ECOLE NATIONALE DES SCIENCES APPLIQUEES

IPSEC VPN TUNNELING

Rapport/Tutorial en Sécurité Réseaux

Zerhouni Adam

1/21/2013

Rapport détaillé sur la mise en place d'un tunnel VPN IPSEC site à site avec configuration sous GNS3 et TEST

Sommaire :

I. Introduction :

Les tunnels VPN sont utilisés pour permettre la transmission sécurisée de données, voix et vidéo entre deux sites (bureaux ou succursales). Le tunnel VPN est créé sur le réseau public Internet et il est crypté à l'aide d'un certain nombre d'algorithmes de chiffrement avancés pour assurer la confidentialité des données transmises entre les deux sites.

ISAKMP (Internet Security Association and Key Management Protocol) et IPSec sont essentiels pour la construction et le chiffrement du tunnel VPN. ISAKMP, aussi appelé IKE (Internet Key Exchange) est le protocole de négociation qui permet à deux hôtes se mettre d'accord sur la façon de construire une association de sécurité IPsec. Négociation ISAKMP se compose de deux phases: la phase 1 et la phase 2.

Phase 1 crée le premier tunnel, qui protège les messages de négociation ISAKMP plus tard. Phase 2 crée le tunnel qui protège les données. IPSec entre alors en jeu pour crypter les données en utilisant des algorithmes de chiffrement et fournit l'authentification, le chiffrement et l'anti-rejeu services.

