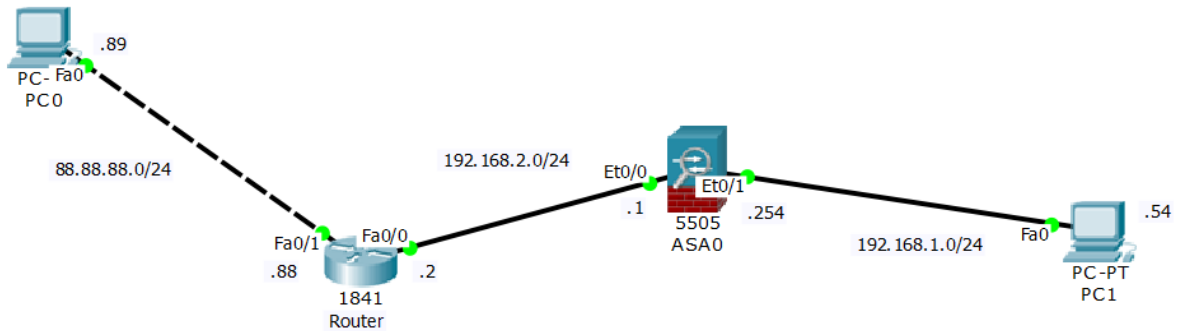


PROJET VPN-IPSec nomade ASA5505

La situation professionnelle repose sur la mise en place d'un VPN nomade sur un Cisco asa5505.

Afin de réaliser cette situation, deux PC ainsi qu'un routeur Cisco 1841 et un pare-feu Cisco asas5505 fonctionnels sont utilisés. Nous avons aussi les logiciels Cisco ASDM et Cisco VPN-Client afin de mettre en place et d'utiliser le VPN nomade.

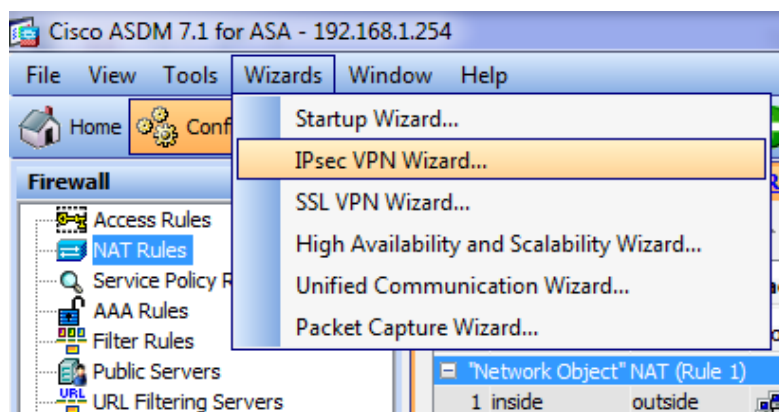


Le but du projet est de se connecter à partir de la machine 88.88.88.89 au réseau 192.168.1.0 via un tunnel VPN IPSec configuré sur le pare-feu ASA5505.

1) Configuration du tunnel VPN IPSec via ASDM

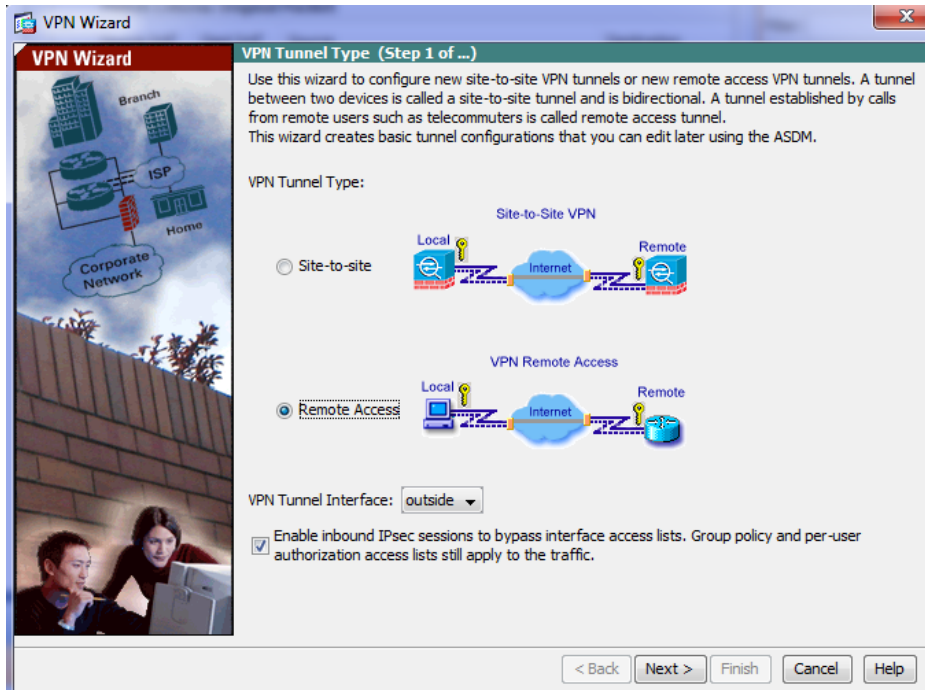
Dans ce tuto, on sous-entend que ASDM est déjà fonctionnel pour administrer le ASA5505(voir PROJET PARE-FEU ASA5505)

