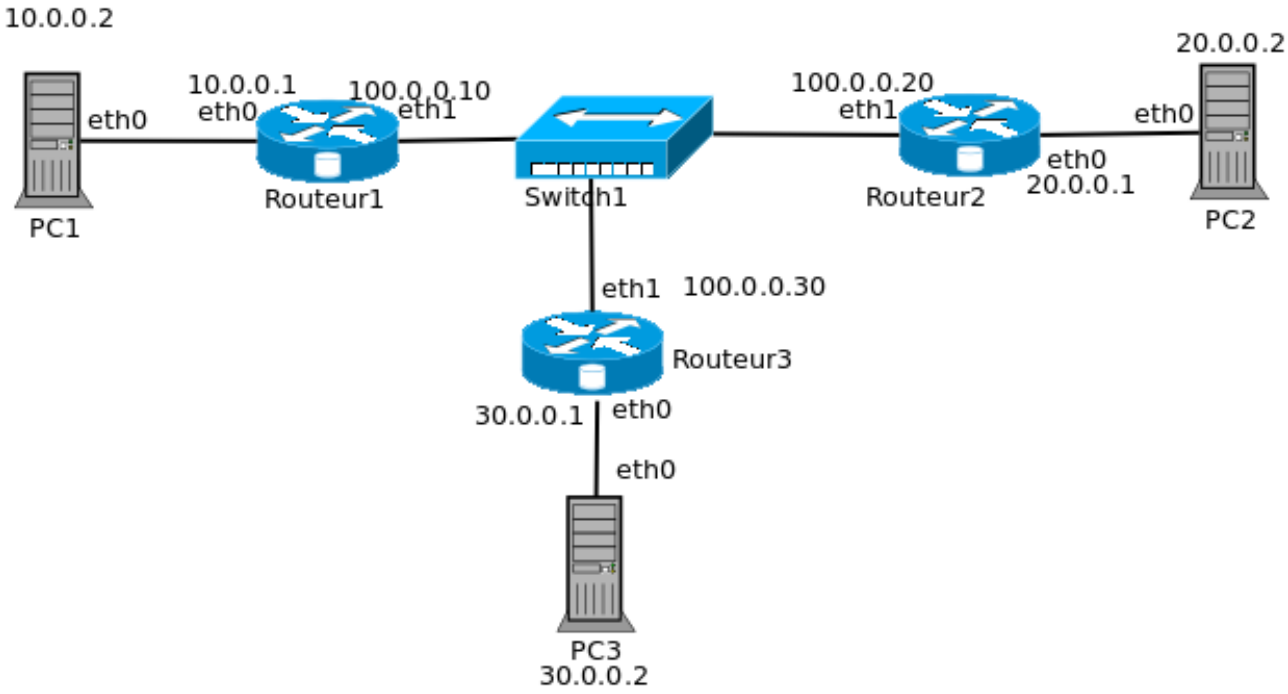
Compréhension de l'utilité d'IPSec et analyse de trame internet

1 Environnement

Vous disposez d'une machine virtuelle (VirtualBox) sur laquelle est installée Trisquel (GNU/Linux basé sur Ubuntu). Vous utiliserez le logiciel netkit pour émuler un réseau composé de pc, de routeurs et de switch. Le réseau se décompose comme ceci :



2 Fonctionnement de netkit

Netkit permet d'émuler un réseau à l'aide de machines virtuelles. Nous l'utiliserons en lançant un laboratoire avec la commande

lstart -p

en étant placé dans le répertoire /home/introsecu/netkit/netki-lab-XXX. **lstart -p** permet de lancer toutes les machines virtuelles an parallèle. Chaque machine virtuelle est lancée dans un terminal. Attention à ne pas confondre les terminaux lors des configurations des machines. Après le lancement, vous devriez obtenir un terminal pour chaque point de la liste suivante :

- PC1 : ordinateur du site 1
- PC2 : ordinateur du site 2

- PC3 : ordinateur espion
- Routeur 1 : Routeur du site 1
- Routeur 2 : routeur du site 2
- Routeur 3 : routeur du site 3
- Switch 1 : switch du site 1

Tous ces équipements sont déjà configurer de manière à pouvoir communiquer mais sans aucune sécurité. Avant de modifier les configurations pour incorporer de la sécurité, tester la configuration actuel pour vérifier que tout fonctionne:

ping pc1 vers pc2

ping pc2 vers pc3

ping pc3 vers pc1

3 Objectifs du TP

L'objectif de ce TP est de comprendre la nécessité d'utiliser des tunnels sécurisés entre deux sites distants d'une même entreprise. Pour cela, vous allez configurer les routeurs 1 et 2 pour créer un tunnel IPSec entre les sites 1 et 2. Vous apprendrez aussi à analyser les trames réseaux. Vous utiliserez le logiciel en ligne de commande *tcpdump* pour réaliser les captures réseaux et *wireshark* pour les analyser.