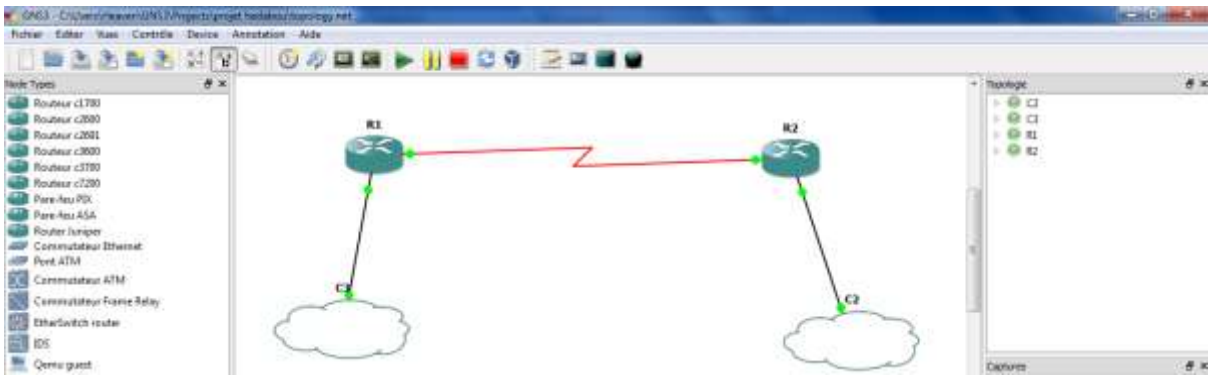
II. Exigences : IPSec VPN

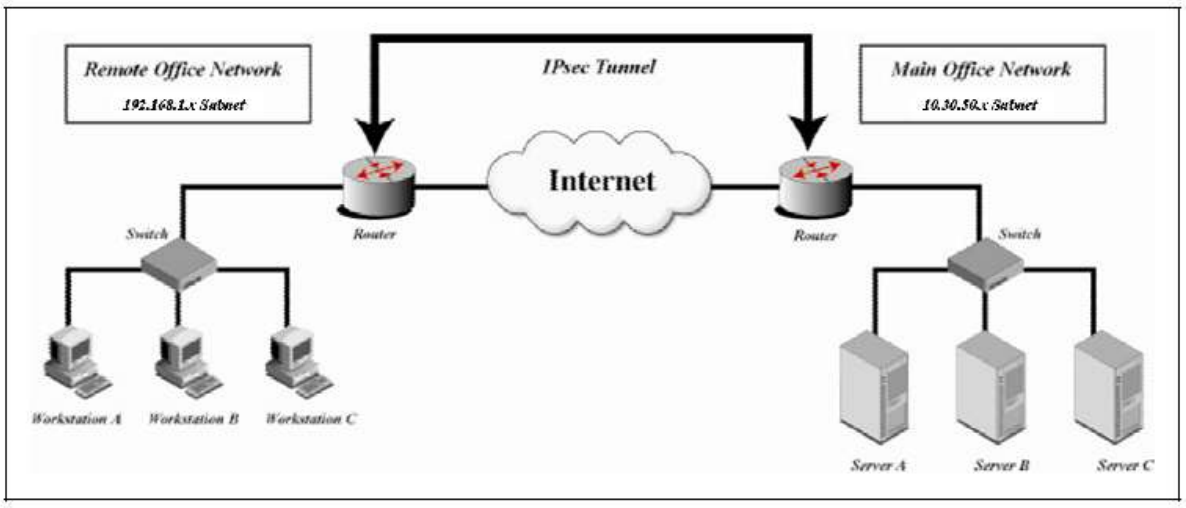
Pour parfaire ce projet, il faut diviser le travail en deux étapes qui sont nécessaires pour obtenir le VPN IPSec Tunnel.

Ces étapes sont les suivantes:

(1) Configuration ISAKMP (phase ISAKMP 1)
(2) Configurez IPSec (ISAKMP phase 2, LCA, Crypto MAP)

Notre exemple de configuration se situe entre deux branches d'une petite entreprise, Main office et Remote Office. Les deux routeurs de branche sont connecter à Internet et de disposent d'une adresse IP statique attribuée par son fournisseur d'accès, comme indiqué sur le schéma:





Pour le Remote Office, j'utilise dans mon exemple l'adresse réseau 192.168.10.0/24 et pour le main Office l'adresse réseau 10.30.50.0/24.

Pour l'interface série du routeur Remote Office l'adresse ip est : 1.1.1.1/24 (public)

Pour l'interface série du routeur Main Office l'adresse ip est : 1.1.1.2/24 (public)

1. Configuration ISAKMP (IKE) - (Phase ISAKMP 1)

IKE n'existe que pour établir une SA (Security Association) pour IPsec. Avant de pouvoir le faire, IKE doit négocier cette SA (une SA ISAKMP) les relations avec les pairs (le/les routeurs de/des site(s) distant.)

Pour commencer, nous allons commencer à travailler sur le site Remote office / routeur (R1).

La première étape consiste à configurer la Politique de phase ISAKMP :

R1(config)# **crypto isakmp policy 1**
R1(config-isakmp)# **encr 3des**
R1(config-isakmp)# **hash Sha**
R1(config-isakmp)# **authentication pre-share**
R1(config-isakmp)# **group 2**
R1(config-isakmp)# **lifetime 86400**

Une description des commandes ci-dessus :

- 3DES – Est un procédé de cryptage utilisé pour la phase 1.
- Sha – Est l'algorithme de hachage
- Pre-share - Utilisation d'une Clé pré-partagée comme méthode d'authentification
- Groupe 2 – L'algorithme d'échange de clef Diffie-Hellman est utiliser
- 86400 – Est la durée de vie de la clé de session. Elle est exprimée en kilo-octets (après-x quantité de trafic, modifier la clé) ou en secondes. La valeur définie est la valeur par défaut.

Il est à noter que La politique ISAKMP de phase 1 est définie de manière globale. Cela signifie que si nous avons cinq différents sites distants (ce qui est souvent le cas vu que les entreprises ont plusieurs filiales généralement), il faut configurer cinq différentes politique ISAKMP de phase 1 (un pour chaque routeur distant). Dans ce cas, notre routeur tentera de négocier un tunnel VPN avec chaque site, et il enverra les cinq politiques puis utilisera la première correspondance reconnu par les deux extrémités.

Maintenant, il faut définir une clé pré partagée pour l'authentification avec les pairs (routeur R2) à l'aide de la commande suivante:

R1(config)# **crypto isakmp key zerhouni address 1.1.1.2**

Chaque fois que R1 tentera d'établir un tunnel VPN avec R2 (1.1.1.2), cette clé pré partagée (zerhouni) sera utilisée.