Commençons maintenant la configuration du Tunnel Vpn Ipsec. Accédez à Wizard > Ipsec VPN Wizard...

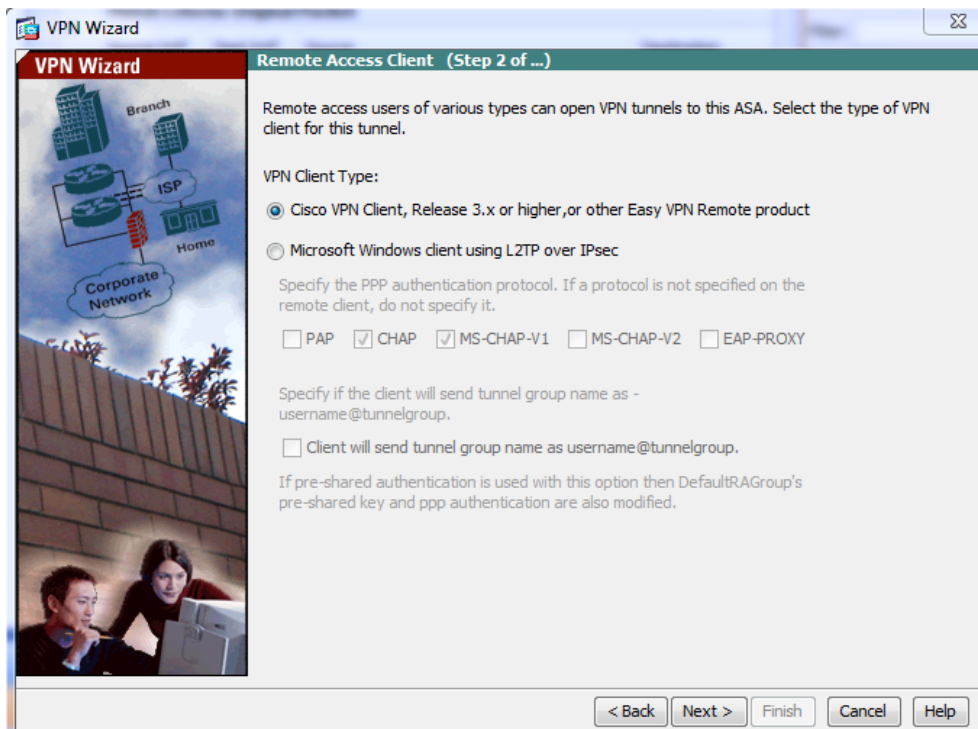


On accède alors à cette fenêtre on nous demande le type de VPN Souhaité.

