

Document traitant de l'implémentation de règles IPSEC dans le cadre du cours de système d'exploitation dispensé par Mr Wilfart à la HELHO département technique Hesit.  
Réalisé par Driancourt Thomas alias Velour contact : kfn\_velour@hotmail.com

### **Présentation du protocole :**

IPSEC ( répondant à la norme RFC 2401 ) est un protocole de la couche 3 de la pile TCP / IP tout comme IP, il fut développé à la base pour la nouvelle version IP c'est-à-dire IPV6 mais nous n'avons pas besoin d'attendre le déploiement de ce nouveau protocole pour utiliser l'IPSEC puisqu'il a été porté pour la version actuelle d'IP c'est-à-dire IPV4.

### **Les services proposés par IPSEC :**

L'IPSEC est un protocole de sécurité, il offre différents services visant à sécuriser les communications entre deux entités ( machine, sous-réseau ). Son principal intérêt est le mode tunneling c'est à dire la création d'un tunnel chiffré à travers un réseau public ou non-sécurisé. De manière succincte, citons quelques propriétés générales des tunnels IPSEC:

- Les données transitant sont chiffrées ( confidentialité ) et protégées ( intégrité )
- Les 2 extrémités sont authentifiées
- Les adresses sources et destinations sont chiffrées, avec IPSec ( IP dans IPSec )
- Ils peuvent présenter, suivant le protocole, des qualités anti-rejeux\*
- L'intégrité des données échangées : permet d'éviter les modifications de paquet pendant le transport ( attaque dite active )

(\* un rejeux étant l'interception et le renvoi d'un paquet sans l'avoir pour autant décrypter pour bénéficier des mêmes avantages que l'expéditeur initial.)

### **Les sous protocoles :**

IPSEC se base sur d'autres protocoles notamment pour chiffrer et contrôler l'intégrité des données, le but de ce document n'étant pas de faire un cours sur le fonctionnement d'IPSEC je les citerai simplement ainsi que leurs normes pour les intéressés qui souhaitent en connaître le fonctionnement.

- IKE : Internet Key Exchange ( RFC 2409 ) comme son nom l'indique le protocole est utilisé pour les échanges de clés publiques clés privées.
- AH : Authentication Header ( RFC 2402 ) permet d'établir de façon certaine l'identité des extrémités du tunnel.
- ESP : Encapsulating Security Payload ( RFC 2406 ) est le protocole utilisé pour le chiffrement des données.

## Implémentation sur un système WINDOWS XP :

Avant d'entrer dans le vif du sujet il est important de définir La SPD ( sécurité Policy Database )

La SPD est une liste ordonnée d'entrées contenant des critères de contrôle d'accès, similaires à des règles de pare-feux. La SPD est statique par défaut car l'ordre des enregistrements qu'elle contient est très important; en effet, plusieurs règles peuvent s'appliquer à un même paquet en théorie mais seule la première sera réellement effective, d'où l'importance de l'ordre. Il est pourtant possible d'avoir des SPDs dynamiques, mais cela requiert un réordonnement à la volée des entrées. Il y a 2 SPDs par interface, une pour le trafic entrant, l'autre pour le trafic sortant. Chaque entrée de ces SPDs précise un traitement à appliquer au paquet pour lequel la règle s'applique (quand le critère de sélection ou sélecteur est vrai); ces traitements sont DROP (jette), BYPASS (laisse passer) ou IPSec PROCESS (traitement avec IPSec). Ce dernier cas précise en outre les paramètres propres à IPSec tel que l'algorithme, etc...

Tout comme les règles d'un pare-feu, les sélecteurs sont les suivants :

- Adresses IP de source et de destination, masques, intervalles...
- Ports de source et de destination
- Protocole supérieur
- Utilisateur ou identifiant de système (ou certificats X.509 réutilisés par les Sas...)

- Premier cas :

Sécurisation des sessions Telnet entre ma machine et un serveur Local ayant comme adresse 192.168.0.1/24 EN MODE TRANSPORT ( c'est à dire sans tunnel )

