Connexion VPN - PC vers routeur Netgear SRX5308 + Netgear VPN Client Lite 5

Présentation et configuration

NOLMË INFORMATIQUE

23 janvier 2014
Créé par : Support technique Nolmë Informatique
Version : 1.5 3

AVERTISSEMENT

LES EXPERIENCES, TESTS ET CONFIGURATIONS PRESENTEES DANS CE DOCUMENT SONT PROPOSES A TITRE INFORMATIF ET EDUCATIF AFIN D'EXPLIQUER SIMPLEMENT CERTAINS CONCEPTS DE BASE. TOUTE UTILISATION EN DEHORS DE CE CADRE EST DE LA RESPONSABILITE DU OU DES PERSONNES REALISANT CES TESTS.

NOLMË INFORMATIQUE DECLINE TOUTE RESPONSABILITE QUANT A L'UTILISATION EVENTUELLES DE TOUTE INFORMATION CONTENUE DUDIT DOCUMENT ET DES CONSEQUENCES DE SON UTILISATION.

LES TENTATIVES NON AUTORISEES DE CHARGEMENT OU DE MODIFICATION DE L'INFORMATION DANS CE DOCUMENT SONT STRICTEMENT INTERDITES ET PEUVENT TOMBER SOUS LE COUP DES LOIS SUR LA FRAUDE INFORMATIQUE AINSI QUE D'AUTRES LOIS FEDERALES ET PROVINCIALES.

LISTE DE REVISION

Version	Date	Commentaires	Auteur
1.4.	2010-11-16	Création du document	Vincent D.
1.5.	2014-01-09	Mise à jour du template	Vincent D.
1.5.0	2014-01-09	Première version	Vincent D.
1.5.1	2014-01-10	Ajout du chapitre 'Pour aller plus loin'	Vincent D.
1.5.2	2014-01-10	Modifications mineures – ajout de liens	Vincent D.
1.5.3	2014-01-23	Inter VLAN Routing, lien TheGreenBow	Vincent D.

SOMMAIRE

I. Introduction

A. Présentation

Les membres de la société Nolmë Informatique sont professionnels qui, au travers de leur expérience personnelle ou professionnelle, partagent leurs connaissances au sein de la communauté.

Le matériel réseau se diversifie de plus en plus avec des fonctions de plus en plus complexes. Entre les versions anglaises et les nouvelles fonctionnalités, il devient parfois difficile de s'y retrouver.

Au travers ce document, vous apprendrez à configurer des produits réseaux précis afin de pouvoir être capable de reproduire et créer vos propres configurations de manière efficace et sécurisée. Vous comprendrez aussi certains aspects et contraintes souvent liés à la technologie.

Ce document n'est pas figé, au travers de vos commentaires et remarques il évoluera avec le temps afin de le rendre encore plus complet.

En espérant qu'il répondre à vos besoins et interrogations sur le sujet.

Bonne configuration,

L'équipe Nolmë Informatique.

B. Contexte

Le but de ce tutoriel est de vous présenter la configuration du client VPN Netgear vers un routeur VPN Netgear afin de créer une connexion sécurisée au travers d'Internet.

Cela permet de travailler à distance (nommé SITE DISTANT) en ayant accès aux fichiers de l'entreprise (nommé SIEGE).

C. Prérequis

Afin d'assimiler la majeure partie de ce document, certains prérequis peuvent être nécessaires. Si le glossaire en fin de document ne répondait pas à vos interrogations, nous vous conseillons de vous documenter sur les sujets en question avant de poursuivre la lecture.

Parmi les prérequis technique :

- Connaissance des réseaux IP
- Principe de fonctionnement basique d'un VPN

Pour pouvoir tester ce tutorial, l'ordinateur de configuration **DOIT SE TROUVER sur le SITE DISTANT**.

Vous devez aussi avoir un accès à l'interface du routeur Netgear SRX5308 du SIEGE. Pour cela, il faut préalablement activer l'option 'Allow Secure HTTP Management' sous l'interface Administration -> Remote Management.

De plus, sous le menu Users -> Users -> admin -> Policies, il faut vérifier que la case 'Deny Login from WAN Interface'est décochée.

Pour ce tutorial, nous supposons que le SITE DISTANT et le SIEGE sont déjà raccordés à Internet.

Le SIEGE doit **OBLIGATOIREMENT** disposer d'une adresse IP publique ou d'un nom DNS (type DynDNS [Site]).

L'ordinateur portable est connecté à l'interface d'administration du routeur Netgear SRX5308 du SIEGE au travers du routeur du SITE DISTANT.

Le routeur Netgear SRX5308 du SIEGE doit impérativement être raccordé à Internet via le port WAN1.

Note : Le client VPN Netgear est basé sur le logiciel TheGreenBow Client VPN IPSec. Le logiciel est disponible en évaluation si nécessaire (Prix indicatif 45-60 € TTC). [Site de l'éditeur].

Merci à Julien Ratinaud du support Netgear qui a contribué à la réalisation de la version 1.5.3.

II. Matériel utilisé

A. Matériels et logiciels utilisés

Les matériels et logiciels utilisés pour cette présentation sont :

- Routeur Netgear SRX5308 - firmware 4.3.0-19. [Téléchargement du firmware]
- Logiciel Netgear VPN Lite Software Version - version 5.50.007. [Téléchargement].

Pour le serveur RADIUS, nous utilisons un NAS Qnap TS-439U-RP – firmware 4.1.0 [Téléchargement du firmware].

Le(s) logiciel(s) complémentaire(s) sont :

- Navigateur Internet Mozilla Firefox 26.0 Fr. [Téléchargement]
- Navigateur Microsoft Internet Explorer 11 Fr. [Téléchargement]

Pour les tests et mesures les appareils et ordinateurs suivants ont été utilisés :

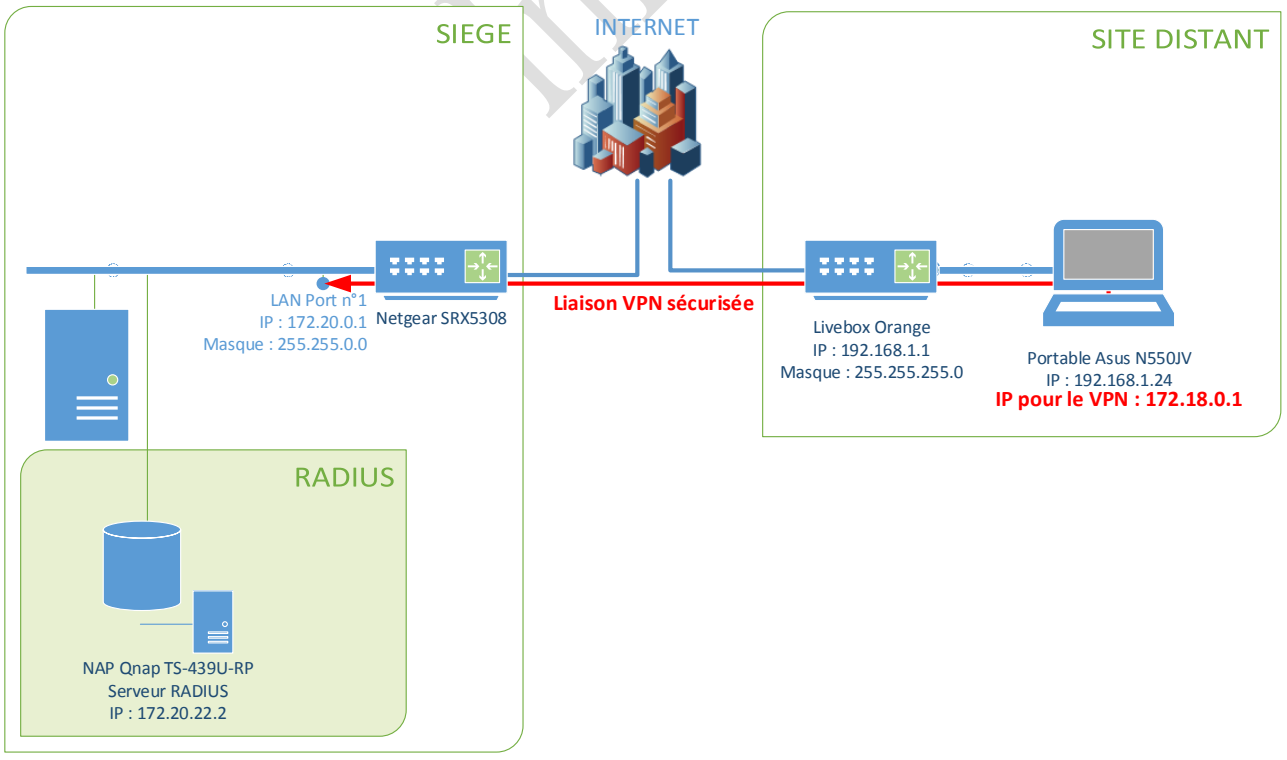
- Ordinateur portable Asus N550JV sous Microsoft Windows 8.1 x64 Pro Fr. [Descriptif]

Le raccordement à Internet est effectué via :

- Siège de l'entreprise : ADSL Orange 4 Mbps
- Site distant : ADSL Orange 8 Mbps

B. Présentation de l'architecture

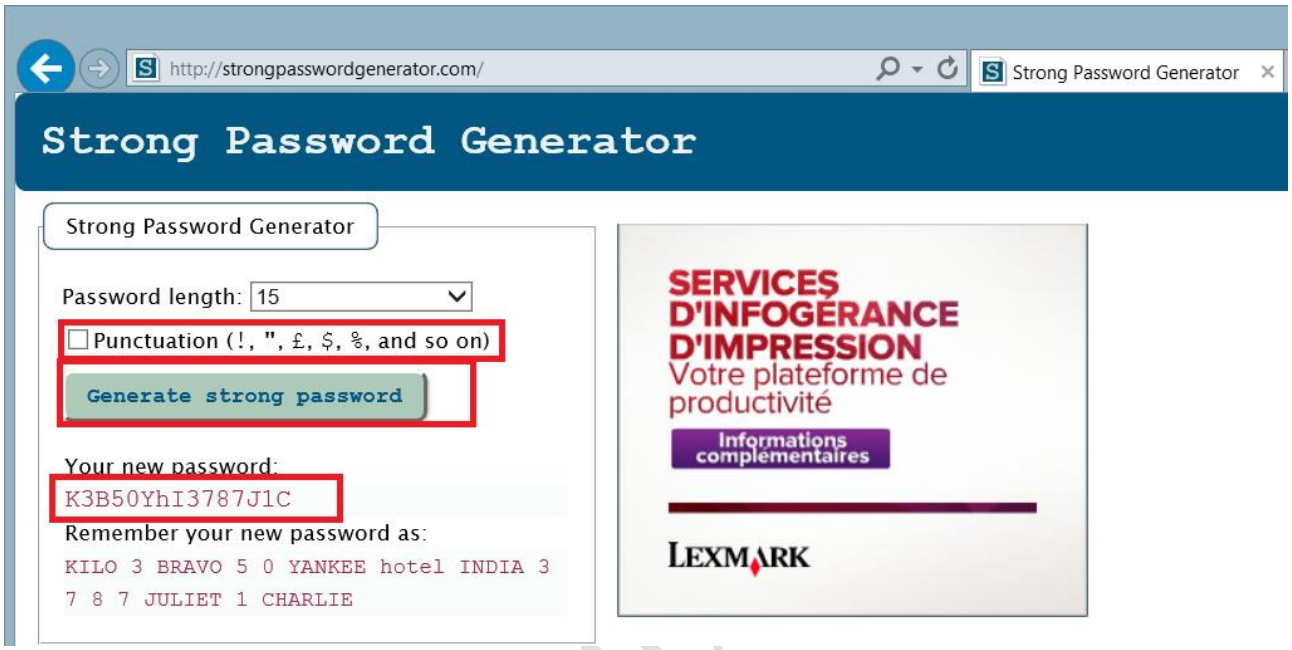
L'architecture que nous utilisons pour ce document est la suivante :



III. Configuration du routeur Netgear SRX5308

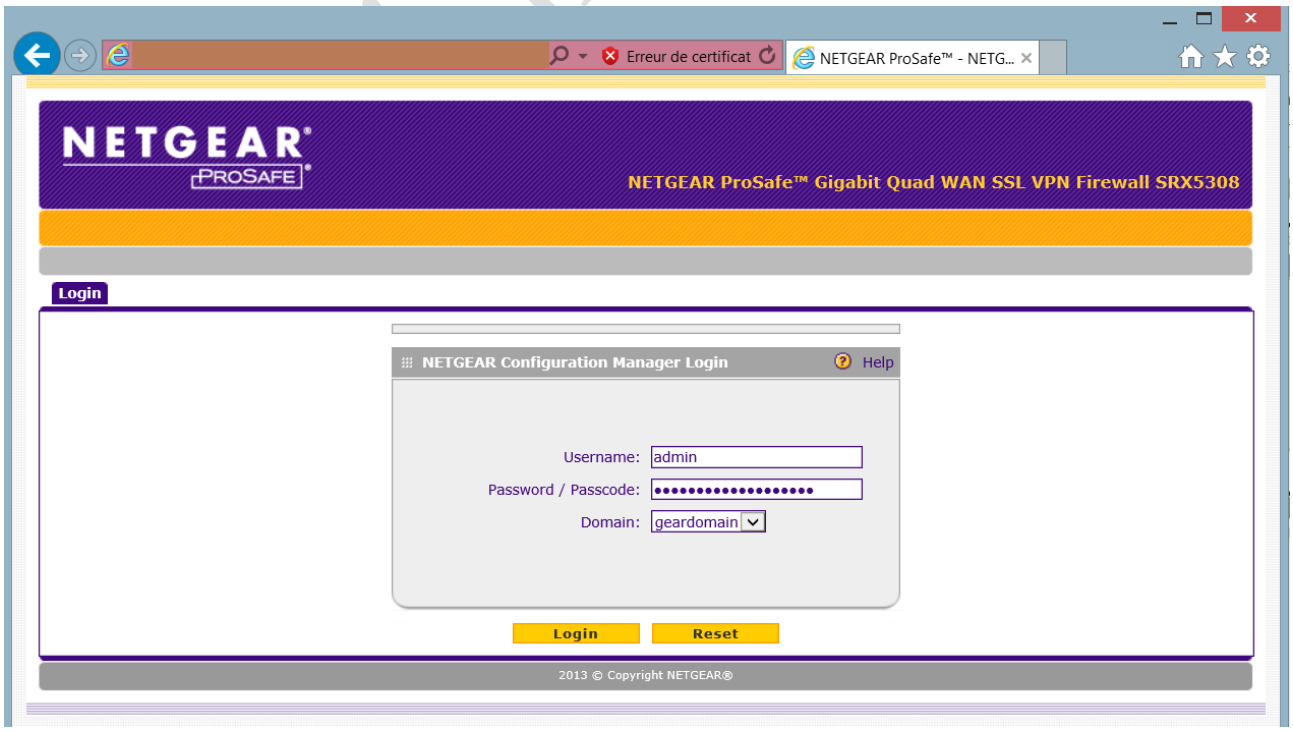
A. Génération d'une clé de cryptage

Nous allons générer une clé de cryptage pour plus tard. Plusieurs sites Internet permettent de générer des clés pseudo-aléatoires. Dans le cas présent, nous avons utilisé le site www.strongpasswordgenerator.com pour générer notre clé : K3B50YhI3787J1C qui doit comprendre entre 8 et 49 caractères.



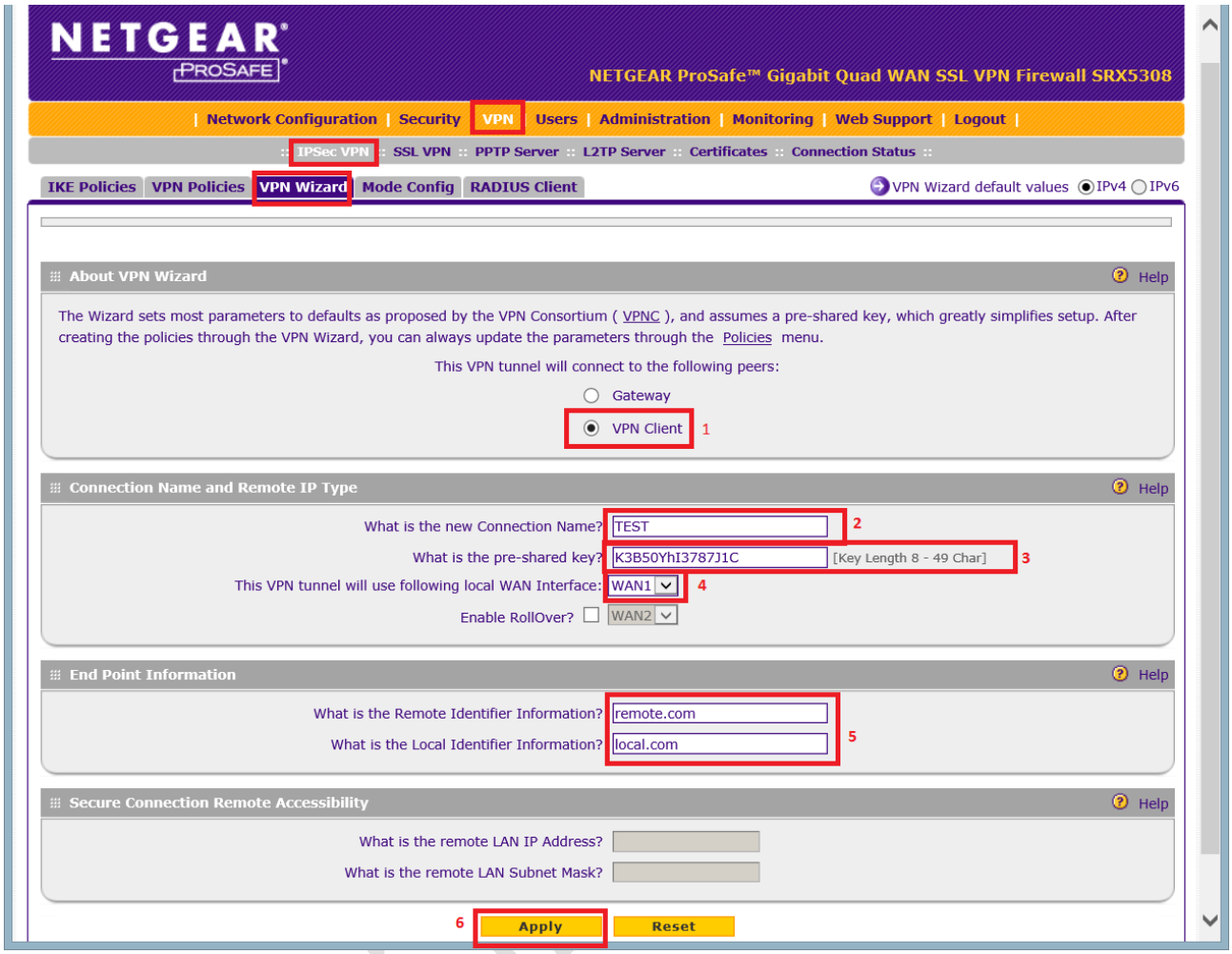
B. Connexion à l'interface du routeur sur le SIEGE

Nous pouvons maintenant nous connecter à l'interface d'administration du routeur du siège.



C. Création de la connexion VPN

Naviguez sur l'interface en suivant le schéma suivant.



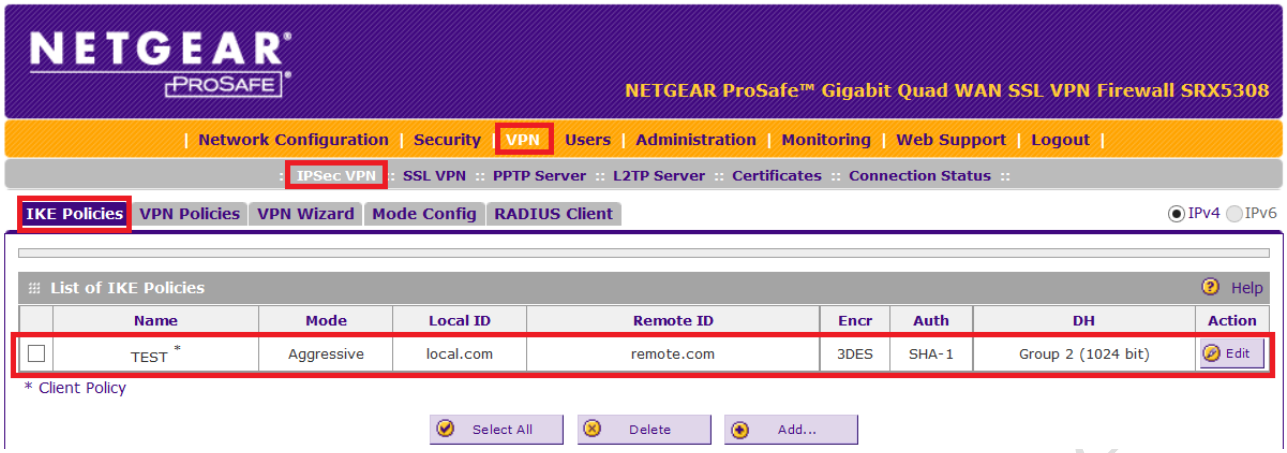
1°) Nous spécifions ici qu'il s'agit d'un accès type Ordinateur à Routeur.
2°) Le nom de la connexion est arbitraire, nous avons choisi TEST.
3°) Nous saisissons la clé de cryptage saisie au III.A
4°) Nous spécifions le port WAN sur lequel créer la connexion tel qu'indiqué dans le I.C
5°) Nous laissons les champs tel qu'ils sont proposés.
6°) Nous pouvons appliquer les changements.