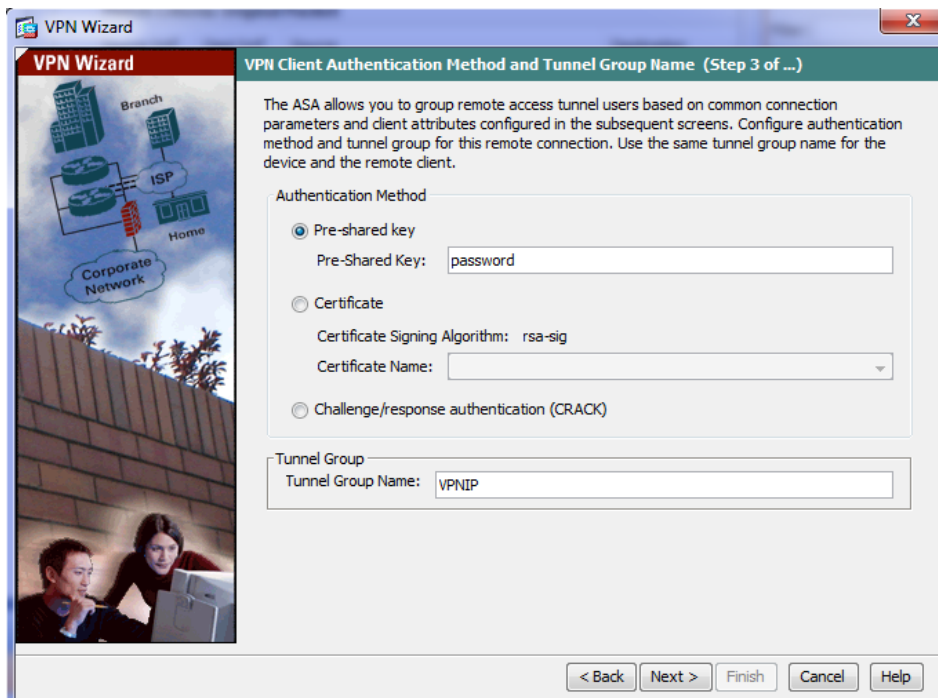
Site to Site est une configuration VPN destinée à sécuriser l'échange entre deux sites et deux réseaux entier, tandis que Remote Access est destinée aux travailleurs à distance qui souhaitent accéder, sécuriser, modifier le réseau d'un seul site.



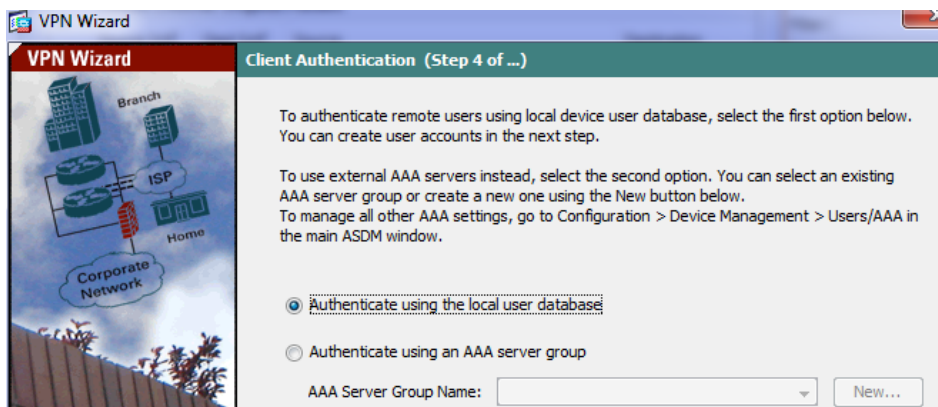
Nous utiliserons le Client VPN Cisco



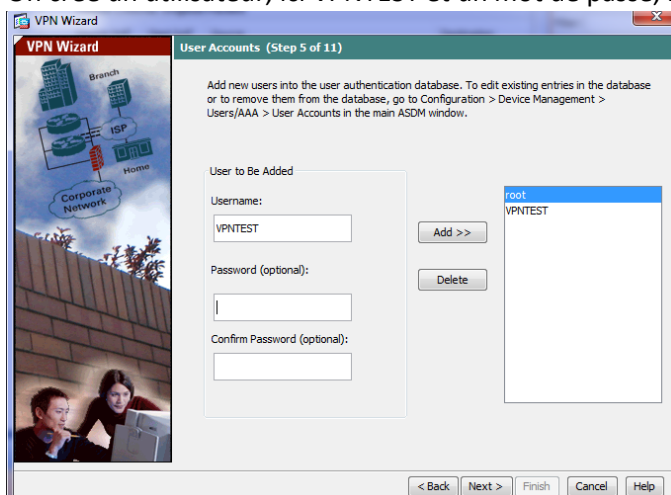
Définition du mot de passe et du nom du tunnel pour établir la connexion.



