

TheGreenBow IPSec VPN Client Guide de Configuration Windows 2000 Server

WebSite : Contact : http://www.thegreenbow.com support@thegreenbow.com

IPSec VPN Router Configuration



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

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

TH	E	6	R	100.00	E	B	NL	6111101
				1				

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 décrirons 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.

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

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.

📑 Paramètres de sécurité locaux			- 🗆 🗵
$ \underline{Action} Affic\underline{h}age \ \underline{\leftarrow} \rightarrow \underline{\textcircled{t}} \underline{\textcircled{t}} \underline{\textcircled{t}} $	2 🗋 主		
Arbre	Nom 🛆	Description	Stratégie attribuée
Paramètres de sécurité	🖄 Client (en r	Communiquer normalement (non sécurisé)	Non
🗄 📴 Stratégies de comptes	Serveur (de	Pour tout le trafic IP, demandez toujours u	Non
🗄 📴 Stratégies locales	Sécuriser le	Pour tout le trafic IP, demandez toujours u	Non
🕀 🧰 Stratégies de clé publique			
Stratégies de sécurité IP sur Ordinateur local			
	J		

 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 ».

Assistant Stratégie de sécuri	Assistant Stratégie de sécurité IP					
	Bienvenue !					
	Cet Assistant vous permet de créer une stratégie de sécurité IP. Vous allez spécifier le niveau de sécurité à appliquer pour des communications avec des ordinateurs ou des groupes d'ordinateurs (sous-réseaux) spécifiques, ainsi que pour des types de trafic IP particuliers.					
	Cliquez sur Suivant pour continuer.					
	< <u>P</u> récédent <u>Suivant</u> Annul	er				

TUEGDEEDEGH 040140304	Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	Doc.version	1.0 – Mai 2004
	VPN version	2.x

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

Assistant Stratégie de sécurité IP	<u>? ×</u>
Nom de stratégie de sécurité IP Donnez un nom à cette stratégie de sécurité et éventuellement une brève description	
<u>N</u> om :	
TheGreenBow	
Description :	
Stratégie de sécurité entre un serveur Windows 2000 server et un client VPN TheGreenBow	×
< <u>P</u> récédent <u>S</u> uivant >	Annuler

• Cliquez sur « Suivant ».

Assistant Stratégie de sécurité IP	? ×
Requêtes pour une communication sécurisée Spécifiez la façon dont cette stratégie répond aux requêtes de communication sécurisée.	Ţ
La règle de réponse par défaut répond aux requêtes de sécurité des ordinateurs distants lorsque aucune autre règle ne s'applique. Pour sécuriser les communicati l'ordinateur doit répondre aux requêtes de communications sécurisées.	ions,
Activer la règle de réponse par défaut.	
< <u>P</u> récédent <u>S</u> uivant >	Annuler

THEGDEEDEGI 1040140304	Doc.R	Ref tgbvpn_cg_Wind2kServer_fr
	Doc.v	/ersion 1.0 – Mai 2004
	VPN v	version 2.x

• 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 ».

Assistant Stratégie de sécurité IP 🛛 💦 🔀
Méthode d'identification de la règle de réponse par défaut Pour ajouter plusieurs méthodes d'authentification, modifiez la règle de réponse par défaut après avoir terminé l'Assistant.
Définissez la méthode initiale pour la règle de sécurité :
Valeurs par défaut de Windows 2000 (Protocole Kerberos V5)
Utiliser un certificat émis par cette Autorité de certification :
Pa <u>r</u> courir
Utiliser cette chaîne pour protéger l'échange de clés (clé pré-partagée) :
abcdef
< <u>P</u> récédent <u>Suivant</u> > Annuler

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

Assistant Stratégie de sécuri	té IP	<u>?</u> ×
	Fin de l'Assistant Stratégie de sécurité IP Vous avez terminé de spécifier les propriétés pour votre nouvelle stratégie de sécurité IP. Pour modifier votre stratégie de sécurité IP maintenant, sélectionnez la case à cocher Modifiez les propriétés, puis cliquez sur Terminer. Modifier les propriété	
	Pour fermer cet Assistant, cliquez sur Terminer.	
	< <u>P</u> récédent Terminer Annu	iler

TUEGDEEDBOUID4014010	Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	Doc.version	1.0 – Mai 2004
	VPN version	2.x

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

Propriétés de TheGreenB	ow	?	x
Règles Général			
Règles de séc distants	urité pour communiquer a	ivec des ordinateurs	
Règles de sécurité <u>I</u> P :			
Liste de filtres IP	Action du filtre	Méthodes d'a Pa	
Oynamique>	Réponse par défaut	Clé pré-partagée Au	
Ajouter <u>M</u> odifi	er Supprimer	Utiliser l'Assistant Ajou	ıt
		OK Annuler	

TH	EG	R		Ė		M	611116	31
			1	/				

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

• Cliquez sur « Suivant ».