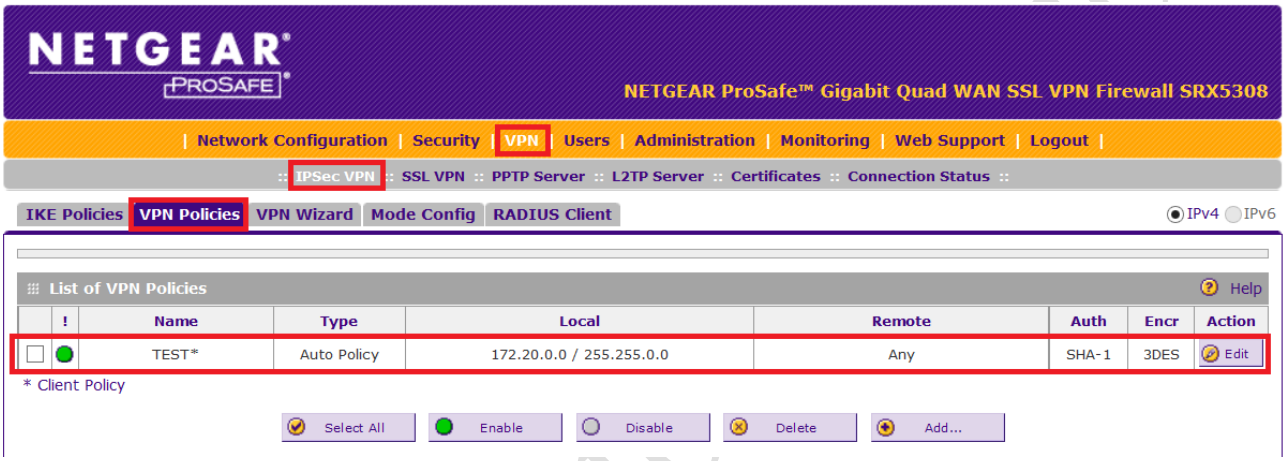
D. Vérifications

L'algorithme de cryptage utilisé automatiquement est 3DES [Wiki].

L'algorithme d'authentification utilisé automatiquement est SHA-1 [Wiki].

En naviguant comme indiqué ci-dessous, vous devez donc avoir le résultat suivant :

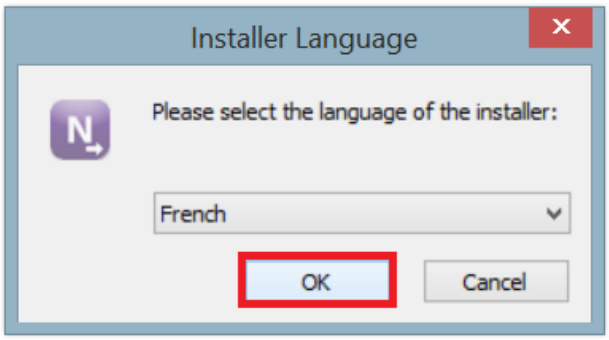


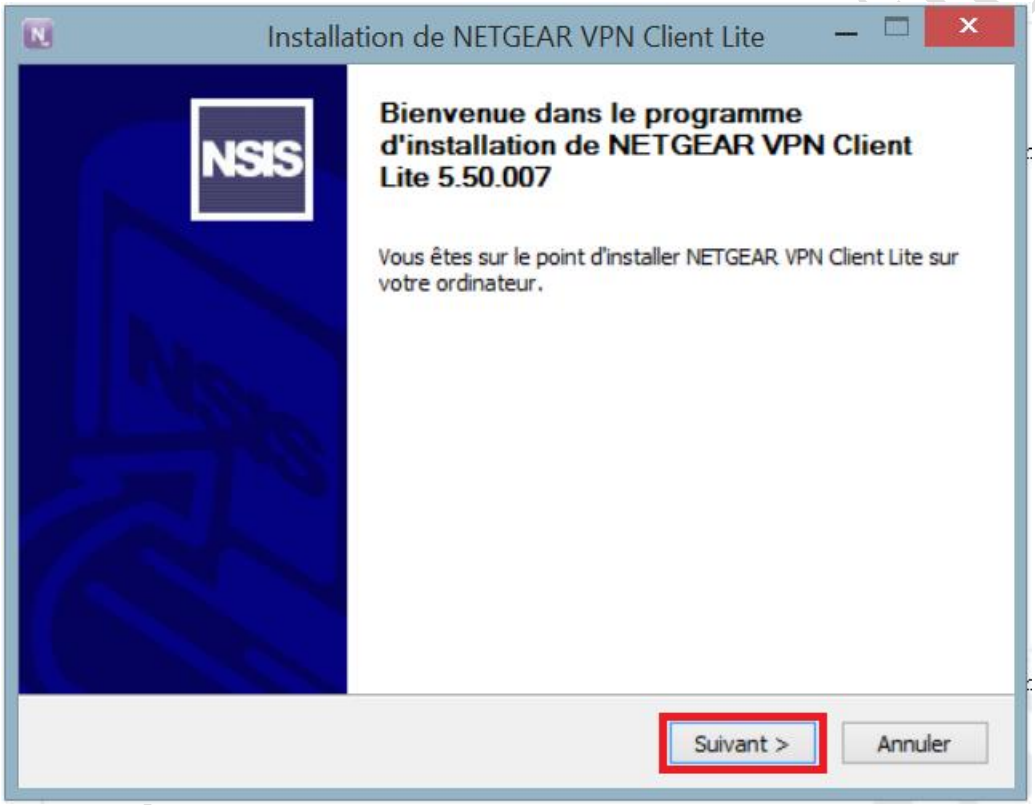


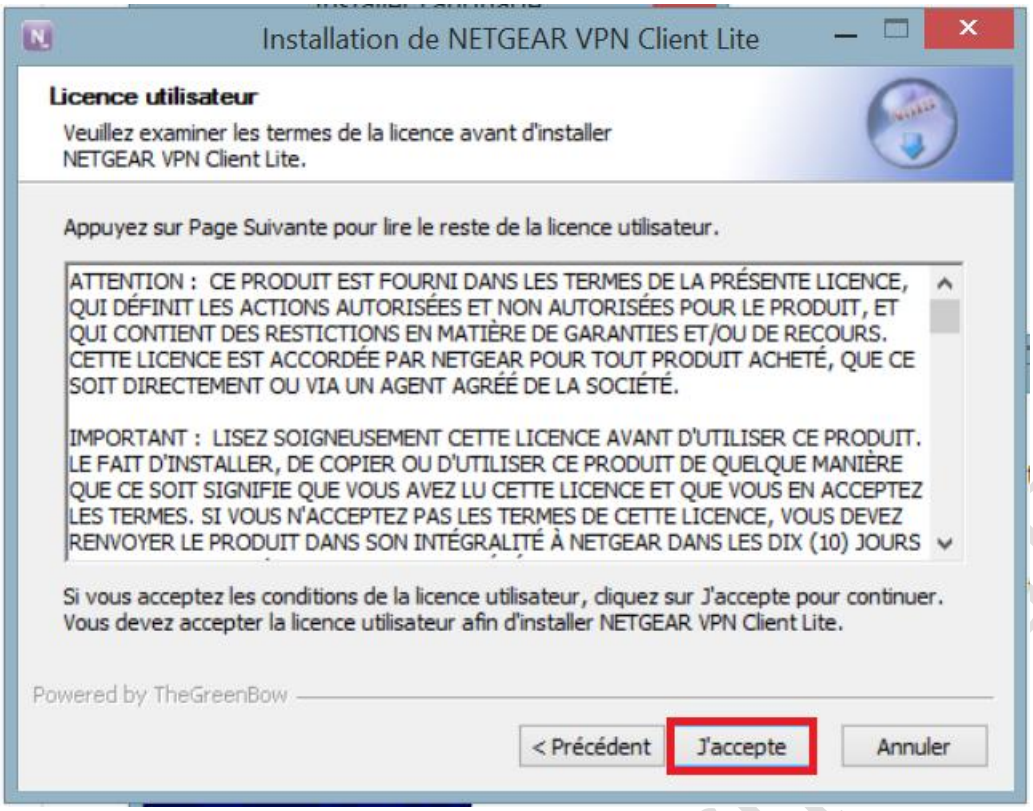
IV. Installation du logiciel

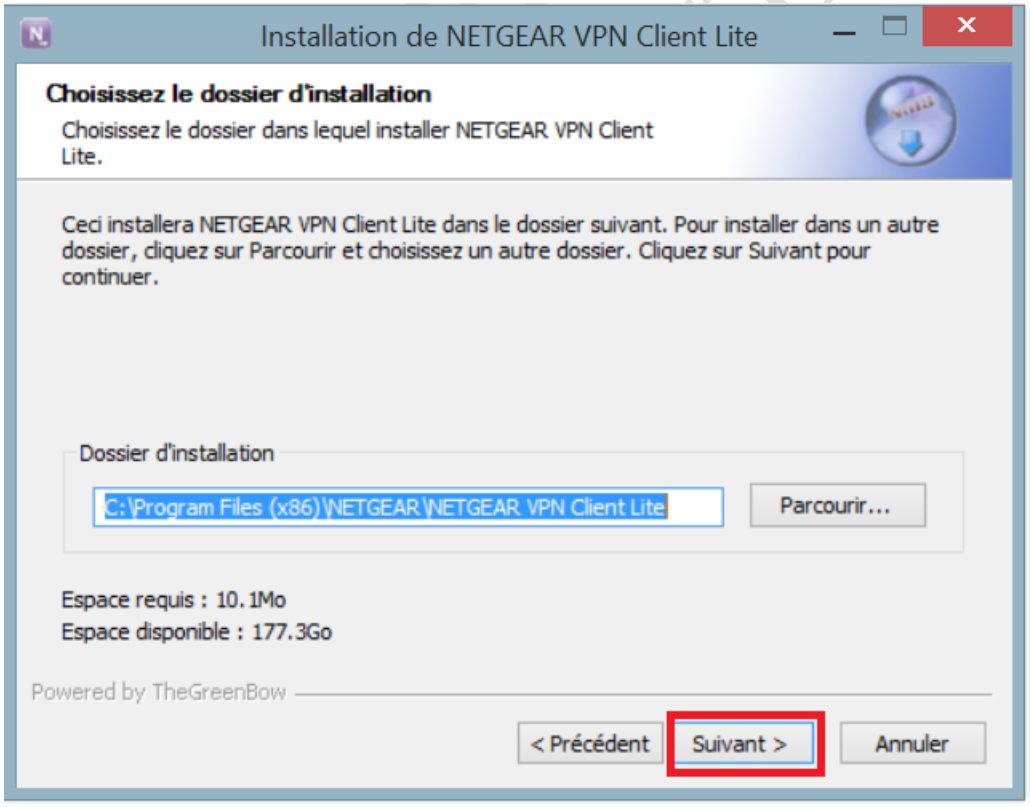
L'installation ne pose pas de problème particulier. Vous devez être en possession d'une clé de licence si vous voulez utiliser le logiciel au-delà de la période d'évaluation de 30 jours.

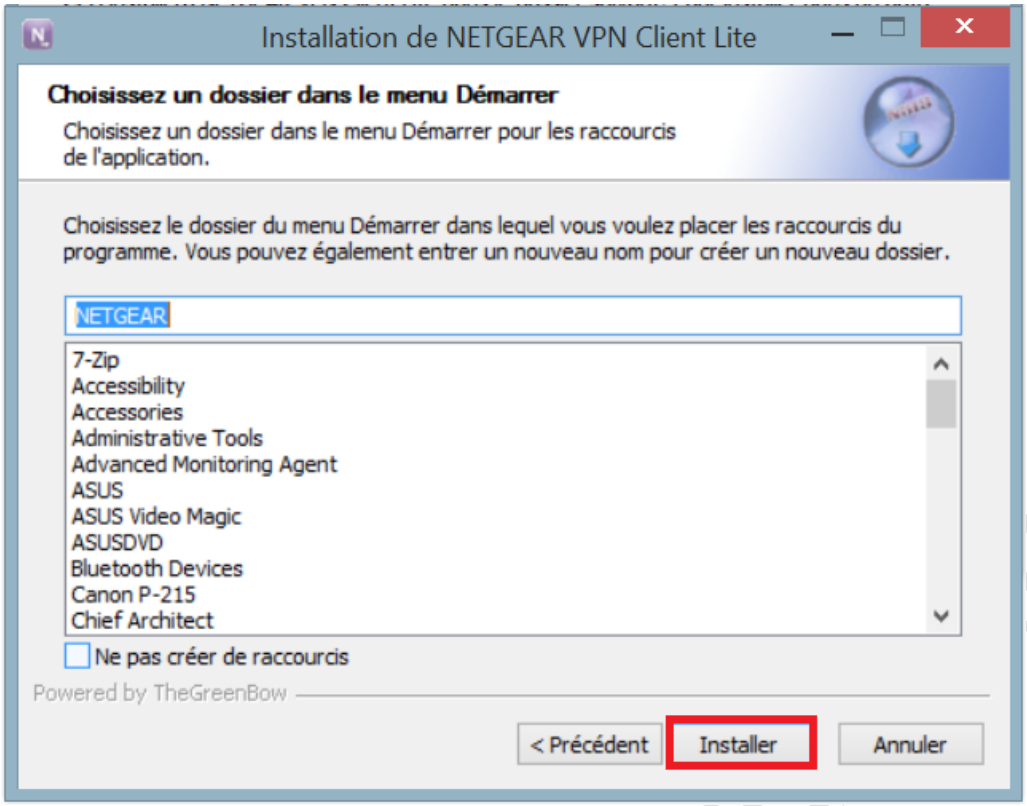
L'UAC de Windows va vous demander confirmation pour l'installation du driver.

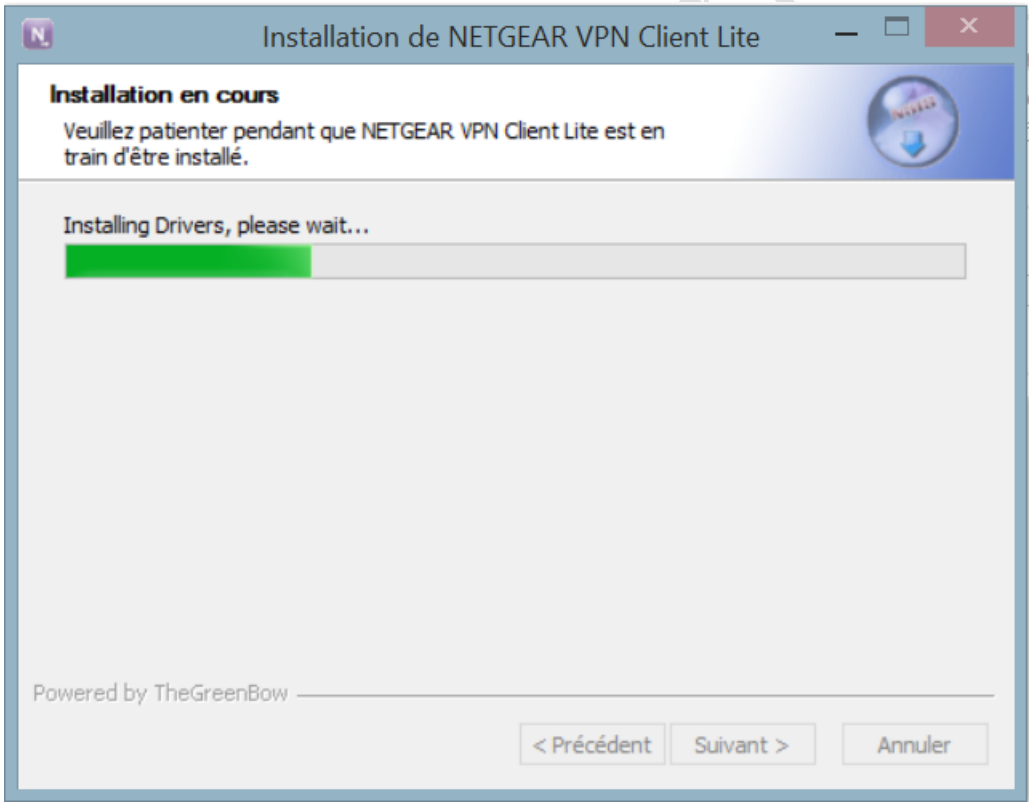


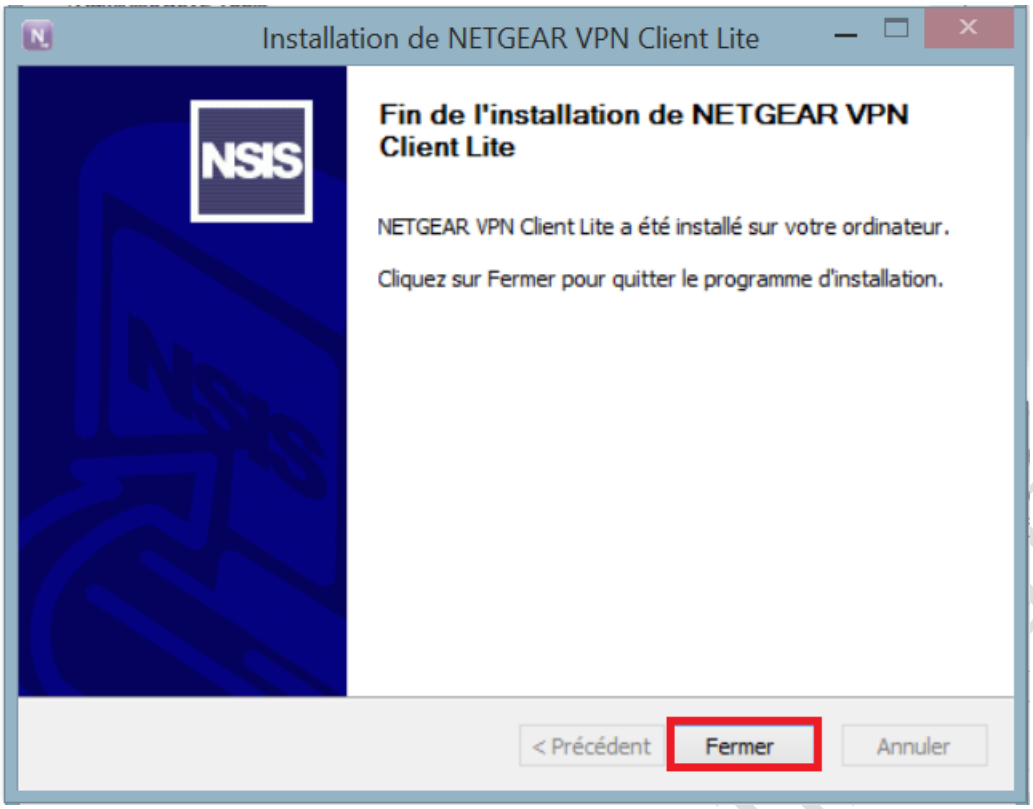



Installation de NETGEAR VPN Client Lite
Licence utilisateur
Veuillez examiner les termes de la licence avant d'installer NETGEAR VPN Client Lite.
Appuyez sur Page Suivante pour lire le reste de la licence utilisateur.
ATTENTION : CE PRODUIT EST FOURNI DANS LES TERMES DE LA PRÉSENTE LICENCE, QUI DÉFINIT LES ACTIONS AUTORISÉES ET NON AUTORISÉES POUR LE PRODUIT, ET QUI CONTIENT DES RESTICTIONS EN MATIÈRE DE GARANTIES ET/OU DE RECOURS. CETTE LICENCE EST ACCORDÉE PAR NETGEAR POUR TOUT PRODUIT ACHETÉ, QUE CE SOIT DIRECTEMENT OU VIA UN AGENT AGRÉÉ DE LA SOCIÉTÉ.
IMPORTANT : LISEZ SOIGNEUSEMENT CETTE LICENCE AVANT D'UTILISER CE PRODUIT. LE FAIT D'INSTALLER, DE COPIER OU D'UTILISER CE PRODUIT DE QUELQUE MANIÈRE QUE CE SOIT SIGNIFIE QUE VOUS AVEZ LU CETTE LICENCE ET QUE VOUS EN ACCEPTEZ LES TERMES. SI VOUS N'ACCEPTEZ PAS LES TERMES DE CETTE LICENCE, VOUS DEVEZ RENVOYER LE PRODUIT DANS SON INTÉGRALITÉ À NETGEAR DANS LES DIX (10) JOURS
Si vous acceptez les conditions de la licence utilisateur, cliquez sur J'accepte pour continuer. Vous devez accepter la licence utilisateur afin d'installer NETGEAR VPN Client Lite.
Powered by TheGreenBow
< Précédent
J'accepte
Annuler


Installation de NETGEAR VPN Client Lite
Choisissez le dossier d'installation
Choisissez le dossier dans lequel installer NETGEAR VPN Client Lite.
Ceci installera NETGEAR VPN Client Lite dans le dossier suivant. Pour installer dans un autre dossier, cliquez sur Parcourir et choisissez un autre dossier. Cliquez sur Suivant pour continuer.
Dossier d'installation
C:\Program Files (x86)\NETGEAR\NETGEAR VPN Client Lite
Parcourir...
Espace requis : 10.1Mo
Espace disponible : 177.3Go
Powered by TheGreenBow
< Précédent
Suivant >
Annuler


Installation de NETGEAR VPN Client Lite
Choisissez un dossier dans le menu Démarrer
Choisissez un dossier dans le menu Démarrer pour les raccourcis de l'application.
Choisissez le dossier du menu Démarrer dans lequel vous voulez placer les raccourcis du programme. Vous pouvez également entrer un nouveau nom pour créer un nouveau dossier.
NETGEAR
7-Zip
Accessibility
Accessories
Administrative Tools
Advanced Monitoring Agent
ASUS
ASUS Video Magic
ASUSDVD
Bluetooth Devices
Canon P-215
Chief Architect
Ne pas créer de raccourcis
Powered by TheGreenBow
< Précédent
Installer
Annuler


Installation de NETGEAR VPN Client Lite
Installation en cours
Veuillez patienter pendant que NETGEAR VPN Client Lite est en train d'être installé.
Installing Drivers, please wait...
Powered by TheGreenBow
< Précédent
Suivant >
Annuler



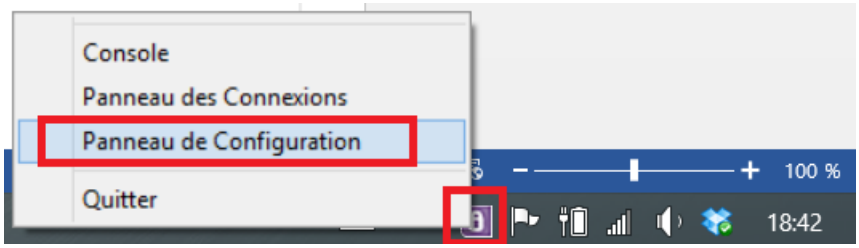
Il ne reste plus qu'à lancer l'application.

