



Configuration détaillée du DG834(G) par Magicsam



Préliminaires

1) Se connecter au routeur :

Se connecter à l'interface de configuration de votre routeur en entrant l'adresse <http://192.168.0.1> depuis votre Navigateur Internet.

Nom d'utilisateur = [admin](#)

Mot de passe = [password](#)

2) S'assurer que votre routeur à bien été livré avec la dernière version du firmware :

- . [Maintenance](#)
- . [Etat du routeur](#)

Etat du routeur**Nom de compte**

Version Firmware: V3.01.25

Port ADSL

Adresse MAC 00:00:00:00:00:00

Adresse IP 000.000.000.0

DHCP PPPOE

Masque sous-réseau IP 255.255.255.255

Adresse IP passerelle 000.000.0.0

Serveur nom de domaine (DNS) 194.117.200.10

194.117.200.15

Port LAN

Adresse MAC 00:00:00:00:00:00

Adresse IP 192.168.0.1

DHCP On

Masque sous-réseau IP 255.255.255.0

Modem

Version Firmware ADSL 4.01.02.00

Etat du Modem Connected

Vitesse de connexion descendante 1248 kbps

Vitesse de connexion montante 160 kbps

VPI 8

VCI 35

Configuration Wireless

Nom (SSID) SSID

Région Europe

Canal 1

Point d'Accès Sans Fil enable

Nom de diffusion disable

Actuellement, dernier beta firmware disponible sur le Forum = **3.01.25**

[Page de Téléchargement DG834G sur le site Netgear France](#)

[Page de Téléchargement DG834G sur le Forum Netgear France](#)

Quelques précisions concernant la mise à jour du firmware :

- Si le firmware déjà présent sur votre routeur vous donne entière satisfaction, s'il fonctionne parfaitement, si aucune des nouvelles fonctionnalités du dernier firmware ne vous intéressent, la mise à jour n'est pas nécessaire.
- Si vous avez des problèmes de stabilité ADSL avec le DG834(G) (perte de synchronisation ADSL, reboot intempestifs, ...) effectuer la mise à jour avec le firmware 2.10.22 ou 3.01.25.

Firmware 3.01.25 compatible ADSL2+ avec Free (pose des problèmes avec les autres FAI)

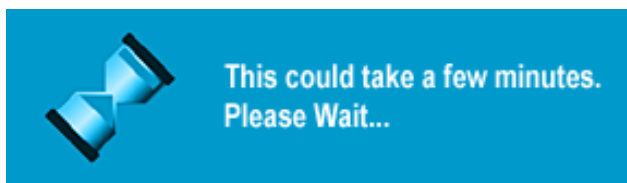
3) Le cas échéant, procéder à la mise à jour du firmware si nécessaire :


- . [Maintenance](#)
- . [Mise à niveau du routeur](#)

Mise à niveau du routeur

Localisez et sélectionnez sur votre disque dur le fichier de mise à niveau:

Cliquer sur le bouton [Parcourir](#) et ouvrir le fichier .img du dernier firmware.
Cliquer ensuite sur le bouton [Télécharger](#) et patienter jusqu'à la fin du traitement, surtout ne pas l'interrompre.



- Pour la mise à jour du firmware, consulter le Tutorial de **NicolasXP**  :
<http://tuto.netgear-forum.com/maj.html>

- En cas de problème lors de la mise à jour du firmware :

[Outil de Réparation DG834\(G\)](#)

[Procédure pour l'outil de Réparation](#)



NOUVEAU : Assistant de mise à jour DG834(G) de Mackila :
(mise à jour du firmware + reset usine + restauration des paramètres de configuration)

[Outil de mise à jour DG834\(G\) beta firmware 2.10.09](#)

[Outil de mise à jour DG834\(G\) beta firmware 2.10.17](#)

[Outil de mise à jour DG834\(G\) firmware 2.10.22](#)

[Outil de mise à jour DG834\(G\) firmware 3.01.25](#)

Configuration de base

1) La partie Modem

. [Assistant de configuration](#) / [Assistant d'installation](#)

Assistant de configuration

Sélectionnez le pays et la langue

Pays:

Langue:

Détection Automatique du Type de Connexion

Cet Assistant de configuration peut détecter le type de connexion Internet dont vous disposez.

Voulez-vous que l'Assistant avancé de configuration essaie de détecter maintenant le type de connexion existante?

Oui

Non. Je préfère configurer le routeur moi-même.

Configurer le pays et la langue.

Puis, choisir [Détection Automatique du Type de Connexion](#) ou [Configuration manuelle du routeur](#).

Bouton [Suivant](#).

Si Configuration manuelle du routeur

- [Configuration / Installation](#)
- [Paramètres de base](#)

Paramètres de base

Votre connexion Internet demande-t-elle un pseudonyme à l'ouverture de session?

Oui

Non

Encapsulation

Pseudo

Mot de passe

Nom de domaine (le cas échéant)

Dépassement délai d'inactivité (en minutes)

Adresse DNS (serveur nom de domaine)

Obtenir automatiquement de l'ISP

Utiliser les serveurs DNS suivants

DNS primaire

. . .

DNS secondaire

. . .

NAT (traduction d'adresse réseau)

Activer

Désactiver

Configurer l'Encapsulation : PPPoE ou PPPoA.

Configurer les paramètres de connexion indiqué par votre FAI (login, mot de passe, DNS).

Laisser le [Dépassement délai d'inactivité](#) à 0 (pour la majorité des configurations).

Laisser [NAT \(traduction d'adresse réseau\)](#) activé.

Permet de masquer l'adresse matériel des PC de votre réseau local.

Seul votre DG834(G) est identifié comme se connectant sur Internet.

Possibilité de modifier de nouveau les paramètres par la suite sans repasser par l'Assistant de configuration en cas de mauvaise configuration.

- [Configuration / Installation](#)
- [Paramètres ADSL](#)

Paramètres ADSL

Méthode de multiplexage

VPI

VCI

Méthode multiplexage

Si PPPoE = LLC

Si PPPoA = VC

VPI/VCI = 8/35 pour la majorité des FAI

2) La partie Routeur

- [Avancés](#)
- [Configuration WAN](#)

Configuration WAN

Connecter automatiquement selon les besoins

Désactiver la protection DOS et Balayage de ports

Serveur DMZ par défaut

Répondre au ping sur le port Internet

Taille MTU (en octets)

S'assurer de cocher l'option [Connecter automatiquement selon les besoins](#).

Afin d'assurer la reconnexion automatique toutes les 24H.

Pour une sécurité optimale, ne pas cocher [Désactiver la protection DOS et Balayage de ports](#), ni [Répondre au ping sur le port internet](#) sauf en cas de nécessité.

Laisser la [Taille MTU](#) par défaut (pour la majorité des configurations).

Configurer un [Serveur DMZ](#) seulement si besoin.

Il s'agit d'une zone démilitarisée, accessible à quiconque sur Internet.

Il suffit simplement d'indiquer l'adresse IP du PC de votre réseau local pour lequel vous souhaitez n'exercez aucune règles de sécurité.

Bien sûr, ouvrir un Serveur DMZ n'est pas l'idéal en termes de sécurité, mais peut s'avérer parfois bien pratique.

. [Avancés](#)

. [Configuration IP LAN](#)

Configuration IP LAN

Configuration TCP/IP LAN

Adresse IP

Masque sous-réseau IP

Direction RIP:

Version RIP

Utiliser le routeur comme Serveur DHCP

Adresse IP de début

Adresse IP de fin

Réservation d'adresse

	#	Adresse IP	Nom du périphérique	Adresse MAC
	1	192.168.0.2	PC 1	00:00:00:00:00:01
	2	192.168.0.3	PC 2	00:00:00:00:00:02
	3	192.168.0.4	PC 3	00:00:00:00:00:03
	4	192.168.0.5	PC 4	00:00:00:00:00:04
	5	192.168.0.6	PC 5	00:00:00:00:00:05
	6	192.168.0.7	PC 6	00:00:00:00:00:06

Cocher l'option [Utiliser le routeur comme Serveur DHCP](#).

Laisser tout le reste par défaut.

Réserver une adresse IP fixe à chaque PC de votre réseau, qu'il soit relié en Wifi ou par câble RJ45 :

. [Réservation d'adresse](#)

. bouton [Ajouter](#)

Réservation d'adresse

Tableau de Réservation d'adresse

	#	Adresse IP	Nom du périphérique	Adresse MAC
	1	192.168.0.2	PC 1	00:00:00:00:00:01
	2	192.168.0.3	PC 2	00:00:00:00:00:02
	3	192.168.0.4	PC 3	00:00:00:00:00:03

Adresse IP

Adresse MAC

Nom du périphérique:

Sélectionner à l'aide du bouton radio le PC désiré dans la liste .

Indiquer l'adresse IP fixe désirée.

Indiquer le nom désiré.

Puis bouton [Ajouter](#).

Réserver les adresses IP depuis le DG834(G) présente plusieurs avantages :

- 1) Pas besoin de configurer chaque carte réseau de tous les PC du réseau en IP fixe (attribution IP dynamique par défaut).
- 2) Possibilité d'associer chaque IP à une adresse matériel MAC pour plus de sécurité.
- 3) Réserver une adresse IP depuis le DG834(G) nous sera d'une grande utilité par la suite, pour définir les Règles Pare-feu ou identifier certains évènements sur le journal système du routeur.

