

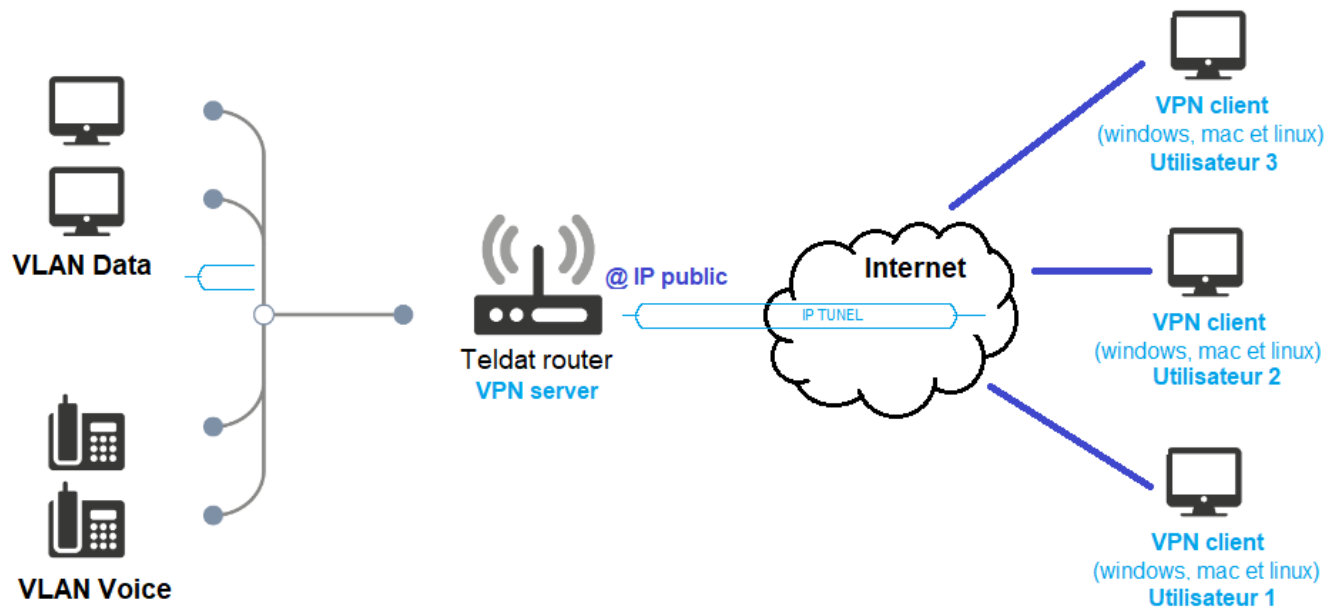
Configuration de VPN IPSEC Nomade sur Bintec

Sommaire

Présentation.....	3
Topologie :	3
Prérequis & Limitations.....	3
Configuration du serveur	3
Déclaration de l'access-list :.....	4
Configuration IPSEC :	4
Activation du proxy-arp :	5
Configuration du client VPN.....	5
Installation et configuration.....	5
Clients Windows	5

Présentation

Topologie :



Prérequis & Limitations

- Lien et routeur Codepi ou VOIP avec une **IP publique**.
- Un ordinateur sous Windows.
- L'installation du client VPN requiers des droits administrateurs sur la machine.
- Une limite max de 30 comptes VPN peuvent être déclarés dans le routeur.
- Chaque identifiant de compte VPN est composé de :
 - **Un nom d'utilisateur**.
 - **Un mot de passe**.
 - **Une clé-partagée** (dite PSK) qui est identique pour tous les comptes.

Configuration du serveur

Cette procédure nécessite d'être en P4(config) et nécessite un redémarrage du bintec. Le pool VPN doit être contenu dans le réseau de l'interface bvi0 et en dehors du pool dhcp.

Dans cet exemple, le réseau bvi0 est égale a : 172.24.6.254/24 et la plage dhcp est de 172.24.6.10 à 172.24.6.70.