Nolmë Informatique – Lieudit Morellière 61360 St Jouin-de-Blavou - FRANCE
E-mail : root@nolme.com – Tél : +33 (0)2 33 85 57 27 – Web : http://www.nolme.com
SARL au capital de 7.500 euros – RCS Alençon 452 954 092 – APE : 9511Z
TVA Intracommunautaire : FR55 452 954 092

V. Configuration de la connexion VPN

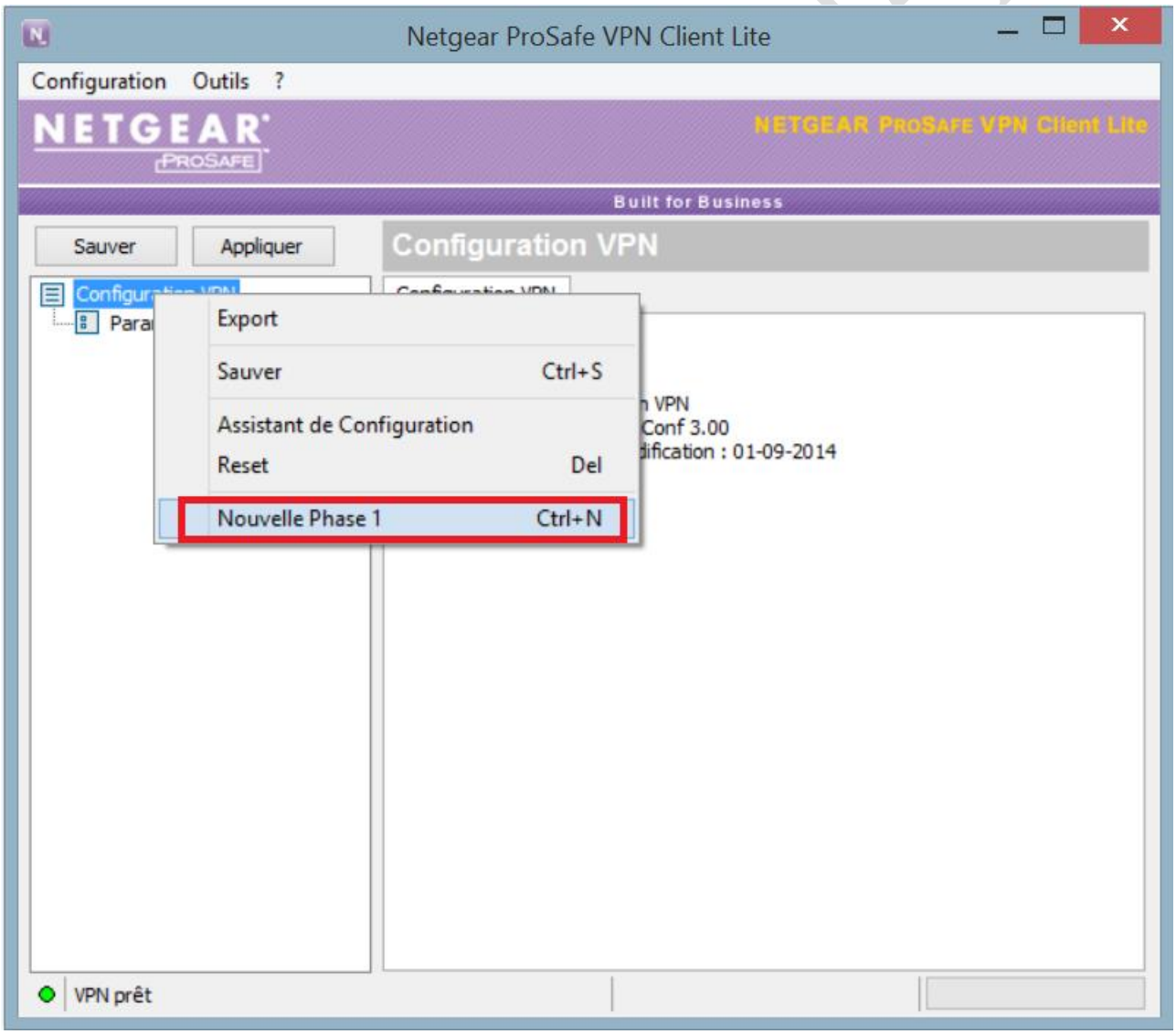
A. Ouverture du panneau de configuration

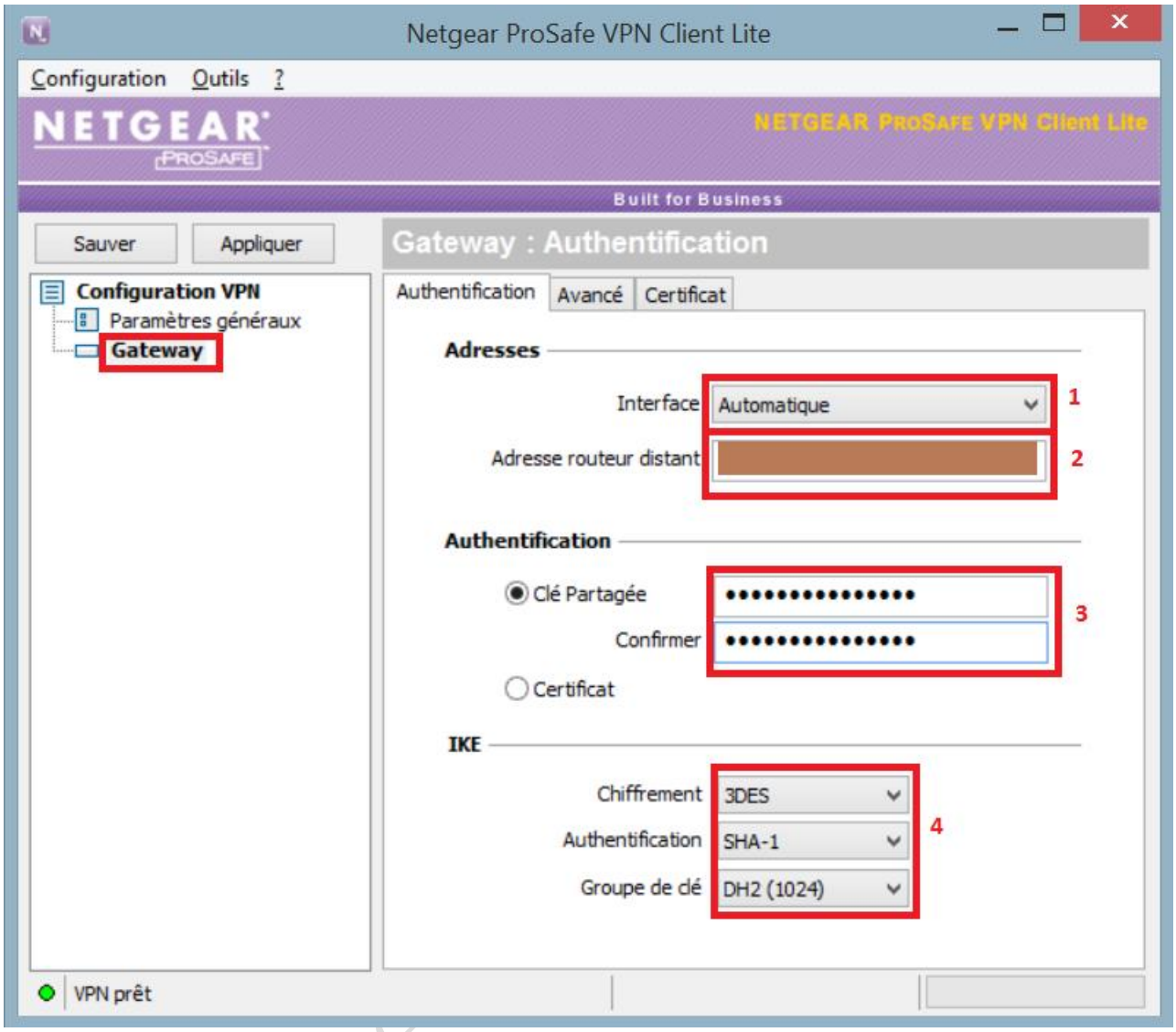
Une fois l'application NETGEAR VPN Client Lite lancée, faites un clic droit sur l'icône dans la barre système et sélectionnez le 'Panneau de Configuration'.



B. Configuration de la Phase 1

Faites un clic droit sur 'Configuration VPN' puis 'Nouvelle Phase 1'.



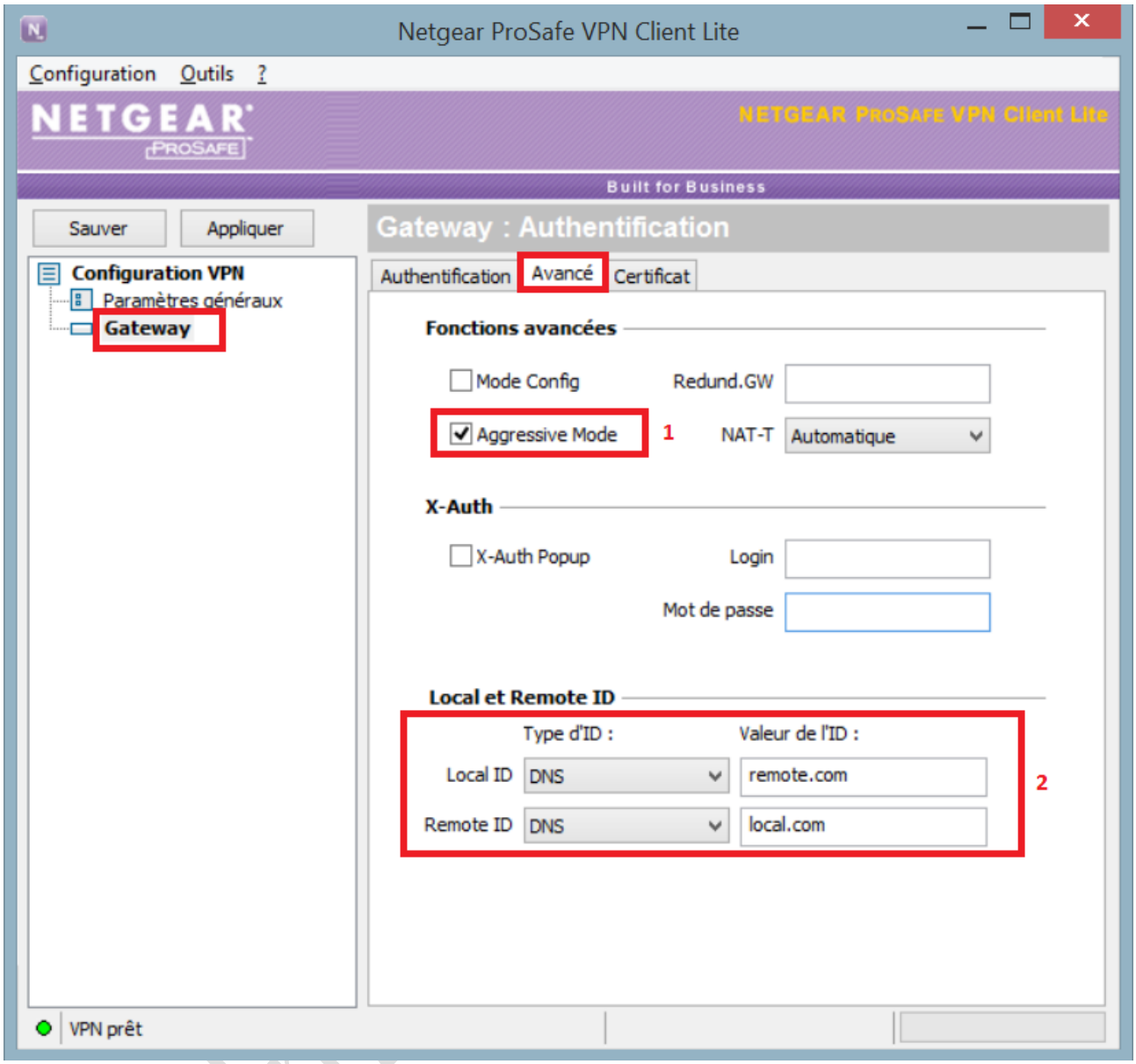


1°) Sélectionnez l'interface 'Automatique' si vous ne voulez pas être tributaire d'une connexion spécifique comme la prise Ethernet ou Wireless.

2°) Indiquez l'adresse IP publique ou le nom DNS du SIEGE.

3°) Saisissez la clé de cryptage saisie au III.A

4°) Pour la phase 1 (IKE), nous vérifions que nous avons bien les mêmes paramètres de sécurité que ceux spécifiés sur le routeur Netgear SRX5308 au III.D.

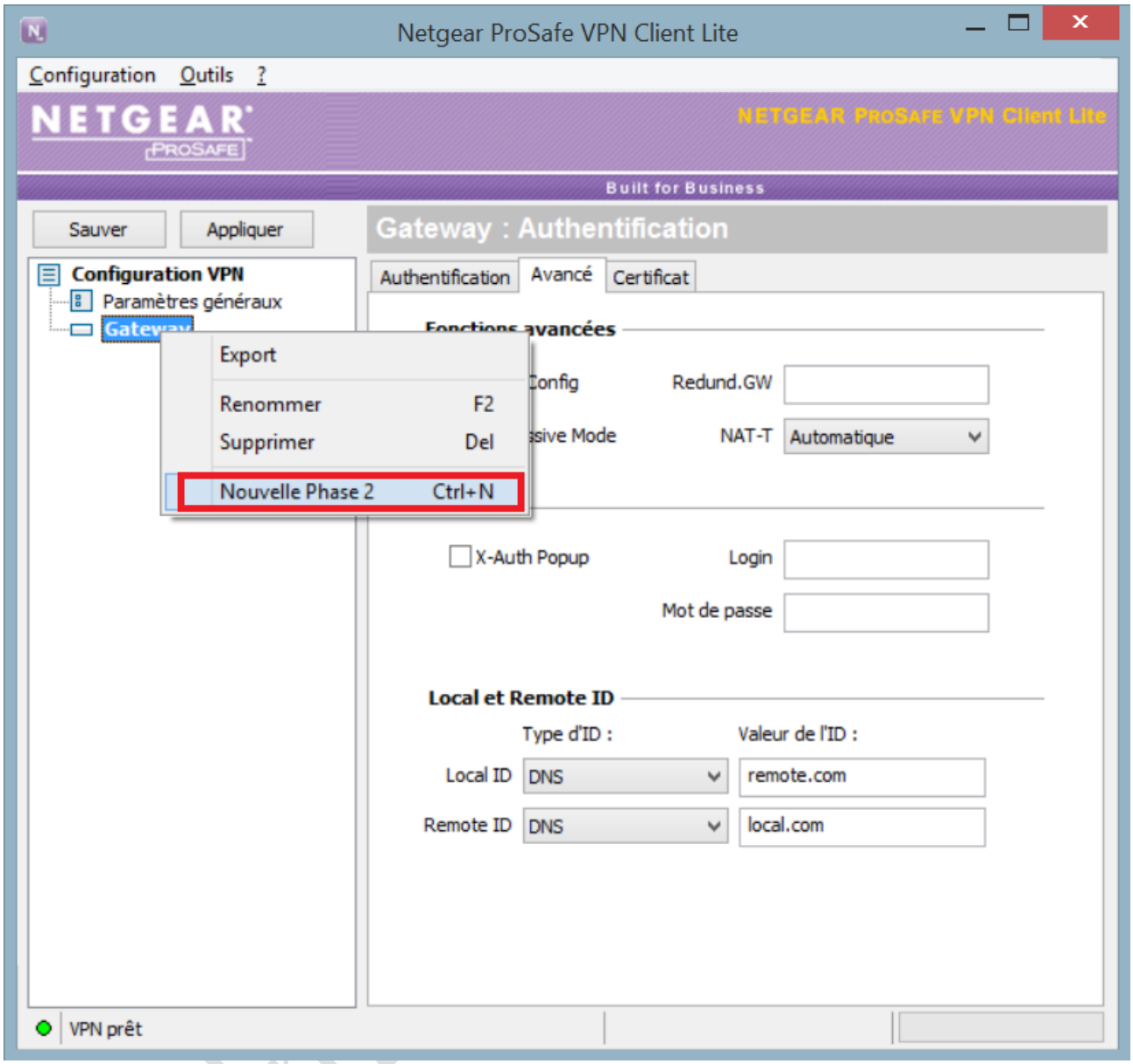


1°) Il faut cocher cette case.

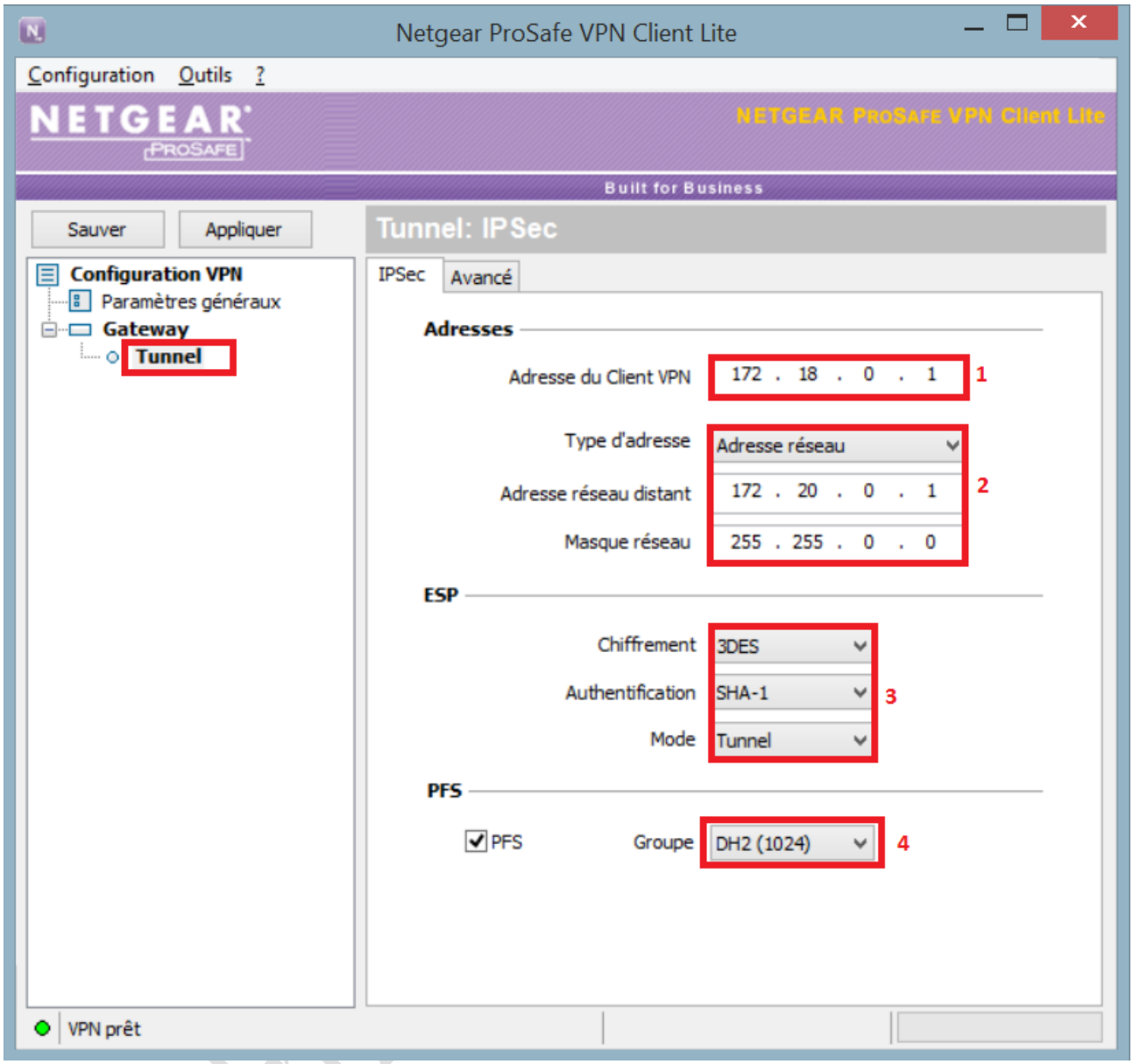
2°) Nous remplissons avec les noms spécifiés au point n°5 de la section III.C. **ATTENTION, les noms sont inversés ici entre Local et Remote.**

C. Configuration de la Phase 2

Pour créer la phase 2, il faut faire un clic droit sur l'élément 'Gateway' crée précédemment et sélectionner 'Nouvelle Phase 2' dans le menu contextuel qui s'ouvre pour enfin sélectionner l'élément 'Tunnel'.