3) La partie Wifi

- . [Configuration / Installation](#)
- . [Paramètres Sans Fil](#)

Paramètres Sans Fil

Réseau Sans Fil

Nom (SSID):

Région:

Canal:

Mode:

Point d'Accès Sans Fil

Activer le Point d'Accès Sans Fil

Autoriser la Diffusion du Nom (SSID)

Wireless Peer-to-Peer Isolation

Liste d'Accès des Stations Sans Fil

Options de sécurité

Disable

WEP

WPA-PSK

WPA-802.1x

- Indiquer le même nom **SSID** que sur vos adaptateurs sans fil.
- Configurer en mode Europe et en Canal 1 (le canal le moins encombré en règle générale).
- Configurer en mode **g seulement** si votre réseau Wifi est constitué uniquement de périphériques 802.11g, dans le cas contraire choisir le mode **g et b**.
- Cocher l'option **Activer le Point d'Accès sans Fil**.
- Décocher l'option **Autoriser la Diffusion du Nom (SSID)** afin de masquer la diffusion du nom SSID de votre réseau local (pour plus de sécurité).
- Cocher l'option **Wireless Peer-to-Peer Isolation** si vous souhaitez interdire l'échange de fichiers entre les PC Wifi de votre réseau local.

Tous les PC Wifi seront invisibles les uns pour les autres sur votre réseau local, seuls les PC filaires connectés en RJ45 au routeur seront disponibles depuis un PC Wifi.

- Activer le contrôle d'accès par adresse MAC.
- [Configuration de la liste d'accès](#)

Liste d'Accès des Stations Sans Fil

Activer le Contrôle d'accès

Stations Sans Fil de Confiance

	Nom du périphérique	Adresse MAC
	PC 3	00:00:00:00:00:03

Stations Sans Fil Disponibles

	Nom du périphérique	Adresse MAC
--	---------------------	-------------

Ajouter une nouvelle station manuellement

Nom du périphérique:

Adresse MAC:

Dans Stations [Sans Fil Disponibles](#), cocher le bouton radio du PC que vous souhaitez autoriser à communiquer en Wifi.

Puis cliquer sur le bouton Ajouter, le PC apparaît alors en [Stations Sans Fil de Confiance](#).

Vous pouvez ensuite cocher l'option [Activer le Contrôle d'Accès](#).

- Activer le cryptage WEP, ou mieux WPA-PSK si vos adaptateurs sans fil le permettent.

- Cryptage WEP

Paramètres Sans Fil

Réseau Sans Fil

Nom (SSID):

Région:

Canal:

Mode:

Point d'Accès Sans Fil

Activer le Point d'Accès Sans Fil

Autoriser la Diffusion du Nom (SSID)

Wireless Peer-to-Peer Isolation

Liste d'Accès des Stations Sans Fil

Options de sécurité

Disable

WEP

WPA-PSK

WPA-802.1x

Cryptage de Sécurité (WEP)

Type d'Authentification:

Niveau de cryptage:

Code de Cryptage de Sécurité (WEP)

Phrase Clef:

Code 1:

Code 2:

Code 3:

Code 4:

. Type d'Authentification = Code partagé

. Niveau de cryptage = 128 bits (pour plus de sécurité)

. Générer une ou plusieurs Phrases Clef, et configurer une Phrase Clef identique sur vos adaptateurs sans fil.

- Cryptage WPA-PSK

Paramètres Sans Fil

Réseau Sans Fil

Nom (SSID):

Région:

Canal:

Mode:

Point d'Accès Sans Fil

Activer le Point d'Accès Sans Fil

Autoriser la Diffusion du Nom (SSID)

Wireless Peer-to-Peer Isolation

Liste d'Accès des Stations Sans Fil

Options de sécurité

Disable

WEP

WPA-PSK

WPA-802.1x

Cryptage de sécurité (WPA-PSK)

Code de Cryptage de Sécurité (WPA)

(8 ~ 64 caractères)

. Simplement entrer une Phrase Clef identique (de minimum 8 caractères) sur le DG834G et sur vos adaptateurs sans fil.

. Penser aussi à installer le Patch WPA Windows XP sur chacun de vos PC (uniquement avec le SP1, déjà présent avec le SP2)

[WindowsXP-KB826942-x86-FRA.exe](#)

Configuration Avancée

1) Le menu **Sécurité / Filtrage de contenu**

. [Planning](#)

(définir un planning utilisé par la suite avec les fonctions [Règles Pare-feu](#), [Blocage de sites](#), et [Journaux](#))

Planning

Jours:

Chaque jour

Lundi

Mardi

Mercredi

Jeudi

Vendredi

Samedi

Dimanche

Heure du jour: (utiliser le format sur 24 heures)

Toute la journée

Heure de début

Heures

Minutes

Heure de fin

Heures

Minutes

Fuseau horaire

Régler pour l'observation de l'heure d'été

Utiliser ce Serveur NTP

Heure actuelle: 2004-07-03 15:36:29

Possibilité de définir un planning par jours et/ou plages horaires.

Fuseau Horaire : (GMT+01:00) pour la France.

Si nécessaire cocher [Régler pour l'observation de l'heure d'été](#) pour ajuster l'heure indiquée par le routeur de + ou - 1H.

Possibilité d'utiliser l'adresse IP d'un Serveur NTP particulier pour maintenir à jour la configuration du Fuseau horaire du DG834(G).

Journaux

Journaux

Heure actuelle: 2004-07-03 15:36:25

Inclure dans le journal

- Tentatives d'accès à des sites bloqués
- Connexions à l'interface Web de ce routeur.
- Fonctionnement du routeur (démarrage, heure d'écriture, etc.)
- Attaques DOS connues et Balayage de ports

Syslog

- Désactiver
- Diffuser sur le LAN
- Envoyer à l'adresse IP du serveur Syslog

- Inclure dans le journal

Permet de configurer les évènements que vous souhaitez que le routeur consigne dans un journal.

Tentatives d'accès à des sites bloqués : est utile uniquement si vous filtrez l'accès Internet de certains PC de votre réseau (**Blocage de sites**).

Fonctionnement du routeur : intéressant dans la mesure où cela laisse un historique (utile en cas de pb de déconnexion ADSL, mauvaise reconnexion des 24H etc ...).

Connexions à l'interface Web de ce routeur : permet de vérifier qui, sur le réseau local, accède au menu de configuration de votre routeur (et donc au paramétrage).

Attaques DOS connues et Balayage de ports : tentatives d'intrusion des vilains hackers.

- [Syslog](#)
Par défaut le laisser désactiver.
N'est utile que si vous souhaitez utiliser un serveur Syslog pour récupérer le journal du DG834(G).

- . [Services](#)
(pour créer des services supplémentaires qui seront ensuite utilisés avec les [Règles Pare-feu](#))

Services

Tableau des services

#	Type de service	Ports
1	Emule UDP	4672
2	Emule TCP	4662
3	BitTorrent	6881 - 7881

Bouton [Ajouter Service Personnalisé.](#)

Ajouter Services

Définition du Service

Nom:

Type:

Port de début:

Port de fin:

Nom : indiquer un nom au service que vous créer.

Type : TCP, UDP ou TCP/UDP.

Port de début, **Port de fin** : plage de ports entrants à autoriser (pour BitTorrent = 6881 à 7881).

Blocage de sites

Blocage de sites

Blocage sur mot-clé

- Jamais
- Selon planning
- Toujours

Tapez ici le Mot-clé ou le Nom de domaine.

Bloquer les sites qui contiennent ces mot-clés ou ces noms de domaine:

Autoriser l'Adresse IP de confiance à visiter les sites bloqués.

Autoriser l'Adresse IP

. . .

- Blocage sur mot-clé

Permet de faire du filtrage de contenu des sites Web (contrôle parentale, blocage des pub, etc ...), soit de façon permanente ([Toujours](#), soit en fonction d'une plage horaire et/ou des jours de la semaine ([Selon planning](#)). Le fonctionnement est assez simple, il suffit d'ajouter un à un dans la liste les mots clés que vous souhaitez voir bloquer.

- Autoriser l'Adresse IP de confiance à visiter les sites bloqués

Permet d'autoriser un des PC du réseau local à avoir accès à l'intégralité des pages Internet, sans tenir compte du [Blocage de sites](#).

. Règles Pare-feu

Règles Pare-feu

Services sortants

	#	Activer	Nom du service	Action	Utilisateurs LAN	Serveurs WAN	Journal
	1		Any(ALL)	BLOCK always	192.168.0.4-192.168.0.254	Any	Never
	Par défaut	Oui	Indifférent	Toujours PERMETTRE	Indifférent	Indifférent	Jamais

Services entrants

	#	Activer	Nom du service	Action	Adresse IP serveur LAN	Utilisateurs WAN	Journal
	1		BitTorrent	ALLOW always	192.168.0.2	Any	Never
	2		FTP	ALLOW always	192.168.0.2	Any	Never
	3		Emule TCP	ALLOW always	192.168.0.2	Any	Never
	4		Emule UDP	ALLOW always	192.168.0.2	Any	Never
	Par défaut	Oui	Indifférent	Toujours BLOQUER	Indifférent	Indifférent	Jamais

Par défaut, le pare feu bloque toutes les communications entrantes et autorise toutes les communications sortantes.

- Services sortants

Exemple d'utilisation : Interdire tout accès Internet à un ou plusieurs PC de votre réseau.

Bouton [Ajouter](#)

Services sortants

Service

Action

Utilisateurs LAN

début: . . .

fin: . . .

Utilisateurs WAN

début: . . .

fin: . . .

Journal

Service : Any(ALL)

Toute une liste de service est déjà à votre disposition.

Un service correspondant à une application ou un protocole de communication déterminé (ex: Http, FTP, News ...).

Vous pouvez par la suite configurer vos propres services, au hasard Emule, BitTorrent, etc ...

Action : Toujours BLOQUER

Vous avez aussi la possibilité de bloquer ou d'autoriser suivant le [Planning](#).

Utilisateurs LAN : adresse IP du ou des PC de votre réseau local.

3 Possibilités :

- Tous = bloquer tous les PC de votre réseau (pour bloquer un service déterminé par exemple).