Déclaration de l'access-list :

```
;
    access-list 200
        description "VPN Client"
        entry 1 default
        entry 1 permit
        entry 1 destination address 172.24.6.80 255.255.255.240
;
```

Configuration IPSEC :

```
;
    protocol ip
; -- Internet protocol user configuration --

;
    pool remotevpn 172.24.6.80 172.24.6.94
    ipsec
; -- IPSec user configuration --
    description "VPN CLIENT"
;
    enable
    assign-access-list 200
;
    template 2 dynamic esp aes128 sha256
    template 2 source-address <IP PUBLIQUE ROUTEUR>
    template 2 life duration seconds 23h50m
    template 2 df-bit clear
;
    template 1 isakmp aes128 sha256
    template 1 life duration seconds 23h50m
    template 1 ike mode aggressive
    template 1 ike natt-version rfc
```

```

template 1 config initiator
template 1 ike method xauth-init-preshared
template 1 ike group two
template 1 keepalive dpd
;

map-template 200 2
key preshared hostname VPN plain <PSK SECURISE>
advanced purge-timeout 30s
advanced pkt-dest-isakmp-dest
advanced dpd no always-send
;

xauth-user test pool remotevpn
xauth-user test password plain <MDP USER>
xauth-user test dns-server 8.8.8.8 8.8.4.4

```

Activation du proxy-arp :

```

network bvi0
; -- Bridge Virtual Interface configuration --
;
ip proxy-arp enable
exit

```

On sauvegarde le routeur avec la commande « save » puis on redémarre le routeur :

Configuration du client VPN

Installation et configuration

Clients Windows

1. Télécharger le client VPN sur <https://www.shrew.net/download/vpn>
2. Choisir la dernière version en date
Ici la version **2.2.2**

Firefox browser window showing the Shrew Soft VPN Client download page. The address bar shows <https://www.shrew.net/download/vpn>.

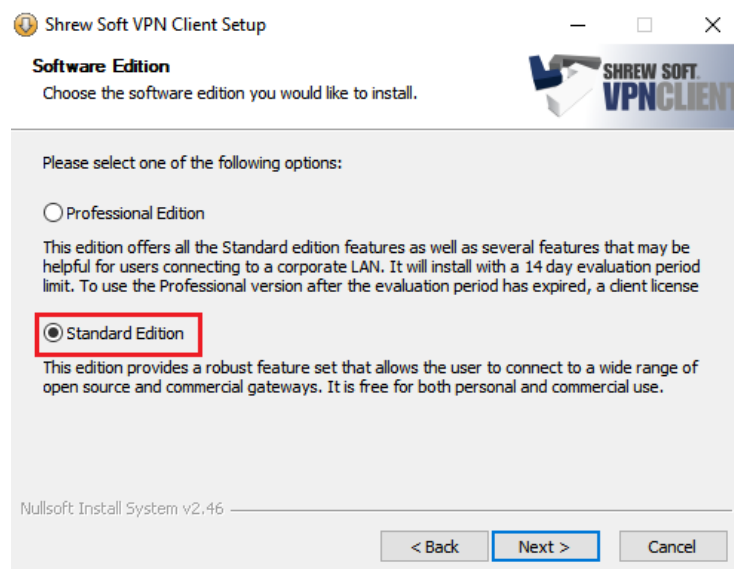
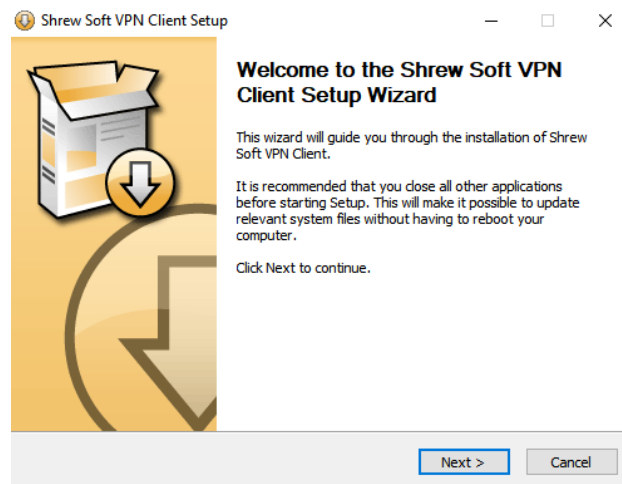
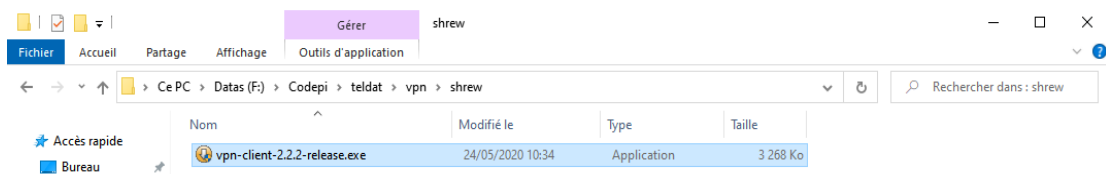
Downloads