2. Configuration IPSEC :

Pour configurer le protocole IPSec on a besoin de configurer les éléments suivants dans l'ordre:

- Créer une ACL étendue
- Créer l'IPSec Transform
- Créer la Crypto Map
- Appliquer crypto map à l'interface publique

L' ACL etendu que l'on crée permettra de définir le trafic qui passera à travers le Tunel VPN. Dans cet exemple, le trafic d'un réseau à l'autre, 192.168.10.0/24 à 10.30.50.0/24.

R1(config)# **ip access-list extended VPN-TRAFFIC**

R1(config-ext-nacl)# **permit ip 192.168.10.0 0.0.0.255 10.30.50.0 0.0.0.255**

L'étape suivante consiste à créer la transformation définie utilisé pour protéger nos données (IPSEC). Je l'ai nommé « TS »:

R1(config)# **crypto ipsec transform-set TS esp-3des esp-md5-hmac**

- **ESP-3DES** – l'algorithme de cryptrage
- **MD5** – l'algorithme de hachage

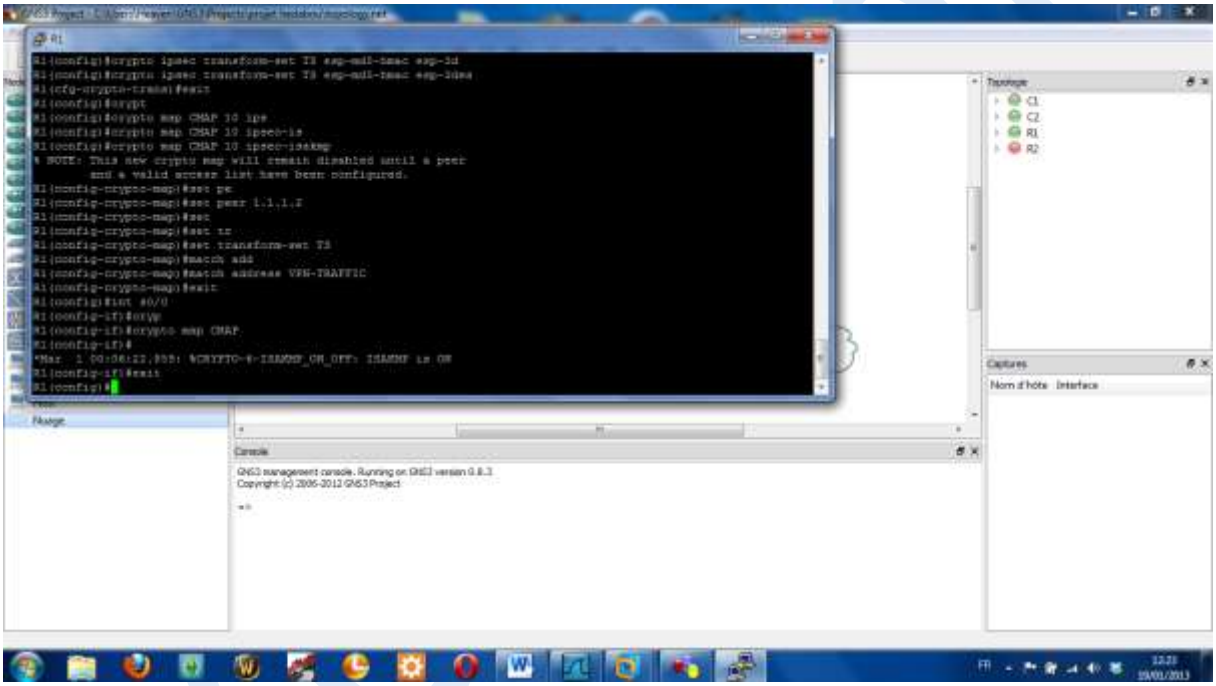
La Crypto map est la dernière étape de l'installation et établie le lien entre ISAKMP définie précédemment et la configuration IPSec :