- Une seule adresse = bloquer un PC déterminé.

- Plage d'adresses = bloquer plusieurs PC (dans mon exemple tous les PC de l'IP 192.168.0.4 à 192.168.0.254).

Utilisateurs WAN : adresse IP Internet (pour bloquer une adresse IP ou une plage d'adresse).

Journal : pour choisir d'inscrire ou non l'évènement dans le journal.

- Services entrants

Exemple d'utilisation : Ouvrir les ports nécessaires pour utiliser un logiciel de P2P (ce qui s'appelle du Port Forwarding).

Services entrants

Service

Action

Envoyer au serveur LAN

. . .

Utilisateurs WAN

début:

. . .

fin:

. . .

Journal

Le principe est exactement le même que pour [Services sortants](#).

Il faut configurer l'IP LAN ([Envoyer au serveur LAN](#)) du PC de votre réseau local sur lequel va être utilisé le service en question.

Il ne vous est par contre pas possible de configurer plusieurs IP pour le même service.

. E-mail

(pour recevoir périodiquement le journal système du routeur)

E-mail

Activer notification par E-mail

Envoyer alertes et journaux par E-mail

Serveur messagerie sortant:

My Mail Server requires authentication

Pseudo

Mot de passe

Envoyer à l'adresse E-mail suivante:

Envoyer immédiatement les alertes par E-mail

En cas de détection d'une attaque DOS.

En cas de détection d'un balayage de port.

Si quelqu'un tente d'accéder à un site bloqué.

Envoyer les journaux selon les conditions suivantes

Jour

Heure a.m. p.m.

- Cocher [Activer notification par E-mail](#) et saisir votre serveur mail sortant.
 - Si votre serveur de mail nécessite une authentification, cocher [My mail Server requires authentication](#) et configurer les paramètres de votre messagerie internet (login, mot de passe).
 - Si vous souhaitez être averti en temps réel des tentatives d'intrusion sur votre réseau (attaque DOS, balayage de port, accès à un site bloqué), cocher [Envoyer immédiatement les alertes par E-mail](#).
 - Configurer la périodicité de réception par E-mail du journal système.
- Dans mon exemple, tous les jours à midi.

2) Le menu Maintenance

. [Etat du routeur](#) (voir photo d'écran dans la partie Préliminaires)

Cette page indique pas mal d'informations bien utile sur la configuration de votre routeur : version du Firmware, adresse IP ADSL attribuée, modem connecté ou non, etc ...

- Bouton [Etat de la Connexion](#)

Etat de la connexion

Heure de connexion	03:17:38
Connexion au serveur	Connected
Négociation	Success
Authentification	Success
Obtention des adresses IP	000.000.00.0
Obtention du masque réseau	255.255.255.255

Pratique pour connecter et déconnecter manuellement la connexion ADSL.

- Bouton [Voir Statistiques](#)

Temps de disponibilité système 03:19:21

Port	Etat	Paquets émis	Paquets reçus	Collisions	Emission B/s	Réception B/s	Temps de disponibilité
WAN	PPPoA	192323	180767	0	5512	9030	03:17:41
LAN	100M/Full	183974	210090	0	9251	5902	03:19:19
WLAN	54M	0	0	0	0	0	00:00:00

Lien ADSL	Downstream	Upstream
Vitesse de connexion	1248 kbps	160 kbps
Atténuation lignen	51 db	22.5 db
Marge de bruit	11 db	23 db

Rafraîchissement
toutes les: (secs)

Quelques informations intéressantes concernant les différentes connexions du routeur (le temps de connexion entre autres).

WAN = Connexion Internet

LAN = Connexion Réseau Local

WLAN = Connexion Wifi

Indique aussi l'atténuation et la marge de bruit de votre ligne.

· Périphériques connectés

Périphériques connectés			
#	Adresse IP	Nom du périphérique	Adresse MAC
1	192.168.0.2	PC 1	00:00:00:00:00:01
2	192.168.0.3	PC 2	00:00:00:00:00:02
3	192.168.0.4	PC 3	00:00:00:00:00:03

Liste des périphériques actuellement connectés au DG834(G).
Cela concerne aussi bien les périphériques filaire que sans fil.

· Sauvegarde Paramètres

Paramètres de sauvegarde
Enregistrer une copie du paramétrage actuel
Restaurer le paramétrage sauvegardé à partir d'un fichier
Revenir au paramétrage d'usine

Permet de sauvegarder/restaurer la configuration dans un fichier.

A noter aussi le bouton [Effacer](#) qui permet de réinitialiser votre DG834(G) au paramétrage d'usine (exactement identique que de faire un reset matériel avec le petit bouton situé à l'arrière du routeur).

. Définir Mot de passe

Définir Mot de passe

Ancien Mot de passe

Nouveau Mot de passe

Répéter Nouveau mot de passe

La connexion Administrateur sera interrompue après une période d'inactivité de minutes.

Afin de modifier le mot de passe par défaut (=password) permettant d'accéder à l'interface de configuration du routeur.

Pour une meilleure sécurité, il est vivement conseillé de systématiquement modifier ce mot de passe.

. Diagnostics

Diagnostics

Sonder une adresse IP

Adresse IP

Effectuer une recherche DNS

Nom Internet:

Adresse IP

Serveur DNS: 194.117.200.10
194.117.200.15

Afficher la table de routage

Redémarrer le routeur

- Sonder une adresse IP

Permet de tester la communication vers une adresse IP locale.

Equivalent à la commande Ping bien connue.

- Effectuer une recherche DNS

Permet de convertir un nom de domaine Internet en adresse IP.

- [Redémarrer le routeur](#)

Permet de réinitialiser le routeur de façon logiciel, cela revient un peu à brancher et débrancher la prise secteur. Option intéressante car moins agressif pour l'électronique que de le débrancher du secteur.

. [Mise à niveau du routeur](#) (voir photo d'écran dans la partie Préliminaires)

Fonction indispensable pour mettre à jour le firmware du routeur.

3) Le menu Avancés

. [Configuration WAN](#) (voir photo d'écran et explications dans la partie Configuration de base)

. [DNS dynamique](#)

DNS dynamique

Utiliser le Service DNS dynamique

Fournisseur de service

Nom d'hôte

Nom d'utilisateur

Mot de passe

Utiliser caractères de substitution

Permet d'affecter un nom de domaine DynDNS.org au routeur.

C'est une façon d'avoir un nom de domaine fixe tout en conservant le bénéfice d'une adresse IP dynamique.

Très utile pour mettre en place un serveur FTP ou faciliter la gestion à distance de votre routeur.



Consulter le Tutorial de **Petit Bill** pour créer votre nom de domaine DynDNS :

<http://www.netgear-forum.com/forum/index.php?showtopic=423>

. [Configuration IP LAN](#) (voir photo d'écran et explications dans la partie Configuration de base)

Gestion à distance

Gestion à distance

Activer la Gestion à distance

Adresse de gestion à distance

http://000.000.00.0:8080

Autoriser accès distant par

Cet ordinateur seulement:

. . .

Plage d'adresses IP :

De

. . .

À

. . .

Tous

Numéro de port

Permet d'accéder à l'interface de configuration de votre routeur depuis un poste distant via Internet.

- Cocher l'option [Activer la Gestion à distance](#).

- Autoriser l'accès distant à un seul ordinateur (une seule adresse IP), une plage d'adresses d'IP ou bien à n'importe quelle adresse IP.

- L'adresse http pour accéder à votre routeur est indiquée dans [Adresse de gestion à distance](#).

Elle est de la forme `http://adresse IP Internet du routeur:8080` (8080 étant le port configuré par défaut pour la gestion à distance).

- A noter que mettre en place une adresse [DNS dynamique](#) (voir un peu plus haut) facilite grandement la gestion à distance.

L'adresse `http://nom de domaine.dyndns.org:8080` permettra d'accéder à l'interface de configuration du routeur sans avoir besoin de connaître son adresse IP Internet à ce moment là.

UPnP

UPnP

Activer le UPnP

Intervalle de diffusion (en minutes)

Durée de vie de diffusion (en sauts)

Tableau des ports UPnP

Actif	Protocole	Port Interne	Port Externe	Adresse IP
-------	-----------	--------------	--------------	------------

Cocher cette option uniquement si vous utilisez MSN Messenger, Azureus ou tout autre logiciel gérant l'UPnP.



Consulter le Tutorial de **Poussin** pour installer l'UPnP sous Windows XP :

<http://www.netgear-forum.com/forum/index.php?showtopic=2678>

Configuration VPN

Depuis le beta firmware 2.10.09 le DG834(G) permet d'établir 5 tunnels VPN (Virtual Private Networking).

Un tunnel VPN permet une connexion sécurisée et cryptée entre votre réseau local, et un réseau local ou un ordinateur distant.

Seul l'échange des données en [Mode Principal](#) est disponible pour l'instant.

Par conséquent :

- Seul l'établissement d'un Tunnel VPN entre deux DG834(G) ou bien entre un DG834(G) ou un autre routeur VPN distant est possible.

- L'établissement d'un Tunnel VPN entre un DG834(G) et un PC distant via Client VPN n'est possible uniquement que si le PC distant n'appartient pas à un réseau avec un routeur utilisant le protocole NAT.

Tunnel entre un DG834(G) et un autre Routeur VPN



Impératif : chaque routeur VPN doit être configuré avec un plan d'adressage IP différent.

Le premier routeur devant être configuré avec les adresses IP LAN et WAN du routeur distant et inversement.

1) Configuration à l'aide de l'assistant VPN :

- . [Avancés - VPN](#)
- . [Assistant de VPN](#)

Assistant VPN

L'assistant règle la plupart des paramètres sur leur valeur par défaut conformément aux recommandations du consortium du VPN (VPNC) et définit une clé prépartagée qui simplifie énormément la configuration.