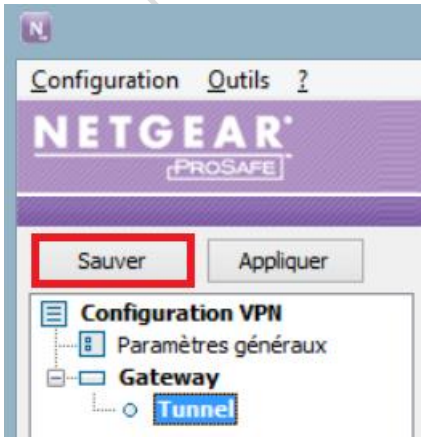
Nolmë Informatique – Lieudit Morellière 61360 St Jouin-de-Blavou - FRANCE
E-mail : root@nolme.com – Tél : +33 (0)2 33 85 57 27 – Web : http://www.nolme.com
SARL au capital de 7.500 euros – RCS Alençon 452 954 092 – APE : 9511Z
TVA Intracommunautaire : FR55 452 954 092



1°) On définit ici l'adresse IP qui sera utilisée par l'ordinateur connecté en VPN. Il est impossible de choisir une adresse IP qui soit incluse dans la plage IP du SIEGE et déconseillé dans la plage du SITE DISTANT.

2°) On utilise les paramètres IP du SIEGE. On retrouve ces paramètres au III.D dans la 2ème copie d'écran.

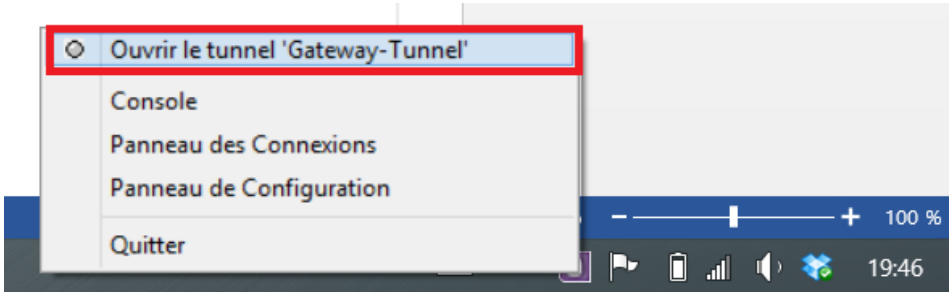
3°) Nous vérifions que nous avons bien les mêmes paramètres de sécurité que ceux spécifiés au III.D



Il ne reste plus qu'à sauvegarder la configuration réalisée comme indiqué dans la copie d'écran précédente.

D. Etablissement de la connexion et vérifications

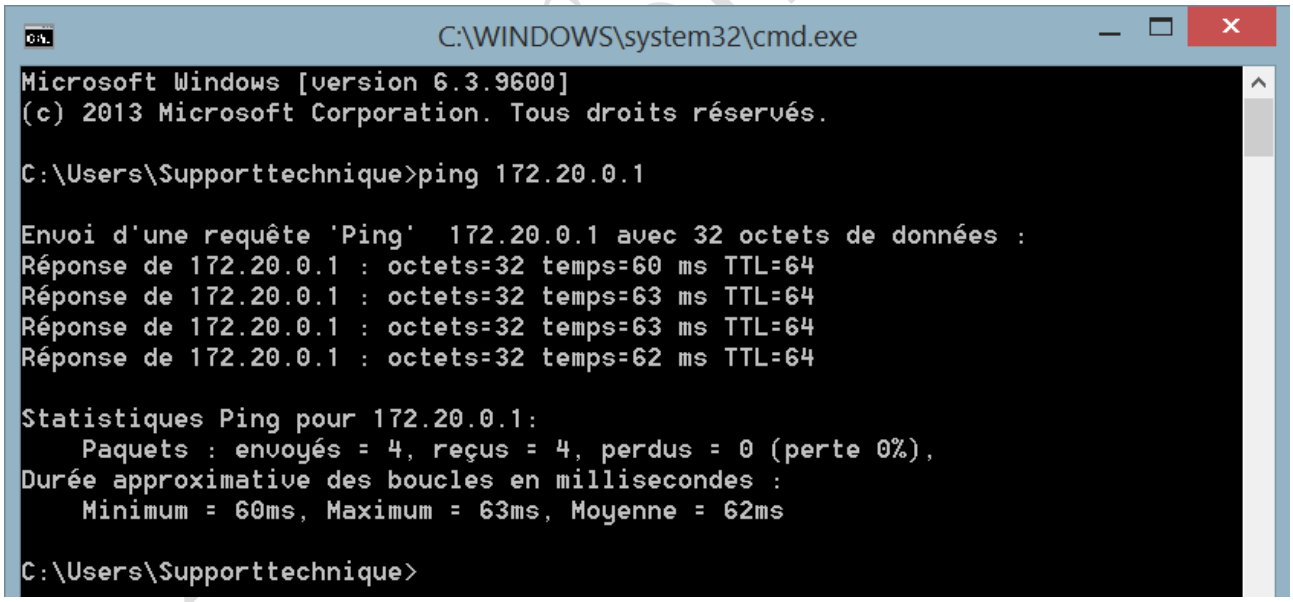
Pour établir la connexion il suffit de faire un clic droit sur l'icône Netgear dans la barre système et cliquer sur l'élément 'Ouvrir le tunnel 'Gateway-Tunnel'' du menu contextuel.



Lorsque la connexion est créée, l'icône devient verte.

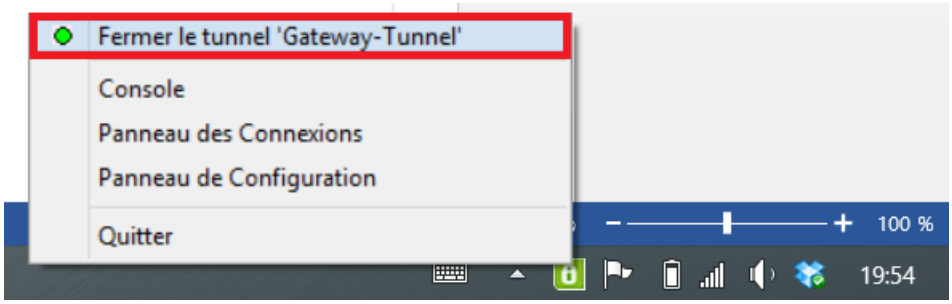
Afin de vérifier que nous avons bien accès aux ressources de l'entreprise, nous ouvrons une invite en ligne de commande (Raccourci clavier : Touche Windows + R, saisir CMD puis ENTREE).

Le routeur du SIEGE ayant l'adresse IP 172.20.0.1, nous utilisons la commande PING.



La commande indique bien que les 4 paquets ont bien été reçus et qu'aucune perte n'a été détectée.

Pour stopper la connexion VPN, il suffit de faire un clic droit sur l'icône Netgear (Verte donc) et sélectionner 'Fermer le tunel 'Gateway-tunnel'' comme ceci :



E. Informations complémentaires

Certains noms ont été choisis pour cette démonstration et peuvent se révéler inadéquat dans un contexte de production.

Autant que possible, donnez des noms explicites à vos connexions surtout si vous devez en avoir plusieurs sur un même ordinateur.

VI. Pour aller plus loin

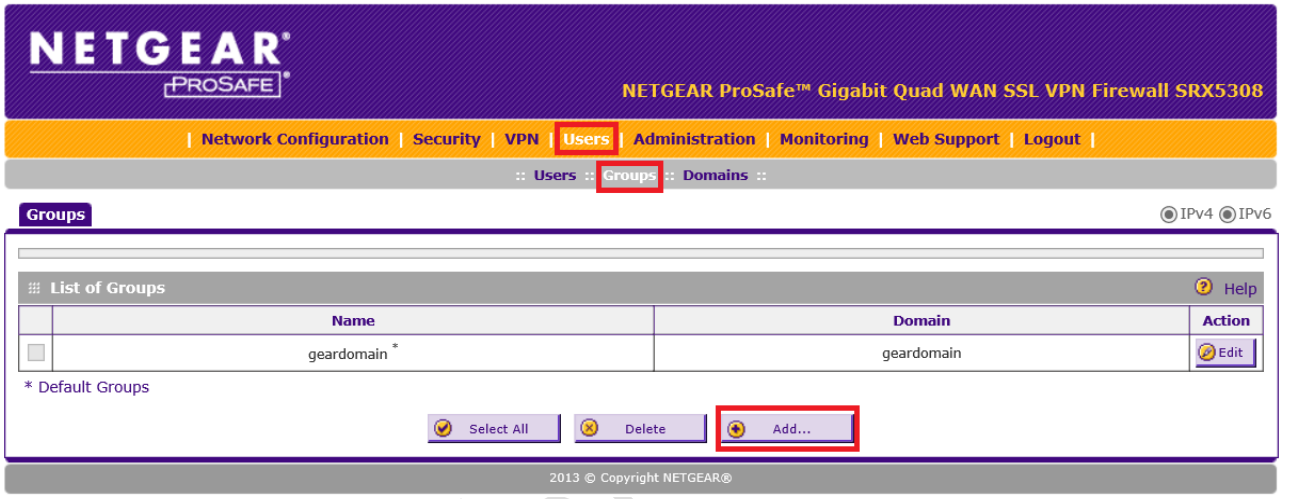
Cette section présente des fonctionnalités avancées.

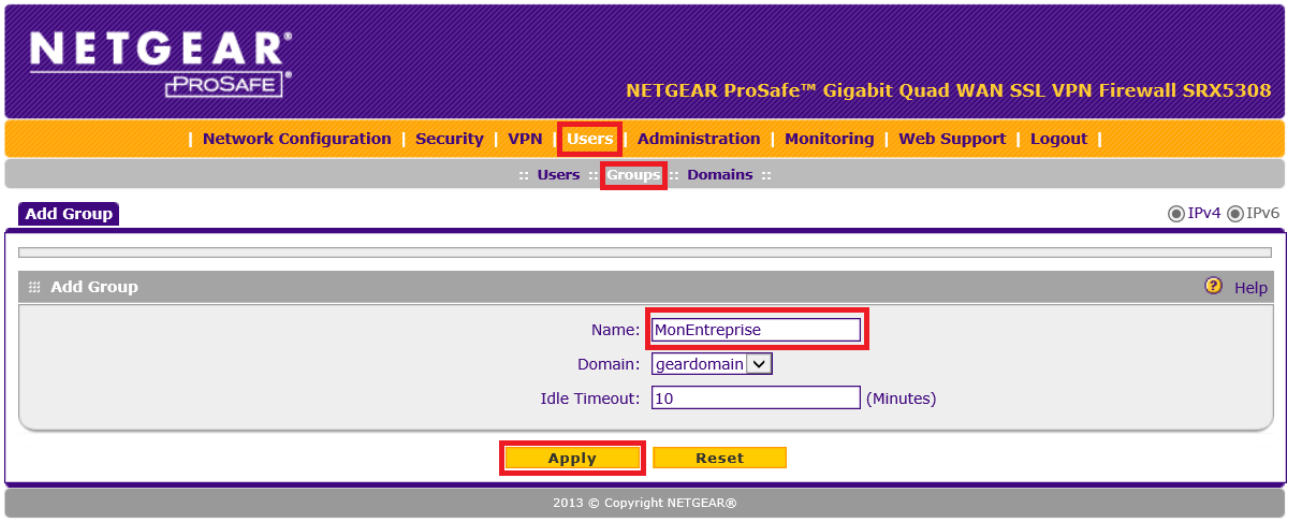
A. Ajout de l'authentification par utilisateur

Afin de renforcer la sécurité en entreprise, il est possible d'ajouter une authentification supplémentaire avec le couple Login/Mot de passe. Le routeur Netgear SRX5308 nous offre entre autre 2 possibilités intéressantes. Soit nous pouvons créer une base d'utilisateurs locale soit utiliser un serveur RADIUS configuré sur un NAS par exemple.

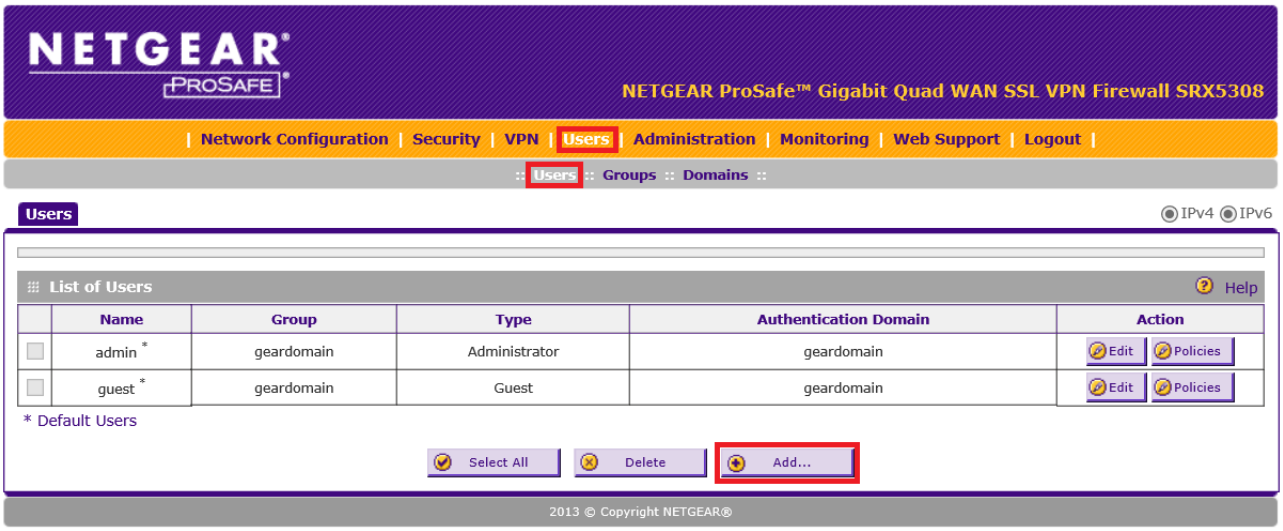
1. Comptes d'utilisateurs sur le routeur

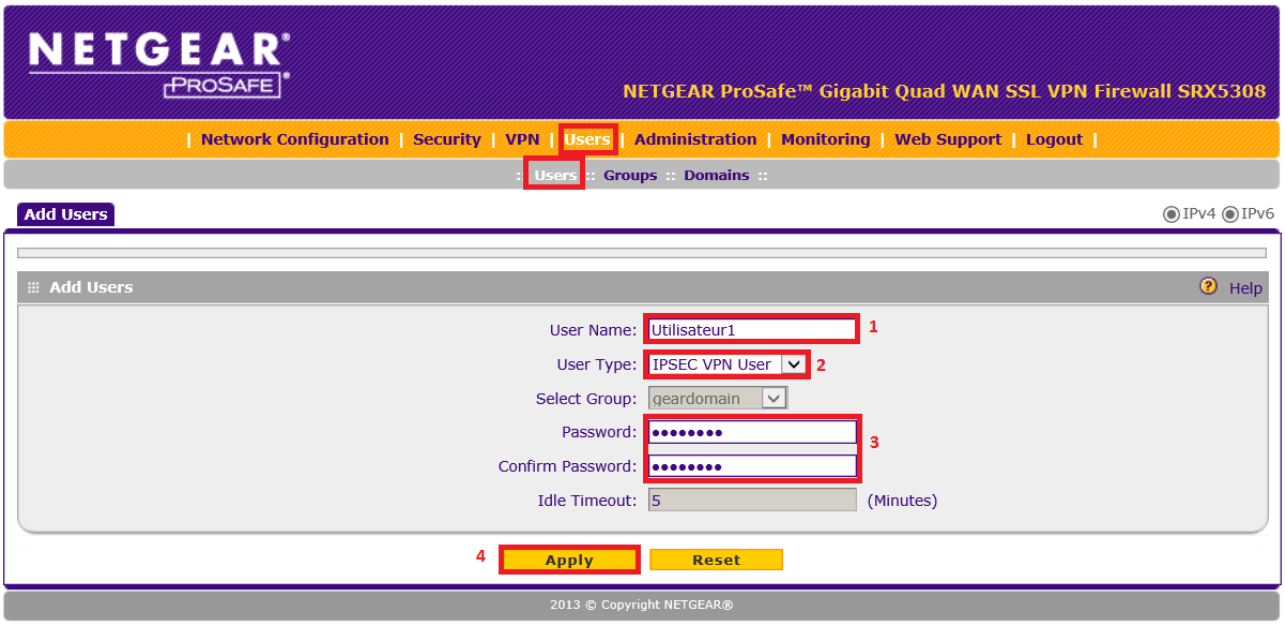
Nous allons créer un groupe d'utilisateur spécifique à l'entreprise que nous appellerons MonEntreprise.





Ensuite, nous pouvons créer nos utilisateurs avec un mot de passe ('password' dans notre cas).



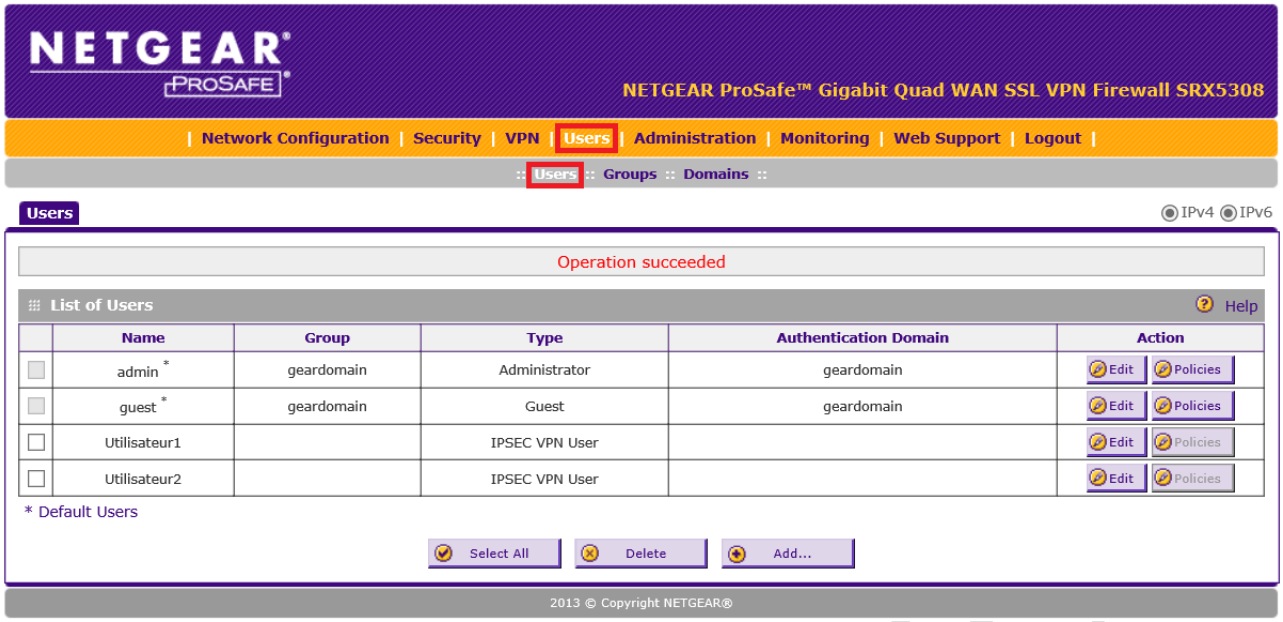


1°) Le nom de l'utilisateur à utiliser pour l'authentification.