R1(config)# **crypto map CMAP 10 ipsec-isakmp**
R1(config-crypto-map)# **set peer 1.1.1.2**
R1(config-crypto-map)# **set transform-set TS**
R1(config-crypto-map)# **match address VPN-TRAFFIC**

Maintenant il suffit d'appliqué la crypto map sur l'interface de sortie de notre routeur :

R1(config)# **interface S0/0**
R1(config- if)# **crypto map CMAP**

Dès que nous appliquons crypto map sur l'interface, nous recevons un message du routeur qui confirme isakmp est: "ISAKMP est ON».



À ce stade, nous avons terminé la configuration VPN IPSec sur le premier Site.

Nous passons maintenant à l'emplacement 2 « routeur 2 » pour terminer la configuration VPN. Les paramètres pour le routeur 2 sont identiques, la seule différence étant les adresses IP par les pairs et les listes d'accès:

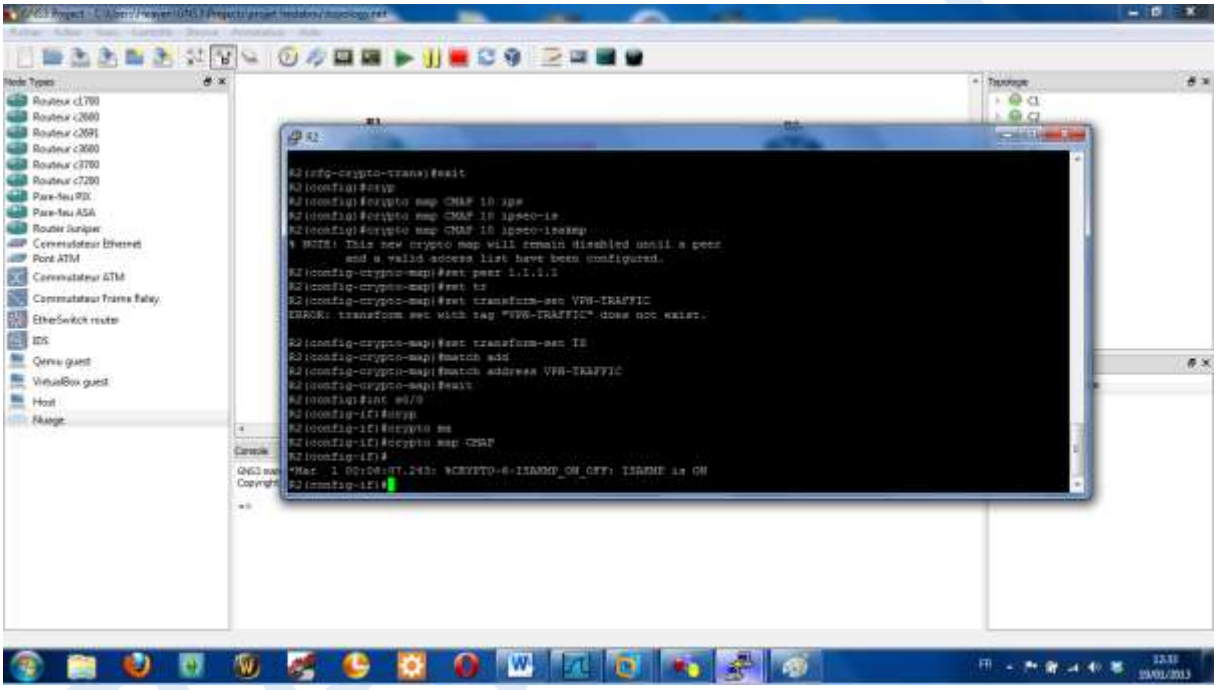
R2(config)# **crypto isakmp policy 1**
R2(config-isakmp)# **encr 3des**
R2(config-isakmp)# **hash sha**
R2(config-isakmp)# **authentication pre-share**
R2(config-isakmp)# **group 2**

