Mise en place de VPN avec IPSec

Préliminaires

TOUJOURS VÉRIFIER QUE VOUS UTILISEZ DU MATÉRIEL EN ÉTAT. Ne jamais supposer que les personnes vous ayant précédé ont fait le ménage !

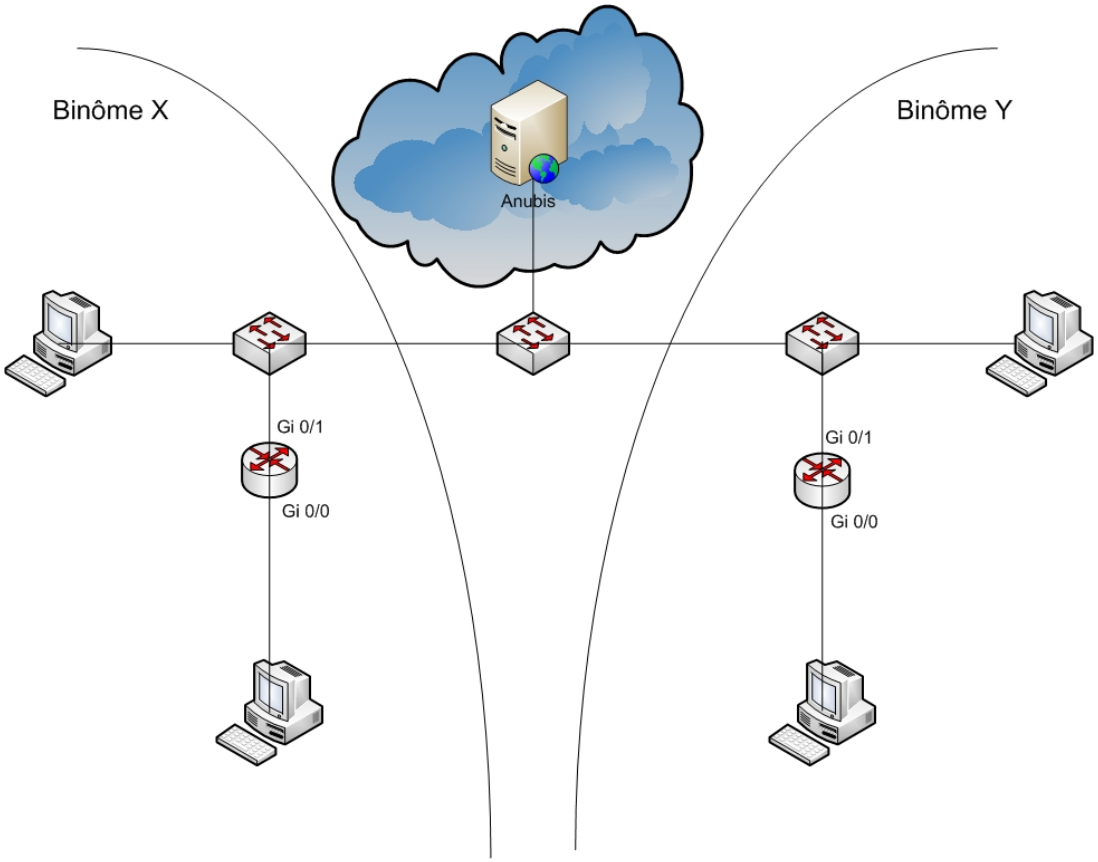
1. Vérifiez que vos machines ont les interfaces intégrées câblées correctement
2. **Si** vous utilisez le switch vérifiez que sa conf est "vide" (`show run, show vlan`)
3. **Si** vous utilisez le routeur vérifiez que sa conf est "vide"
4. Si vos conf ne sont pas "vide" passez à l'étape nettoyage en fin de TP pour y remédier

1 Objectif du TP

Relier deux sites d'une même entreprise par un tunnel sécurisé par IPSec. Dans une première configuration, vous utiliserez le protocole AH (pas de chiffrement des données) puis vous utiliserez le protocole ESP (chiffrement des données) à clef manuelle. Vous mettrez ensuite en œuvre le protocole IKE pour échanger des clefs. Le protocole IKE sera utilisé dans une premier temps avec des clefs partagées et dans un deuxième temps avec un clef publique RSA.

2 Mise place des deux sites

Pour ce TP vous travaillerez avec un binôme voisin. Câblez votre poste selon le schéma ci-dessous.