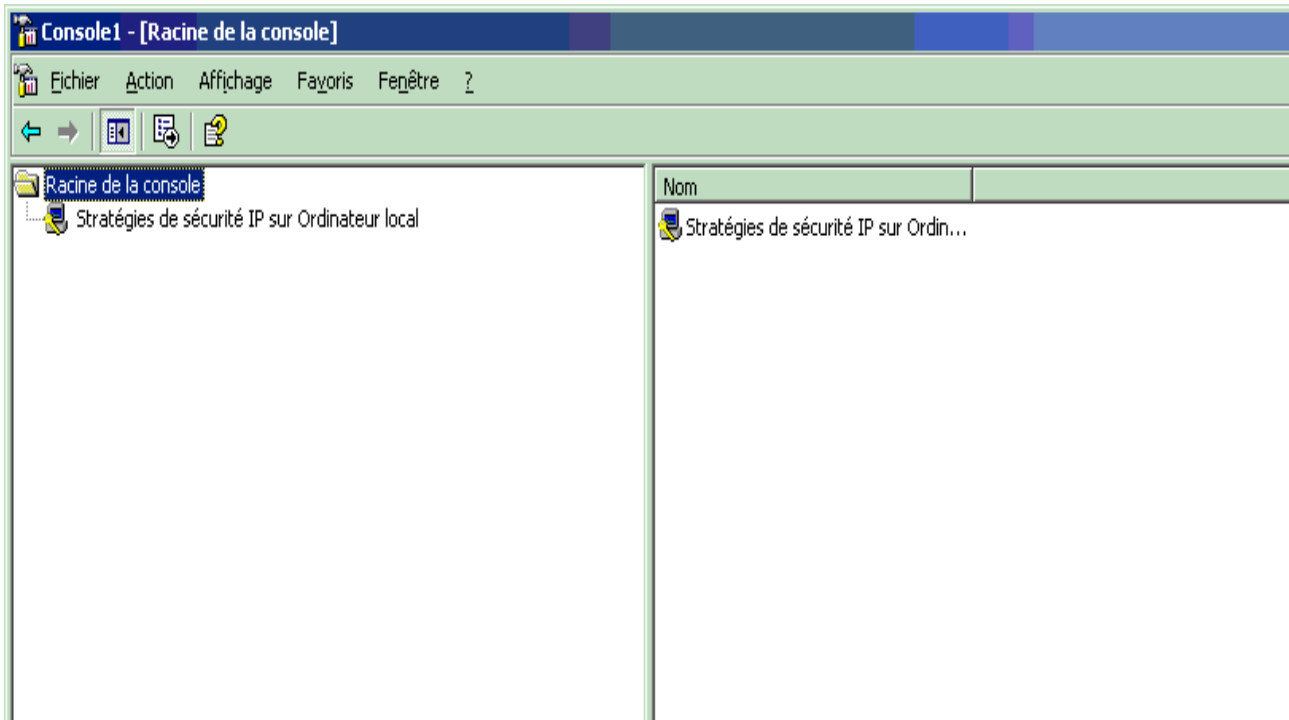
- Deuxième cas :

Etablir un tunnel entre un sous-réseau A ayant pour adresse 192.168.13.0/24 et un sous-réseau B ayant pour adresse 192.168.15.0/24. La machine 1 a l'adresse 192.168.13.1 et la machine 2 a l'adresse 192.168.15.1

Allons-y lançons le MMC ( Microsoft Management Console ) démarrer -> exécuter -> mmc  
Le logiciel enfichable qui nous intéresse est : Stratégie de sécurité sur l'ordinateur Local on va donc l'ajouter à la console. ( voir MOC pour plus d'information ou à cette adresse :

<http://www.microsoft.com/France/TECHNET/Produits/WIN2000S/INFO/info.asp?mar=/FRANCE/TECHNET/Produits/WIN2000S/INFO/mmcovvw.html>

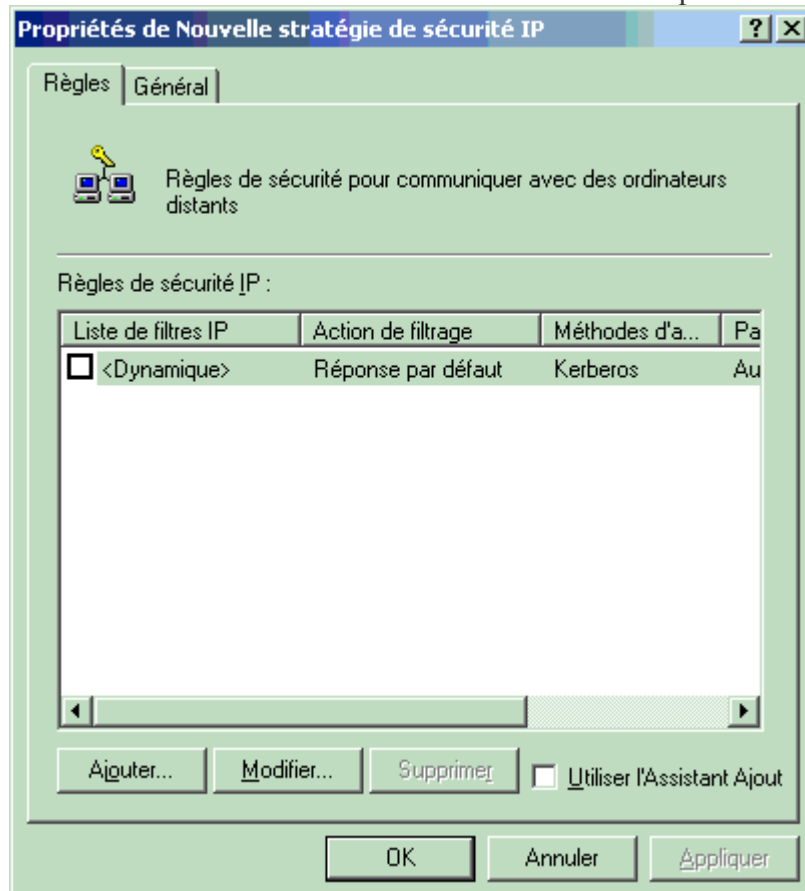
Voilà à quoi ressemblera votre premier écran :



Ensuite nous allons faire un clic droit sur Stratégie de sécurité IP sur Ordinateur local et choisir l'option créer une stratégie de sécurité IP.