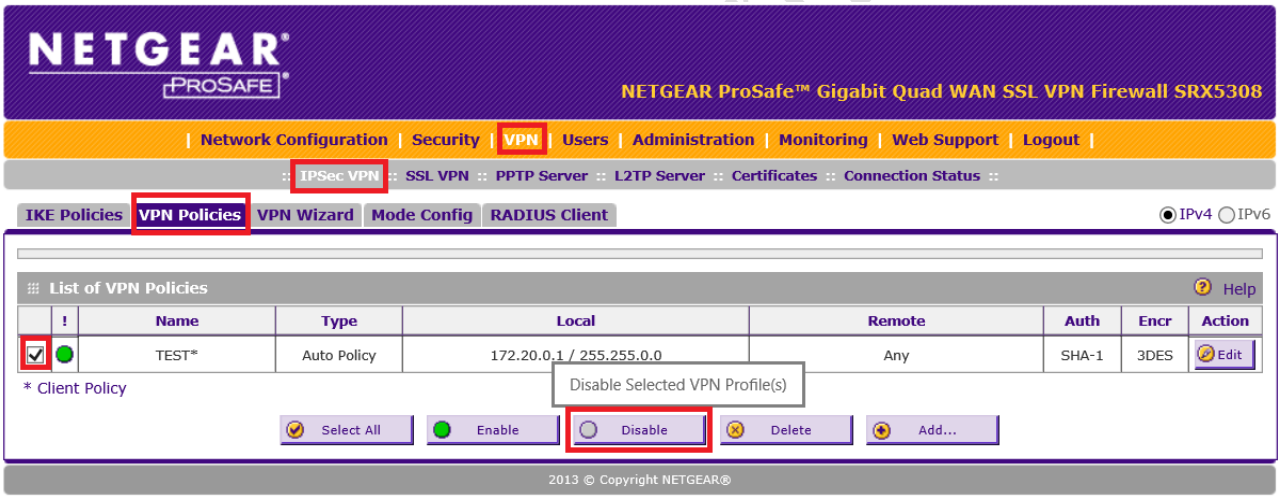
2°) Nous spécifions le type de l'utilisateur pour correspondre au VPN.

3°) Nous spécifions un mot de passe. En production, il est conseillé d'utiliser un mot de passe long et robuste.

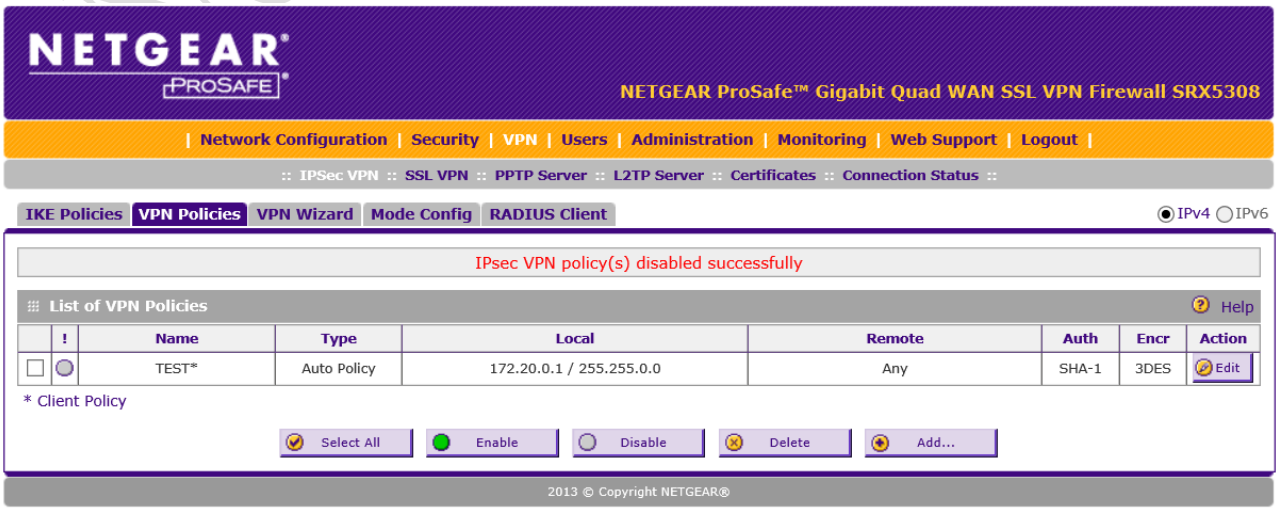
Voici ce que nous obtenons :



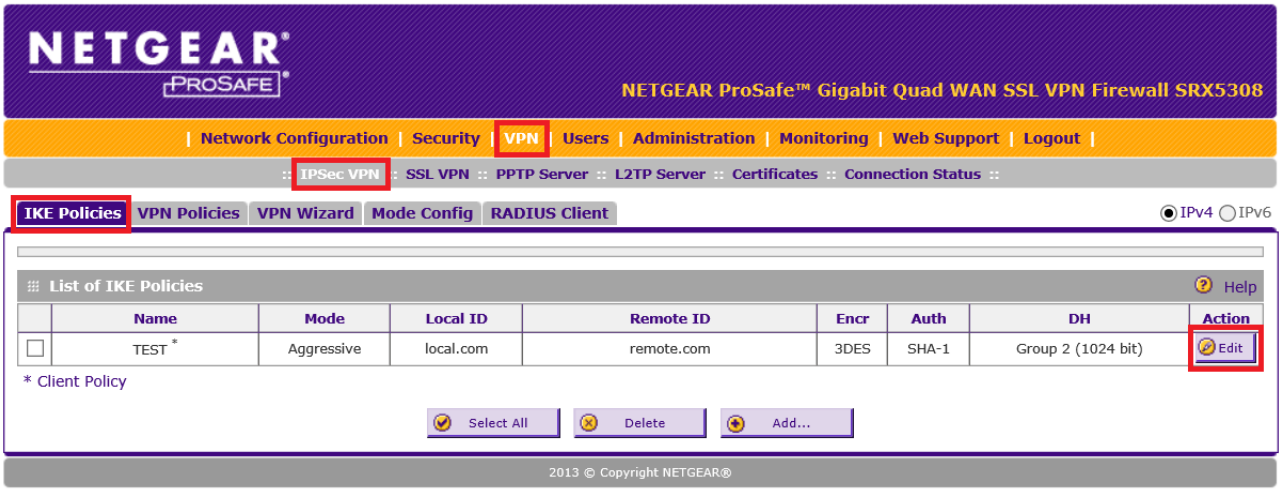
Ensuite, il faut modifier les paramètres de connexion IKE. Il faut d'abord désactiver la Phase 2 (VPN Policies) avant de pouvoir modifier la Phase 1 (IKE Policies) comme ceci :



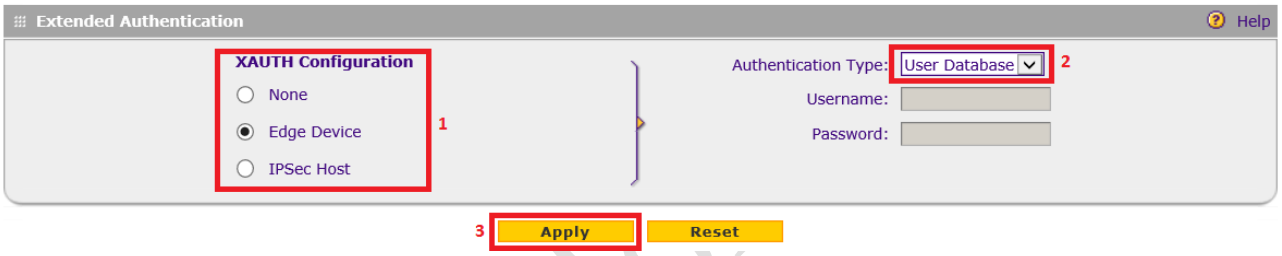
Nous obtenons la confirmation :



Ensuite, nous pouvons éditer la Phase 1 :



En naviguant jusqu'en bas de la page, nous allons paramétrer l'authentification étendue.

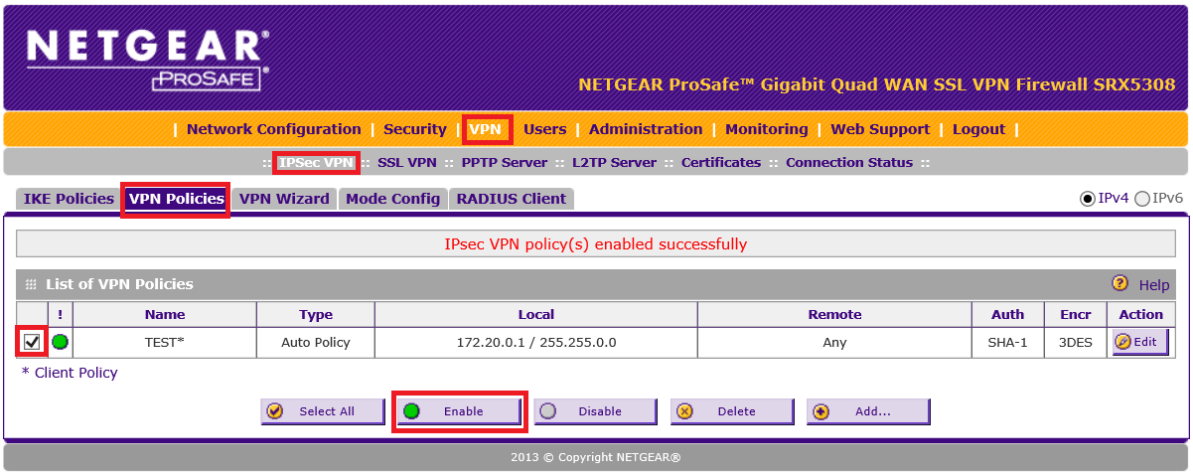


1°) En sélectionnant 'Edge Device' sous 'XAUTH Configuration', nous activons le routeur en tant que concentrateur VPN.

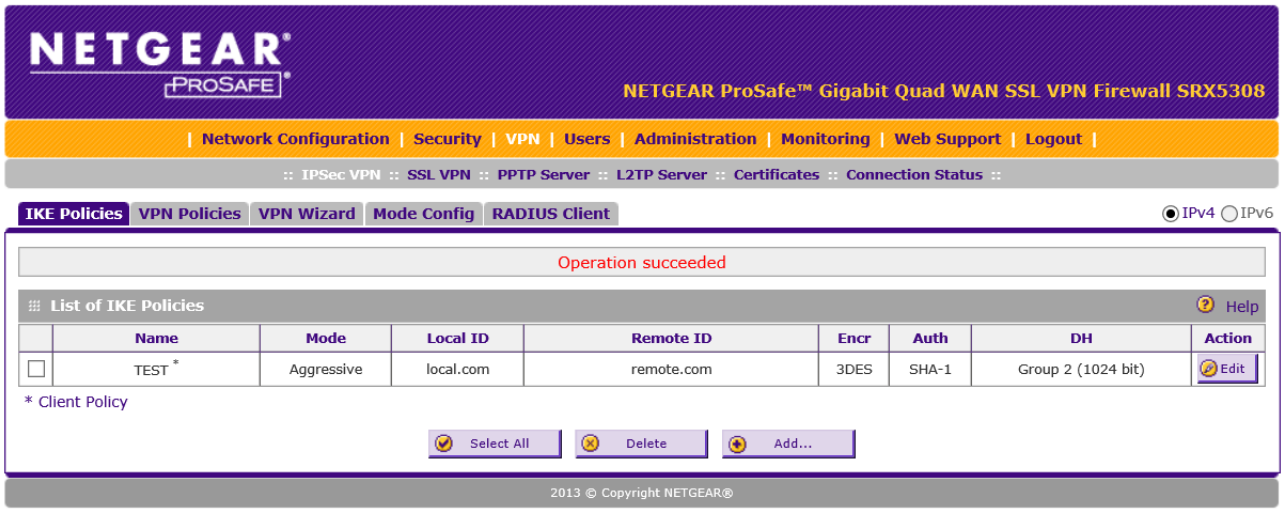
2°) Maintenant, il est possible de sélectionner la base d'utilisateur locale au routeur.

3°) On applique les paramètres.

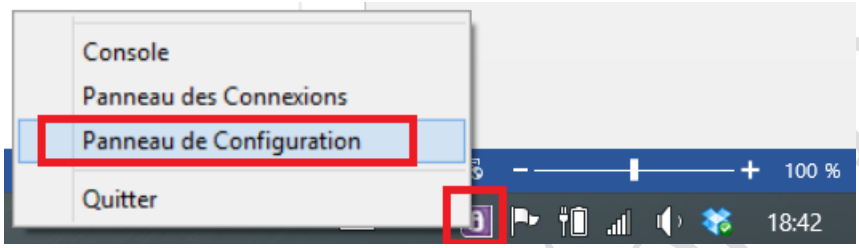
4°) Pensez à réactiver la Phase 2 comme ceci :

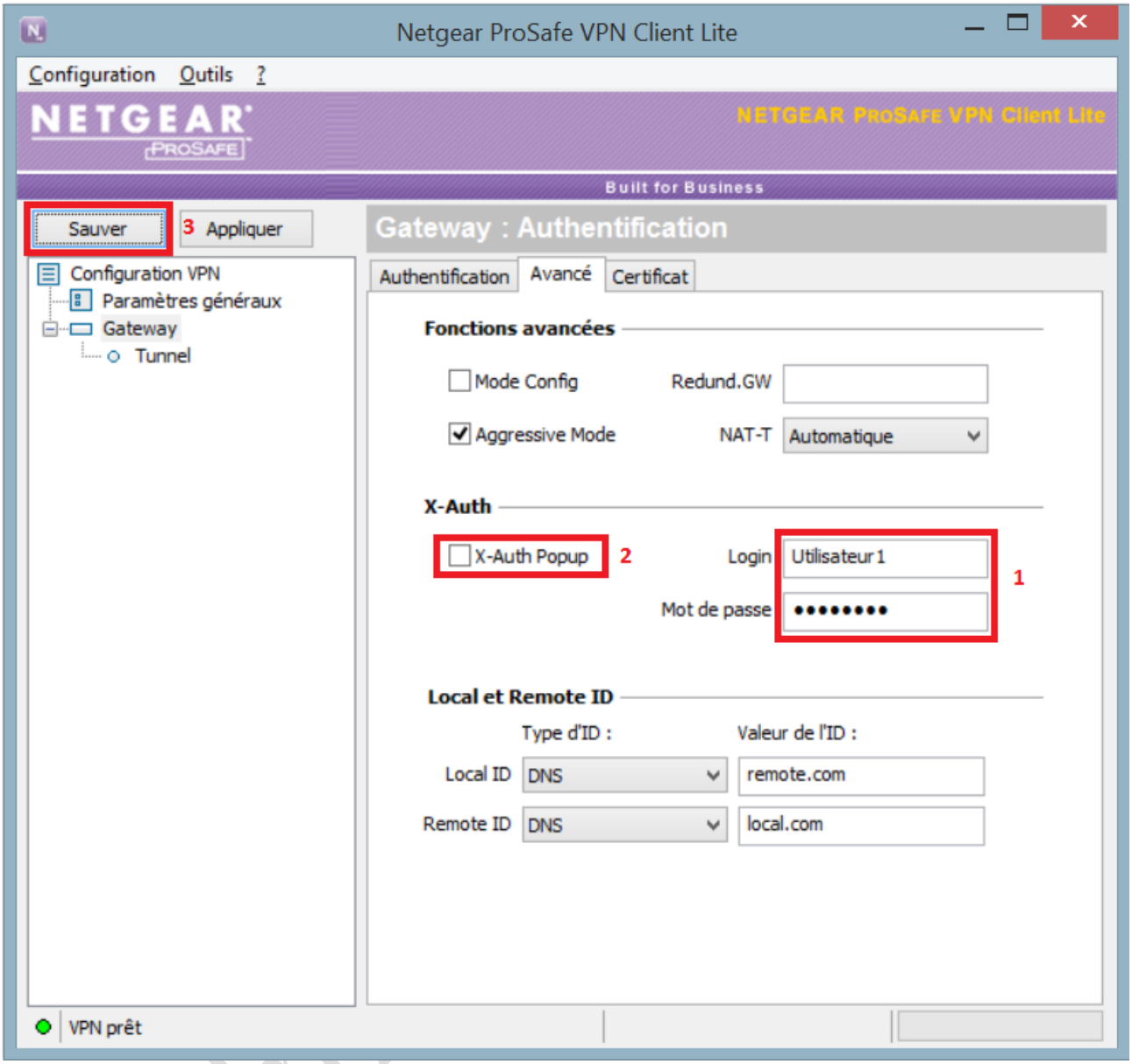


L'interface nous confirme le succès de l'opération. A partir de ce moment-là, IL N'EST PLUS POSSIBLE DE MONTER le VPN crée antérieurement.



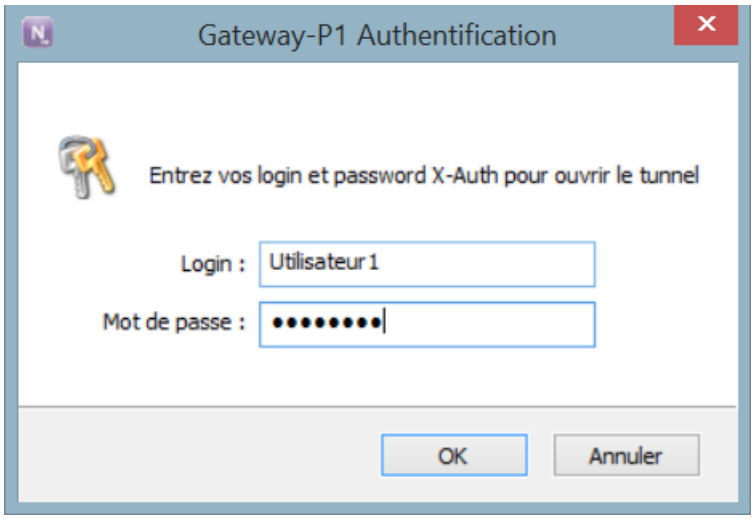
Maintenant, nous devons modifier les paramètres du client logiciel Netgear. Ouvrer la console avec un clic droit comme précédemment :





1°) Dans la partie Gateway, onglet Avancé, nous configuration l'authentification avec l'un des comptes crée ('Utilisateur1' dans cet exemple).

2°) Vous avez la possibilité de laisser le logiciel afficher une boîte d'authentification plutôt que de saisir en dur les identifiants. Cela peut être utile si l'on veut renforcer la sécurité en cas de vol de l'appareil ou d'ordinateur avec une même session partagée.



Attention, si vous ne saisissez pas assez vite les identifiants, un timeout vous refuse la connexion.

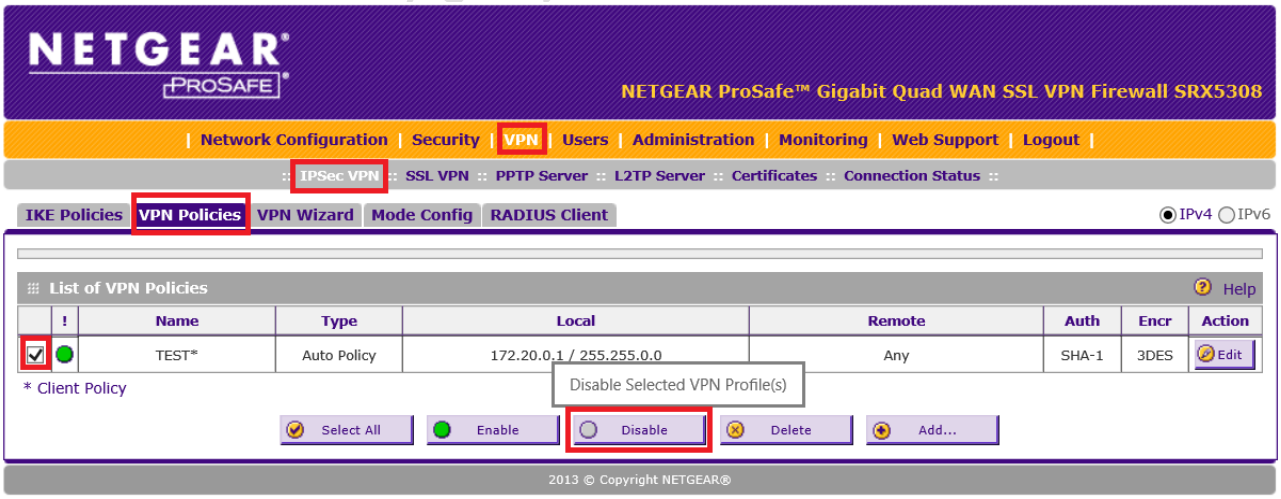
3°) Sauvegardez les paramètres et lancez la connexion pour vérifier le fonctionnement comme indiqué au chapitre V.D.

2. Comptes d'utilisateurs sur un serveur RADIUS

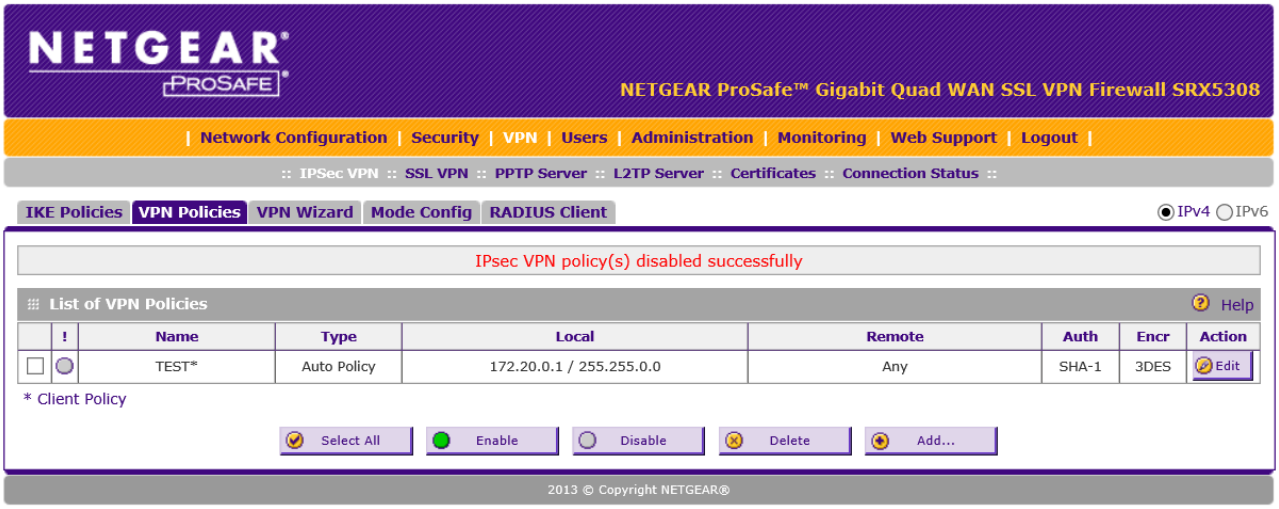
Pour l'authentification RADIUS, nous allons supposer que votre serveur RADIUS est fonctionnel et que vous avez créé un utilisateur nommé 'Utilisateur3' et le mot de passe 'password'. Nous présenterons un tutoriel prochainement sur la configuration RADIUS.