Après avoir créé les politiques à l'aide de l'assistant VPN, vous pouvez toujours actualiser les paramètres à l'aide des liens de paramètres VPN affichés dans le menu de gauche.

Cliquer sur le bouton [Suivant](#).

Assistant VPN

Etape 1 de 3 : Nom de la connexion et type d'IP distante

Quel est le nouveau nom de la connexion ?

Quel est la clé prépartagée ?

Ce tunnel VPN se connectera à :

Une passerelle VPN distante

Un client VPN distant (monoposte)

Saisir un nom de connexion et une clé prépartagée.

Choisir ensuite le type de périphérique distant avec lequel la connexion VPN sera établie, ici [passerelle VPN distante](#) pour un autre routeur VPN.

Puis cliquer sur le bouton [Suivant](#).

Assistant VPN

Etape 2 de 3 : L'adresse IP distante ou le nom Internet

Quelle est l'adresse IP WAN ou le nom Internet ?

Configurer l'adresse IP ou le nom de domaine Internet du routeur distant.

Puis cliquer sur le bouton [Suivant](#).

Assistant VPN

Etape 3 de 3 : Accessibilité à distance à une connexion sûre

Quelle est l'adresse IP du LAN **distant** et le masque du sous-réseau ?

Adresse IP	.	.	.
Masque sous-réseau:	.	.	.

Configurer l'adresse IP et le masque de sous réseau du routeur distant qui utilisera le tunnel VPN.

Puis cliquer sur le bouton [Suivant](#).

Assistant VPN

Résumé

Veillez vérifier vos entrées :

Nom de la connexion :	VPN
Point final VPN distant :	netgear2.dyndns.org
Accès du client distant :	By Subnet
IP distante :	192.168.1.0 / 255.255.255.0
Identif. distante :	
Accès du client local :	Par sous-réseau
IP local :	192.168.0.1 / 255.255.255.0
Identif. locale :	

Vous pouvez cliquer [ici](#) pour afficher les paramètres recommandés par le VPNC.

Cliquez sur le bouton **Terminé** pour enregistrer les modifications.

Un écran récapitulatif apparaît.

Cliquer sur le bouton [Terminé](#) pour valider la configuration du tunnel VPN.

Le Tunnel VPN est alors disponible sur la page [Politiques VPN](#), il est maintenant possible de compléter certains paramètres de configuration manuellement à l'aide du bouton [Editer](#).

2) Configuration manuelle :

- . [Avancés - VPN](#)
- . [Politiques VPN / Règles VPN](#)

Politiques VPN**Tableau des politiques**

	#	Activer	Nom	Type	Local	Distant	ESP
	1		VPN	Auto	192.168.0.1 / 255.255.255.0	192.168.1.0 / 255.255.255.0	3DES

Cliquer sur le bouton [Ajouter une politique automatique](#).

VPN - Politique automatique**Généralités**

Nom de la politique

Point final VPN distant

Type d'adresse :

Données de l'adresse :

Activer NETBIOS

LAN local

Adresse IP

Adresse simple/de départ : . . .

Adresse finale : . . .

Masque sous-réseau: . . .

LAN distant

Adresse IP

Adresse IP simple/de départ : . . .

Adresse IP finale : . . .

Masque sous-réseau: . . .

IKE

Sens

Mode d'échange

Groupe Diffie-Hellman (DH)

Type d'identité locale

Données

Type d'identité distante

Données

Paramètres

Algorithme de cryptage

Algorithme d'authentification

Clé prépartagée

Durée de vie logicielle

(Secondes)

Activer PFS (Perfect Forward Security)

Saisir un nom de politique.

Configurer l'adresse du [Point final VPN distant](#), une [Adresse IP fixe](#) ou un [Nom de domaine complètement qualifié](#) correspondant au routeur VPN distant.

Cocher l'option [Activer NETBIOS](#).

En [LAN Local](#) choisir [Adresse de sous-réseau](#) et configurer l'adresse IP de votre routeur VPN ainsi que le masque de sous réseau.

En [LAN distant](#) choisir [Adresse de sous-réseau](#) et configurer le plan d'adressage IP du routeur VPN distant (ici 192.168.1.0 / 255.255.255.0).

Configurer la politique [IKE](#) :

- . Sens = [Initiateur et Répondeur](#) (choisir [Répondeur uniquement](#) pour n'autoriser seulement que les communications entrantes)
- . Mode d'échange = [Mode principal](#) (le seul disponible pour le moment)
- . Groupe Diffie-Hellman (DH) = [Groupe 5 \(1536 Bit\)](#) (le plus sécurisé)
- . Type d'identité local = [Adresse IP WAN](#) ou [Nom de domaine complètement qualifié](#) (adresse Internet IP fixe ou Nom de domaine Internet de votre routeur)
- . Type d'identité distante = [Adresse IP](#) ou [Nom de domaine complètement qualifié](#) (adresse Internet IP fixe ou Nom de domaine Internet du routeur VPN distant)

Configurer les paramètres de sécurité [IKE](#) :

- . Algorithme de cryptage = 3DES (niveau de cryptage le plus sécurisé)
- . Algorithme d'authentification = SHA-1 (algorithme d'authentification le plus sécurisé)
- . Saisir la même [Clé prépartagée](#) que sur le routeur VPN distant
- . Durée de vie logicielle = 28800 (temps en secondes au bout duquel la connexion sécurisée expire)

Cocher l'option [Activer PFS \(Perfect Forward Security\)](#) (optimise la sécurité en changeant la clé à intervalles réguliers).

Puis cliquer sur le bouton [Appliquer](#) pour valider les paramètres de configuration.

3) Etablir la connexion VPN :

- . [Avancés - VPN](#)
- . [Etat VPN / Statut VPN](#)

Etat/journal VPN

Cliquer sur le bouton [Etat VPN](#).

Tunnels VPN actuels (SA)

#	SPI (entrée)	SPI (sortie)	Nom de la politique	Point final distant	Action	Durée de vie logicielle	Durée de vie matérielle
1	---	---	VPN	---		---	---

Cliquer sur le bouton [Connect](#) correspondant au Tunnel VPN que vous souhaitez établir.

Tunnels VPN actuels (SA)

#	SPI (entrée)	SPI (sortie)	Nom de la politique	Point final distant	Action	Durée de vie logicielle	Durée de vie matérielle
1	f892e903	81238a22	VPN	00.00.000.00		28335	28335

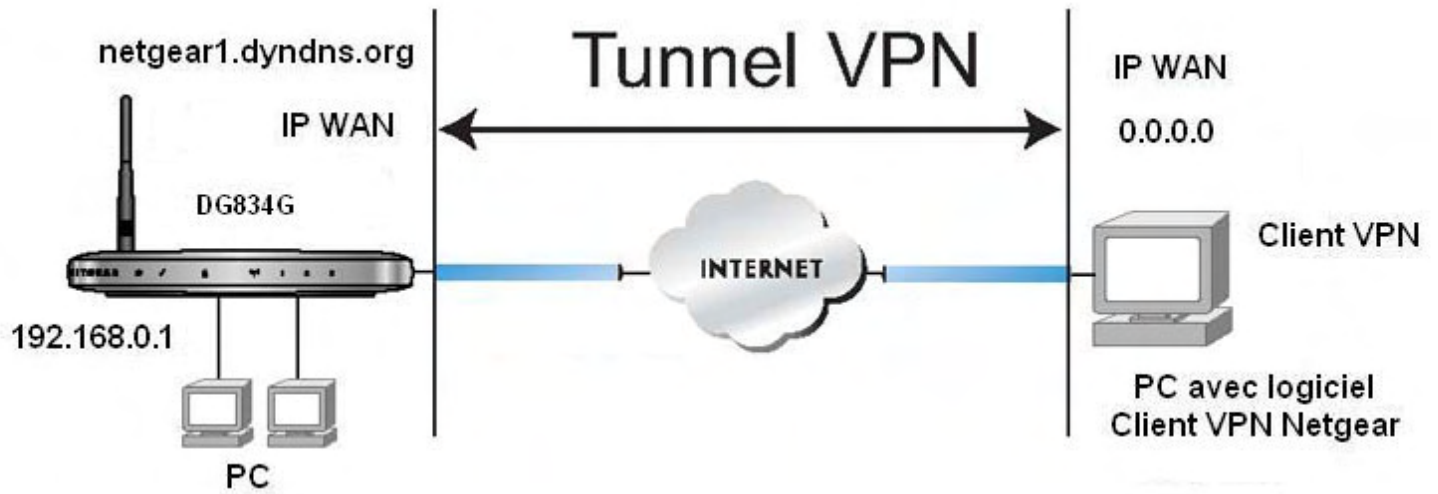
Au bout de quelques secondes le Tunnel VPN est actif (le [journal VPN](#) (voir plus haut) permet également de constater l'établissement du Tunnel VPN).

Le bouton [Drop](#) permettant de déconnecter manuellement le Tunnel VPN.

Pour accéder à l'interface de configuration du routeur VPN distant, simplement ouvrir votre Navigateur Internet et entrer l'adresse IP local du routeur de la forme ***http://192.168.x.x***.

Pour accéder aux ressources partagées d'un PC distant, simplement ouvrir l'Explorateur Windows et accéder au PC par son adresse IP local de la forme ***\\192.168.x.x***.

Tunnel entre un DG834(G) et un PC distant équipé du logiciel Client VPN Netgear



Impératif : le DG834(G) et le PC distant équipé du logiciel Client VPN doivent être configurés avec un plan d'adressage IP différent.

Rappel : L'établissement d'un Tunnel VPN entre un DG834(G) et un PC distant via Client VPN n'est possible uniquement que si le PC distant n'appartient pas à un réseau avec un routeur utilisant le protocole NAT.