R2(config-isakmp)# **lifetime 86400**

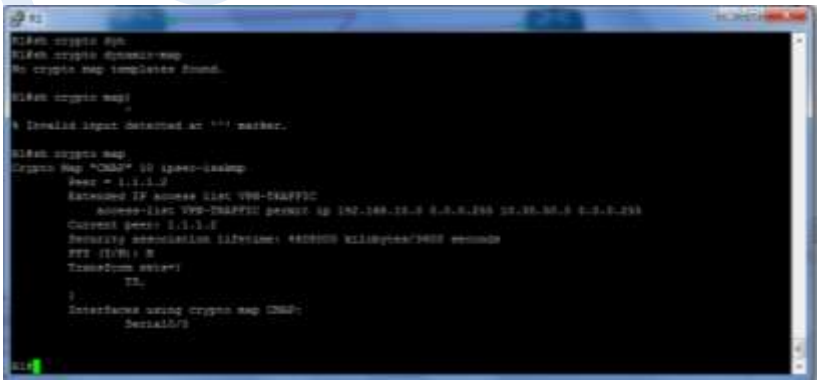
R2(config)# **crypto isakmp key zerhouni address 1.1.1.1**
R2(config)# **ip access-list extended VPN-TRAFFIC**
R2(config-ext-nacl)# **permit ip 10.30.50.0 0.0.0.255 192.168.10.0 0.0.0.255**

R2(config)# **crypto ipsec transform-set TS esp-3des esp-md5-hmac**
R2(config)# **crypto map CMAP 10 ipsec-isakmp**
R2(config-crypto-map)# **set peer 1.1.1.1**
R2(config-crypto-map)# **set transform-set TS**
R2(config-crypto-map)# **match address VPN-TRAFFIC**

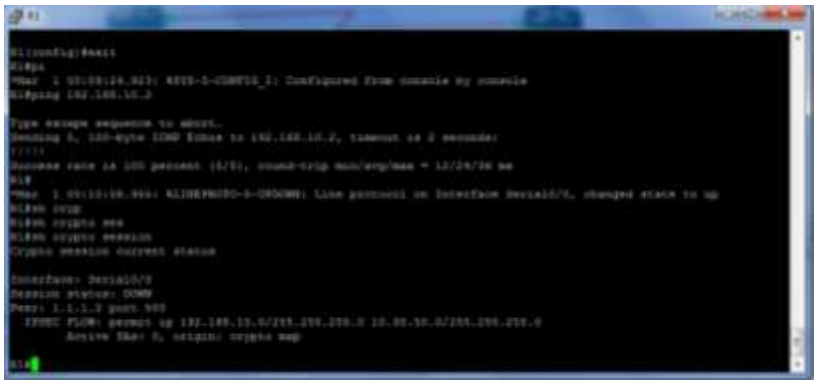
R2(config)# **interface S0/0**
R2(config- if)# **crypto map CMAP**



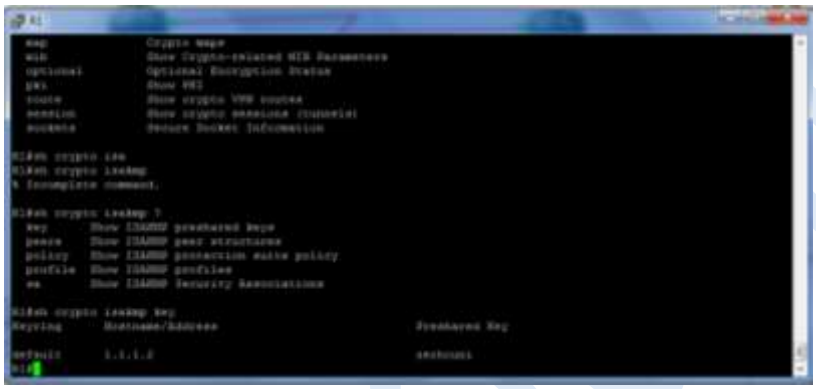
Pour les paramètres ISAKMP sous R1 voici les SHOW run :