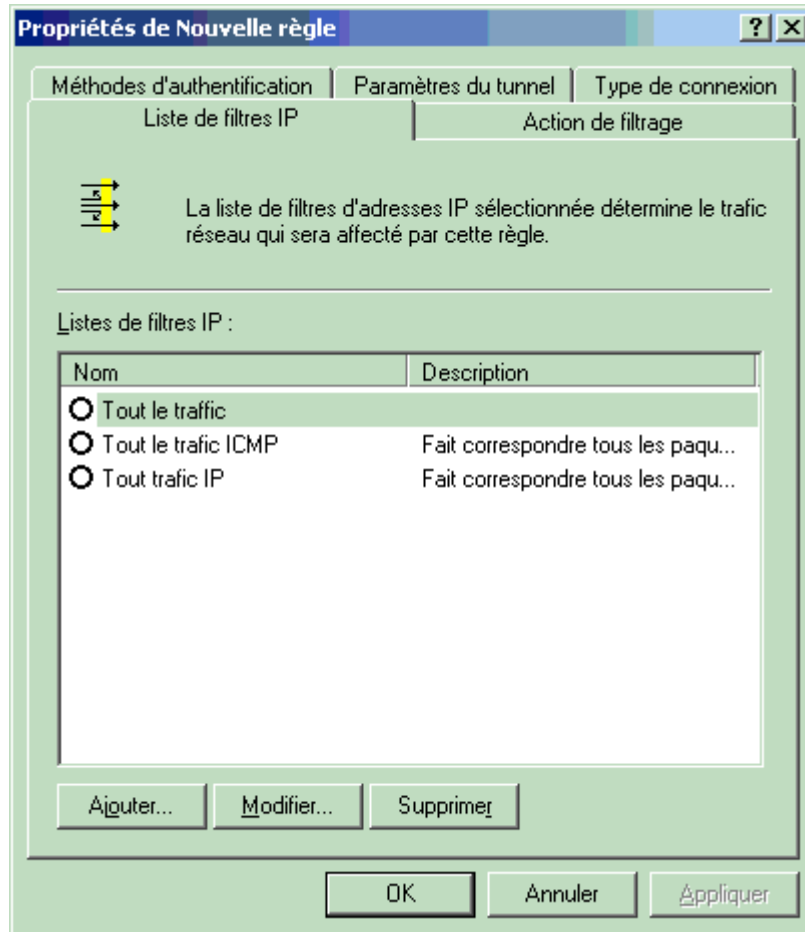
L'assistant se lance et nous demande de donner un nom à la stratégie ect ... on clique sur suivant ( ha qu'est ce que sa peut être chiant d'être assisté par Windows XP :) )

Enfin après les clics sur le bouton suivant nous arrivons sur la fenêtre qui nous intéresse :



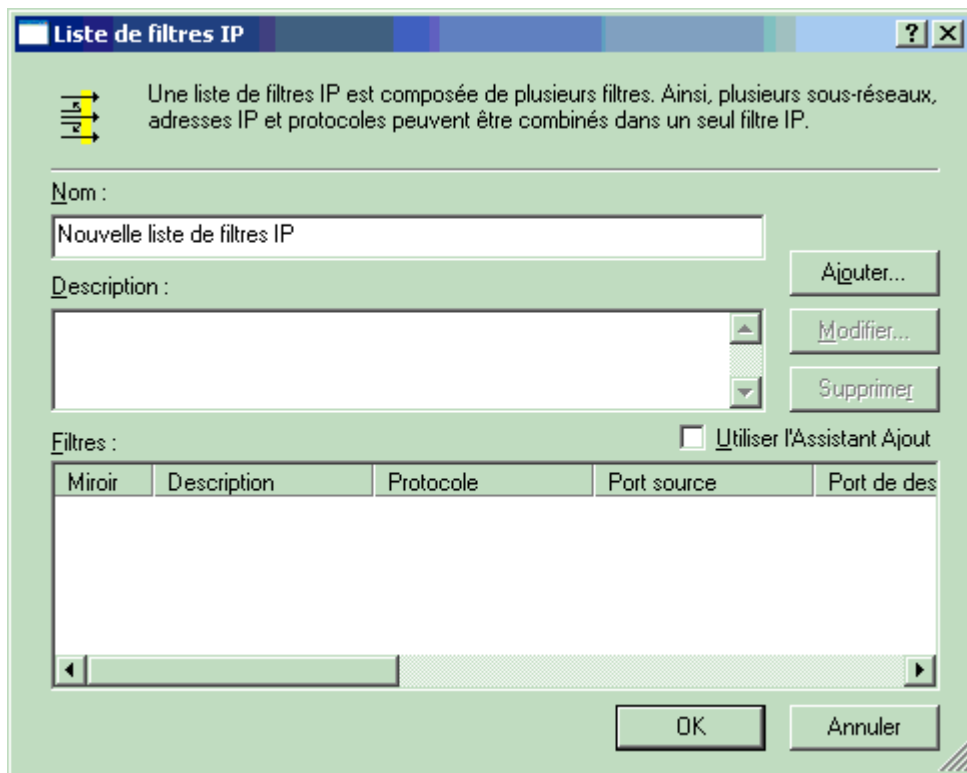
Je conseille de décocher la case Utiliser l'Assistant Ajout. ;)