I. Configuration du DG834(G)

1) Configuration à l'aide de l'assistant VPN :

- . [Avancés - VPN](#)
- . [Assistant de VPN](#)

Assistant VPN

L'assistant règle la plupart des paramètres sur leur valeur par défaut conformément aux recommandations du consortium du VPN (VPNC) et définit une clé prépartagée qui simplifie énormément la configuration.

Après avoir créé les politiques à l'aide de l'assistant VPN, vous pouvez toujours actualiser les paramètres à l'aide des liens de paramètres VPN affichés dans le menu de gauche.

Cliquer sur le bouton [Suivant](#).

Assistant VPN

Etape 1 de 3 : Nom de la connexion et type d'IP distante

Quel est le nouveau nom de la connexion ?

Quel est la clé prépartagée ?

Ce tunnel VPN se connectera à :

Une passerelle VPN distante

Un client VPN distant (monoposte)

Saisir un nom de connexion et une clé prépartagée.

Choisir ensuite le type de périphérique distant avec lequel la connexion VPN sera établie, ici [client VPN distant \(monoposte\)](#) pour un PC distant équipé d'un logiciel client VPN.

Puis cliquer sur le bouton [Suivant](#).

Assistant VPN

Résumé

Veillez vérifier vos entrées :

Nom de la connexion :	VPNClient
Point final VPN distant :	Client PC
Accès du client distant :	Monoposte
IP distante :	Dynamic
Identif. distante :	
Accès du client local :	Par sous-réseau
IP local :	192.168.0.1 / 255.255.255.0
Identif. locale :	

Vous pouvez cliquer [ici](#) pour afficher les paramètres recommandés par le VPNC.

Cliquez sur le bouton **Terminé** pour enregistrer les modifications.

Un écran récapitulatif apparaît.

Cliquer sur le bouton [Terminé](#) pour valider la configuration du tunnel VPN.

Le Tunnel VPN est alors disponible sur la page [Politiques VPN](#), il est maintenant possible de compléter certains paramètres de configuration manuellement à l'aide du bouton [Editer](#).

2) Configuration manuelle :

- . [Avancés - VPN](#)
- . [Politiques VPN / Règles VPN](#)

Politiques VPN**Tableau des politiques**

	#	Activer	Nom	Type	Local	Distant	ESP
	1		VPNClient	Auto	192.168.0.1 / 255.255.255.0	---	3DES

Cliquer sur le bouton [Ajouter une politique automatique.](#)

VPN - Politique automatique**Généralités**

Nom de la politique

Point final VPN distant

Type d'adresse :

Données de l'adresse :

Activer NETBIOS

LAN local

Adresse IP

Adresse simple/de départ : . . .

Adresse finale : . . .

Masque sous-réseau: . . .

LAN distant

Adresse IP

Adresse IP simple/de départ : . . .

Adresse IP finale : . . .

Masque sous-réseau: . . .

IKE

Sens

Mode d'échange

Groupe Diffie-Hellman (DH)

Type d'identité locale

Données

Type d'identité distante

Données

Paramètres

Algorithme de cryptage

Algorithme d'authentification

Clé prépartagée

Durée de vie logicielle

(Secondes)

Activer PFS (Perfect Forward Security)

Saisir un nom de politique.

Configurer l'adresse du [Point final VPN distant](#) sur [Adresse IP WAN](#).

En [LAN Local](#) choisir [Adresse de sous-réseau](#) et configurer l'adresse IP de votre DG834(G) ainsi que le masque de sous réseau.

En [LAN distant](#) configurer en [Monoposte - pas de Sous-réseau Adresse Simple](#).

Configurer la politique **IKE** :

- . Sens = [Initiateur et Répondeur](#) (choisir [Répondeur uniquement](#) pour n'autoriser seulement que les communications entrantes)
- . Mode d'échange = [Mode principal](#) (le seul disponible pour le moment)
- . Groupe Diffie-Hellman (DH) = [Groupe 2 \(1024 Bit\)](#). Type d'identité local = [Adresse IP WAN](#) ou [Nom de domaine complètement qualifié](#) (adresse Internet IP fixe ou Nom de domaine Internet de votre routeur)
- . Type d'identité distante = [Adresse IP](#)

Configurer les paramètres de sécurité **IKE** :

- . Algorithme de cryptage = [3DES](#) (niveau de cryptage le plus sécurisé)
- . Algorithme d'authentification = [SHA-1](#) (algorithme d'authentification le plus sécurisé)
- . Saisir la même [Clé prépartagée](#) que sur le Client VPN Distant
- . Durée de vie logicielle = [28800](#) (temps en secondes au bout duquel la connexion sécurisée expire)

Puis cliquer sur le bouton [Appliquer](#) pour valider les paramètres de configuration.

3) Etablir la connexion VPN :

- . [Avancés - VPN](#)
- . [Etat VPN / Statut VPN](#)

Etat/journal VPN

Cliquer sur le bouton [Etat VPN](#).

Tunnels VPN actuels (SA)

#	SPI (entrée)	SPI (sortie)	Nom de la politique	Point final distant	Action	Durée de vie logicielle	Durée de vie matérielle
1	---	---	VPNClient	---		---	---

Cliquer sur le bouton [Connect](#) correspondant au Tunnel VPN que vous souhaitez établir.

Tunnels VPN actuels (SA)

#	SPI (entrée)	SPI (sortie)	Nom de la politique	Point final distant	Action	Durée de vie logicielle	Durée de vie matérielle
1	f892e903	81238a22	VPNClient	00.00.000.00		28335	28335

Au bout de quelques secondes le Tunnel VPN est actif (le [journal VPN](#) (voir plus haut) permet également de constater l'établissement du Tunnel VPN).

Le bouton [Drop](#) permettant de déconnecter manuellement le Tunnel VPN.

Pour accéder aux ressources partagées du PC distant, simplement ouvrir l'Explorateur Windows et accéder au PC par son adresse IP local de la forme **\\192.168.x.x**.

II. Configuration du Client VPN Netgear sur le PC distant

1) Installer le logiciel Client VPN Netgear depuis le CD :

Vous devrez insérer le CD d'installation de Windows pour terminer l'installation du Client VPN Netgear.

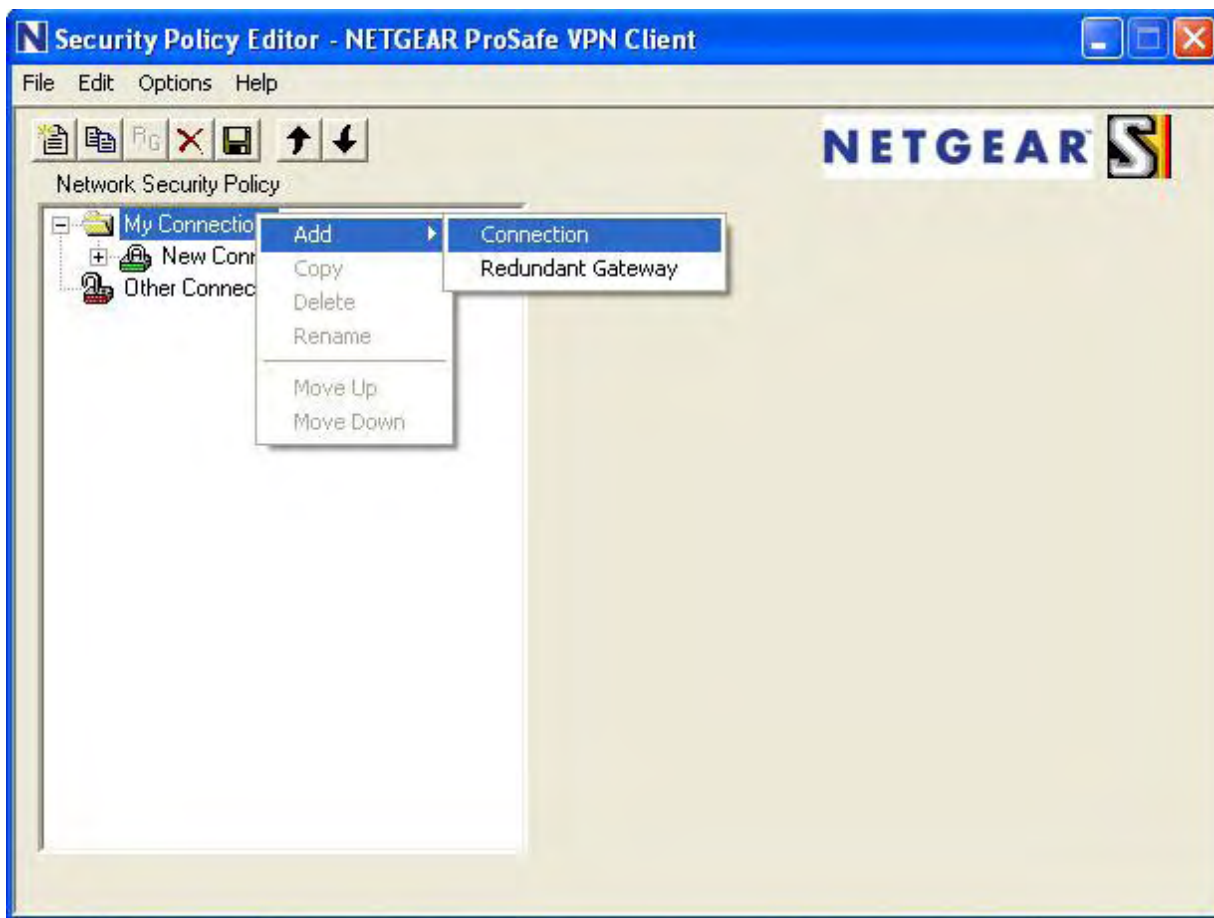
Un redémarrage du PC sera également nécessaire une fois l'installation effectuée.