PC Linux eth0	20.20.X.1/24
PC XP ou Linux	Espion
Routeur Gi0/0	20.20.X.254/24
Routeur Gi0/1	30.30.30.X/24
Anubis	30.30.30.30/24

N'oubliez pas d'ajouter une route statique à votre routeur, pour indiquer que pour joindre le poste voisin il faut passer par leur routeur.

```
Router(config)#ip route 20.20.Y.0 255.255.255.0 30.30.30.Y
```

Vérifiez la connectivité.

3 Mise en place d'un tunnel IPSec en AH

Vous allez configurer le tunnel IPSec avec le protocole AH. Les différentes opérations sont à réaliser de chaque côté du tunnel de manière symétrique. On peut schématiser les étapes de configuration ainsi :

1. Définir dans une ACL, le flux devant passer dans le tunnel

2. Définir un ou plusieurs ensembles des règles à appliquer : le *transform-set*
3. Définir quel ensemble de règles sera utilisé avec quel flux : la *crypto map*
4. Appliquer cette *map* à une interface donnée

Tout le nettoyage des mémoires caches et associations de sécurité en cours se fait grâce à la commande `clear`. Par exemple : `clear crypto sa`.

3.1 Travail à réaliser

Après avoir configuré le tunnel (aux deux extrémités) et avoir configuré un monitoring de port sur le switch pour pouvoir capturer les paquets circulant dans le tunnel :

Question 1 *Faites un ping sur le réseau passant par le tunnel et un autre sur 30.30.30.30 (ne passant pas par le tunnel IPSec). Relevez les trames de ping dans les deux cas, comparez et analysez les. Notez les différences et l'intérêt du tunnel ainsi configuré.*

3.2 Rappel sur les longueurs de clés

Protocole	Longueur de clé
DES ou 3DES	64 bits
AES	96, 128 ou 256 bits
SHA-1	160 bits

3.3 Opérations à effectuer pour configurer un tunnel IPSec sans utiliser IKE (clefs manuelles)

1) Spécifier par une liste d'accès les paquets IP qui doivent être protégés.

2) Spécifier l'ensemble (*transform set*) des protocoles de sécurité qui seront utilisés ainsi que les algorithmes correspondants de chiffrement.

`crypto ipsec transform-set` *transform-set-name transform1*	Défini le *transform-set*
`initialization-vector size [4|8]`	Optionnel
`mode [tunnel|transport]`	Optionnel. En mode tunnel par défaut

3) Combinaisons possibles de protocoles et algorithmes utilisables dans les *transform set*

— Authentification avec AH : ah-md5-hmac ou ah-sha-hmac
— Authentification avec ESP : esp-md5-hmac ou esp-sha-hmac
— Chiffrement avec esp : esp-des ou esp-3des ou esp-aes ou esp-SEAL

4) Création des tunnels IPSec avec clefs manuelles

`crypto map` *map-name seq-num* `ipsec-manual`	Défini la *crypto-map*
`match address` *access-list-id*	Spécifie l'ACL qui défini le trafic à passer dans le tunnel
`set peer` *[hostname — ip-address]*	Spécifie l'autre bout du tunnel
`set transform-set` *transform-set-name*	Donne le *transform-set* à suivre
`set session-key inbound ah` *spi hex-key-data*	Définit la clé à utiliser sur les paquets en entrée pour le protocole AH
`set session-key outbound ah` *spi hex-key-data*	Définit la clé à utiliser sur les paquets en sortie pour le protocole AH
`set session-key inbound esp` *spi cipher hex-key-data [authenticator hex-key-data]*	Défini les clés à utiliser (chiffrement et auth.) sur les paquets en entrée pour le protocole ESP
`set session-key outbound esp` *spi cipher hex-key-data [authenticator hex-key-data]*	Définit les clés à utiliser (chiffrement et auth.) sur les paquets en sortie pour le protocole ESP

5) Application à l'interface sur laquelle IPSec est utilisé.

`crypto map map-name`	Application de la *crypto-map* à l'interface

4 Mise en place d'un tunnel IPSec en ESP

Question 2 *Modifiez la configuration précédente pour pouvoir fonctionner en ESP et répondez aux mêmes questions.*

5 Utilisation du protocole IKE avec "pre-share key" pour la création des SA IPSec et des clefs de sessions IPSec

La *pre-share key* connue des deux *pairs* permet à IKE d'effectuer le transfert des clefs de manière sécurisée.

5.1 Travail à réaliser

Configurez IKE et modifiez le paramétrage d'IPSec :

Question 3 *Faites un ping sur le réseau passant par le tunnel. Relevez le dialogue "IKE/ISAKMP" et les trames de ping. Expliquez et analysez les trames du dialogue IKE/ISAKMP.*

5.2 Opérations à effectuer pour mettre en œuvre IKE

Les opérations suivantes sont soit à rajouter à la configuration précédente soit modifient la configuration précédente.