Sur le SRX5308, lorsque vous utilisez une authentification RADIUS, le routeur VERIFIE D'ABORD dans sa base locale si aucun compte n'est déjà défini. Ce point, fort pratique peut aussi être source d'erreurs d'authentification.

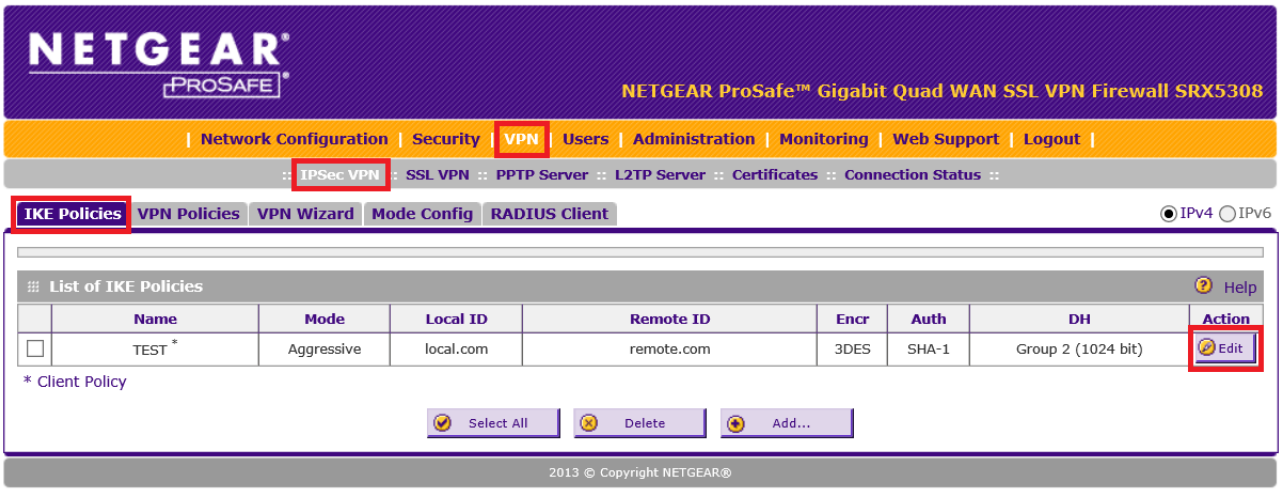
Il faut modifier les paramètres de connexion IKE. Il faut d'abord désactiver la Phase 2 (VPN Policies) avant de pouvoir modifier la Phase 1 (IKE Policies) comme ceci :



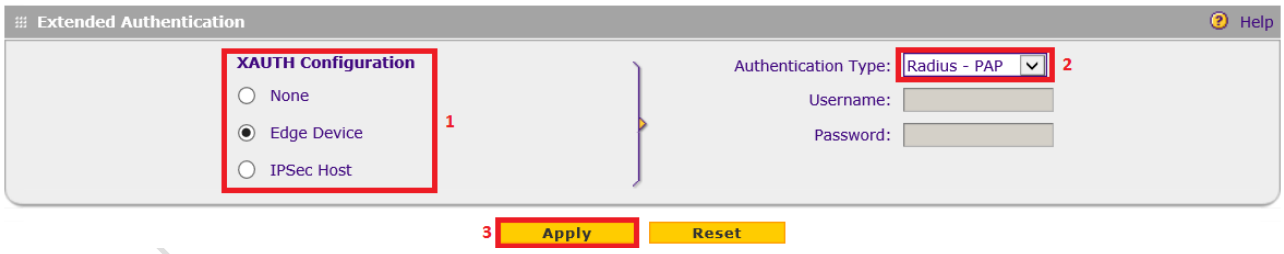
Nous obtenons la confirmation :



Ensuite, nous pouvons éditer la Phase 1 :



En naviguant jusqu'en bas de la page, nous allons paramétrer l'authentification étendue.

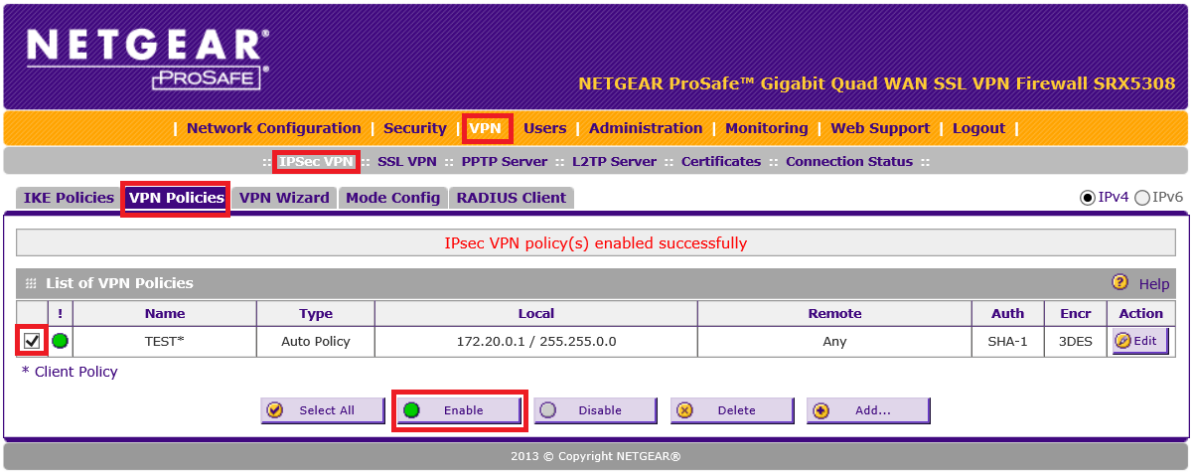


1°) En sélectionnant 'Edge Device' sous 'XAUTH Configuration', nous activons le routeur en tant que concentrateur VPN.

2°) Maintenant, il est possible de sélectionner notre serveur RADIUS (Radius – PAP dans notre cas).

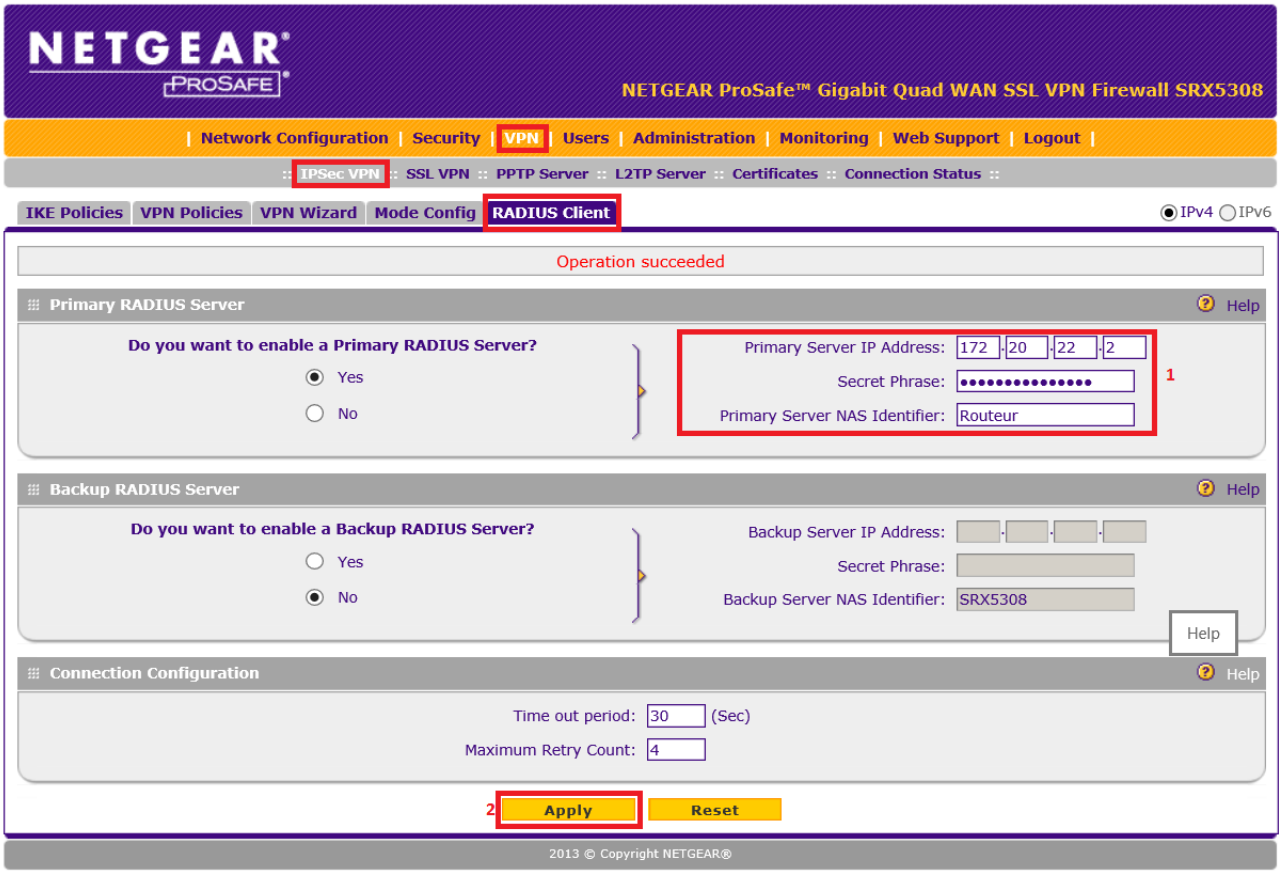
3°) On applique les paramètres.

4°) Pensez à réactiver la Phase 2 comme ceci :



L'interface nous confirme le succès de l'opération. A partir de ce moment-là, IL N'EST PLUS POSSIBLE DE MONTER le VPN crée antérieurement.

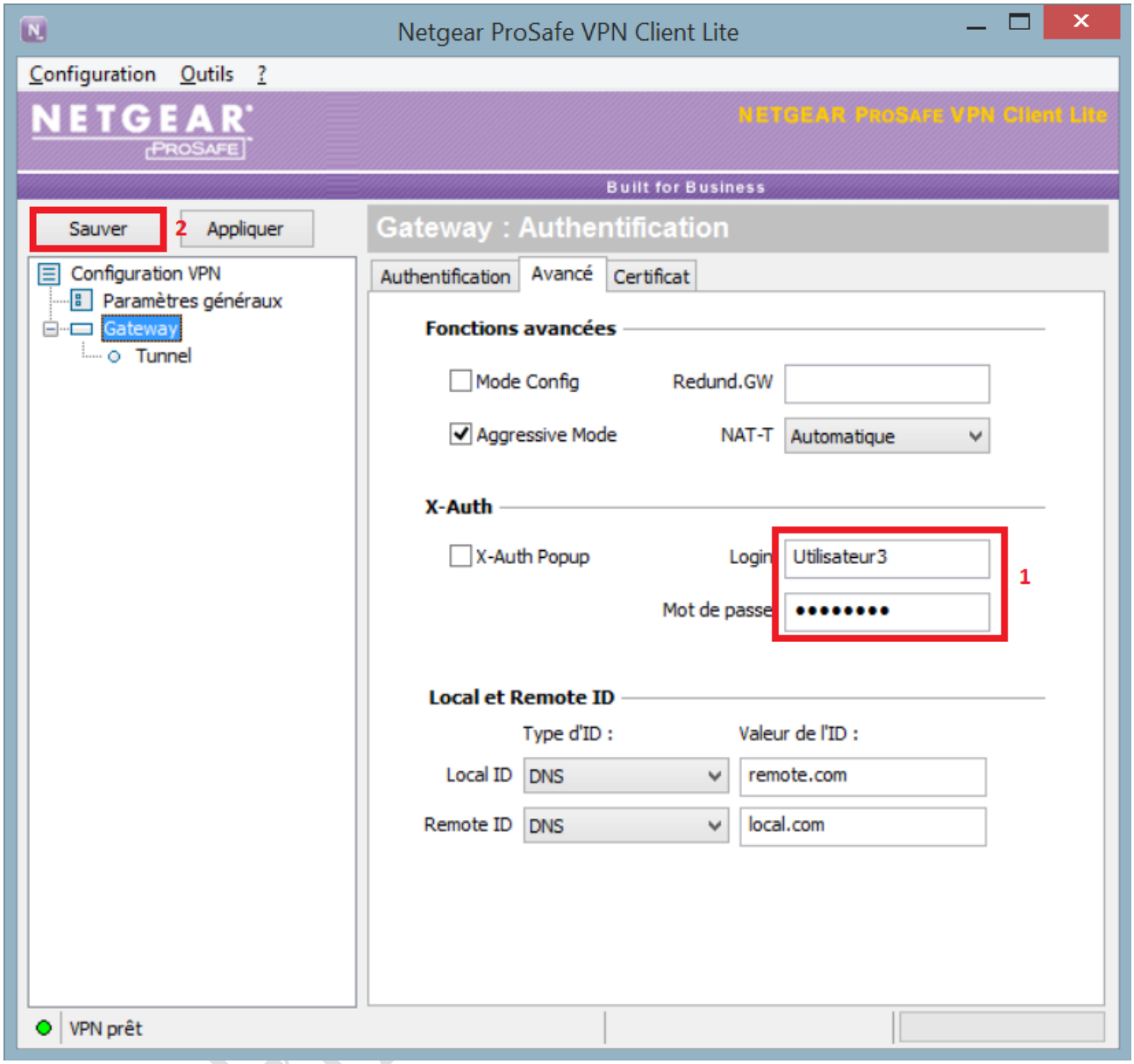
Il faut créer la liaison entre le routeur et le serveur RADIUS maintenant :



1°) Nous configurons l'adresse IP du serveur RADIUS. **Le champ 'Secret Phrase' et suivant DOIVENT ETRE IDENTIQUES à ceux saisis sur le serveur RADIUS.**

2°) Nous pouvons appliquer les paramètres maintenant.

Nous devons maintenant modifier le client logiciel comme suit :



1°) Nous entrons le compte Utilisateur3 crée sur le serveur RADIUS. Nous utilisons un compte différent pour ne pas entrer en conflit avec les comptes crées localement sur le routeur.

2°) Sauvegardez les paramètres et lancez la connexion pour vérifier le fonctionnement comme indiqué au chapitre V.D.

.

VII. Pour aller (encore) plus loin

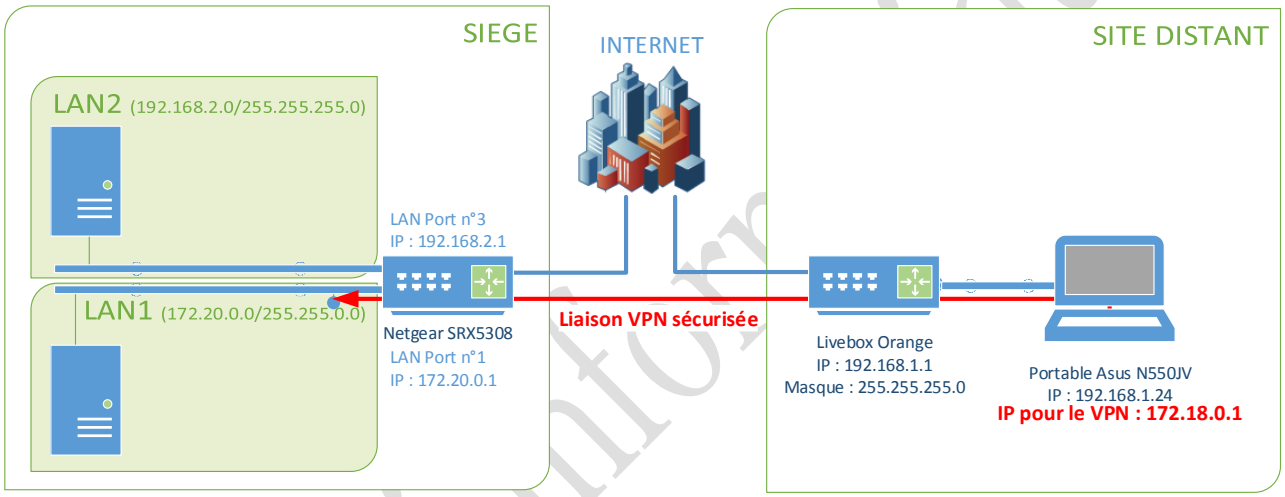
A. Inter-VLAN Routing

Le routeur Netgear SRX5308 permet de créer plusieurs réseaux LANs afin de segmenter un réseau, de l'étendre si une plage IP devient trop encombrée, séparer le réseau professionnel de celui de la maison…

Lors de la connexion VPN distante, il est parfois utile de pouvoir accéder à ces différents réseaux.

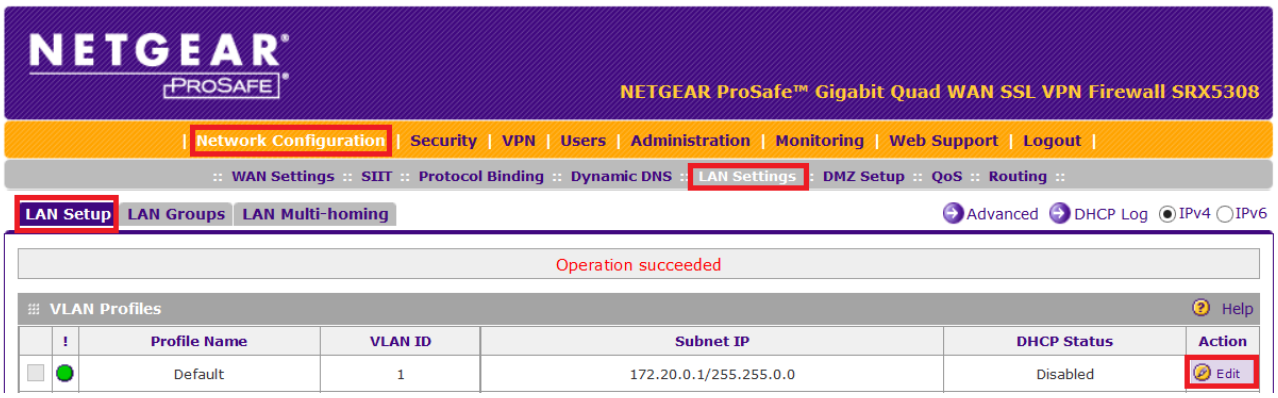
Dans notre exemple, **nous n'utiliserons pas la configuration réalisée précédemment** et repartons de 0. Le routeur est configuré de la sorte :

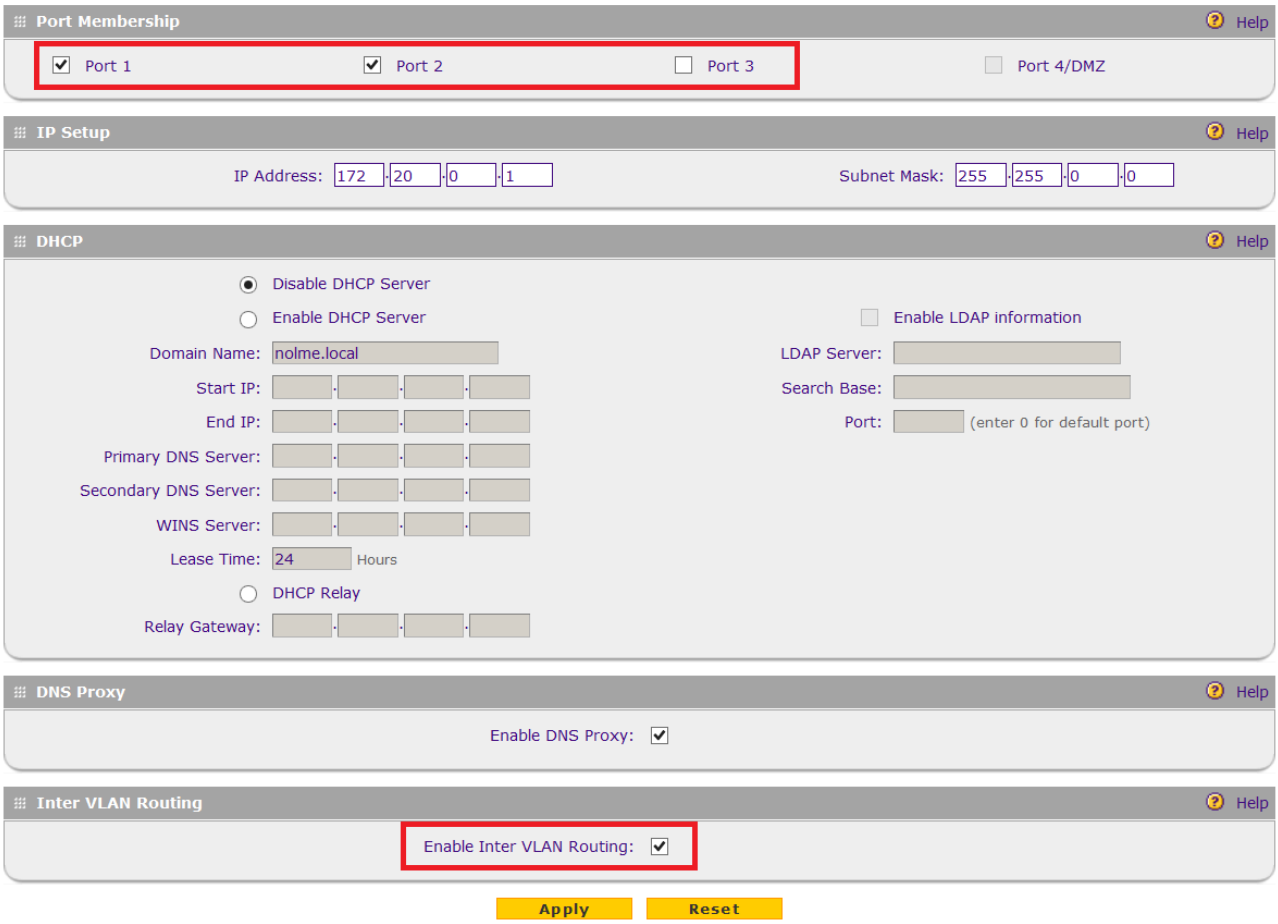
- Port LAN n°1 et n°2 - IP : 172.20.0.1 / 255.255.0.0
- Port LAN n°3 – IP : 192.168.2.1 / 255.255.255.0
- Port LAN n°4 – IP : Configuré en DMZ (non utilisé dans ce tutorial)