Assistant Règle de sécurité	<u>? ×</u>
	Bienvenue ! Une règle de sécurité détermine le moment du déclenchement des actions de sécurité selon des critères tels que la source, la destination, et le type de trafic IP; ils sont définis dans la liste des filtres IP de la règle de sécurité.
	Une règle de sécurité contient un ensemble d'actions qui sont déclenchées lorsqu'une communication correspond au critère de la liste des filtres IP.
- Alter	Actions de sécurisation : - Attributs de tunnel IP - Méthodes d'authentification - Actions de filtrage
	Cliquez sur Suivant pour continuer.
	< <u>Précédent</u> <u>Suivant</u> Annuler

• 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 »

Assistan	t Règ	le de s	sécurité						? >
Point L d	Point de sortie du tunnel Le point d'arrêt du tunnel est l'ordinateur de tunneling le plus proche de la destination du trafic IP, tel que spécifié par la liste de filtres IP de règles de sécurité.								
U pi oi	In tunr rivé av rdinate	hel IPSe vec le rr eurs.	ec permet nême nive	aux pao au de si	quets de écurité	e travers qu'une (ser un réseau connexion pr	a d'interconnexionivée directe ent	on public ou re deux
s	pécifie) Ce <u>t</u>	ez le po te règle	int de terr ne spéci	ninaison íie aucu	du tun n tunne	nel pour I	la règle de s	écurité IP :	
0) Le j	point d'a	arrêt du tu	innel est	spécifi	é par ce	ette adresse	!P :	
		192	. 168	. 1	•	3			
						<	: <u>P</u> récédent	<u>S</u> uivant >	Annuler

THECOEEDDON 1 040140104	Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	Doc.version	1.0 – Mai 2004
	VPN version	2.x

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

Assistant Règle de sécurité		'×
Type de réseau La règle de sécurité doit être appliquée à un	n type de réseau.	Ş
Sélectionnez le type de réseau :		
	< <u>P</u> récédent <u>S</u> uivant > Annuler	

THECOEÉDOMI 104040404	Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	Doc.version	1.0 – Mai 2004
	VPN version	2.x

 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 ».

Assistant Stratégie de sécurité IP	? ×
Méthode d'authentification Pour ajouter plusieurs méthodes d'authentification, modifiez la règle de sécurité après avoir terminé l'Assistant Règle de sécurité IP.	Ī
Définissez la méthode initiale pour la règle de sécurité : <u>V</u> aleurs par défaut de Windows 2000 (Protocole Kerberos V5) <u>U</u> tiliser un certificat émis par cette Autorité de certification : Pa <u>r</u> couri Utiliser cette <u>c</u> haîne pour protéger l'échange de clés (clé pré-partagée) :	ſ
abcdef	×
< <u>P</u> récédent <u>S</u> uivant >	Annuler

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

Assista	nt Règle de sécurité		<u>? ×</u>						
List	Liste de filtres IP Sélectionner la liste de filtres IP pour le type de trafic IP auquel cette règle de sécurité s'applique.								
	Si aucun des filtres IP présents dans la liste suivante ne correspond à vos besoins, cliquez sur Ajouter pour en créer un nouveau. Listes de filtres IP :								
	Nom	Description	Ajouter						
	 Tout le trafic ICMP Tout trafic IP 	Fait correspondre tous les paq Fait correspondre tous les paq	<u>M</u> odifier S <u>u</u> pprimer						
		< <u>P</u> récédent <u>S</u> uivan	it > Annuler						

THECOEEDDON 1 04014/0304	Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	Doc.version	1.0 – Mai 2004
	VPN version	2.x

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

📲 Liste de	e filtres IP			? X
	Une liste de filtres IP es adresses IP et protocok	t composée de plusieurs es peuvent être combine	s filtres. Ainsi, plusieurs és dans un seul filtre IF	s sous-réseaux, ^D .
<u>N</u> om :				
serveur	2000			
<u>D</u> escripti	on :			Ajouter
Trafic se	erveur 2000 vers client Tł	neGreenBow	<u> </u>	<u>M</u> odifier
			v	Supprimer
<u>F</u> iltres :			🔽 <u>U</u> tiliser IV	Assistant Ajout
Miroir	Description	Protocole	Port source	Port de des
•			OK	► Annuler

THECDEEDEMI 1040410404	Ľ	Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	[Doc.version	1.0 – Mai 2004
	١	VPN version	2.x

• 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 ».

Assistant Filtre		? ×
Source du trafic IP Spécifiez l'adresse source du trafic IP.		Ē
<u>A</u> dresse source :		
Mon adresse IP		
	< <u>P</u> récédent <u>S</u> uivant >	Annuler

THEGDEEDEGI 1040140104		Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	1	Doc.version	1.0 – Mai 2004
	`	VPN version	2.x

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

Assistant Filtre										? ×
Destination du trafic IP Spécifiez l'adresse de desti	nation du	tral	fic IP.						Ē	A
<u>A</u> dresse de destination :										
Une adresse IP spécifique						-				
<u>A</u> dresse IP :	192	•	168	•	1	•	3			
<u>M</u> asque de sous-réseau :	255		255		255		255			
	1									
			<	Pr	écéden	it [<u>S</u> uivar	nt >	Annule	er

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

Assistant Filtre			? ×
Type de protocole IP Sélectionnez le type de protocole IP. Si ce t spécifierez aussi le port IP.	ype prend en charg	e les ports IP, vous	Ē
Sélectionnez un type de protocole :			
	< <u>P</u> récédent	<u>S</u> uivant >	Annuler

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

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



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

📲 Liste d	e filtres IP			<u>? ×</u>
	Une liste de filtres IP es adresses IP et protocol	t composée de plusieur: es peuvent être combin	s filtres. Ainsi, plusieurs és dans un seul filtre IF	s sous-réseaux, ^D .
<u>N</u> om :				
serveur	2000			
<u>D</u> escripti	ion :			Ajouter
Trafic se	erveur 2000 vers client TI	heGreenBow		<u>M</u> odifier
			V	Supprime <u>r</u>
<u>F</u> iltres :			🔽 🛄tiliser IV	Assistant Ajout
Miroir	Description	Protocole	Port source	Port de des
Oui		N'IMPORTE LEQ	N'IMPORTE LEQ	N'IMPORTI
•				F
			<u> </u>	Annuler

