiffrement: DES
  - Authentification: MD5
  - Mode: Tunnel
  - Ouvrir au Boot
- PFS:  Groupe: None
- Buttons: 'Ouvrir le tunnel' and 'Appliquer les Règles'

Annotations with arrows point to the 'Adresse locale' and 'Adresse distante' fields:

- 'Vous devez définir une adresse virtuelle statique ici.' points to the 'Adresse locale' field.
- 'Entrer l'adresse IP du serveur distant.' points to the 'Adresse distante' field.

The status bar at the bottom left shows a green circle and the text 'VPN prêt'.

Configuration Phase 2

## 4 Ouvrir le tunnel

1. Cliquer sur "Appliquer les Règles"
2. Cliquer sur "Ouvrir le tunnel", ou lancer une connexion (ex.: ping)
3. Cliquer sur "Console" si vous voulez accéder aux logs VPN.

## 5 En cas de problème.

Configurer une liaison VPN entre deux ordinateurs est une tâche ardue. Il suffit qu'un seul paramètre manque, (par exemple la non sélection d'un algorithme de chiffrement ou d'authentification) pour que le tunnel ne monte pas. De nombreux outils sont disponibles pour déterminer le dysfonctionnement d'une liaison VPN.

En ce qui concerne le serveur Microsoft Windows 2000 Server, consultez, en cas de problème, le document Q257225 dans la base de connaissances de Microsoft :

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q257225>

### 5.1 Un analyseur réseau : ethereal

Ethereal est un logiciel gratuit qui permet l'analyse de paquets IP ou TCP transitant par une carte réseau. Ce logiciel est disponible sur le site <http://www.ethereal.com/>. Il permet de suivre facilement le dialogue protocolaire entre deux ordinateurs. Pour son installation et son exploitation, se référer à la documentation spécifique du logiciel.

Ci-dessous, un exemple de dialogue réussi entre le Client IPSec VPN TheGreenBow et le serveur Microsoft Windows 2000 Server.

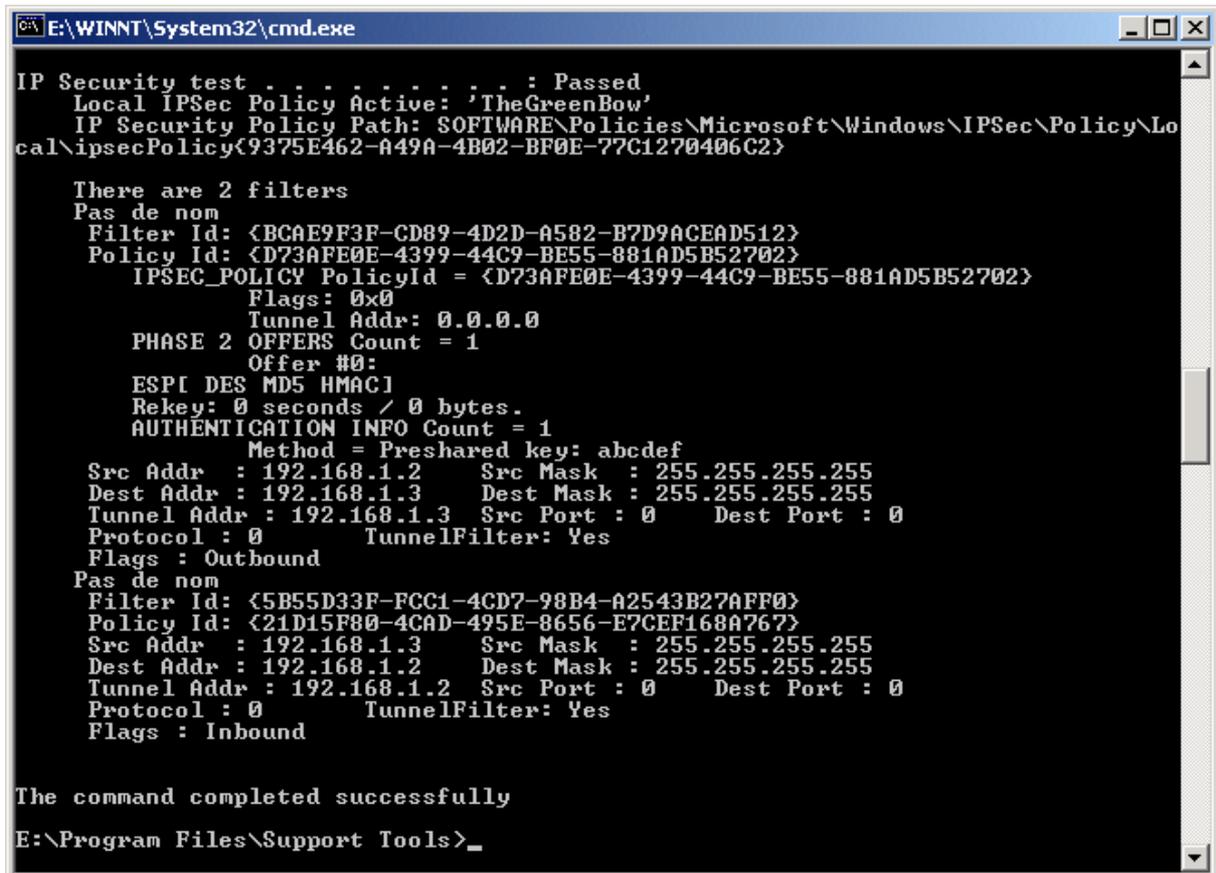
No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
2	0.153567	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
3	0.205363	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
4	0.257505	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
5	0.300882	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
6	0.310186	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
7	0.313742	192.168.1.3	192.168.1.2	ISAKMP	Quick Mode
8	0.321913	192.168.1.2	192.168.1.3	ISAKMP	Quick Mode
9	0.323741	192.168.1.3	192.168.1.2	ISAKMP	Quick Mode
10	0.334980	192.168.1.2	192.168.1.3	ISAKMP	Quick Mode
11	0.691160	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x919bfabc)
12	1.692568	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x919bfabc)
13	1.693164	192.168.1.2	192.168.1.3	ESP	ESP (SPI=0x53a5925e)
14	2.693600	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x919bfabc)
15	2.694026	192.168.1.2	192.168.1.3	ESP	ESP (SPI=0x53a5925e)