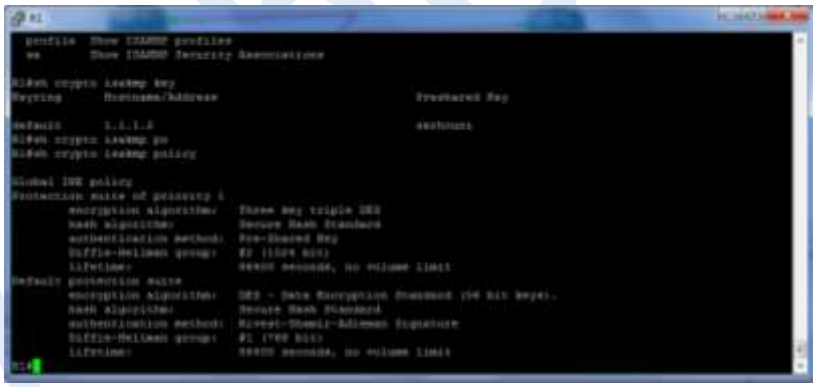
Sh Crypto map



Sh crypto session



Sh crypto isakmp key

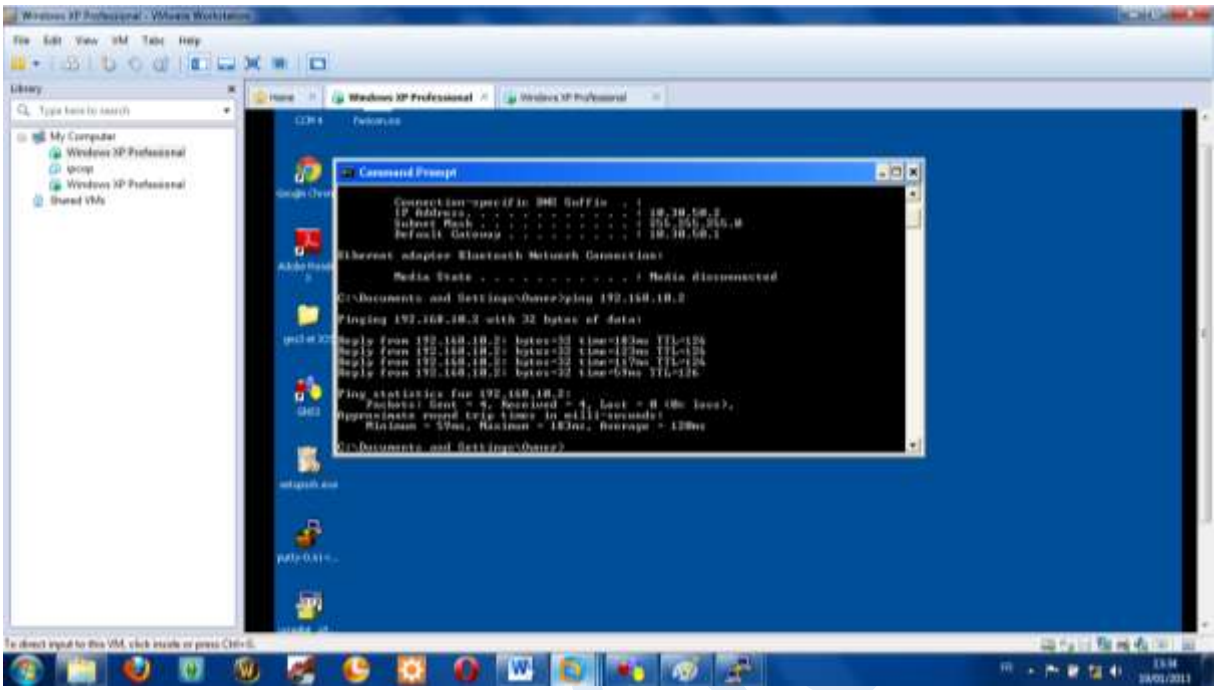


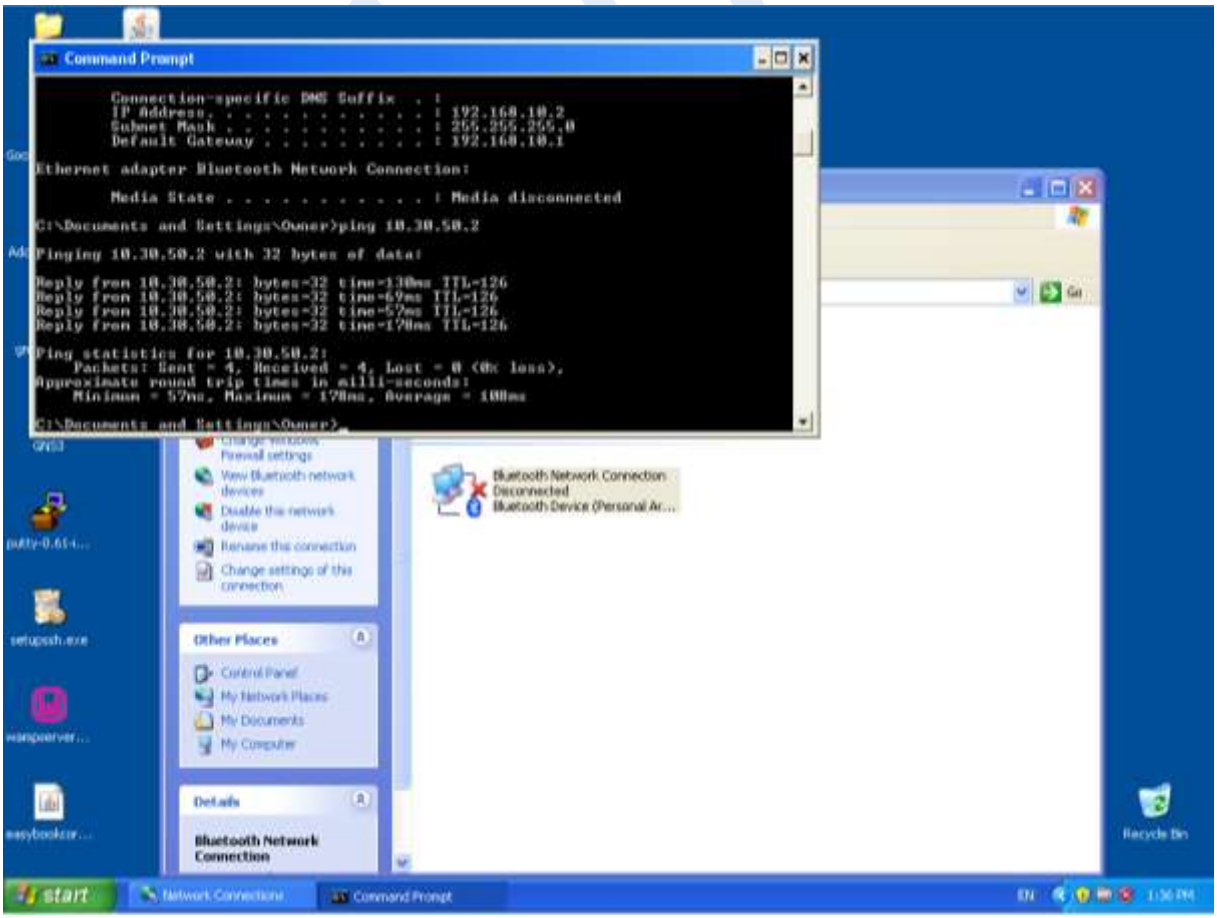
Sh crypto isakmp policy

Au niveau de R2 nous retrouvons exactement les mêmes résultats.

III. TEST DE PING et Sniffing Wireshark:

Après configuration, on peut tester d'envoyé des données entre les deux pc qui se trouvent dans 2 sites distant, on peut voir que le ping et les données passent :





MAIS SURTOUT QUE LES DONNEES PASSENT A TRAVERS LE TUNNEL VPN IPSEC PRECEDEMENT CREER ET QUE LES DONNEES QUI TRANSITENT SONT BIEN CHIFFRER :