THEGDEEDEGI 1040140304	Doc.F	Ref tgbvpn_cg_Wind2kServer_fr
	Doc.v	version 1.0 – Mai 2004
	VPN	version 2.x

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

Assista	ant Règle de sécurité		?×					
Lis	Liste de filtres IP Sélectionner la liste de filtres IP pour le type de trafic IP auquel cette règle de sécurité s'applique.							
	Si aucun des filtres IP présents dar cliquez sur Ajouter pour en créer u Listes de filtres IP :	ns la liste suivante ne correspond à v n nouveau.	vos besoins,					
	Nom	Description	Ajouter					
	 serveur 2000 Tout le trafic ICMP Tout trafic IP 	Trafic serveur 2000 vers clien Fait correspondre tous les paq Fait correspondre tous les paq	<u>M</u> odifier S <u>u</u> pprimer					
		< <u>P</u> récédent <u>S</u> uivan	t> Annuler					

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

Assistant Règle de sécurité		<u>? ×</u>					
Action du filtre Sélectionner l'action de filtrage pour cette règle de sécurité.							
Si aucune action de filtrage de la li: Ajouter pour en créer une nouvelle filtrage. Actions du filtre :	ste suivante ne correspond à vos b . Sélectionnez l'Assistant Ajout pou	esoins, cliquez sur r créer une action de iser l'Assistant Aiout					
Actions ou nice .	Description	Aioutor					
Nom	Description						
O Autoriser O Demandez la sécurité (optio	Permettre à des paquets IP n Accepte les communications	<u>M</u> odifier					
O Exiger la sécurité	Accepte les communications	Supprim <u>e</u> r					
	< <u>P</u> récédent <u>S</u> uiva	nt > Annuler					

TH	EG	R	1000	É	 B	N L	88119	81
		1	4					

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

• Cliquez sur « Suivant ».



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

Action du filtre	<u>? ×</u>
Nom d'action de filtre Donnez un nom à cette action de filtrage et une brève description (facultative)	1
<u>N</u> om :	
Filtre IpSec	
Description :	
Algorithmes utilisés pendant la Phase 2	×
< <u>P</u> récédent <u>S</u> uivant >	Annuler

TUEGDEEDEGUI 040140104		Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	1	Doc.version	1.0 – Mai 2004
	`	VPN version	2.x

• Cliquez sur « Négocier la sécurité » puis sur « Suivant ».

Action du filtre		? ×
Options générales d'actions de filtre Définissez le comportement de l'action de fil	ltrage.	10
C Autoriser		
○ <u>R</u> efuser		
Mégocier la sécurité		
	< <u>P</u> récédent <u>S</u> uivant > Annule	r

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

Assistant Action de filtrage	×		
Communiquer avec des ordinateurs qui ne prennent pas en charge IPSec Communiquer avec des ordinateurs qui ne prennent pas en charge IPsec peut entraîner des risques pour la sécurité de votre réseau.			
Voulez-vous autoriser les communications avec des ordinateurs qui ne prennent pas en charge IPSec ?			
Ne pas communiquer avec des ordinateurs qui ne prennent pas en charge IPSec.			
 Revenir à des communications non sécurisées. 			
Revenir à des communications non sécurisées. Utilisez cette option s'il y a des ordinateurs qui ne prennent pas en charge IPSec sur votre réseau. Communiquer avec des ordinateurs qui ne prennent pas en charge IPsec peut entraîner des risques pour la sécurité de votre réseau.			
< <u>P</u> récédent <u>S</u> uivant > Annuler			

TUEGDEEDEGUI 04014010	Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	Doc.version	1.0 – Mai 2004
	VPN version	2.x

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

Assistant Méthode de sécurité	? ×
Sécurité du trafic IP Spécifiez une méthode de sécurité pour le trafic IP. Pour ajouter plusieurs méthodes de sécurité, modifiez l'action de filtrage après avoir terminé l'Assistant.	1697
Cette action de filtrage nécessite au moins une méthode de sécurité pour le trafic IP.	
 <u>E</u>levée (transport de données sécurisé encapsulé) Les données seront cryptées, authentifiées et non modifiées. <u>M</u>oyenne (en-tête authentifié) Les données seront authentiques et non modifiées, mais ne seront pas cryptées. <u>Personnalisée</u> <u>Pa</u>ramètres 	
< <u>P</u> récédent <u>S</u> uivant > An	nuler

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

Paramètres personnalisés de la méthode de sécurité					
Spécifiez les paramètres pour cette méthode de sécurité personnalisée.					
Intégrité des adresses et des données sans cryptage (AH) :					
Algorithme d'intégrité :					
MD5 Cruntage et intégrité des données (ESP) :					
Algorithme d'intégrité :					
MD5					
Algorithme de cryptage :					
DES					
Paramètres de la clé de session :					
<u>G</u> enerer une nouvelle cle tous les : <u>Generer une nouvelle cle toutes les : <u>Generer une nouvelle cle toutes les : </u></u>					
kilo-octets secondes					
OK Annuler					

TUEGDEEDEGUID101010	Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	Doc.version	1.0 – Mai 2004
	VPN version	2.x

• 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 ».