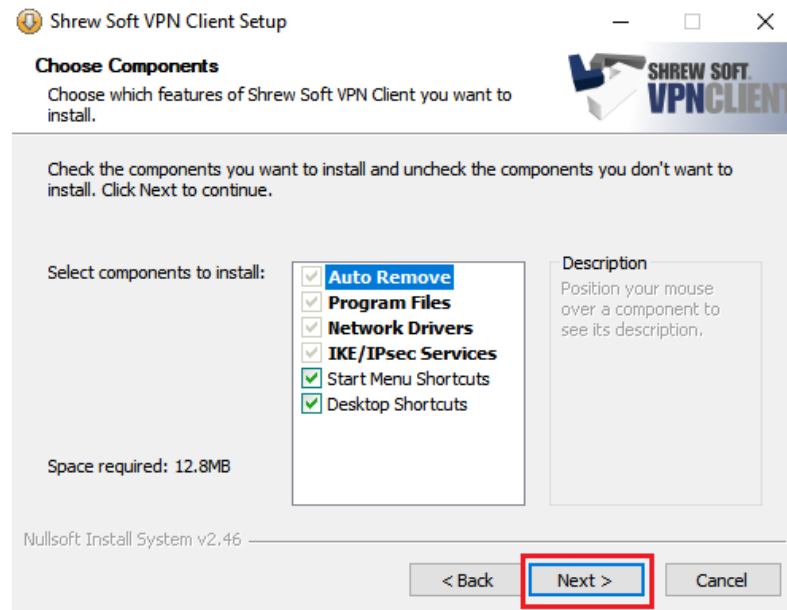
STABLE RELEASE

Date	Build	OS Support	Download	Changelog
Jul 01 2013	2.2.2-release	Windows 2K/XP/Vista/7/8	- Installer	client
Jun 05 2013	2.2.1-release	Windows 2K/XP/Vista/7/8	- Installer	client like

3. Installation du logiciel

Dans le répertoire où se trouve le programme, exécuter celui-ci de la manière suivante



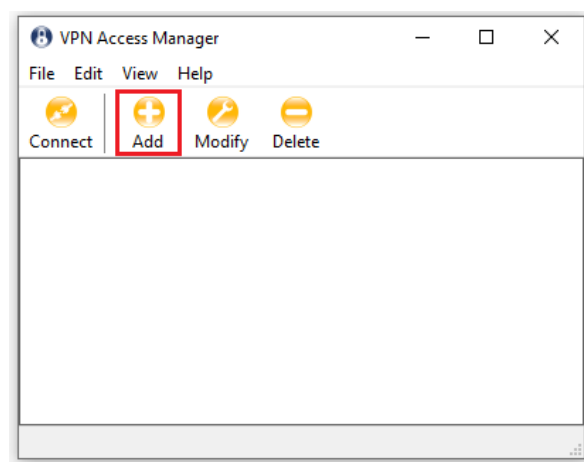


Une fois installée, icône sur le bureau sera représentée comme ceci :