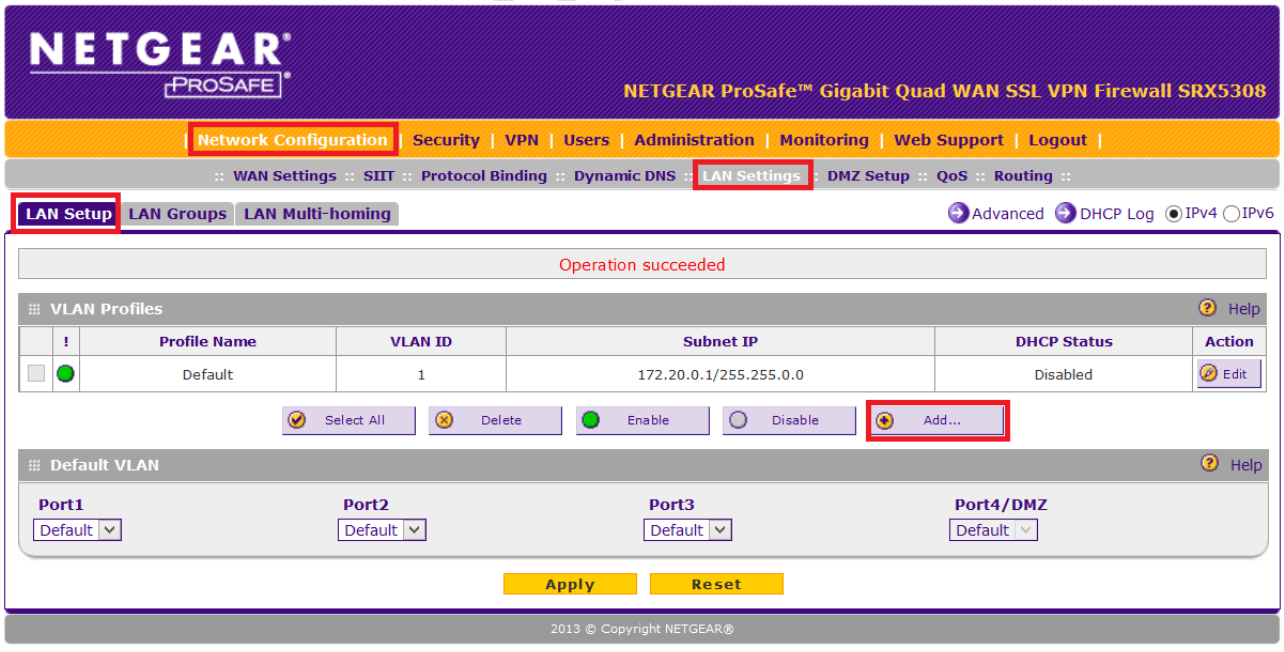
1. Création du 2ème LAN

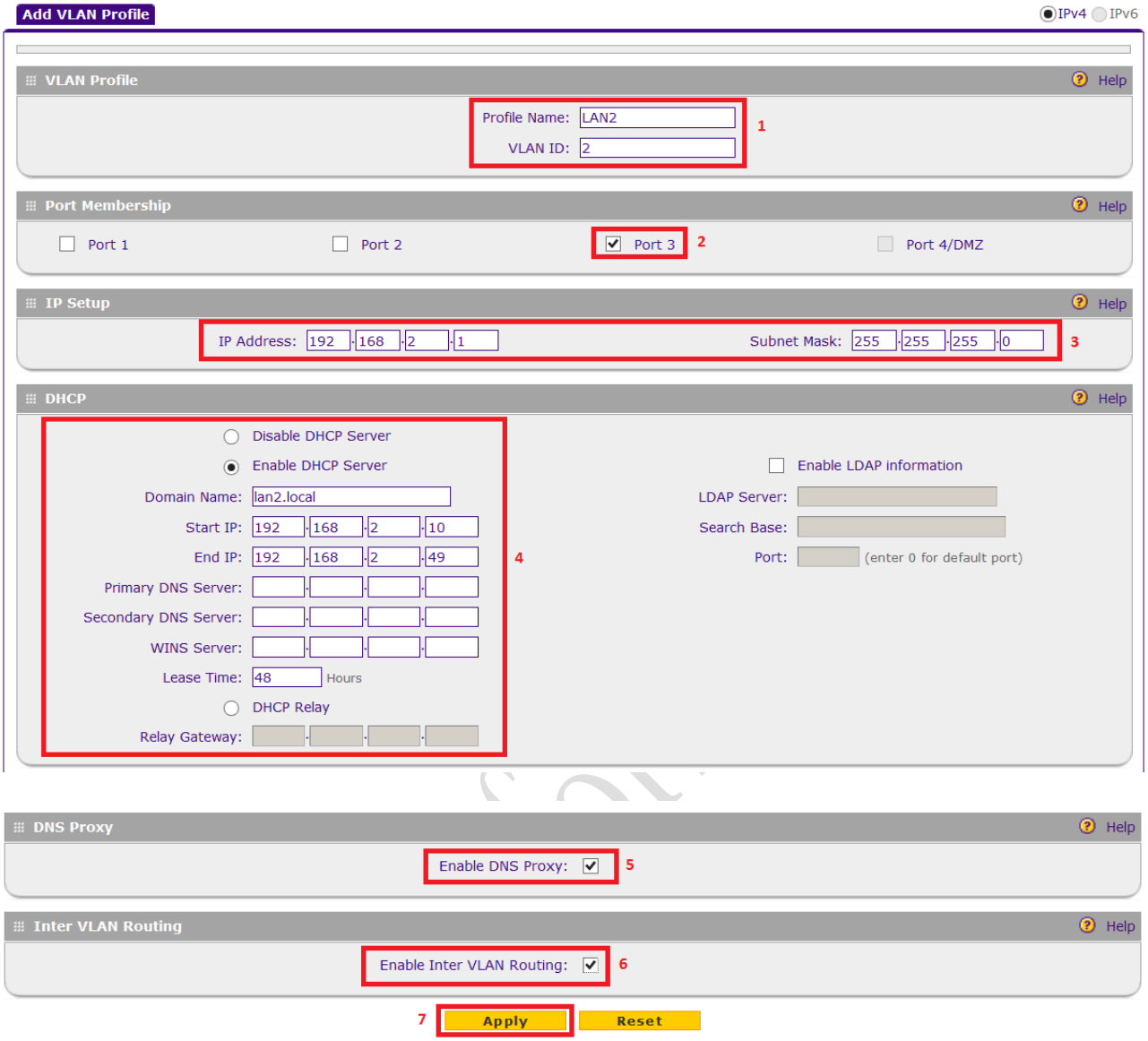
Dans un premier temps, il convient de modifier les ports du routeur associé au LAN1 et d'activer l'option de routage inter-VLAN afin que les 2 réseaux puissent communiquer par la suite.





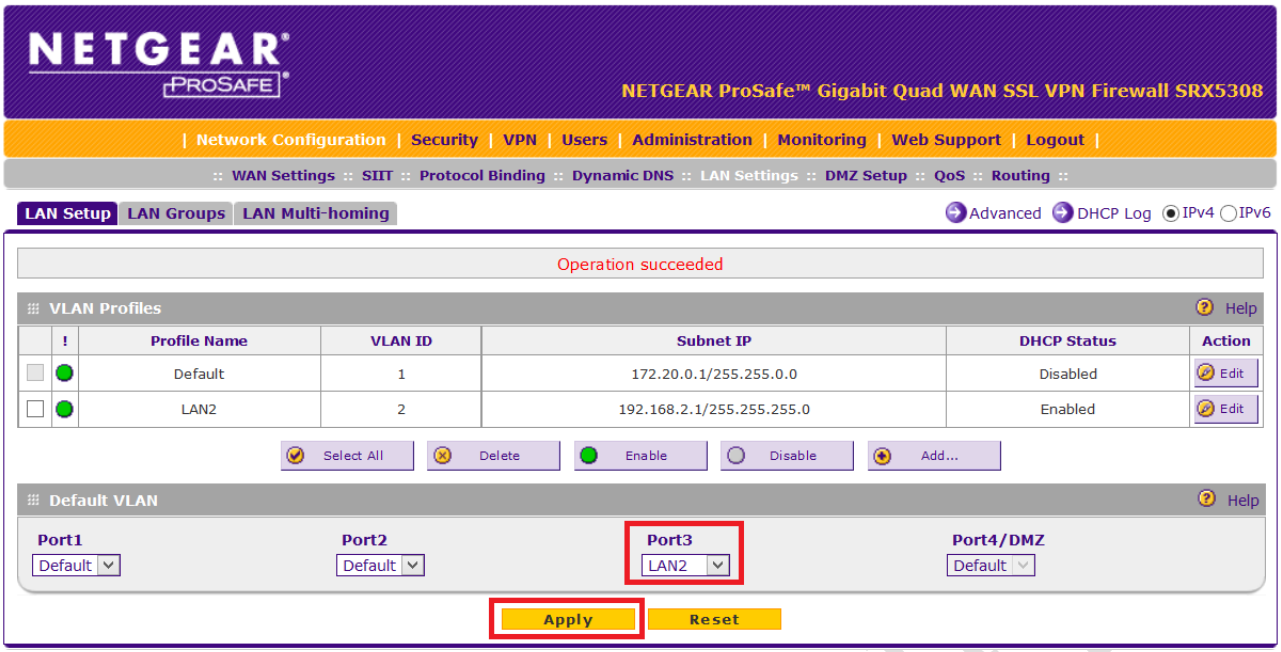
Ensuite, il faut créer le 2ème LAN



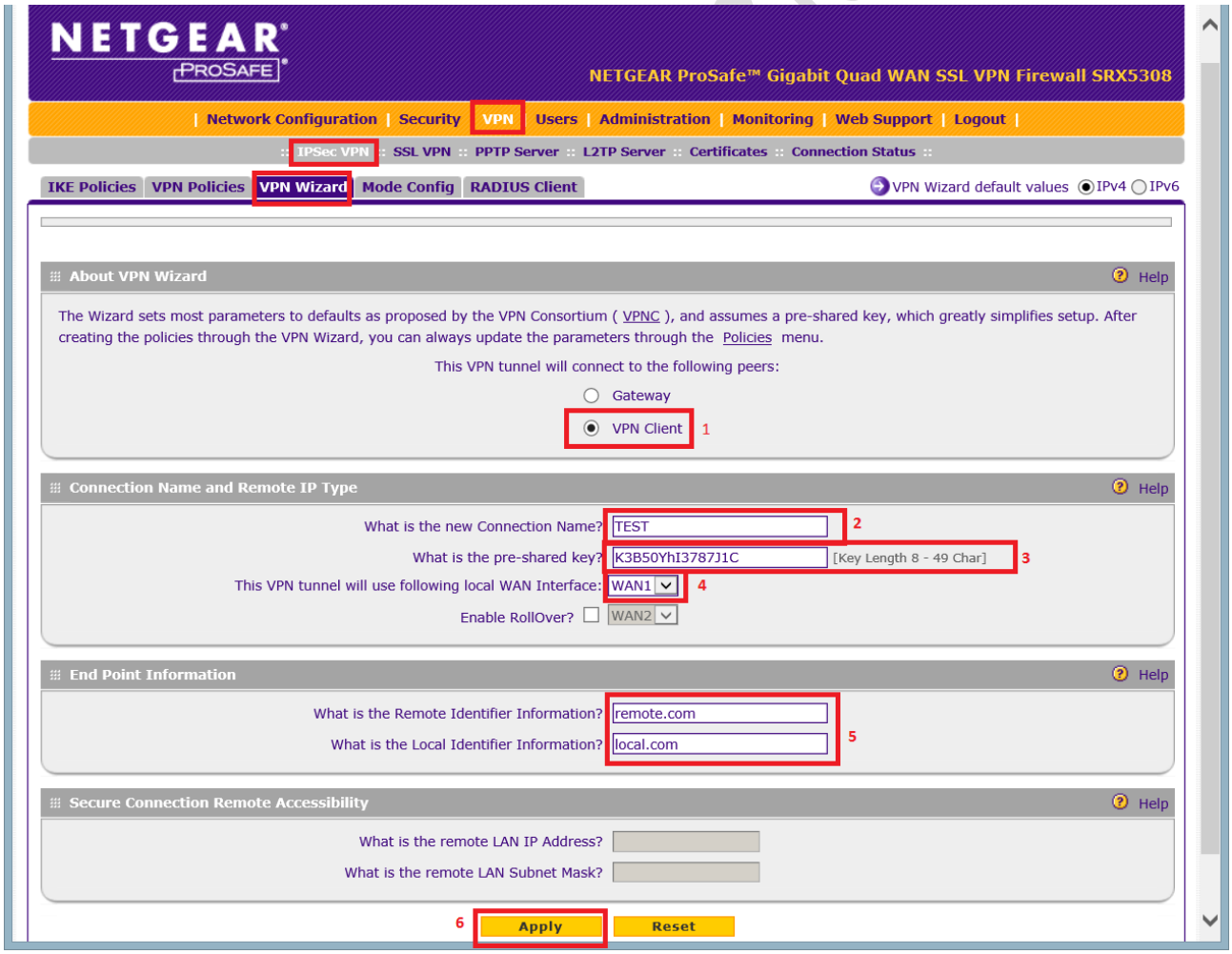


- Etape 1 : Définition d'un nom d'usage et d'un VLAN ID différent du LAN1.
- Etape 2 : Sélection du port n°3 affecté à ce nouveau LAN.
- Etape 3 : Définition de la plage IP du LAN2.
- Etape 4 : Configuration d'un serveur DHCP par commodité.
- Etape 5 : Activation du DNS proxy.
- Etape 6 : Activation de l'Inter VLAN Routing pour communiquer avec le LAN1.
- Etape 7 : Application des paramètres.

Nous vérifions à présent que les ports sont bien répartis comme il le faut.



2. Configuration du VPN sur le routeur



1°) Nous spécifions ici qu'il s'agit d'un accès type Ordinateur à Routeur.

2°) Le nom de la connexion est arbitraire, nous avons choisi TEST.

3°) Nous saisissons la clé de cryptage saisie au III.A

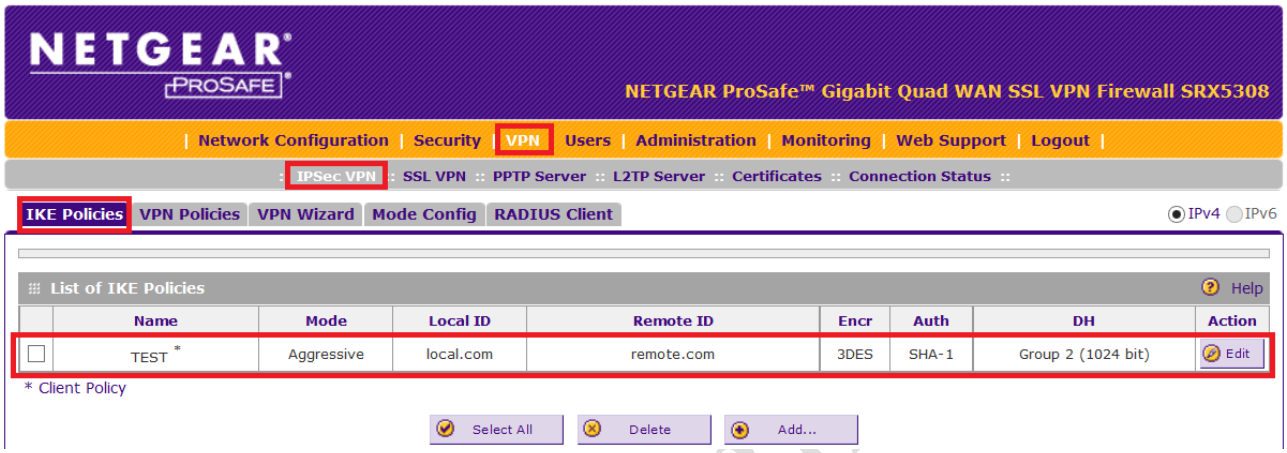
4°) Nous spécifions le port WAN sur lequel créer la connexion tel qu'indiqué dans le I.C

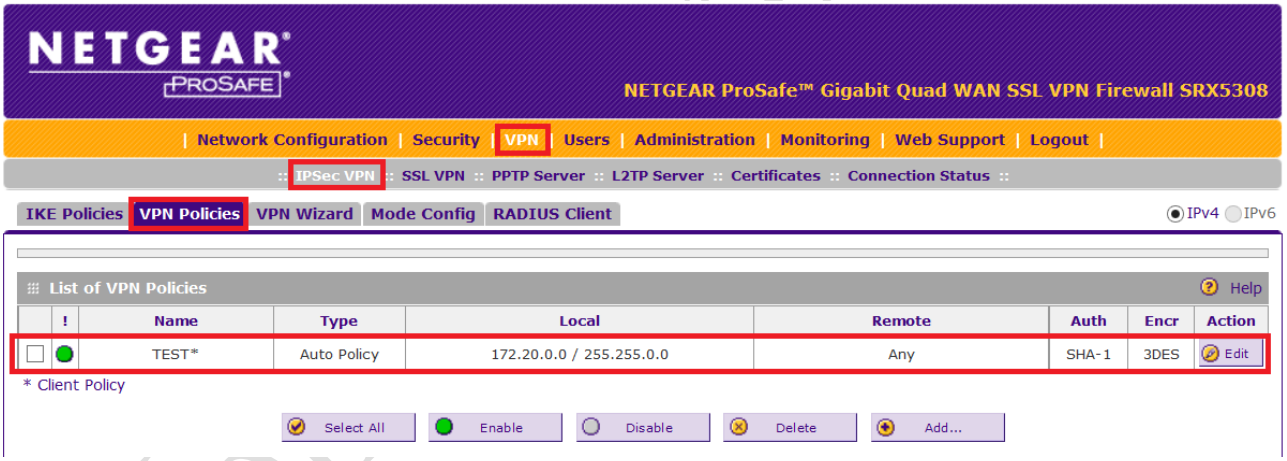
5°) Nous laissons les champs tel qu'ils sont proposés.

6°) Nous pouvons appliquer les changements.

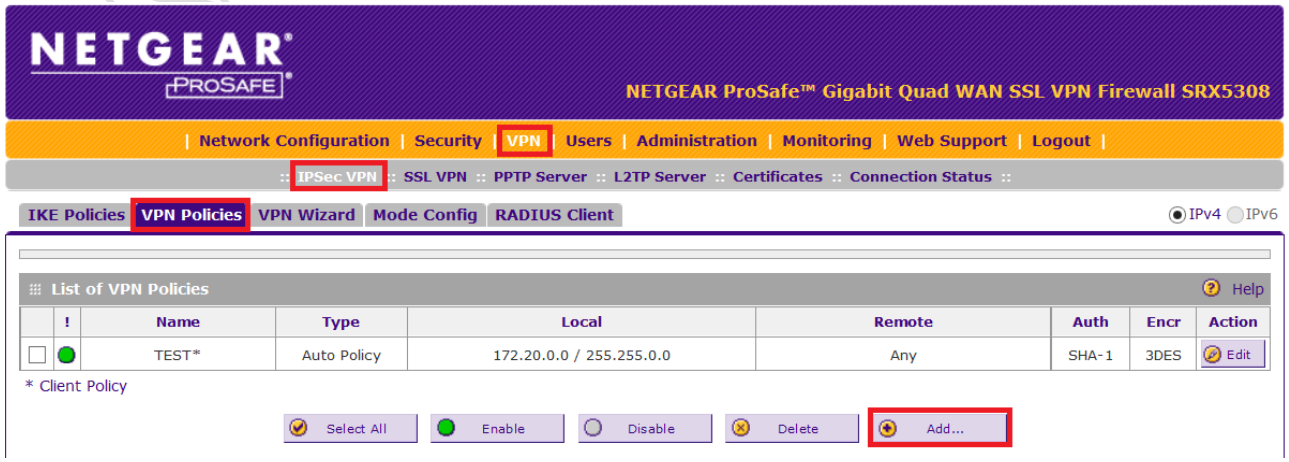
L'algorithme de cryptage utilisé automatiquement est 3DES [Wiki]. L'algorithme d'authentification utilisé automatiquement est SHA-1 [Wiki].