Assistant Règle de sécurité		<u>? ×</u>			
Action du filtre Sélectionner l'action de filtrage pour cette règle de sécurité.					
Si aucune action de filtrage de la lis Ajouter pour en créer une nouvelle. filtrage.	ste suivante ne correspond à vos b . Sélectionnez l'Assistant Ajout pour	esoins, cliquez sur créer une action de			
Actions du filtre :	🔽 Util	ser l'Assistant Ajout			
Nom	Description	Ajouter			
 O Autoriser O Demandez la sécurité (optio O Exiger la sécurité ⊙ Filtre IpSec 	Permettre à des paquets IP n Accepte les communications Accepte les communications Algorithmes utilisés pendant la	<u>M</u> odifier Supprim <u>e</u> r			
	< <u>P</u> récédent <u>S</u> uivar	nt > Annuler			

THECDEEDEMI 104014/0104	[Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	[Doc.version	1.0 – Mai 2004
	١	VPN version	2.x

• Cliquez sur « Terminer ».

Assistant Règle de sécurité	<u>? ×</u>
	Fin de l'Assistant Nouvelle règle
	Vous avez terminé de spécifier les propriétés pour votre nouvelle règle.
	Pour modifier vos règles de sécurité maintenant, sélectionnez la case à cocher Modifier les propriétés, puis cliquez sur Terminer.
	Pour fermer cet Assistant, cliquez sur Terminer.
	< <u>P</u> récédent Terminer Annuler

THECOECOECOM 10401/0101	Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	Doc.version	1.0 – Mai 2004
	VPN version	2.x

• 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.

Propriétés de Nouvelle règle	<u>? ×</u>
Méthodes d'authentification Para Liste de filtres IP	mètres du tunnel Type de connexion Action de filtrage
La liste de filtres IP sélé sera sécurisé avec cet	ectionnée spécifie quel trafic du réseau te règle.
Listes de filtres IP :	
Nom	Description
🖸 serveur 2000	Trafic serveur 2000 vers client T
O Tout le trafic ICMP	Fait correspondre tous les paqu
Ajouter <u>M</u> odifier	Supprime <u>r</u>
0	K Annuler Appliquer

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

 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 »

Propriétés de TheGreenB	ow	1	? ×
Règles Général			
Règles de séc distants	urité pour communiquer a	vec des ordinateurs	
Règles de sécurité <u>I</u> P :			
Liste de filtres IP	Action du filtre	Méthodes d'a Pa	
serveur 2000	Filtre IpSec	Clé pré-partagée 19	
Oynamique>	Réponse par défaut	Clé pré-partagée Au	4
•		J	1
Ajouter Modifi	er Supprimer	Utiliser l'Assistant Aj	out
	Fermer	nnuler <u>Applique</u>	er

• Cliquez sur « Suivant ».



THECOEEDDOM 104014/0304	Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	Doc.version	1.0 – Mai 2004
	VPN version	2.x

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

Assistant Règle de sécurité
Point de sortie du tunnel Le point d'arrêt du tunnel est l'ordinateur de tunneling le plus proche de la destination du trafic IP, tel que spécifié par la liste de filtres IP de règles de sécurité.
Un tunnel IPSec permet aux paquets de traverser un réseau d'interconnexion public ou privé avec le même niveau de sécurité qu'une connexion privée directe entre deux ordinateurs.
Spécifiez le point de terminaison du tunnel pour la règle de sécurité IP :
C Cette règle ne spécifie aucun tunnel
• Le point d'arrêt du tunnel est spécifié par cette adresse <u>IP</u> :
< <u>P</u> récédent <u>S</u> uivant > Annuler

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

Assistant Règle de sécurité		? ×
Type de réseau La règle de sécurité doit être appliquée à un ty	pe de réseau.	Ī
Sélectionnez le type de réseau : <u>I</u> outes les connexions réseau <u>Réseau local</u> <u>A</u> ccès distant		
	< <u>P</u> récédent <u>S</u> uiva	nt > Annuler

THECOECODONI 040140104	[Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	1	Doc.version	1.0 – Mai 2004
	N	VPN version	2.x

 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 ».

stant Stratégie de sécurité IP				? ×
Héthode d'authentification Pour ajouter plusieurs méthodes d'authentific après avoir terminé l'Assistant Règle de sécu	ation, modifiez la rité IP.	règle de l	sécurité	圓
Définissez la méthode initiale pour la règle de	sécurité :			
○ Valeurs par défaut de Windows 2000 (Province 1998)	otocole Kerberos	: V5)		
O <u>U</u> tiliser un certificat émis par cette Autorite	é de certification	:		
			Parce	ourir
 Utiliser cette <u>c</u>haîne pour protéger l'écha 	nge de clés (clé	pré-partag	 jée):	
abcdef				<u> </u>
				-
	< Précédent	Suivan	•	Annuler

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

Assistant Règle de sécurité		? ×
Liste de filtres IP Sélectionner la liste de filtres l sécurité s'applique.	P pour le type de trafic IP auquel cette rè	egle de
Si aucun des filtres IP présent cliquez sur Ajouter pour en cré Listes de filtres IP :	s dans la liste suivante ne correspond à v éer un nouveau.	vos besoins,
Nom	Description	Ajouter
O serveur 2000 O Tout le trafic ICMP O Tout trafic IP	Trafic serveur 2000 vers clien Fait correspondre tous les paq Fait correspondre tous les paq	<u>M</u> odifier S <u>u</u> pprimer
	< <u>P</u> récédent <u>S</u> uivan	it > Annuler

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

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

🖪 Liste de	e filtres IP			<u>? ×</u>
	Une liste de filtres IP es adresses IP et protocole	t composée de plusieurs es peuvent être combiné	s filtres. Ainsi, plusieurs és dans un seul filtre IF	sous-réseaux,).
<u>N</u> om :				
client Tł	neGreenBow			
Descripti	ion :			Ajouter
Trafic cl	ient∏heGreenBow -> ser	veur 2000	<u> </u>	Modifier
				Supprimer
<u>F</u> iltres :			🔽 <u>U</u> tiliser IV	Assistant Ajout
Miroir	Description	Protocole	Port source	Port de des
1			OK	► Annuler

• Cliquez sur « Suivant ».