Frame 1 (142 bytes on wire, 142 bytes captured)  
 Ethernet II, Src: 00:50:04:ad:f2:73, Dst: 00:10:b5:07:2f:ff

## 5.2 Netdiag.exe

L'utilitaire Netdiag.exe est disponible avec les outils de support de Microsoft Windows 2000 Server (Support Tools). Se référer à la base de connaissances Q257225 pour plus d'informations.

Dans une fenêtre CMD.EXE, taper netdiag /test:ipsec /debug. L'application affiche dans la fenêtre les informations suivantes :



```
E:\WINNT\System32\cmd.exe

IP Security test . . . . . : Passed
Local IPsec Policy Active: 'TheGreenBow'
IP Security Policy Path: SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Local\ipsecPolicy{9375E462-A49A-4B02-BF0E-77C1270406C2}

There are 2 filters
Pas de nom
Filter Id: {BCAE9F3F-CD89-4D2D-A582-B7D9ACEAD512}
Policy Id: {D73AFE0E-4399-44C9-BE55-881AD5B52702}
IPSEC_POLICY PolicyId = {D73AFE0E-4399-44C9-BE55-881AD5B52702}
Flags: 0x0
Tunnel Addr: 0.0.0.0
PHASE 2 OFFERS Count = 1
Offer #0:
ESPI DES MD5 HMAC1
Rekey: 0 seconds / 0 bytes.
AUTHENTICATION INFO Count = 1
Method = Preshared key: abcdef
Src Addr : 192.168.1.2   Src Mask : 255.255.255.255
Dest Addr : 192.168.1.3   Dest Mask : 255.255.255.255
Tunnel Addr : 192.168.1.3   Src Port : 0   Dest Port : 0
Protocol : 0   TunnelFilter: Yes
Flags : Outbound
Pas de nom
Filter Id: {5B55D33F-FCC1-4CD7-98B4-A2543B27AFF0}
Policy Id: {21D15F80-4CAD-495E-8656-E7CEF168A767}
Src Addr : 192.168.1.3   Src Mask : 255.255.255.255
Dest Addr : 192.168.1.2   Dest Mask : 255.255.255.255
Tunnel Addr : 192.168.1.2   Src Port : 0   Dest Port : 0
Protocol : 0   TunnelFilter: Yes
Flags : Inbound

The command completed successfully

E:\Program Files\Support Tools>_
```

	Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	Doc.version	1.0 – Mai 2004
	VPN version	2.x

## 6 Contacts

Info et mise à jour sur le site web : <http://www.thegreenbow.com>

Support technique par email : [support@thegreenbow.com](mailto:support@thegreenbow.com)

Contacts commerciaux par téléphone au +33 1 43 12 39 37 ou par email : [info@thegreenbow.com](mailto:info@thegreenbow.com)