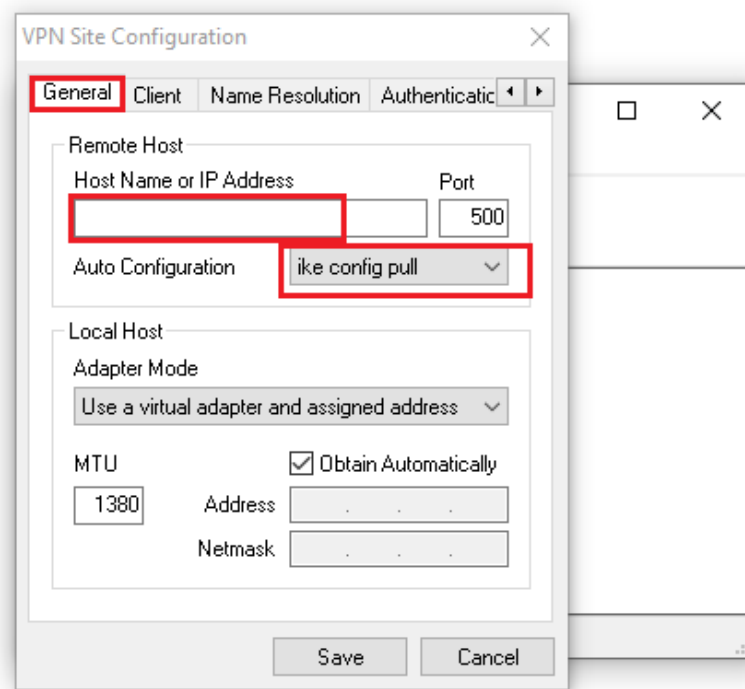


4. Création d'une configuration

Pour créer une nouvelle configuration, cliquer sur l'icône + (Add).

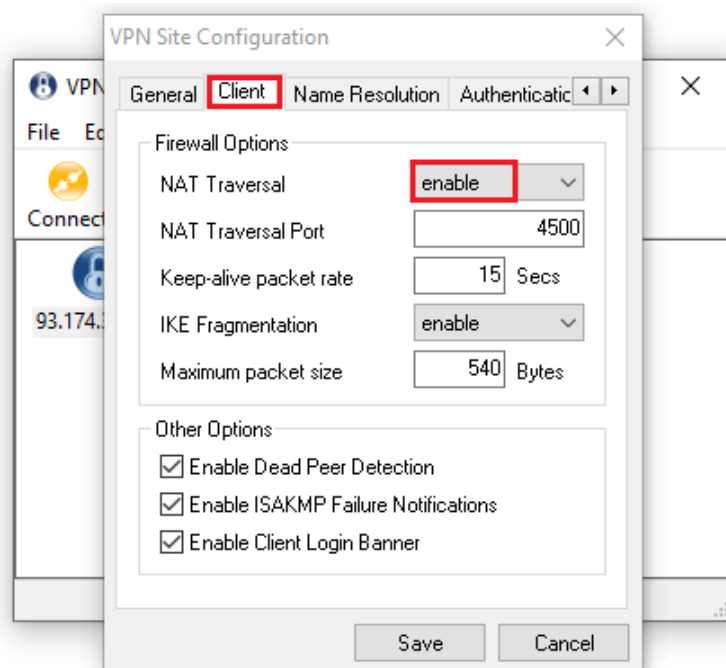


Configurez l'onglet General comme suit :