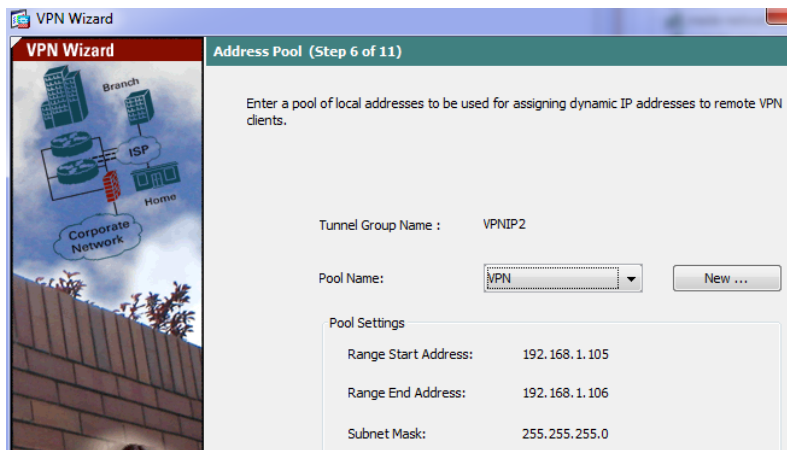
Utilisation du compte local, l'étape suivante en permet la création si elle n'a pas encore été faite.



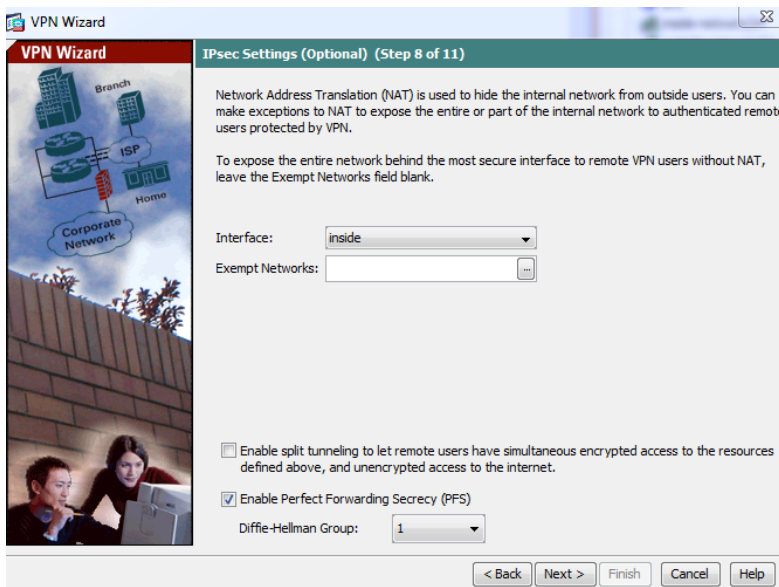
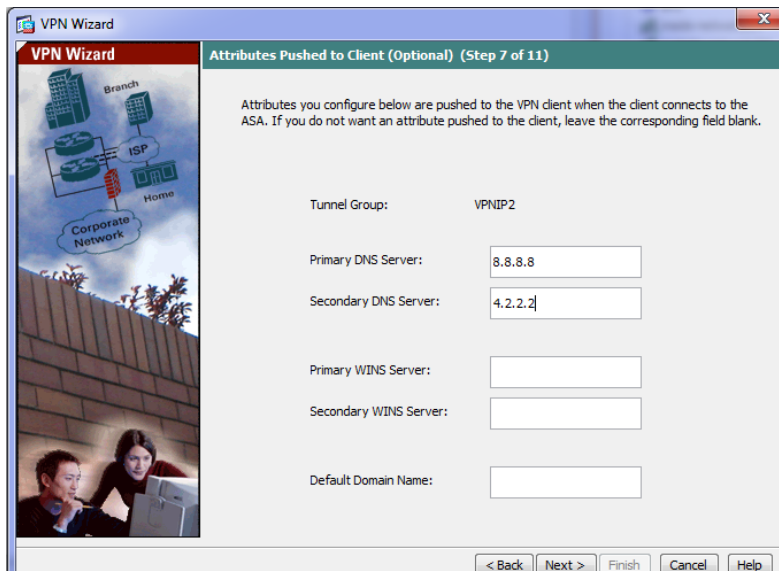
On crée un utilisateur, ici VPNTTEST et un mot de passe, ici password.