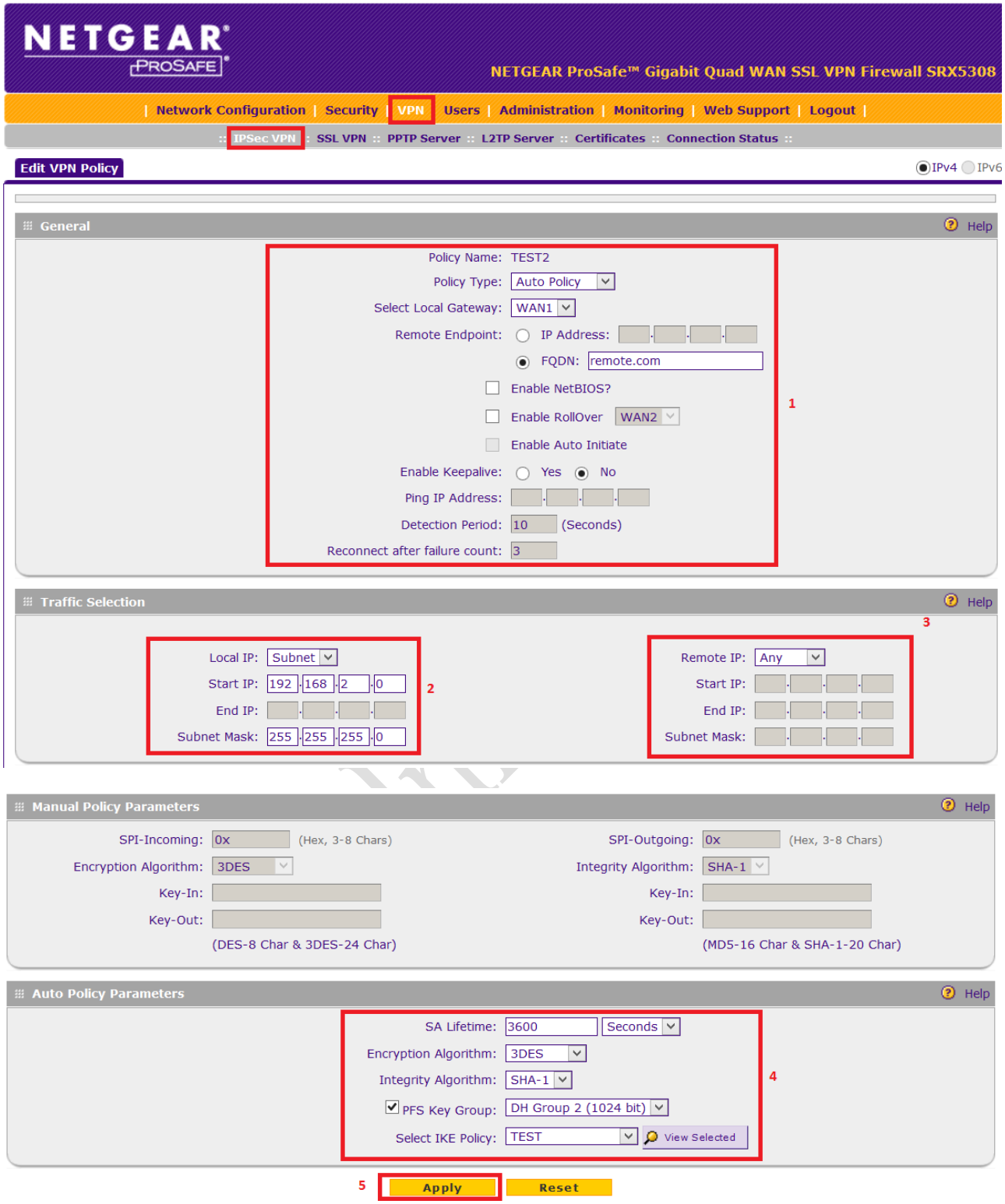
En naviguant comme indiqué ci-dessous, vous devez donc avoir le résultat suivant :





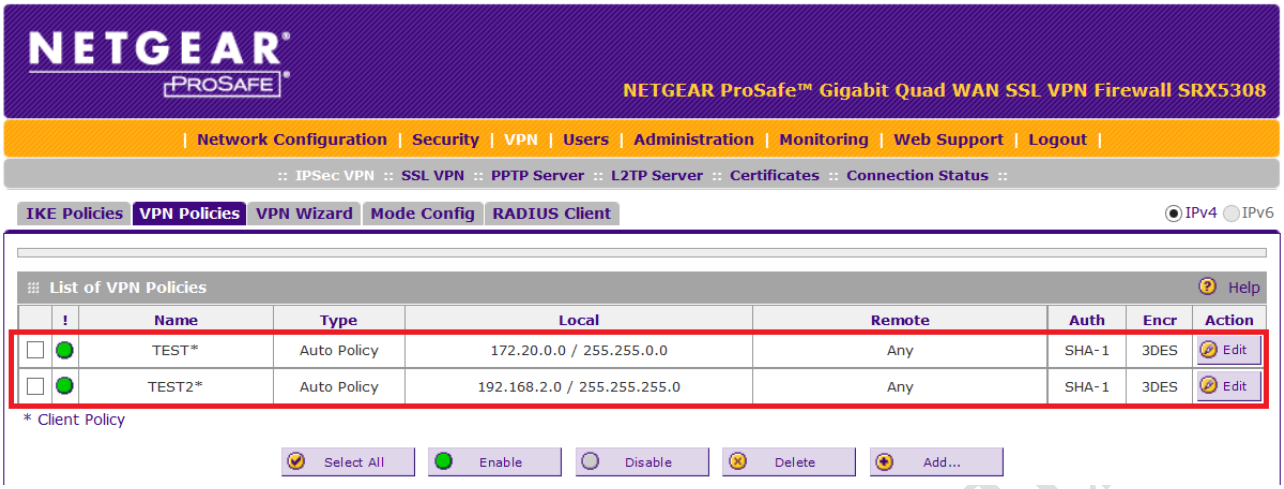
Maintenant nous devons rajouter la Policy relative au 2ème réseau (LAN2).





- Etape 1 : On crée notre politique pour le LAN2.
- Etape 2 : On spécifie la plage IP qui sera utilisée par le LAN2.
- Etape 3 : On autorise toutes les adresses IP.
- Etape 4 : On utilise les paramètres par défaut et on sélectionne la phase 1 (IKE) créée avec le Wizard.
- Etape 5 : On applique les paramètres.

On doit obtenir le résultat suivant :

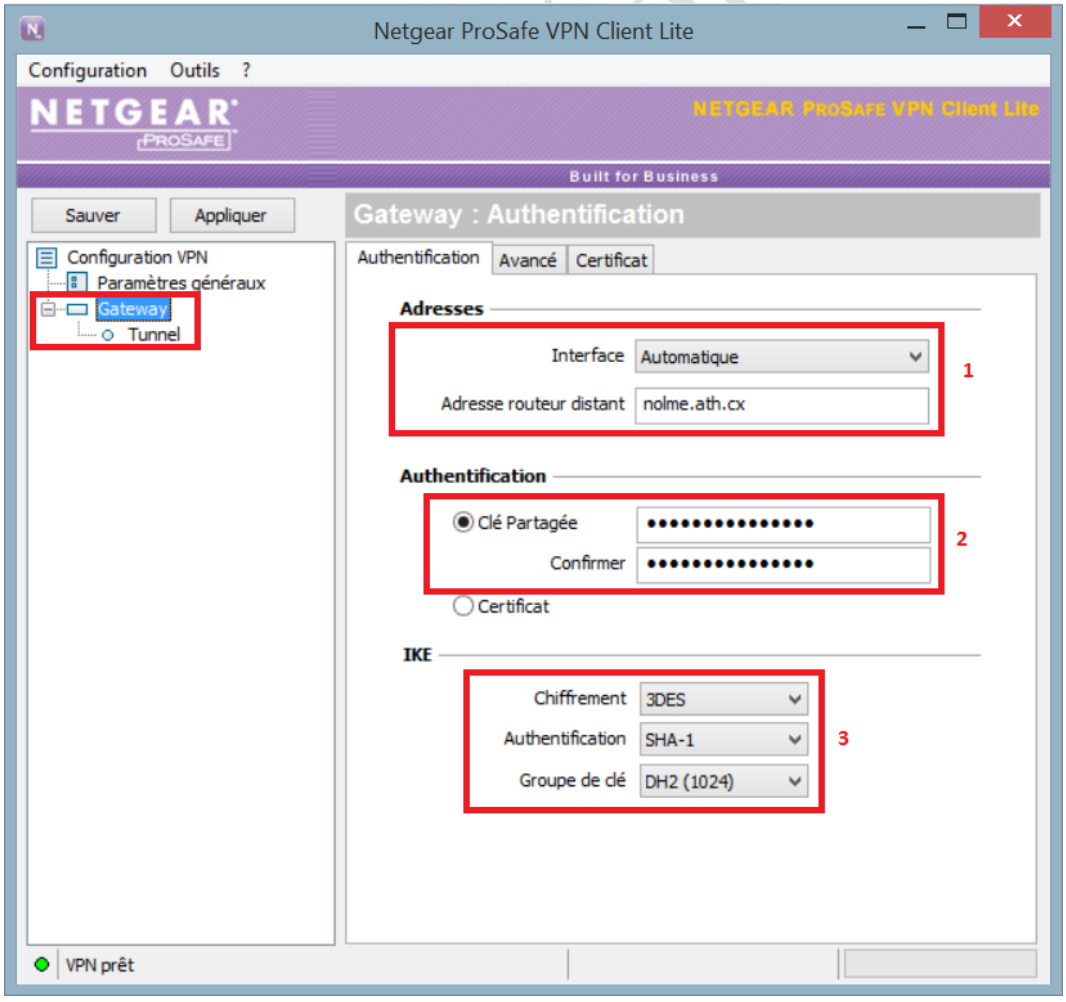


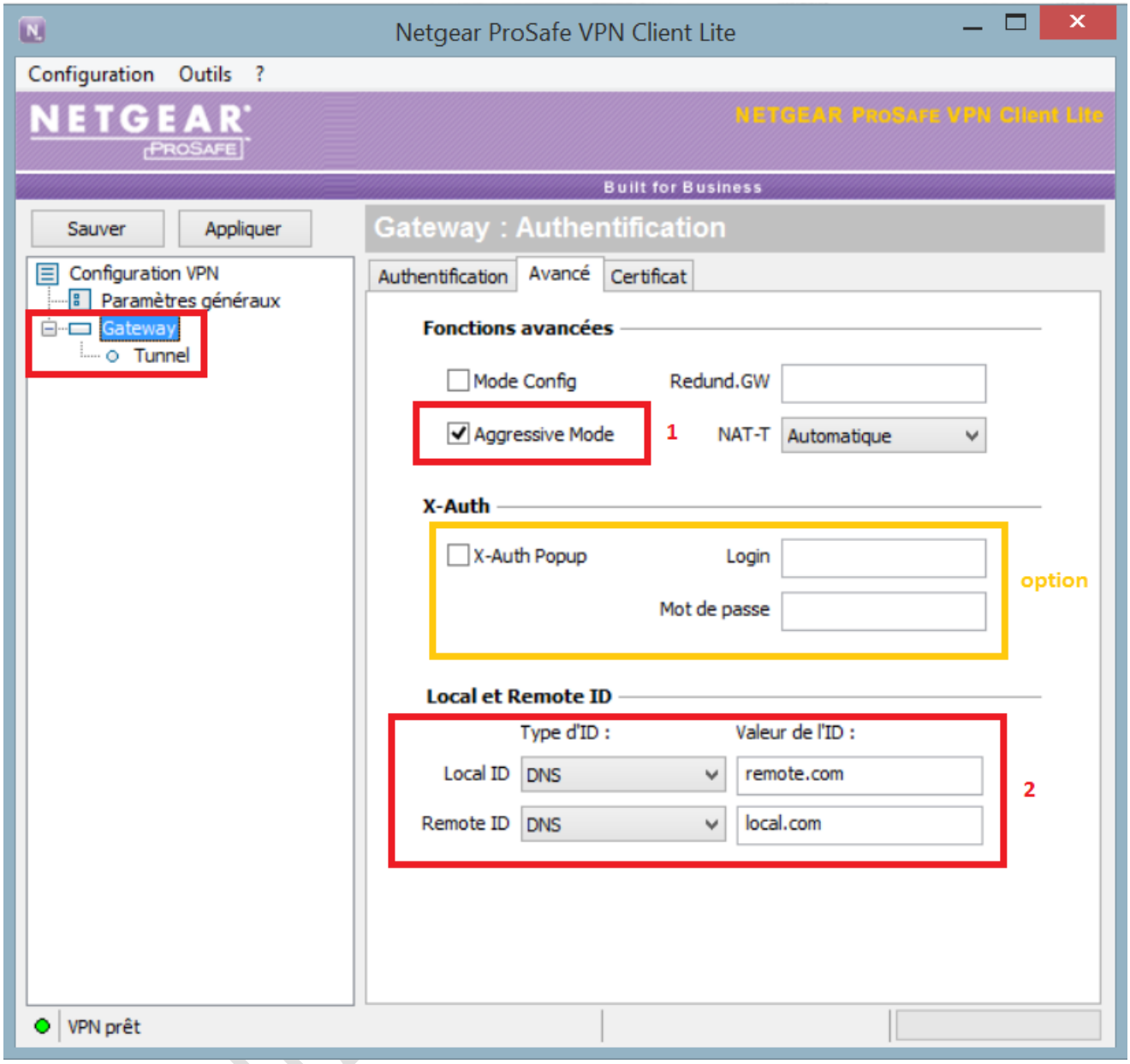
Nous voyons donc en Phase 2, nos 2 réseaux IP.

3. Configuration du client VPN logiciel

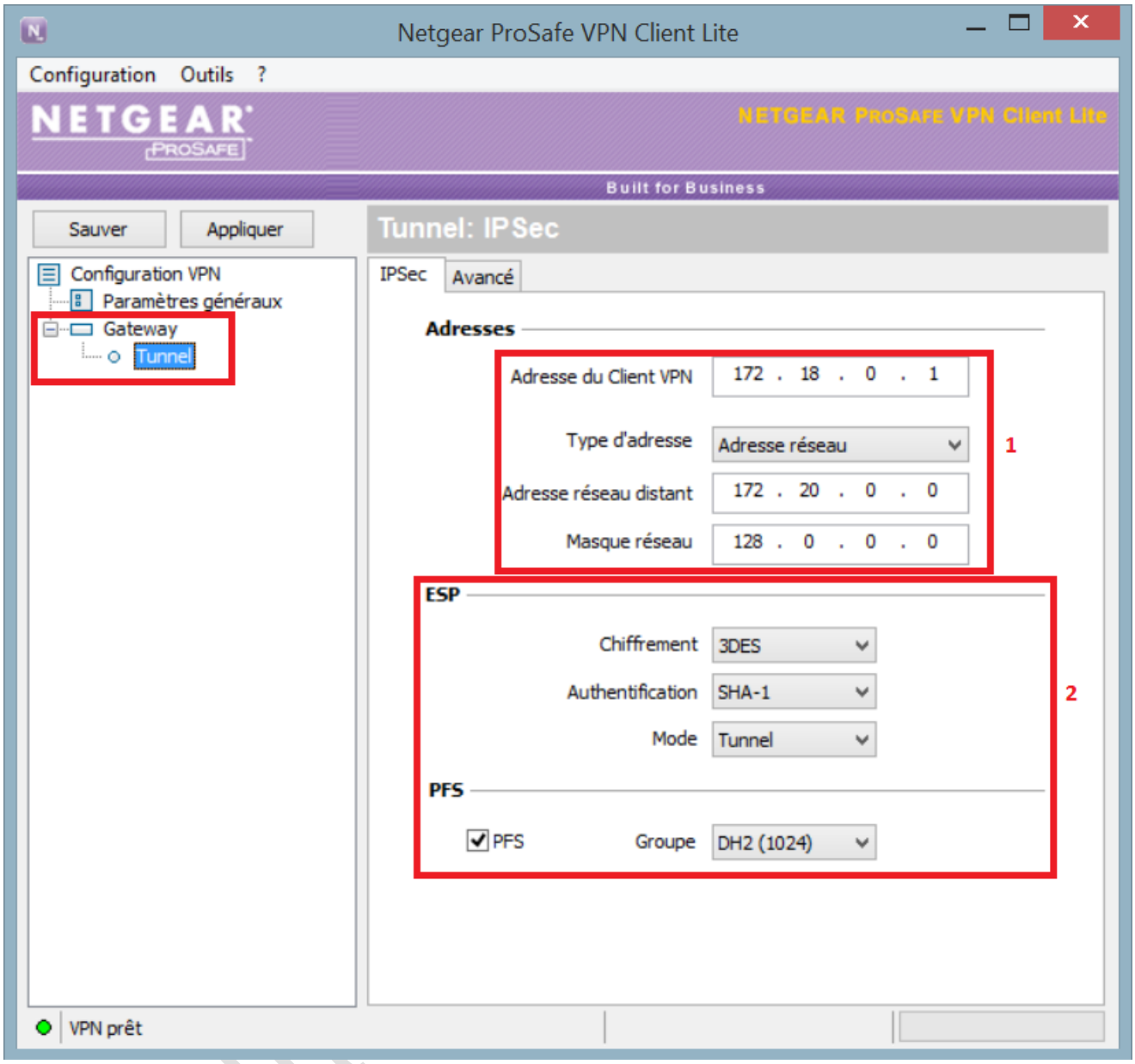
Nous considérons que le logiciel Netgear VPN Client Lite est installé comme précisé au Chapitre IV.

Du fait de la configuration des plages IP très distinctes, nous ne pouvons pas utiliser de plage IP qui fonctionne. Nous devons jouer sur le masque réseau de sous-réseau en Phase 2. La configuration reste similaire au Chapitre V.





Dans ce chapitre, nous n'avons pas configuré l'authentification RADIUS dans un but de simplification.



- Etape 1 : On spécifie l'adresse IP du LAN1 qui est numériquement inférieure à celle du LAN2. Le masque de sous-réseau est pris au plus large pour couvrir les LAN1 et LAN2.
- Etape 2 : On utilise les paramètres par défaut.
- Etape 3 : On sauvegarde la configuration
- Etape 4 : On teste la connexion comme montré au Chapitre V, section D.

VIII. Annexes

A. Liens

Release Notes du clientVPN Lite Software Version 5.50.007.

Manuel utilisateur Netgear ProSAFE VPN Client version 5.5 (en anglais) – avril 2013.

(Obsolète) Guide de configuration du client VPN (en anglais).

B. Glossaire

CLI : Command Line Interface. Interpréteur de commande.

DHCP : Dynamic Host Configuration Protocol. Protocole réseau permettant d'attribuer automatiquement une adresse IP.

DMZ : Sous-réseau informatique isolé.

DNS : Domain Name System. Système de correspondance entre adresse IP et nom.

FAI : Fournisseur d'Accès à Internet ou Provider.

LAN : Local Area Network. Réseau informatique local.

MTU : Taille maximale d'un paquet réseau pouvant être transmis en une fois.

RADIUS: Protocole client/serveur permettant de centraliser les données d'authentification.

VLAN : Virtual LAN. Réseau informatique logique indépendant.

VPN : Virtual Private Network. Réseau privé de communication sécurisé.

WAN : Wide Area Network. Réseau informatique couvrant une grande zone géographique.

WEP : Wired Equivalent Privacy. Mode de cryptage de communication pour les réseaux sans fil. Ce mode de sécurité est aujourd'hui obsolète du fait de sa faible robustesse face aux attaques.

WPA : Wi-Fi Protected Access. Mode de cryptage de communication pour les réseaux sans fil. Il tend aujourd'hui à être remplacé par le WPA2 plus sécurisé.

C. Logiciels tiers

Au cours de ce document, il se peut que certains logiciels soient utilisés pour un point de vue technique ou simplement pour vérifier le fonctionnement d'un appareil. Ils sont présentés ici sommairement afin de comprendre leur utilité. Si toutefois vous désirez approfondir vos connaissances sur ces logiciels, nous vous invitons à visiter le site Internet de l'éditeur du logiciel en question.

Filezilla : Client et serveur FTP pour Windows

NetSNMP: Outils de ligne de commande pour la supervision SNMP

NetStumbler 0.4.0 : Logiciel d'analyse de réseaux sans fil

PuTTY : Client Telnet / SSH pour Windows

Solarwinds - Kiwi SysLog Server : Serveur SYSLOG pour Windows (version gratuite ou payante)

TheGreenBow : Client VPN IPSec

WinPCap : Librairie de capture de trames réseaux pour Windows

Wireshark : Logiciel d'analyse de trames réseaux

NOTES