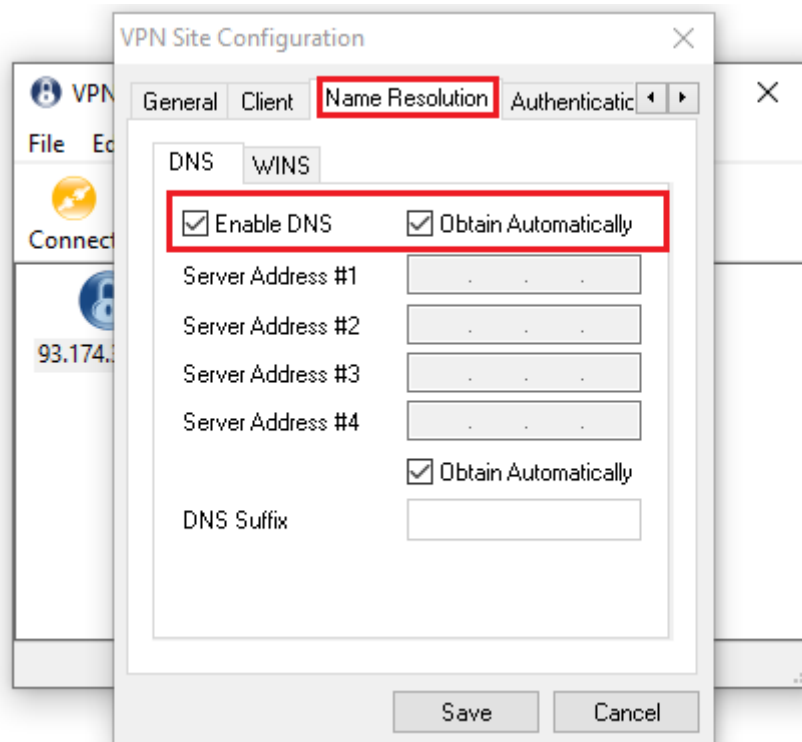


- Hostname or IP: **l'IP publique de votre routeur**
- Auto Configuration - **ike config pull**
- Adapter Mode - **Use an existing adapter and current address**
- Selectionner l'option '**Obtain Automatically**'.

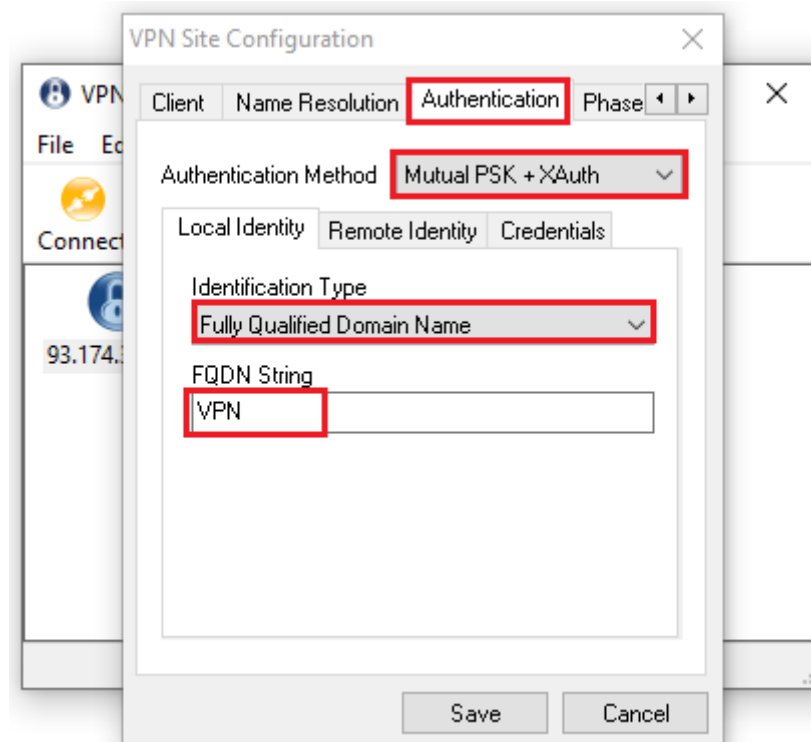
Vérifiez que l'onglet Client ressemble a celui-ci :



Idem pour l'onglet "Name Resolution" :

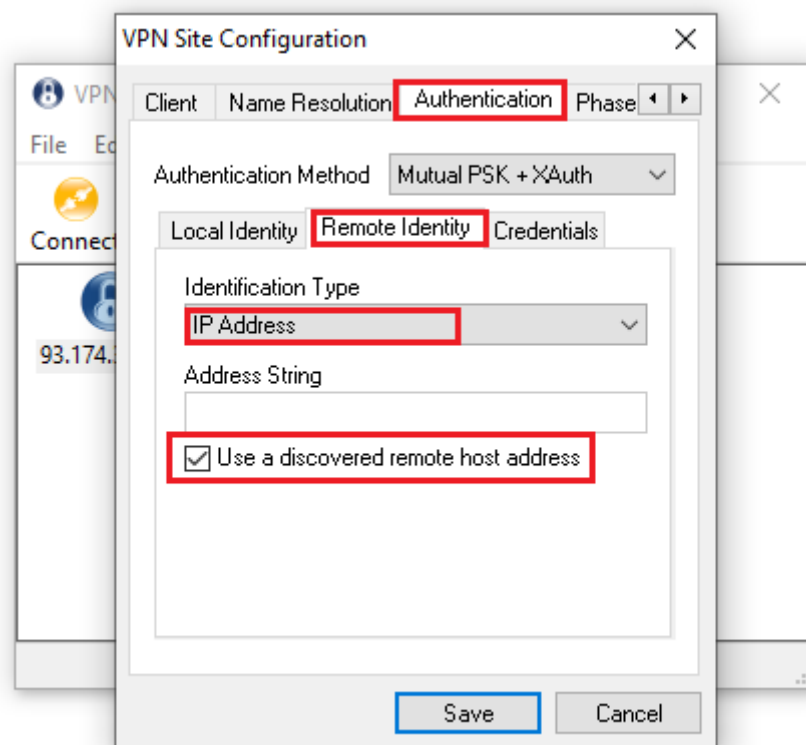


Configurez l'onglet Authentication:

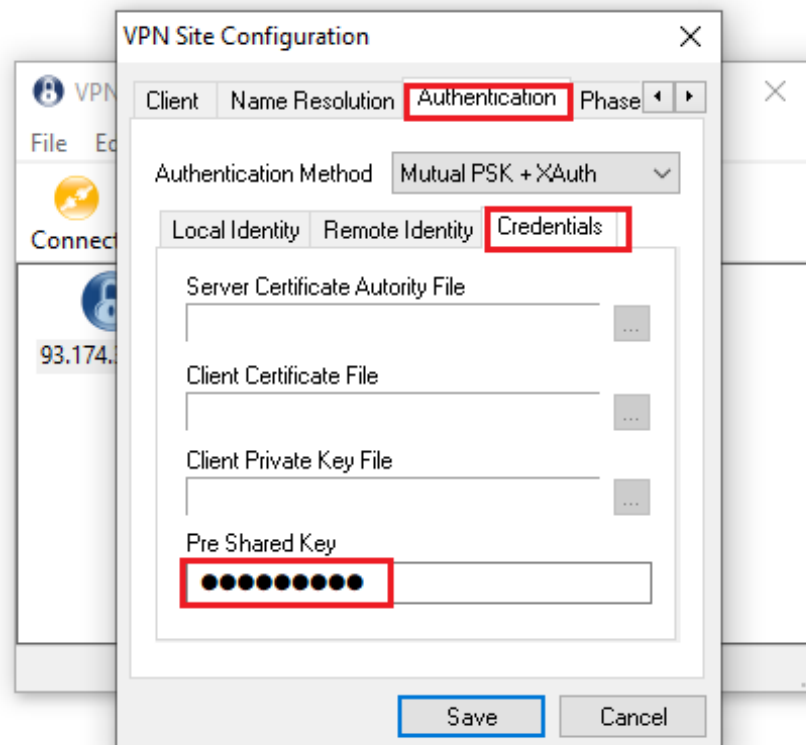


- a. *Authentication Method* : **Mutual PSK + XAuth**
- b. *Identification Type* : **Fully Qualified Domain Name**
- c. *FQDN String* : **VPN**