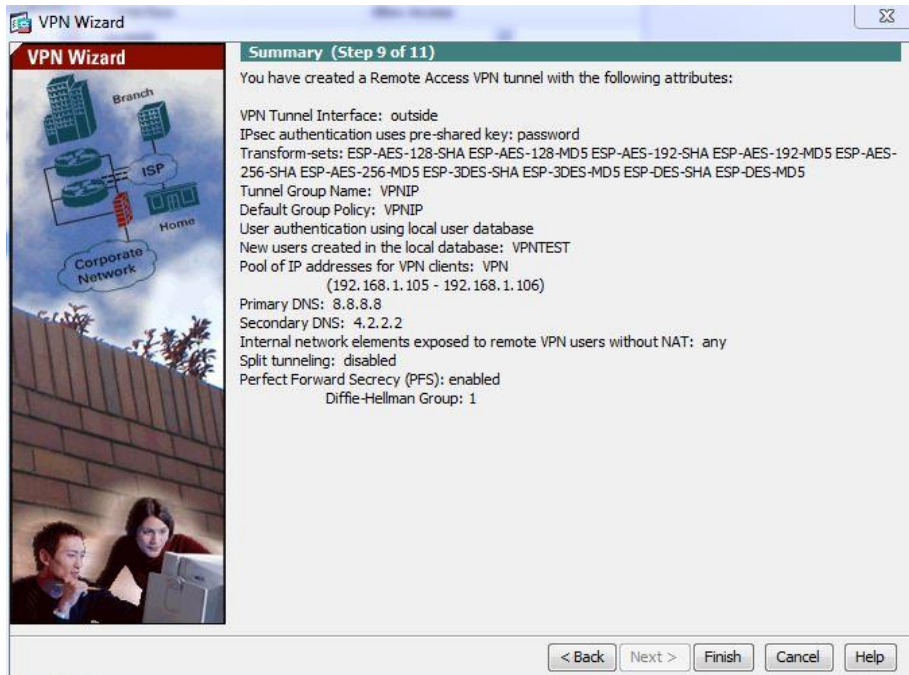
Définition d'un POOL d'adresses pour les ou la connexions