C'est ici que l'on attaque les choses sérieuses, nous allons ajouter notre stratégie de sécurité en cliquant sur le bouton Ajouter. Notre système nous demande donc maintenant les propriétés de la stratégie. Deux protocoles sont déjà présents dans la liste de filtre IP à savoir IP et ICMP ainsi que l'option ' Tout le trafic '.



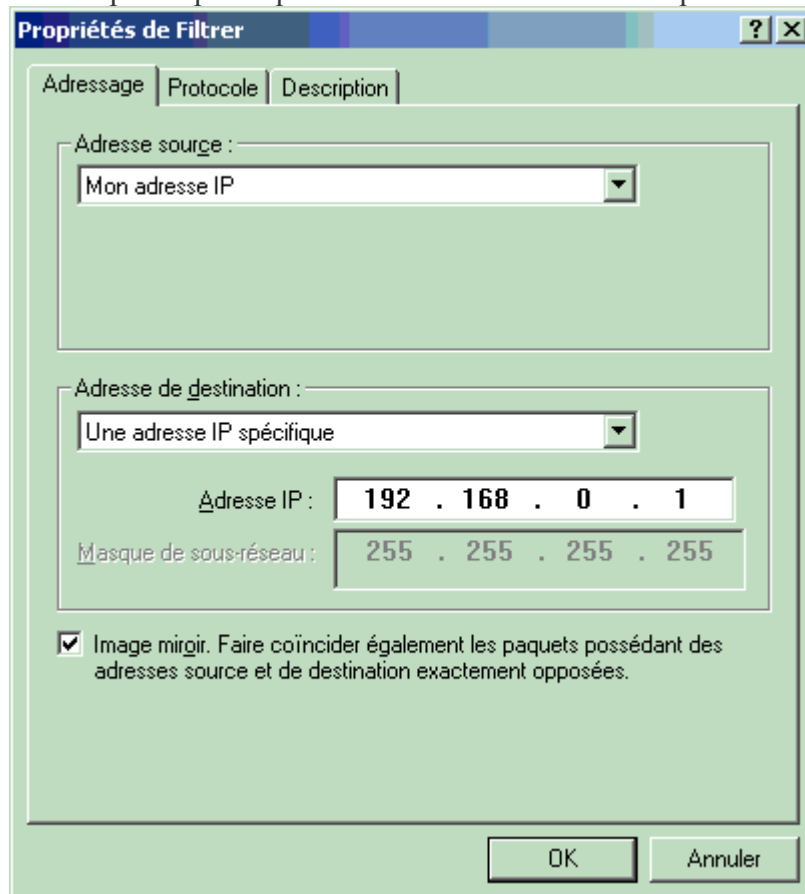
Je vous propose de créer une stratégie qui crypte les connexion Telnet ( pour rappel le serveur telnet utilise le port 23 et le client le port 107 pour le client le tout en TCP)

- Allons-y nous allons définir les SPD pour notre stratégie, il y en aura une pour le trafic sortant et une pour le trafic entrant. Pour ce faire nous cliquons sur Ajouter.