Assistant Filtre IP	<u>?</u> ×
	Bienvenue !
J	Cet Assistant vous permet de spécifier la source, la destination, et le type de trafic souhaités pour le filtrage du trafic IP.
	Cet Assistant crée des filtres miroirs qui s'appliquent de la même manière au trafic IP entrant et sortant.
	Vous pouvez ajouter des filtres multiples pour construire une liste de filtres IP qui permet de vérifier les paquets IP pour des ordinateurs de sources ou de destinations multiples, ou encore pour différents types de trafic.
	Cliquez sur Suivant pour continuer.
	< <u>P</u> récédent <u>Suivant</u> Annuler

THECDEEDE®N 1040140104	Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	Doc.versi	on 1.0 – Mai 2004
	VPN vers	ion 2.x

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

Assistant Filtre										? ×
Source du trafic IP Spécifiez l'adresse source d	lu trafic If	P.								Ē
<u>A</u> dresse source :										
Une adresse IP spécifique						•				
<u>A</u> dresse IP :	192		168	•	1	•	3			
<u>M</u> asque de sous-réseau :	255		255		255		255			
			<	: <u>P</u> r	écéden	it [<u>S</u> uivar	it >	Ann	uler

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

Assistant Filtre	?×
Destination du trafic IP Spécifiez l'adresse de destination du trafic IP.	Ē
Adresse de destination :	
Mon adresse IP	
< <u>P</u> récédent <u>S</u> uivant >	Annuler

TUEGDEEDEGUI 040140104	Do	oc.Ref	tgbvpn_cg_Wind2kServer_fr
	Do	oc.version	1.0 – Mai 2004
	VP	PN version	2.x

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

Assistant Filtre	? ×
Type de protocole IP Sélectionnez le type de protocole IP. Si ce type prend en charge les ports IP, vous spécifierez aussi le port IP.	Ē
Sélectionnez un type de protocole :	
< Précédent Suivant > Ar	nuler
< <u>P</u> récédent <u>S</u> uivant > Ar	nnuler

• Cliquez sur « Terminer »



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

• Cliquez sur « Fermer ».

🖁 Liste de	filtres IP			? ×				
	Une liste de filtres IP est composée de plusieurs filtres. Ainsi, plusieurs sous-réseaux, adresses IP et protocoles peuvent être combinés dans un seul filtre IP.							
<u>N</u> om :								
client Th	eGreenBow							
	on :			Ajouter				
Trafic cli	ent TheGreenBow -> ser	veur 2000	-	<u>M</u> odifier				
1				supprimer				
<u>F</u> iltres :				ssistant Ajout				
Miroir	Description	Protocole	Port source	Port de des				
Oui		N'IMPORTE LEQ	N'IMPORTE LEQ	N'IMPORTI				
•				•				
			<u>F</u> ermer	Annuler				

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

Assistant Règle de sécurité		<u>? ×</u>					
Liste de filtres IP Sélectionner la liste de filtres IP pour le type de trafic IP auquel cette règle de sécurité s'applique.							
Si aucun des filtres IP présents dans la liste suivante ne correspond à vos besoins, cliquez sur Ajouter pour en créer un nouveau. Listes de filtres IP :							
Nom	Description	Ajouter					
 client TheGreenBow serveur 2000 Tout le trafic ICMP Tout trafic IP 	Trafic client TheGreenBow -> Trafic serveur 2000 vers clien Fait correspondre tous les paq Fait correspondre tous les paq	<u>M</u> odifier S <u>u</u> pprimer					
	< <u>P</u> récédent <u>S</u> uivar	nt > Annuler					

THECHECHERGHIM	[Doc.Ref	tgbvpn_cg_Wind2kServer_fr
]	Doc.version	1.0 – Mai 2004
	1	VPN version	2.x

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

Assistant Règle de sécurité							
Action du filtre Sélectionner l'action de filtrage pour cette règle de sécurité.							
Si aucune action de filtrage de la liste suivante ne correspond à vos besoins, cliquez sur Ajouter pour en créer une nouvelle. Sélectionnez l'Assistant Ajout pour créer une action de filtrage.							
Ac <u>t</u> ions du filtre :	I▼ <u>U</u> tilis	ser l'Assistant Ajout					
Nom	Description	Ajouter					
O Autoriser	Permettre à des paquets IP n						
O Demandez la sécurité (optio	Accepte les communications	Modifier					
O Exiger la sécurité	Accepte les communications	Supprimer					
O Filtre IpSec	Algorithmes utilisés pendant la						
,							
	< <u>P</u> récédent <u>S</u> uivan	t> Annuler					

• Cliquez sur « Terminer ».



THECOECOECOR (10401/0101	Do	oc.Ref	tgbvpn_cg_Wind2kServer_fr
	Do	oc.version	1.0 – Mai 2004
	VP	PN version	2.x

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

Propriétés de Nouvelle règle	<u>? ×</u>
Méthodes d'authentification Para Liste de filtres IP	mètres du tunnel Type de connexion Action de filtrage
La liste de filtres IP sélé sera sécurisé avec cet	ectionnée spécifie quel trafic du réseau te règle.
Listes de filtres IP :	
Nom	Description
O client TheGreenBow	Trafic client TheGreenBow -> se
O serveur 2000	Trafic serveur 2000 vers client T
O Tout le trafic ICMP	Fait correspondre tous les paqu
O Tout trafic IP	Fait correspondre tous les paqu
Ajouter <u>M</u> odifier	Supprimer
0	K Annuler Appliquer

THECDEEDBOHIM	Doc.Ref	tgbvpn_cg_Wind2kServer_f
	Doc.version	1.0 – Mai 2004
	VPN version	2.x

• Cliquez sur l'onglet « Fermer ».