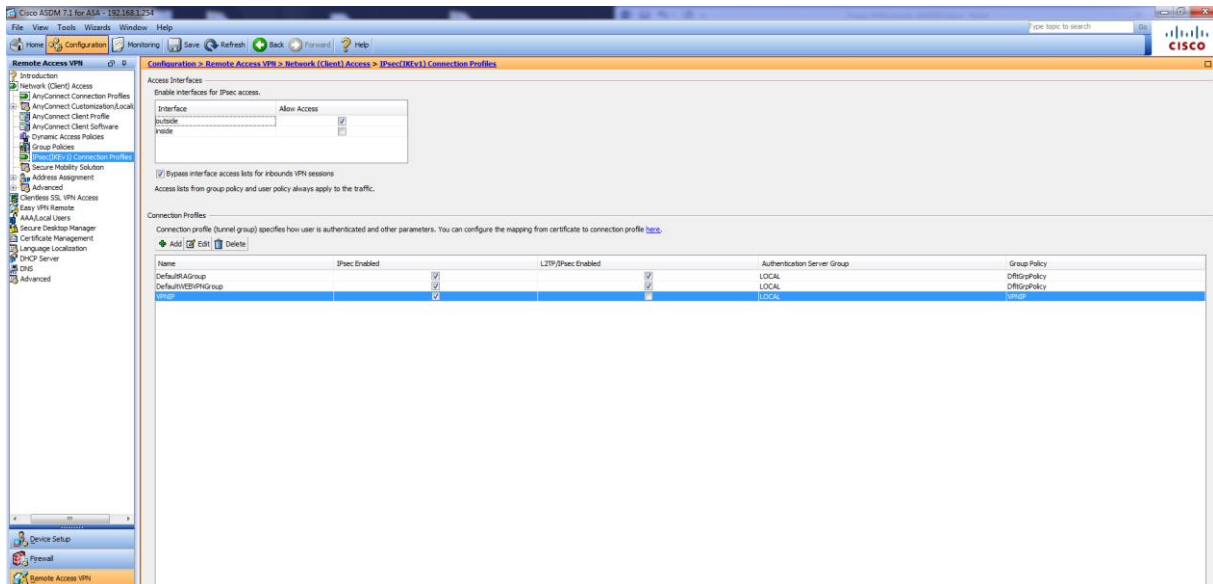
DNS



Enfin une fenêtre récapitulative de la configuration va apparaître

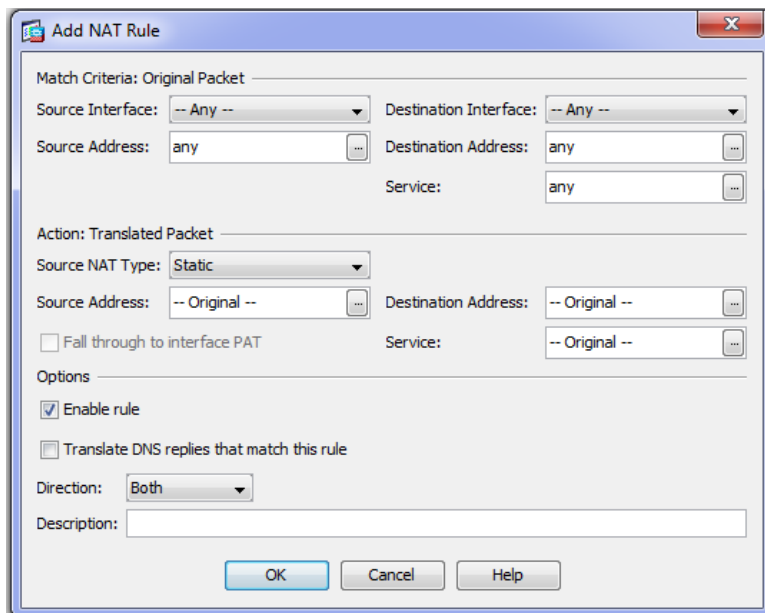
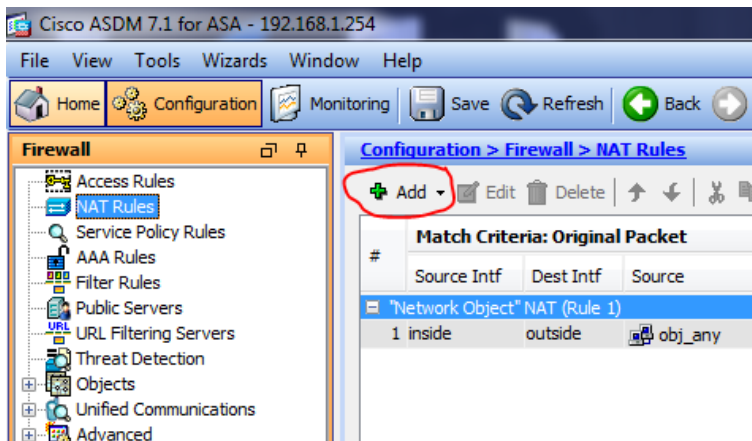


On peut voir que notre profile VPN a été créé

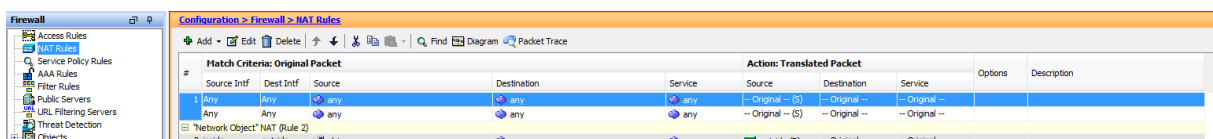


Une dernière étape est nécessaire pour faire fonctionner le tunnel VPN IPSec sur le pare-feu asa5505 :

Crée la règle de NAT suivante :



Voici la règle créée :