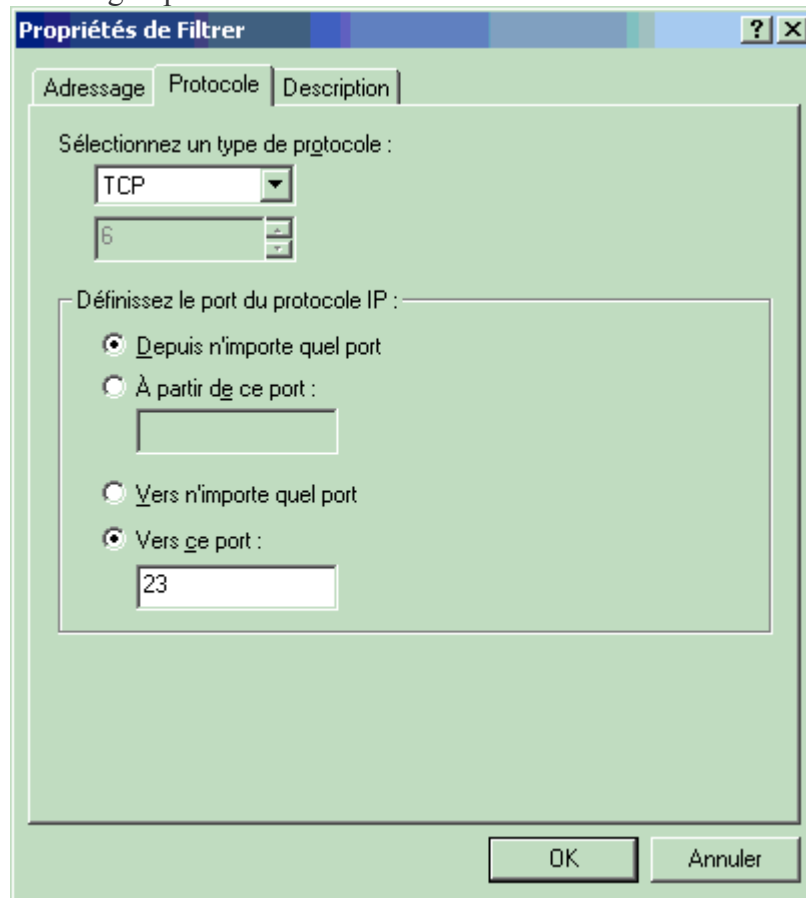
- Ici aussi décocher la case Utiliser l'Assistant Ajout

Nous donnerons un nom à notre filtre, appelons le telnet sortant. Quand ceci est fait nous allons ajouter le protocole et les ports spécifiques à nos sessions telnet en cliquant sur Ajouter

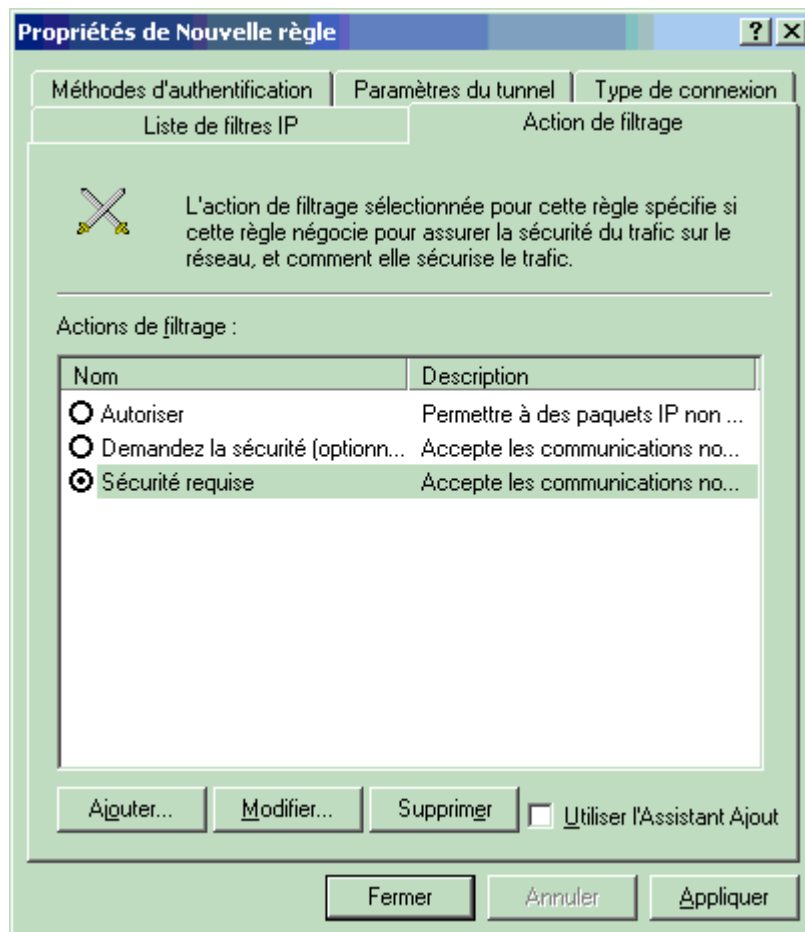


Nous voilà devant l'adressage, nous choisissons comme adresse source : ' Mon adresse IP ' et comme adresse de destination celle du serveur, dans notre exemple 192.168.0.1 ( laissons la case Image miroir cochée, j'avoue ne pas avoir cherché à quoi elle sert réellement )

Passons maintenant à l'onglet protocole



Comme renseigné plus haut nous choisissons le protocole TCP et nous définissons le protocole de destination qui est 23. Vous pouvez à présent entrer une description dans l'onglet description ou appuyer sur OK. On peut appuyer sur OK dans la fenêtre ' Liste de filtre ' et on revient donc dans la fenêtre ' Propriétés de Nouvelle règle ' et on y aperçoit notre nouveau filtre qui porte le nom telnet sortant. Nous allons sélectionner notre filtre et passer à l'onglet ' Action de Filtrage '