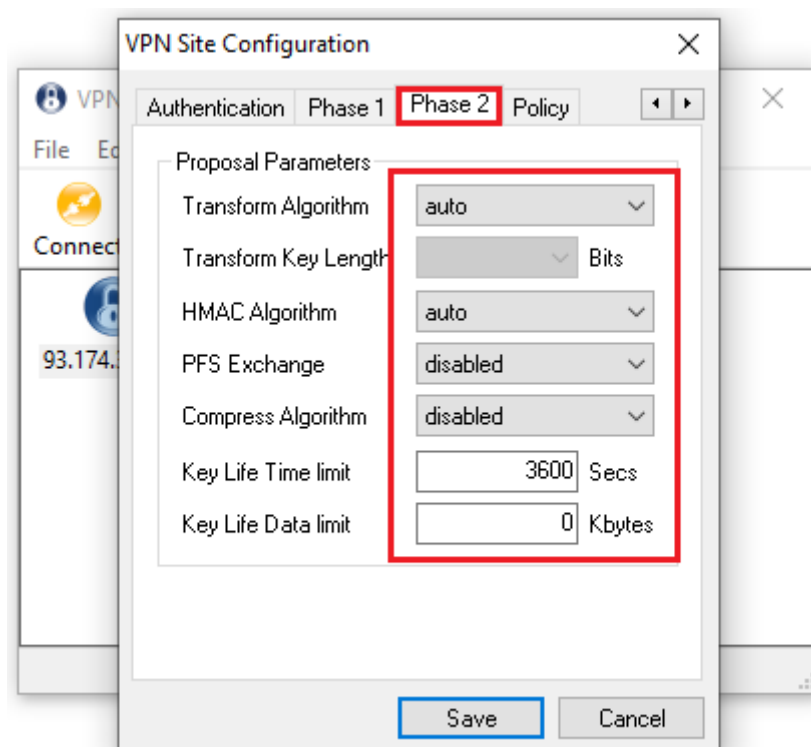
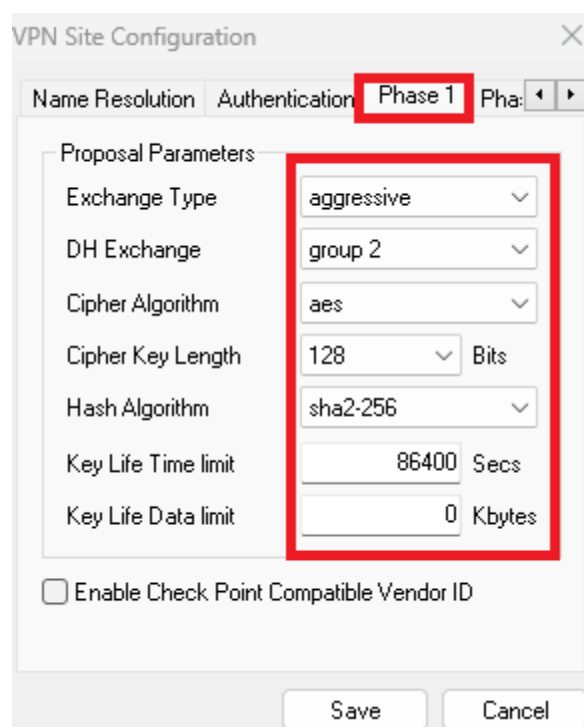
Vérifiez que le sous-onglet Remote Identity est configuré comme suit :



Le sous-onglet Credentials doit contenir la **Clé Partagée** que nous vous avons fait parvenir :

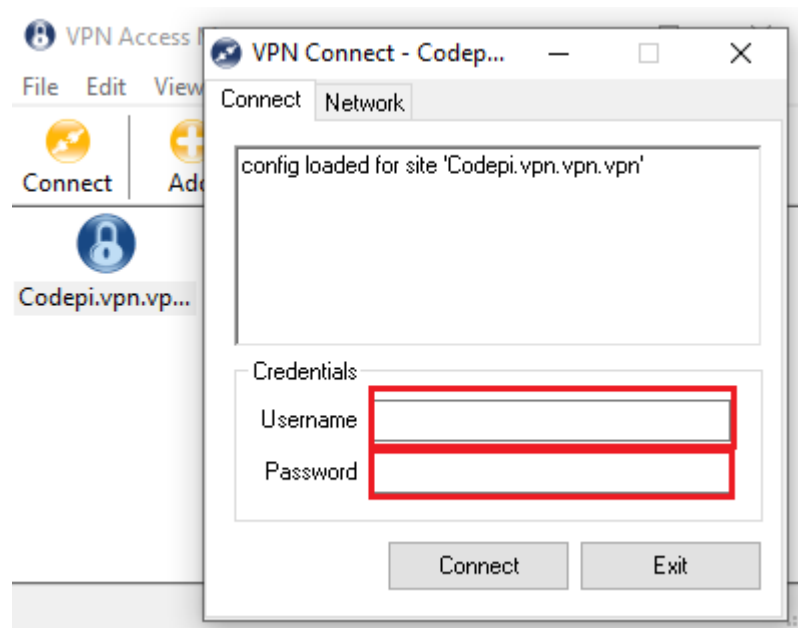


Vérifiez en dernier que les phases 1 & 2 correspondent aux captures d'écran ci-dessous, puis sauvez en cliquant sur le bouton Save



5. Lancement de la connexion

Pour lancer la connexion, double-cliquez sur l'icône représentant un cadena bleu :



Une fenêtre s'offre à vous vous demandant de rentrer **votre nom d'utilisateur et le mot de passe** (voir ci-dessus), validez en cliquant sur le bouton Connect.