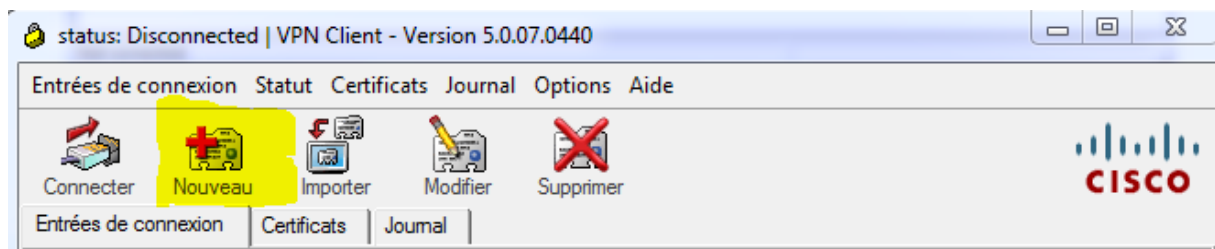


2) CISCO VPN client

Remarque : Sous Windows 10 l'installation est plus particulière et nécessite quelques manipulations.

Suivre le Tutoriel : <https://www.dominicdesbiens.com/articles/comment-installer-et-faire-fonctionner-le-client-cisco-vpn-5-x-avec-windows-10.html>

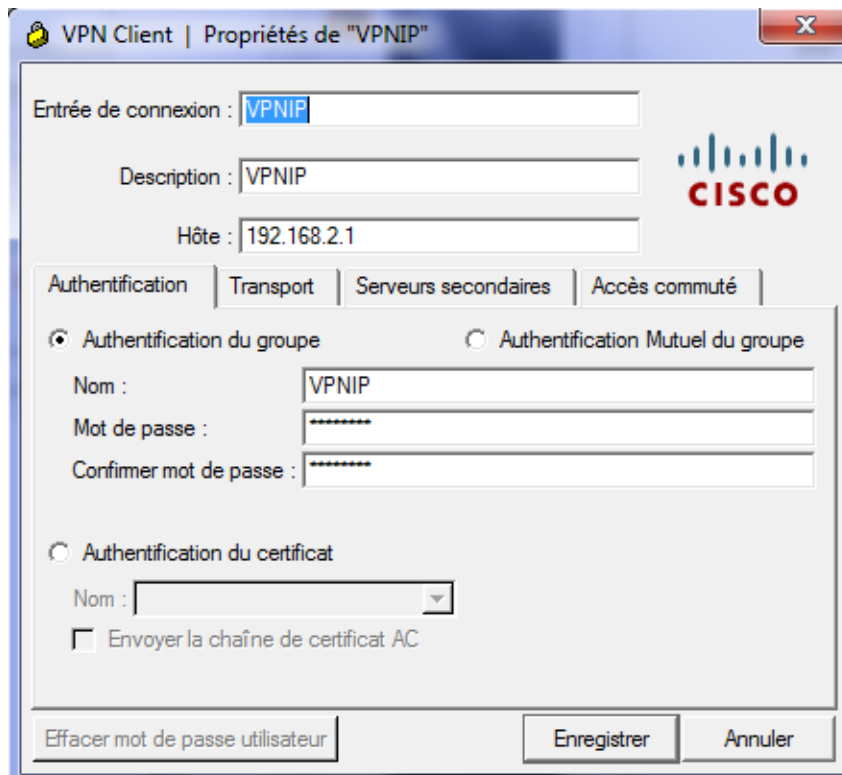
Sur CISCO VPN client, sélectionner nouveau :



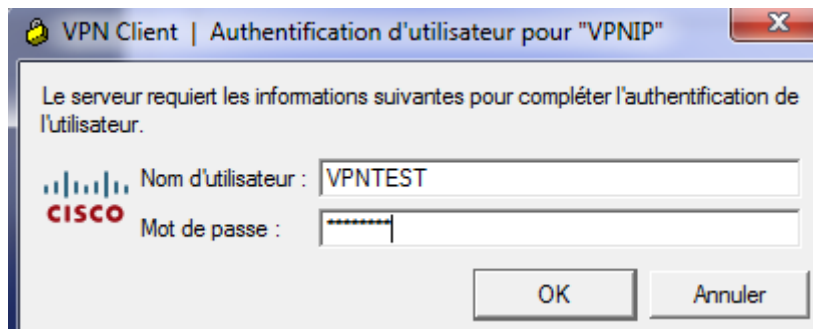
Comme vous pouvez le voir il faut entrer les informations précédemment configurées sur le ASA5505.