2) Configurer une connexion réseau :

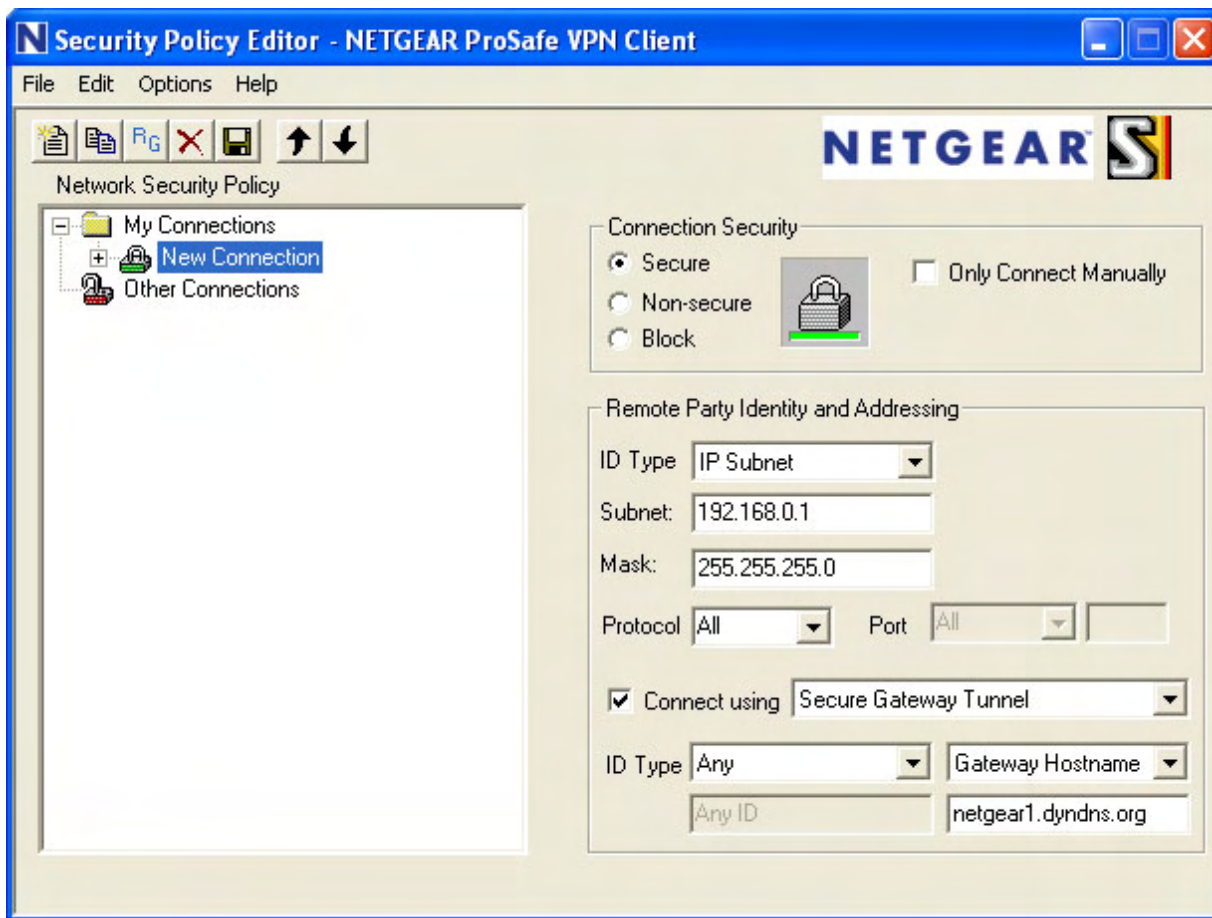
Dans la Barre des tâches de Windows, cliquer avec le bouton droit de la souris sur l'icône [NETGEAR ProSafe VPN Client](#).

Cliquer sur [Security Policy Editor](#) dans le menu déroulant.

Puis créer une nouvelle connexion ([Add Connection](#)).



Configurer cette connexion.



Configurer [Connection Security](#) sur [Secure](#).

Configurer [ID Type](#) sur [IP Subnet](#) et entrer **192.168.0.1 / 255.255.255.0** en [Subnet](#) et [Mask](#) (adresse IP LAN et masque de sous réseau du DG834(G) distant).

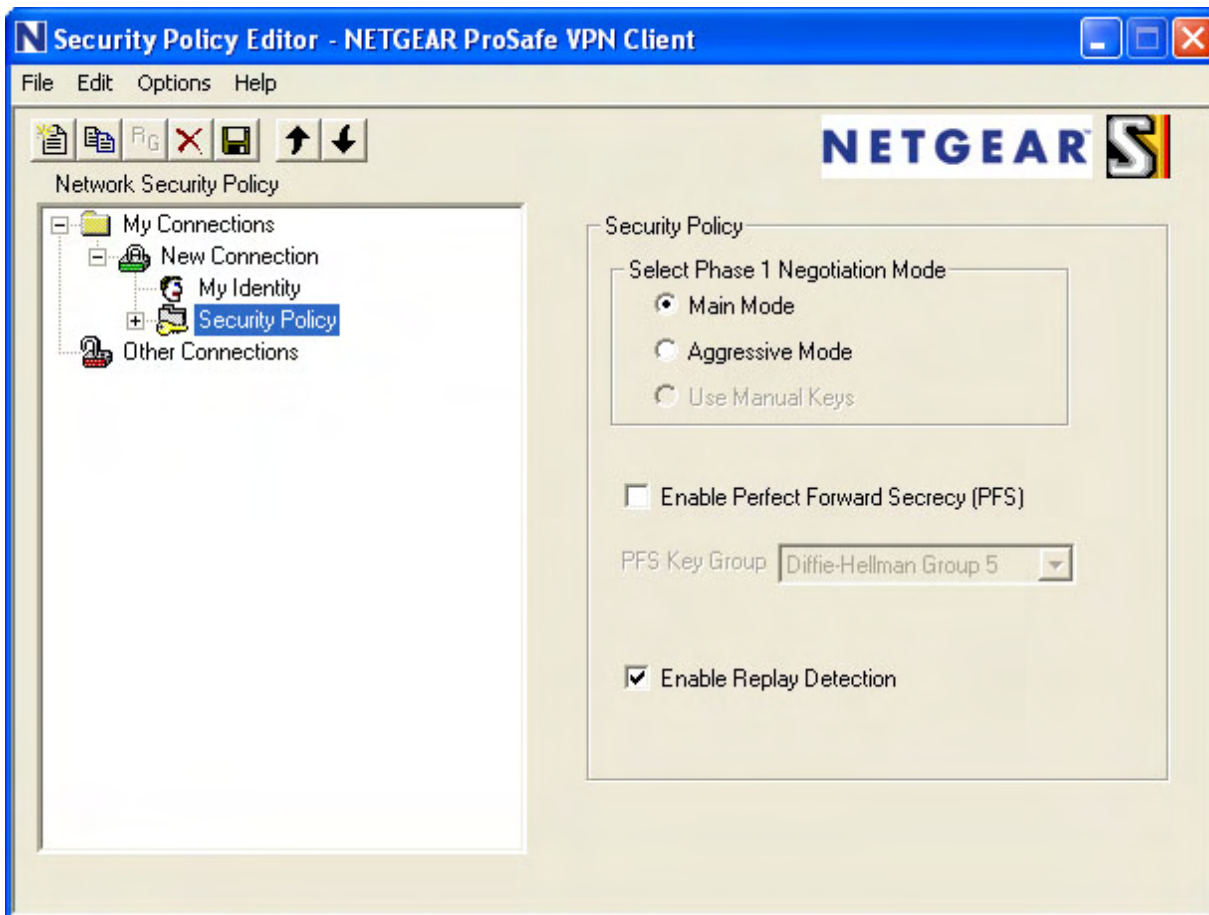
Configurer [Protocol](#) sur [All](#).

Cocher l'option [Connect Using](#) et la paramétrer sur [Secure Gateway Tunnel](#).

Configurer [ID Type](#) sur [Any](#) ou [IP Address](#) et saisir l'adresse IP WAN du DG834(G) distant.

Si [ID Type](#) configuré sur [Any](#), configurer ensuite le nom de domaine ([Gateway Hostname](#)) du DG834(G) distant.