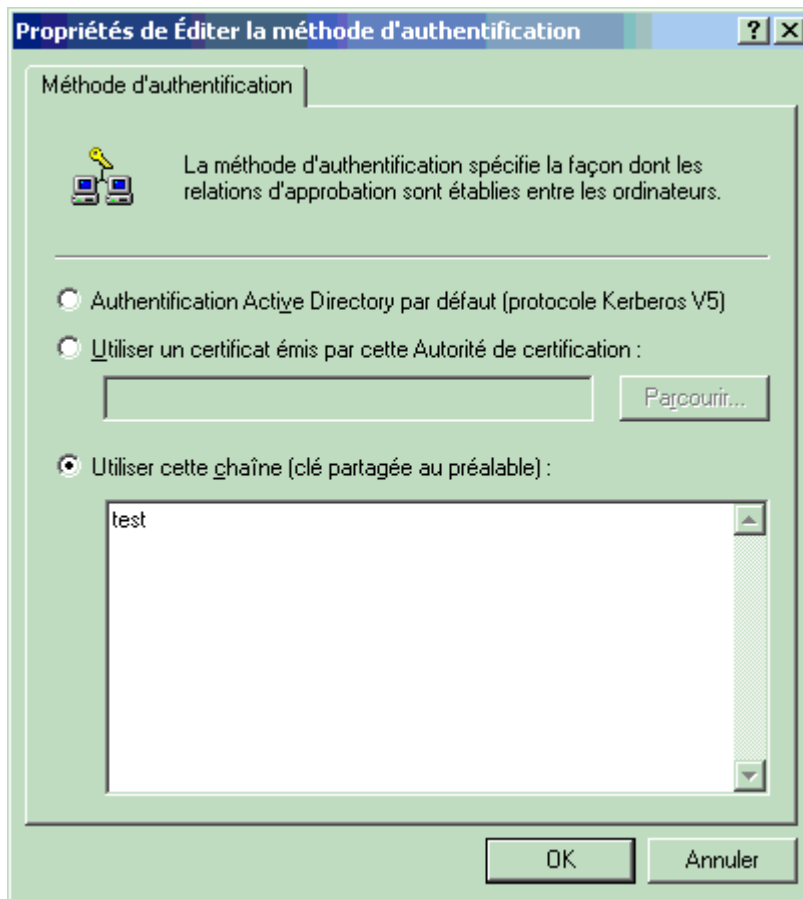


C'est ici qu'on s'amuserait le plus ^\_^ mais on ne va pas compliquer les choses plus qu'elles ne le sont, nous allons simplement choisir ' Sécurité requise '

Remarque : c'est ici que vous pouvez choisir les différents protocoles qui ont été cités dans l'introduction AH et ou ESP ainsi que les protocoles de IKE comme 3DES et MD5, si vous bidouillez avec les protocoles, rappelez-vous que l'ordre est important ;-)

Onglet ' Méthode d'Authentification'

Comme je doute que vous ayiez un serveur Active directory avec Keberos d'actif ( et comme je n'en ai pas moi meme ) entrons une chaîne secrète. ( la capture d'écran et sur la page d'après )