Hôte : IP de l'interface outside de l'ASA5505.

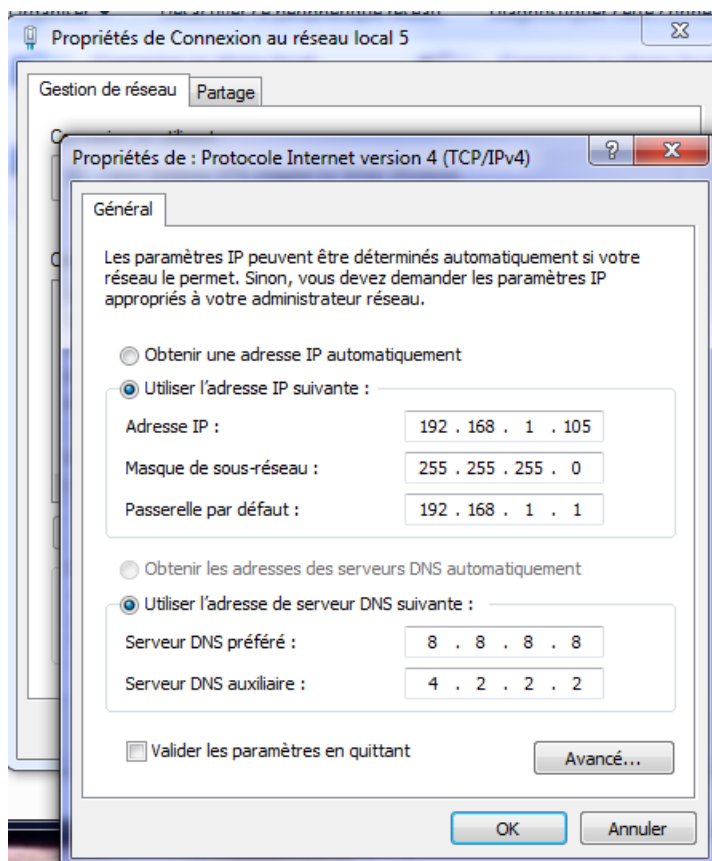
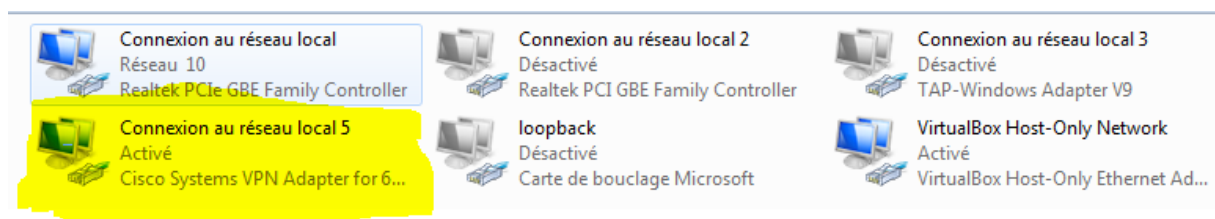
Nom : « tunnel-group-name » configuré précédemment.



Ensuite il suffit de se connecter au VPN précédemment ajouté :

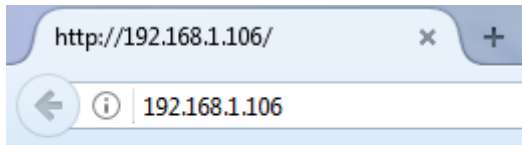


Une fois connecté au VPN, une nouvelle carte réseau est activée et une adresse du VPN pool lui a été attribuée :



3) TEST du tunnel VPN

Afin de tester que la connexion VPN est bien établie, on test de joindre un serveur web en 192.168.1.106 et on test de ping la machine en 192.186.1.54 :



bonjour sivr 192.168.1.106

```
C:\Users\etudiantsio>ping 192.168.1.54

Envoi d'une requête 'Ping' 192.168.1.54 avec 32 octets de données :
Réponse de 192.168.1.54 : octets=32 temps=2 ms TTL=128
Réponse de 192.168.1.54 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.1.54 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.1.54 : octets=32 temps=1 ms TTL=128

Statistiques Ping pour 192.168.1.54:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms

C:\Users\etudiantsio>
```

On voit que la communication s'effectue bien.