TheGreenBowde TheGree	nBow		? ×
Règles Général			
Règles de séc distants	urité pour communiquer a	vec des ordinateurs	:
Règles de sécurité <u>I</u> P :			
Liste de filtres IP	Action du filtre	Méthodes d'a	Pa
🗹 serveur 2000	Filtre IpSec	Clé pré-partagée	19
🗹 client TheGreenBow	Filtre IpSec	Clé pré-partagée	19
Oynamique>	Réponse par défaut	Clé pré-partagée	Au
Alouter Modifi	er Supprimer	 Utiliser l'Assistan 	t Ajout
	Fermer	nnuler <u>A</u> ppl	iquer

 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 ».

🚦 Paramètres de sécurité locaux			<u>_ ×</u>
Action Affichage ← → 🔁 🖬 🗔	😫 🛛 🛅 🚠		
Arbre	Nom 🛆	Description	Stratégie attribuée
Paramètres de sécurité	🖄 Client (en r	Communiquer normalement (non sécurisé)	Non
🗄 🔂 Stratégies de comptes	Serveur (de	Pour tout le trafic IP, demandez toujours u	Non
🗄 🚾 Stratégies locales	🔊 Sécuriser le	Pour tout le trafic IP, demandez toujours u	Non
🗄 💼 Stratégies de clé publique	🔯 TheGreenBow	Stratégie de sécurité entre un serveur Win	Oui
🔍 😓 Stratégies de sécurité IP sur Ordinateur local			
	J		

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

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.

TheGreenBow VPN Client				
Fichier Configuration Outils	?			
THEGREENB		VPN Clie	nt-	
Console	Authentificatio	on		L'adresse de la
 Paramètres Connexions 	Nom (Phase 1) Interface	CnxVpn1		soit son adresse IP
	Adresse distante	192.168.1.2		Solt Soll adlesse DNS.
CnxVpn1	Clé Partagée	*****		abcdef
	Confirmer	Gestion des Certificats		abcdef
	- IKE Chiffrement	DES Avancé		
	Groupe de clé	DH768		
	A	Appliquer les f	Règles	
O VPN prêt				

Configuration Phase 1

TLECDEEDERIN	Doc.R	ef tgbvpn_cg_Wind2kServer_fr
	Doc.ve	ersion 1.0 – Mai 2004
	VPN v	ersion 2.x

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.

📀 TheGreenBow VPN Client		
Fichier Configuration Outils	?	
	Configuration IPSec	Vous devez définir une adresse virtuelle statique ici.
Paramètres	Nom (Phase 2) CnxVpn1	
Connexions Configuration CnxVpn1	Adresse locale 192 . 168 . 1 . 3 Adresse distante 192 . 168 . 1 . 2 Masque réseau 0 . 0 . 0 . 0 ESP Chiffrement DES Authentification MD5 Mode Tunnel Mode Tunnel Authentification MD5	Entrer l'adresse IP du serveur distant.
	PFS Groupe None Ouvrir le tunnel	
	Appliquer les Règles	
O 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.

THEGI	RE			M	68111	61
		1				

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

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 <u>http://www.ethereal.com/</u>. 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.