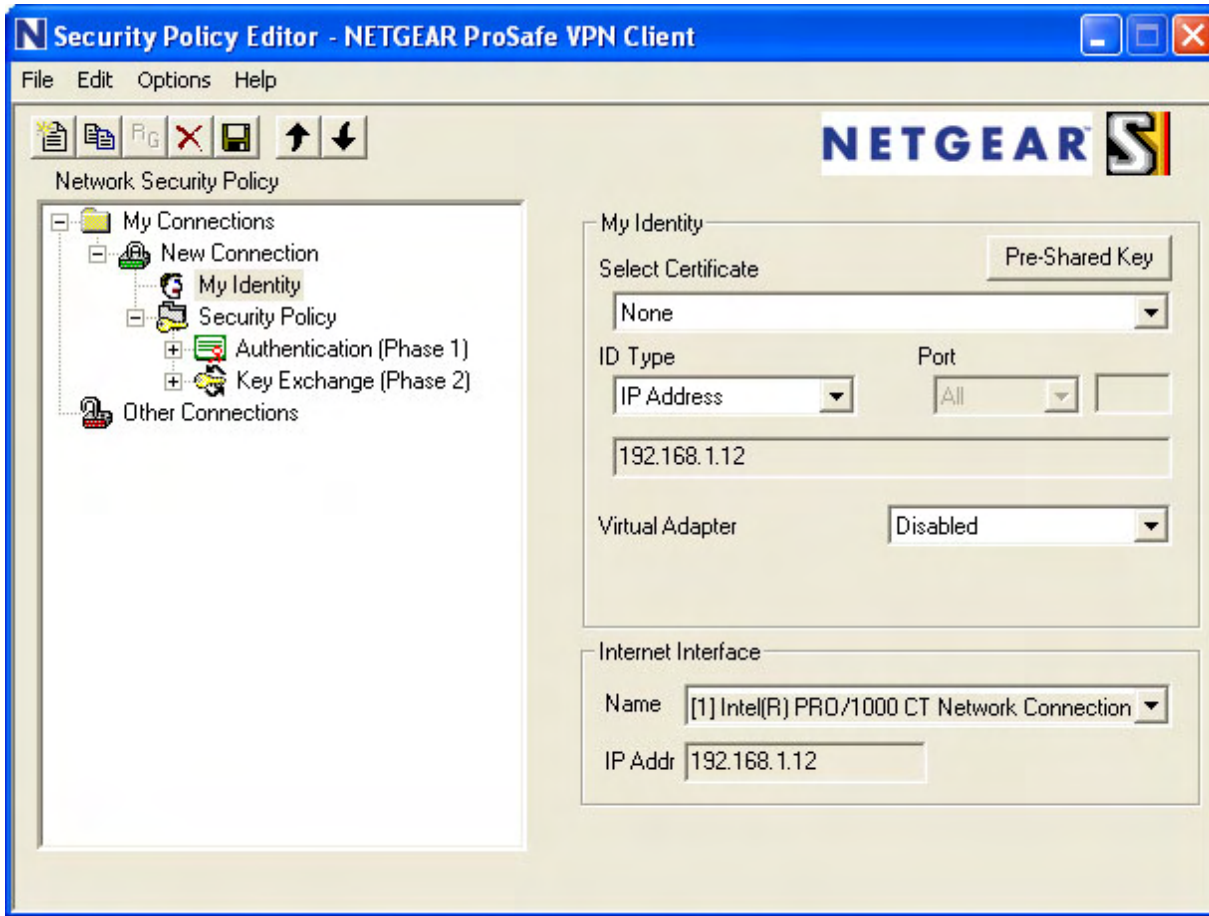
3) Configurer les paramètres de politique :



Sélectionner [Main Mode](#).

Cocher l'option [Enable Replay Detection](#).

4) Configurer les paramètres d'identification :

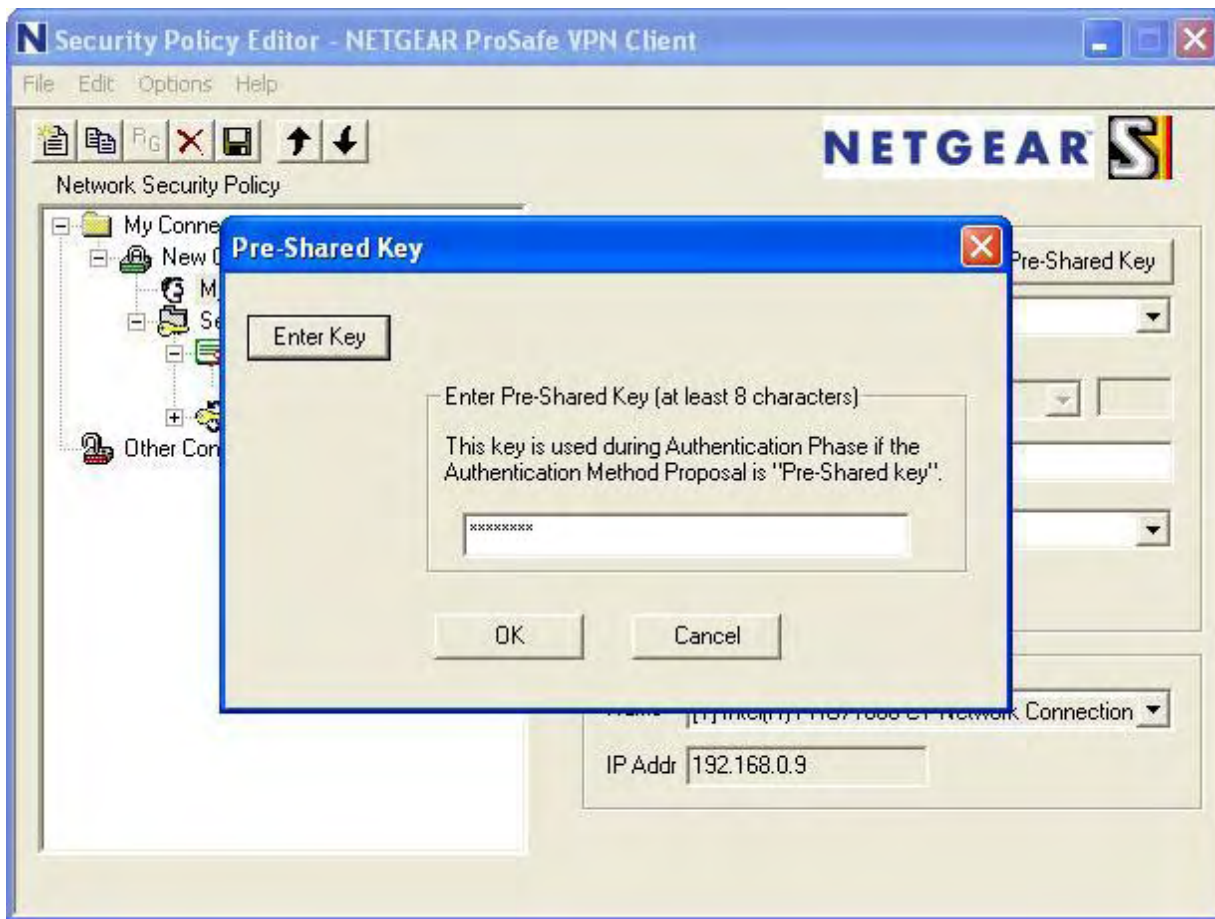


Configurer [Select Certificate](#) sur [None](#).

Configurer [ID Type](#) sur [IP Address](#).

En [Internet Interface](#) sélectionner votre carte réseau Ethernet à l'aide du champ [Name](#).

Puis cliquer sur le bouton [Pre-Shared Key](#).

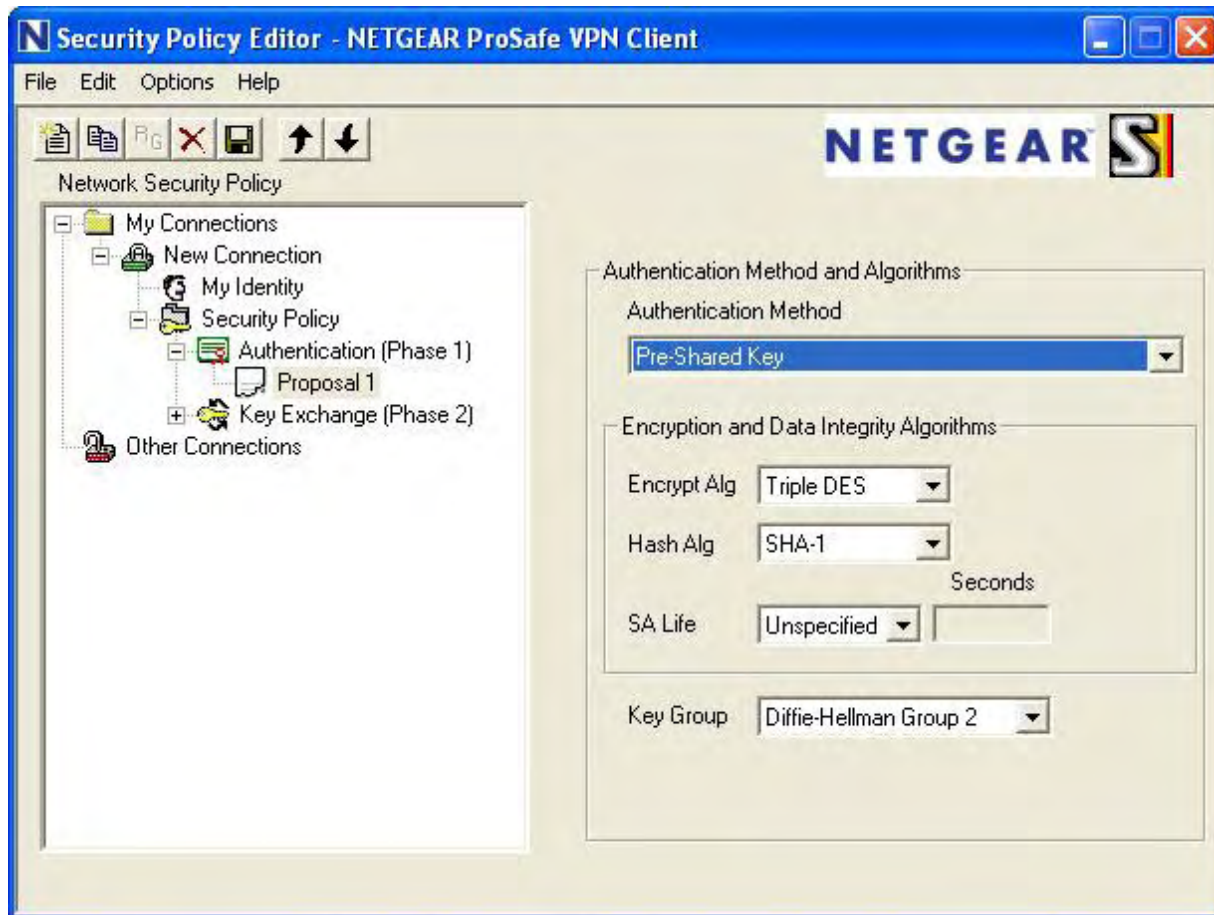


Cliquer sur le bouton [Enter Key](#).