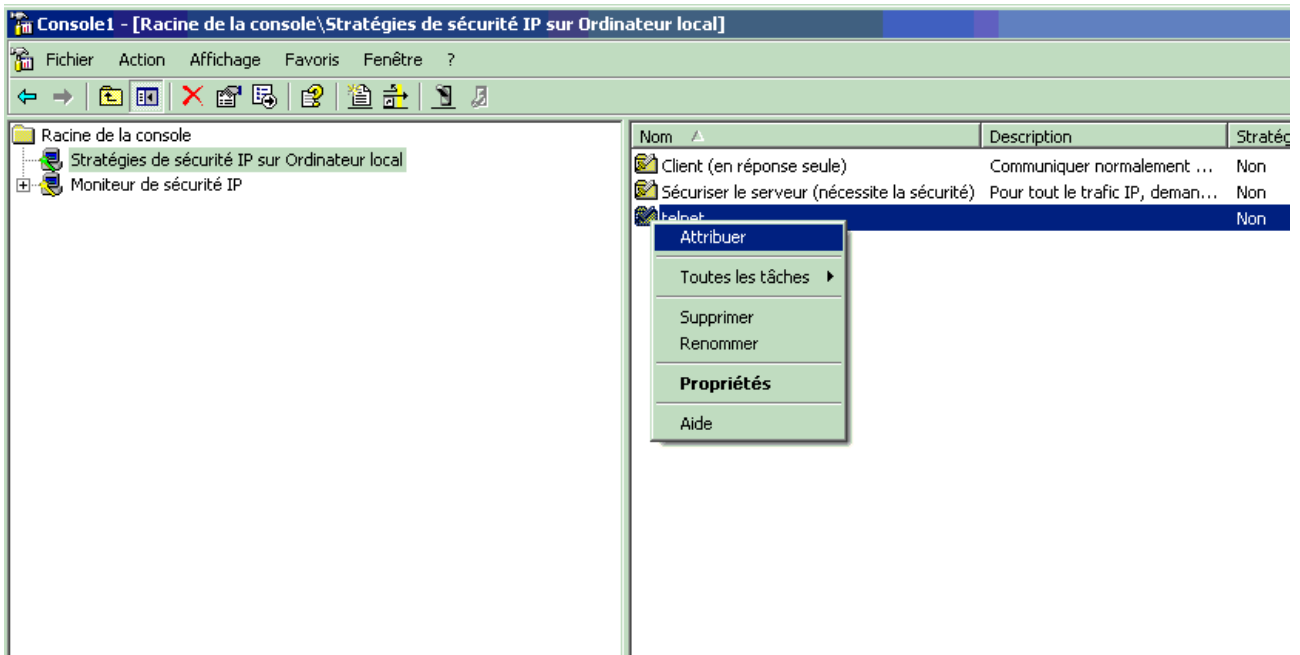


cliquez sur Ok, vous revenez donc dans la fenêtre précédente, supprimez l'authentification Kerberos et passons à l'onglet ' Type de connexion ' dans notre cas nous choisissons connexion locale. Ensuite vérifiez que dans l'onglet ' paramètre du tunnel ' que le bouton sélectionné est bien sur : Cette règle ne définit aucun tunnel

Voilà la SPD du trafic sortant est paramétrée. Nous recommenceront l'opération pour le trafic entrant, le filtre ne sera donc plus le même. En ce qui concerne l'adressage nous renseignerons comme adresse source une adresse spécifique qui sera celle du serveur 192.168.0.1 et comme adresse de destination : Mon adresse ip. Nous choisissons le protocole TCP avec n'importe quel port source mais nous choisissons 107 pour le port de destination. Pour tout le reste le paramétrage est identique à ceux que nous avons réalisés jusque maintenant.

Nous sommes tout content nous avons paramétré le client, si vous avez compris le principe vous devriez savoir paramétrer le serveur sans soucis ;-). Pour ceux qui se demanderaient comment faire c'est la même chose que le client sauf que le trafic entre sur le port 23 et sort sur le 107 ....

Voyons maintenant comment vérifier si nos connexions sont sécurisées. Bien entendu il faut attribuer la stratégie des deux cotés ( client / serveur ) en faisant un clic droit sur la stratégie -> attribuée



Comme vous pouvez le remarquer sur cette nouvelle capture d'écran j'ai ajouté le logiciel enfichable moniteur de sécurité IP. Ajoutez le et descendez dans l'arborescence pour trouver votre machine. Faites un clic droit et choisissez statistiques, vous voyez les statistiques du protocole IKE et IPSEC dans une nouvelle fenêtre. Après avoir lancé une connexion telnet sur le serveur voilà les résultats obtenus :

The screenshot shows the 'NATAKU - Statistiques de sécurité IP' window. It contains two tables: 'Statistiques IKE' and 'Statistiques IPSEC'. Both tables have columns for 'Paramètres' and 'Statistiques'.

Statistiques IKE :	
Paramètres	Statistiques
Acquisition active	1
Réception active	0
Échecs d'acquisition	0
Échecs de réception	0
Échecs d'émission	0
Acquisition de la taille du ...	2
Réception de la taille du s...	2
Échec des négociations	0
Cookies non valides reçus	0
Acquisition totale	1
Obtention totale de SPI	1
Ajouts de clés	1
Mises à jour de clés	1
Obtenir les échecs SPI	0
Échec de l'addition de clés	0
Échec de la mise à jour d...	0
Taille de la liste ISADB	0
Taille de la liste de conn...	0
Mode principal Oakley	1
Mode rapide Oakley	1
Associations logicielles	0

Statistiques IPSEC :	
Paramètres	Statistiques
Associations de sécurité ac...	0
Associations de sécurité dé...	0
Opérations de clés en attente	0
Ajouts de clés	1
Suppressions de clé	1
Nouvelles clés	0
Tunnels actifs	0
Paquets SPI erronés	0
Paquets non décryptés	0
Paquets non authentifiés	0
Paquets avec détection de...	0
Octets confidentiels envoyés	907
Octets confidentiels reçus	1869
Octets authentifiés envoyés	1680
Octets authentifiés reçus	2504
Octets de transport envoyés	1687
Octets de transport reçus	3496
Octets envoyés dans les tu...	0
Octets reçus dans les tunnels	0
Octets déchargés envoyés	0
Octets déchargés recus	0

Remarquez les paquets confidentiels envoyés, ce qui signifie que ma session telnet était bien chiffrée et donc sûre.