NoTimeSourceDestinationProtocolInfo10.000000192.168.1.3192.168.1.2ISAKMPIdentity Protection (Main Mode)20.153567192.168.1.2192.168.1.3ISAKMPIdentity Protection (Main Mode)30.205363192.168.1.3192.168.1.2ISAKMPIdentity Protection (Main Mode)40.257505192.168.1.2192.168.1.3ISAKMPIdentity Protection (Main Mode)50.300882192.168.1.3192.168.1.2ISAKMPIdentity Protection (Main Mode)60.310186192.168.1.2192.168.1.3ISAKMPIdentity Protection (Main Mode)70.313742192.168.1.3192.168.1.2ISAKMPQuick Mode80.321913192.168.1.2192.168.1.3ISAKMPQuick Mode90.323741192.168.1.3192.168.1.2ISAKMPQuick Mode100.334980192.168.1.3192.168.1.2ESPESP110.691160192.168.1.3192.168.1.2ESPESP (SPI=0x919bfabc)121.692568192.168.1.3192.168.1.2ESPESP131.693164192.168.1.3192.168.1.3ESPESP (SPI=0x919bfabc)131.693600192.168.1.3192.168.1.3ESPESP (SPI=0x53a5925e)142.693600192.168.1.2192.168.1.3ESPESP (SPI=0x53a5925e)152.694026192.168.1.2192.168.1.3ESPESP (SPI=0x53a5925e)							— —
10.000000192.168.1.3192.168.1.2ISAKMPIdentity Protection (Main Mode)20.153567192.168.1.2192.168.1.3ISAKMPIdentity Protection (Main Mode)30.205363192.168.1.3192.168.1.2ISAKMPIdentity Protection (Main Mode)40.257505192.168.1.2192.168.1.3ISAKMPIdentity Protection (Main Mode)50.300882192.168.1.3192.168.1.2ISAKMPIdentity Protection (Main Mode)60.310186192.168.1.2192.168.1.2ISAKMPIdentity Protection (Main Mode)70.313742192.168.1.3192.168.1.2ISAKMPIdentity Protection (Main Mode)80.321913192.168.1.3192.168.1.2ISAKMPQuick Mode90.323741192.168.1.2192.168.1.2ISAKMPQuick Mode100.334980192.168.1.2192.168.1.3ISAKMPQuick Mode110.691160192.168.1.3192.168.1.2ESPESP121.692568192.168.1.3192.168.1.2ESPESP (SPI=0x919bfabc)131.693164192.168.1.2192.168.1.3ESPESP142.693600192.168.1.3192.168.1.2ESPESP (SPI=0x919bfabc)152.694026192.168.1.2192.168.1.3ESPESP152.694026192.168.1.2192.168.1.3ESPESP	No. 🗸	Time	Source	Destination	Protocol	Info	
2 0.153567192.168.1.2192.168.1.3ISAKMPIdentity Protection (Main Mode)3 0.205363192.168.1.3192.168.1.2ISAKMPIdentity Protection (Main Mode)4 0.257505192.168.1.2192.168.1.3ISAKMPIdentity Protection (Main Mode)5 0.300882192.168.1.3192.168.1.2ISAKMPIdentity Protection (Main Mode)6 0.310186192.168.1.2192.168.1.2ISAKMPIdentity Protection (Main Mode)7 0.313742192.168.1.3192.168.1.2ISAKMPIdentity Protection (Main Mode)8 0.321913192.168.1.2192.168.1.3ISAKMPQuick Mode9 0.323741192.168.1.2192.168.1.2ISAKMPQuick Mode10 0.334980192.168.1.2192.168.1.3ISAKMPQuick Mode11 0.691160192.168.1.3192.168.1.2ESPESP12 1.692568192.168.1.3192.168.1.2ESPESP13 1.693164192.168.1.2192.168.1.3ESPESP14 2.693600192.168.1.3192.168.1.2ESPESP15 2.694026192.168.1.3192.168.1.3ESPESP15 2.694026192.168.1.2192.168.1.3ESPESP15 2.694026192.168.1.2192.168.1.3ESPESP15 2.694026192.168.1.2192.168.1.3ESPESP15 2.694026192.168.1.2192.168.1.3ESPESP15 2.694026192.168.1.2192.168.1.3ESPESP15 2.694026192.168.1.2192.168.1.3 <td>1</td> <td>0.000000</td> <td>192.168.1.3</td> <td>192.168.1.2</td> <td>ISAKMP</td> <td>Identity Protection (Main Mode)</td> <td></td>	1	0.000000	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)	
3 0.205363192.168.1.3192.168.1.2ISAKMPIdentity Protection (Main Mode)4 0.257505192.168.1.2192.168.1.3ISAKMPIdentity Protection (Main Mode)5 0.300882192.168.1.3192.168.1.2ISAKMPIdentity Protection (Main Mode)6 0.310186192.168.1.2192.168.1.3ISAKMPIdentity Protection (Main Mode)7 0.313742192.168.1.2192.168.1.2ISAKMPIdentity Protection (Main Mode)8 0.321913192.168.1.2192.168.1.2ISAKMPQuick Mode9 0.323741192.168.1.2192.168.1.2ISAKMPQuick Mode10 0.334980192.168.1.2192.168.1.3ISAKMPQuick Mode11 0.691160192.168.1.3192.168.1.2ESPESP (SPI=0x919bfabc)12 1.692568192.168.1.3192.168.1.2ESPESP (SPI=0x919bfabc)13 1.693164192.168.1.3192.168.1.3ESPESP (SPI=0x919bfabc)13 1.693600192.168.1.3192.168.1.2ESPESP (SPI=0x919bfabc)15 2.694026192.168.1.2192.168.1.3ESPESP (SPI=0x919bfabc)15 2.694026192.168.1.2192.168.1.3ESPESP (SPI=0x53a5925e)	2	0.153567	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)	
4 0.257505192.168.1.2192.168.1.3ISAKMPIdentity Protection (Main Mode)5 0.300882192.168.1.3192.168.1.2ISAKMPIdentity Protection (Main Mode)6 0.310186192.168.1.2192.168.1.3ISAKMPIdentity Protection (Main Mode)7 0.313742192.168.1.2192.168.1.2ISAKMPIdentity Protection (Main Mode)8 0.321913192.168.1.2192.168.1.2ISAKMPQuick Mode9 0.323741192.168.1.3192.168.1.2ISAKMPQuick Mode10 0.334980192.168.1.2192.168.1.2ISAKMPQuick Mode11 0.691160192.168.1.3192.168.1.2ESPESP (SPI=0x919bfabc)12 1.692568192.168.1.3192.168.1.3ESPESP (SPI=0x919bfabc)13 1.693164192.168.1.2192.168.1.2ESPESP (SPI=0x919bfabc)14 2.693600192.168.1.3192.168.1.2ESPESP (SPI=0x53a5925e)14 2.693600192.168.1.2192.168.1.3ESPESP (SPI=0x53a5925e)15 2.694026192.168.1.2192.168.1.3ESPESP (SPI=0x53a5925e)	3	0.205363	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)	
50.300882192.168.1.3192.168.1.2ISAKMPIdentityProtection (Main Mode)60.310186192.168.1.2192.168.1.3ISAKMPIdentityProtection (Main Mode)70.313742192.168.1.3192.168.1.2ISAKMPQuick Mode80.321913192.168.1.2192.168.1.3ISAKMPQuick Mode90.323741192.168.1.3192.168.1.2ISAKMPQuick Mode100.334980192.168.1.2192.168.1.2ISAKMPQuick Mode110.691160192.168.1.3192.168.1.2ESPESP (SPI=0x919bfabc)121.692568192.168.1.3192.168.1.3ESPESP (SPI=0x919bfabc)131.693164192.168.1.3192.168.1.3ESPESP (SPI=0x919bfabc)142.693600192.168.1.3192.168.1.2ESPESP (SPI=0x919bfabc)152.694026192.168.1.2192.168.1.3ESPESP (SPI=0x919bfabc)	4	0.257505	192.168.1.2	192.168.1.3	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 192.168.1.2 192.168.1.3 ESP ESP (SPI=0x919bfabc) 15 2.694026 192.168.1.2 192.168.1.3 ESP ESP (SPI=0x53a5925e)	5	0.300882	192.168.1.3	192.168.1.2	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 192.168.1.2 192.168.1.3 ESP ESP (SPI=0x919bfabc) 15 2.694026 192.168.1.2 192.168.1.3 ESP ESP (SPI=0x53a5925e)	6	i 0.310186	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main 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=0x53a5925e) 15 2.694026 192.168.1.2 192.168.1.3 ESP ESP (SPI=0x53a5925e)	7	0.313742	192.168.1.3	192.168.1.2	ISAKMP	Quick Mode	
90.323741192.168.1.3192.168.1.2ISAKMPQuick Mode100.334980192.168.1.2192.168.1.3ISAKMPQuick Mode110.691160192.168.1.3192.168.1.2ESPESP(SPI=0x919bfabc)121.692568192.168.1.3192.168.1.2ESPESP(SPI=0x919bfabc)131.693164192.168.1.2192.168.1.3ESPESP(SPI=0x53a5925e)142.693600192.168.1.3192.168.1.2ESPESP(SPI=0x53a5925e)152.694026192.168.1.2192.168.1.3ESPESP(SPI=0x53a5925e)	8	3 0.321913	192.168.1.2	192.168.1.3	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)	9	0.323741	192.168.1.3	192.168.1.2	ISAKMP	Quick Mode	
11 0.691160192.168.1.3192.168.1.2ESPESP(SPI=0x919bfabc)12 1.692568192.168.1.3192.168.1.2ESPESP(SPI=0x919bfabc)13 1.693164192.168.1.2192.168.1.3ESPESP(SPI=0x53a5925e)14 2.693600192.168.1.3192.168.1.2ESPESP(SPI=0x919bfabc)15 2.694026192.168.1.2192.168.1.3ESPESP(SPI=0x53a5925e)	10	0.334980	192.168.1.2	192.168.1.3	ISAKMP	Quick Mode	
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)	11	0.691160	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)	12	1.692568	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x919bfabc)	
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)	13	; 1.693164	192.168.1.2	192.168.1.3	ESP	ESP (SPI=0x53a5925e)	
15 2.694026 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)	
						•	
Erame 1 (142 bytes on wire 142 bytes captured)	H Er al	mo 1 (142	hutes on wire	142 bytes cantu			E
Pringer 1 (142 bytes on whe, 142 bytes capter on 10:55:07:25:65		Ле I (I42 и оррот II (Dytes on whie, spa: 00:50:04:5	142 Dytes captur d:f2:72 Det: 00	-eu) 0.10.65.0	07.3f.ff	