Puis saisir la clé partagée (la même que celle configurée sur le DG834(G) VPN distant) et cliquer sur le bouton [OK](#).

5) Configurer les paramètres de cryptage :

- Authentication (phase 1) :

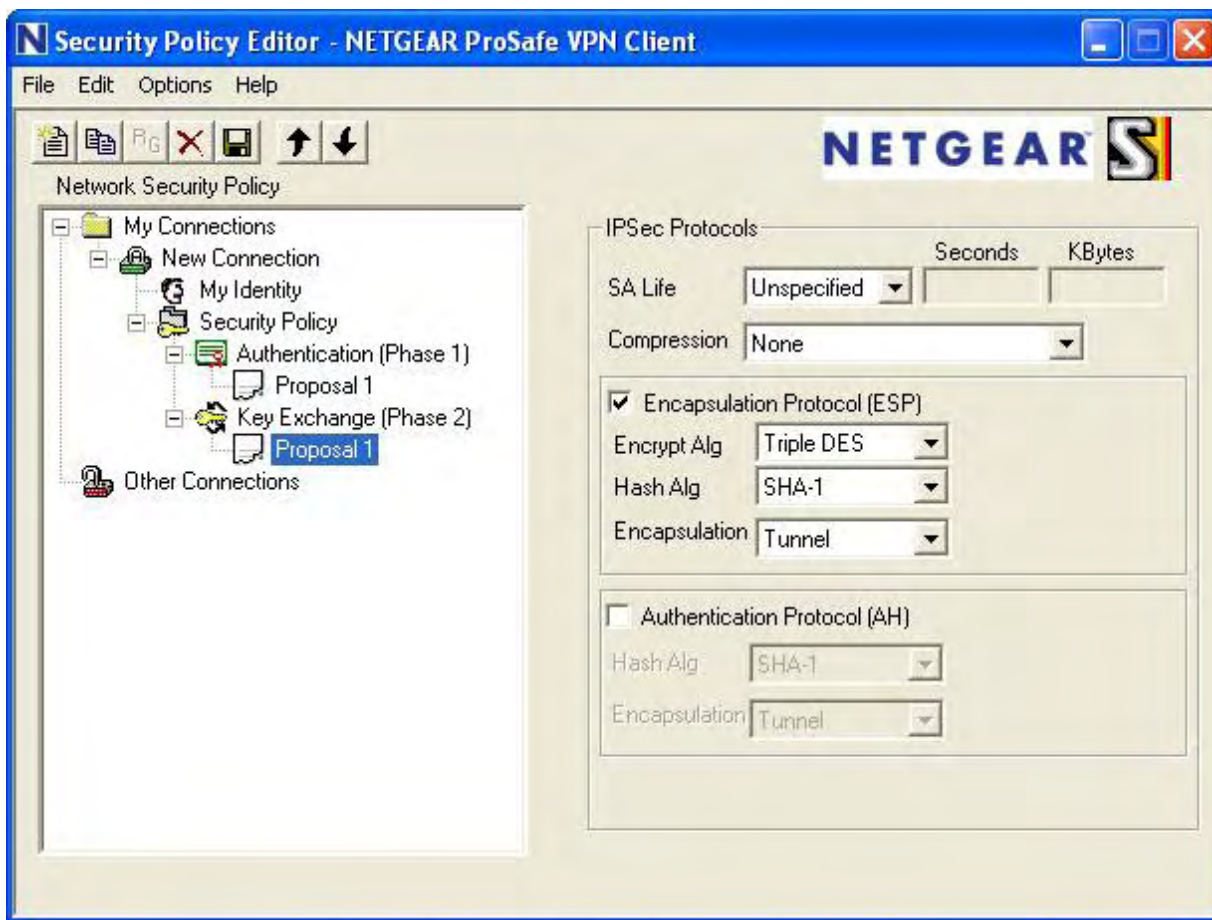


Configurer [Authentication Method](#) sur [Pre-Shared Key](#).

Puis configurer les paramètres de cryptage :

- . [Encrypt Alg](#) = [Triple DES](#)
- . [Hash Alg](#) = [SHA-1](#)
- . [SA Life](#) = [Unspecified](#)
- . [Key Group](#) = [Diffie-Hellman Group 2](#)

- Key Exchange (phase 2) :



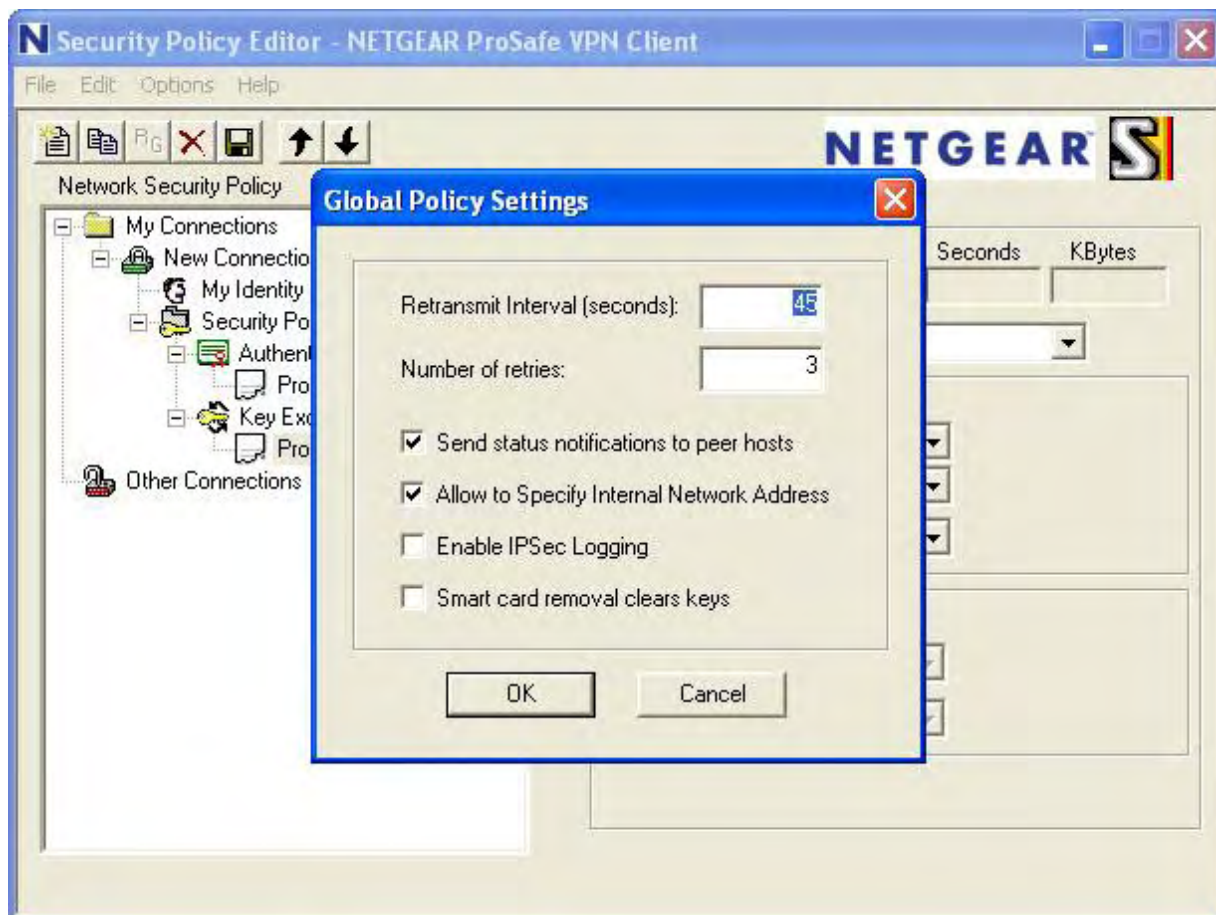
Configurer SA Life sur Unspecified et Compression sur None.

Puis Configurer les paramètres ESP :

- . Encrypt Alg = Triple DES
- . Hash Alg = SHA-1
- . Encapsulation = Tunnel

6) Configurer les paramètres généraux de politique :

Menu [Options](#) puis cliquer sur [Global Policy Settings](#).



Configurer [Retransmist Interval](#) sur 45 secondes.

Cocher les options [Send Status notifications to peer hosts](#) et [Allow to Specify Internal Network Address](#).

7) Sauvegarder les paramètres de configuration du Client VPN :

Menu [File](#) puis cliquer sur [Save](#) ou bien cliquer sur la petite icone en forme de disquette.

8) Etablir la connexion VPN :

Dans la Barre des tâches de Windows, cliquer avec le bouton droit de la souris sur l'icône [NETGEAR ProSafe VPN Client](#).

Se déplacer sur [Connect...](#) dans le menu déroulant.

Puis cliquer sur la connexion correspondant au Tunnel VPN que vous souhaitez établir : [My Connections\Nom de connexion](#).

Sur le même principe [Disconnect...](#) permet de déconnecter manuellement le Tunnel VPN.


Les options [Log Viewer...](#) et [Connection Monitor...](#) sont également utiles pour vérifier que le Tunnel VPN est bien établi.

Pour accéder à l'interface de configuration du routeur VPN distant, simplement ouvrir votre Navigateur Internet et entrer l'adresse IP local du routeur de la forme **[http://192.168.x.x](#)**.

Pour accéder aux ressources partagées d'un PC distant, simplement ouvrir l'Explorateur Windows et accéder au PC par son adresse IP local de la forme **\\192.168.x.x**.

[FAQ](#)

Plus de questions ?

Consulter la FAQ de **Prolag**  :

<http://www.netgear-forum.com/forum/index.php?showtopic=9294>