1) Validation de ISAKMP

```
crypto isakmp enable
```

2) Création de la Politique IKE (à faire en plus de la configuration précédente).

Il s'agit de mettre en œuvre une *politique* pour assurer la sécurité des échanges de clefs.

Opérations pour mettre en place la *politique* :

`crypto isakmp policy` *priority*	Identifie la politique à créer
`encryption [des | 3des | aes]`	l'algo de chiffrement
`hash [sha|md5]`	L'algo de hachage
`authentication [rsa-sig | rsa-encr | pre-share]`	La méthode d'authentification
`group [1|2|5]`	Le groupe Diffie-Hellman
`lifetime` *seconds*	Durée de vie de la SA

Les paramètres par défaut sont : chiffrement DES-CBC 56 bits, hachage SHA1, authentification RSA-sig, Diffie-Hellman 768 bits durée de vie 1 jour.

Vous utiliserez les paramètres par défaut sauf pour l'authentification que vous définirez en *pre-share*.
Priority peut être défini de façon arbitraire car il n'y aura qu'une *politique*.

3) Association d'une clef (pre-share) avec l'adresse de l'extrémité opposée du tunnel (à faire en plus de la configuration précédente) :
`crypto isakmp key` *keystring* `address` *peer-address*
IMPORTANT : La *pre-share key* doit être la même aux 2 extrémités du tunnel !

4) Suppression de la map de la configuration précédente
`no crypto map map-name`

NB : La suppression de la map précédente demande au préalable de supprimer l'association de la map précédente avec l'interface sur laquelle elle était appliquée. (`no crypto map map-name`)

5) puis création d'une nouvelle map en lisant bien les messages affichés :
`crypto map map-name seq-num IPSec-isakmp`

6) Association de la nouvelle map avec l'interface sur laquelle elle est appliquée
`crypto map map-name`

6 Utilisation du protocole IKE avec des clefs publiques RSA pour l'échange des clefs de sessions IPSec

Toutes les clefs utilisées par IKE puis IPSec dérivent des clefs créées par l'algorithme RSA et l'échange des clefs publiques. Cet échange sera réalisé ici "manuellement" et de façon non sécurisée mais il pourrait être fait par l'utilisation de certificats.

6.1 Opérations à effectuer pour mettre en œuvre IKE avec des clefs RSA

1) Modifier la "politique" de la configuration précédente en spécifiant comme paramètre d'authentification "rsa-sig"

2) Création des clefs et visualisation de la clef publique locale (à enregistrer manuellement sur le routeur distant). Vous utilisez SCP/anonymous ftp/HTTP/SSH/clé USB pour transmettre la clef publique d'une table à l'autre (Attention, le serveur ftp fait une résolution inverse, modifiez le fichier `/etc/hosts` en conséquence).

`ip domain name` *name*	Nom quelconque
`crypto key generate rsa [usage-keys]`	Génére la clé RSA
`show crypto key mypubkey rsa`	Visualise votre clé, qu'il faudra transmettre

3)Enregistrement de la clef publique sur le routeur distant

`crypto key pubkey-chain rsa`	Entre dans le mode de configuration d'une clé publique
`addresse-key` *key-address*	Indique la clé publique RSA du *peer* que vous allez spécifier
`key-string`	Spécifie la clé du *peer*

6.2 Travail à réaliser

Après avoir modifié la configuration, refaites les mêmes tests et relevés que pour les manipulations précédentes.

NB : La transmission manuelle de la clef publique du routeur distant est fastidieuse. Il existe une méthode utilisant une Autorité de Certification pour assurer un transfert sécurisé de la clef publique. Cette méthode n'est pas utilisable ici, car il n'y a pas de CA en place dans la salle.

7 Nettoyage

Pour remettre la salle en état. **Si** vous avez utilisez le routeur :
`Router#copy flash:base-1900.cfg startup-config`
Éteindre le routeur.

Si vous avez utilisé le switch :
`Switch# delete flash:vlan.dat` **si** vous avez fait des vlan
`Switch# erase startup-config`
Éteindre le switch

Recâbler correctement, si nécessaire les câbles gris sur les machines.

Sur le PC XP, repasser l'interface réseau en DHCP et éteindre la machine.
Attention les scripts suivants effacent tout
Sur le PC Linux, lancer le script `/script/init_machine.sh` puis le script `/script/init_reseau.sh`.