THECDEEDEGN 1040140304	Doc.Ref	tgbvpn_cg_Wind2kServer_fr
	Doc.version	1.0 – Mai 2004
	VPN version	2.x

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
                                                                                                                                                                                                                 <u>- 🗆 ×</u>
                                                                                                                                                                                                                              *
 IP Security test . . . . . . . . . : Passed
Local IPSec Policy Active: 'TheGreenBow'
IP Security Policy Path: SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Lo
cal\ipsecPolicy{9375E462-A49A-4B02-BF0E-77C1270406C2}
IΡ
          There are 2 filters
Pas de nom
Filter Id: {BCAE9F
Policy Id: {D73AFE
                                           <BCAE9F3F-CD89-4D2D-A582-B7D9ACEAD512>
<D73AFE0E-4399-44C9-BE55-881AD5B52702>
DLICY PolicyId = <D73AFE0E-4399-44C9-BE55-881AD5B52702>
                      IPSEC_POLICY PolicyId
             IPŠEC_POLICY PolicyId = {D73AFE0E-4399
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 : 25
Dest Addr : 192.168.1.3 Dest Mask : 25
Tunnel Addr : 192.168.1.3 Src Port : 0
Protocol : 0 TunnelFilter: Yes
                                                                                                                   : 255
: 255
            Tunnel Huur - 17.
Protocol : Ø
Flags : Outbound
Pas de nom
Filter Id: (5B55)
Policy Id: (21D1)
                                                                  TunnelFilter:
                                                                                                        Yes
                                            <5855D33F-FCC1-
            Filter 1d: \SBS5D33F-FCC1-4CD7-9
Policy Id: \21D15F80-4CAD-495E-8
Src Addr : 192.168.1.3 Src M
Dest Addr : 192.168.1.2 Dest
Tunnel Addr : 192.168.1.2 Src P
Protocol : Ø TunnelFilter:
Flags : Inbound
                                                                                      4CD7
                                                                                                   98R4
                                                                                                                 A2543B27AFF0
                                                                                                  -8656
                                                                                                               -E7CEF168A76
                                                                                       Src Mask
Dest Mask
                                                                                                                         255.255.
                                                                                                                                               255
                                                                                                                       255.255.255.
                                                                                                                                                          255
                                                                                        Src Port :
lter: Yes
                                                                                                                      Ø
                                                                                                                                    Dest
                                                                                                                                                 Port
                                                                                                                                                                     И
The command completed successfully
E:\Program Files\Support Tools>_
```

THEG	RE	E	TB	

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 : <u>http://www.thegreenbow.com</u>

Support technique par émail : <u>support@thegreenbow.com</u>

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