Deuxième cas :

Le tunnel ^^ paramétrons la machine 1 ( qui appartient au sous réseau A je le dis au cas ou ) alors, pour ne pas tout reprendre depuis le début, j'ose imaginer que vous savez créer la stratégie de sécurité et ajouter un filtre, nous reprenons donc ici :

The screenshot shows the 'Propriétés de Filtrer' dialog box with the following configuration:

- Tab: Adressage
- Source Address: Un sous-réseau IP spécifique (dropdown), 192.168.13.0 (IP), 255.255.255.0 (Mask)
- Destination Address: Un sous-réseau IP spécifique (dropdown), 192.168.15.0 (IP), 255.255.255.0 (Mask)
- Checkbox:  Image mirrir. Faire coïncider également les paquets possédant des adresses source et de destination exactement opposées.

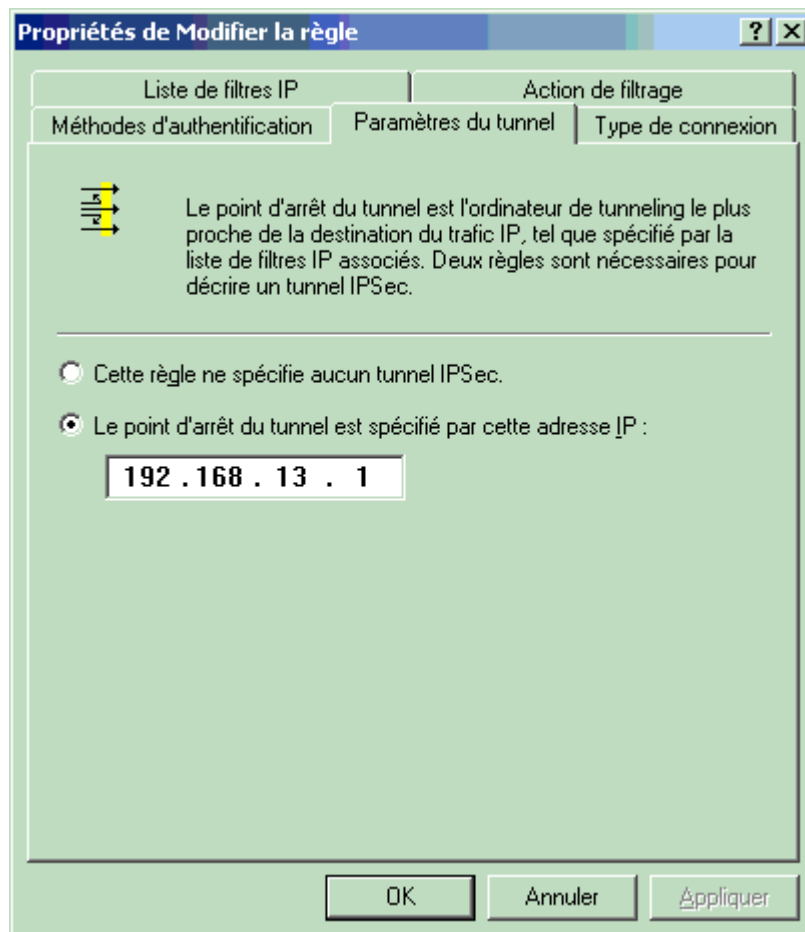
Bien entendu cette fois les adresses sont des adresses de sous réseau respectivement A et B. C'est ici que vous saurez si vous avez compris, quel nom ai-je donné à ce filtre entrant ou sortant ??

Réponse : Sortant

Dans l'onglet protocole je choisis : ' n'importe lequel ' pour que tout le trafic passe par le tunnel

Pour le filtre entrant je renseigne comme adresse source une adresse de sous reseau spécifique et dans ce cas ci ce sera 192.168.15.0 avec comme masque 255.255.255.0 et l'adresse de destination sera bien entendu 192.168.13.1 avec comme masque 255.255.255.0. Comme pour le trafic sortant dans l'onglet protocole je choisis : ' n'importe lequel '

Une fois les filtres définis vous en selectionez un, entrant par exemple et définissez l'action de filtrage à : ' Sécurité requise ' puis changez l'authentification comme vu précédemment et enfin cliquez sur l'onglet ' paramètre du tunnel '



Toute la subtilité se trouve ici, car pour le trafic entrant le point d'arrêt du tunnel est la machine 1 ( nous allons de la France vers l'Espagne par un tunnel où sortons nous ? En Espagne. Si on va de B vers A ou sortons nous ? Dans le réseau A par la machine 1 )  
C'est pourquoi dans cette capture d'écran le point d'arrêt a été réglé a 192.168.13.1 ( parce qu'on paramètré le trafic entrant donc de B vers A )  
Naturellement pour configurer le trafic sortant nous régleront le point d'arrêt du tunnel sur l'adresse 192.168.15.1 ( nous allons d'Espagne en France où sort-on ? En France !! si nous sortons nous allons de A vers B ou sort-on ?? En B donc par la machine 2. ^\_^

Et voilà rien de bien compliqué maintenant en sachant tout ça vous devriez savoir paramètrer la machine 2, attribuer les stratégies et vérifier dans les statistiques qu'un tunnel a bel et bien été créé.

Remerciements :

Merci à Lucie qui a vérifié et corrigé mon orthographe ;-) et à Antoine pour avoir participé aux diverses recherches