4 Quelques informations sur IPSec

Le protocole IP ne fournit aucun service de sécurité et est donc vulnérable à des attaques. IPSec est donc utilisé pour sécuriser le trafic IP. IPSec est standardisé et est obligatoirement intégré aux piles IPv6. Ceci n'oblige en rien son utilisation. Il est seulement obligatoire dans la pile. IPSec apporte des mécanismes d'intégrité des données et d'authentification de la source (HMAC, Signature). Il protège contre le rejeu et assure la confidentialité des données à l'aide de chiffrement. Il intervient sur la couche 3 du modèle OSI. Il fournit donc une sécurité de bout en bout pour l'utilisation du mode transport où il protège la couche 4 et plus. En mode tunnel, il fournit une protection point à point (par exemple, entre deux passerelles) où il protège la couche 3 et plus. Ses utilisations principales sont de connecter, de manière sécurisés et transparente, deux sites distants d'une même entreprise, entre un poste et un site ou encore entre un poste et un autre poste.

5 Travail à faire

1. Lancer le laboratoire avec la commande **lstart -p** en vous plaçant dans le répertoire **/home/introsecu/netkit/netkit-lab-XXX**
2. Configurer les routeurs pour qu'ils supportent IPSec

3. Capturer les trames directement sur le switch. Vous capturerez les trames entre PC2 et PC1 et entre PC2 et PC3.

Les manipulations suivantes seront à effectuer sur les routeurs 1 et 2. Avant de faire les configurations il va falloir charger manuellement chaque module noyau utile :

modprob ah4 : à utiliser pour ah

modprob esp4 : à utiliser pour esp

Pour configurer les routeurs, il va falloir entrer différentes commandes dans le *shell*. Il faudra tout d'abord modifier le fichier **/etc/racoon/setkey.conf**[1] en y ajoutant les configurations suivantes :

5.1 Configuration pour AH :

Le protocole AH apporte les propriétés de sécurités suivantes :

Authentification : Seul les utilisateurs autorisés ont accès aux services après identification

Intégrité : Être sur que les données n'ont pas été modifiées

Protection contre le rejeu : Détecter une retransmission de paquets

```
#!/usr/sbin/setkey -f
flush;
spdflush;

# Associations de sécurité avec le protocole AH
add @source @dest ah 0×200 -m transport -A hmac-sha1 clef;
add @dest @source ah 0×300 -m transport -A hmac-sha1 clef;

# Politiques de sécurité
spdadd @source @dest any -P out ipsec
        ah/transport//require;

spdadd @dest @source any -P in ipsec
        ah/transport//require;
```

Ensuite, il faut mettre à jour les droits sur les fichiers *setkey.conf* avec la commande suivante !

chmod 600 /etc/racoon/setkey.conf

Puis lancer une mise à jour :

1 Si le fichier n'existe pas il faudra le créer.

setkey -f /etc/racoon/setkey.conf

Pour vérifier les modifications il faut entrer les commandes suivantes :

setkey -D : Afficher la BD d'association de sécurité (SA)
setkey -DP : Afficher la BD de politique de sécurité (SP)

La clef peut être entrée au format hexadécimal (chiffre [0-9] et lettre [a-f]) de la manière suivante :

0xa9182efadc394838df48592ca39573a

0x est utilisé pour dire que la chaîne suivante est de l'hexadécimal.

Les clefs sont différentes en entrée (**in**) et en sortie (**out**). Pensez à inverser les **in** et **out** des **spdadd** sur la configuration de l'équipement en face :

- **sur routeur1 :**
  - **spdadd 100.0.0.20 100.0.0.10 any -P out ipsec ah/transport//require;**
  - **spdadd 100.0.0.10 100.0.0.20 any -P in ipsec ah/transport//require;**
- **sur routeur2 :**
  - **spdadd 100.0.0.20 100.0.0.10 any -P in ipsec ah/transport//require;**
  - **spdadd 100.0.0.10 100.0.0.20 any -P out ipsec ah/transport//require;**

Quelques explications :

flush : efface la base de données des associations de sécurité.

spdflush : efface la base de données des politiques de sécurité

add : ajoute l'association de sécurité dans la base de données des Ass. @**source** et @**dest** sont les adresses ip des terminaux des bouts du tunnel. **ah** permet de spécifier que l'on veux utiliser le protocole AH (donc de l'authentification). **0X200** est le SPI. -m transport indique que l'on utilise le mode transport. **-A** pour définir l'algorithme d'authentification et **hmac-sha1** le nom de l'algorithme. **clef** est la clef utiliser pour le hmac.

Un *association de sécurité* permet de définir quel sous protocole (AH ou ESP), quel mode (transport ou tunnel) quel algorithme de chiffrement (pour ESP) et quel algorithme d'authentification utiliser. Une AS est unidirectionnelle. C'est-à-dire qu'il faut une AS pour le flux entrant et une autre pour le flux sortant. Pour une AS il faudra une Politique de Sécurité. Une AS est identifié à l'aide du SPI, de l'adresse destination et de l'identifiant du protocole de sécurité. L'index de paramètre de sécurité (SPI) permet d'identifier de façon unique une AS. Il est transporté

dans chaque paquets pour que l'équipement au bout du tunnel puisse retrouver l'AS à utiliser pour ce paquet.

spdadd : La commande *spdadd* s'utilise comme ceci :

spdadd @source @dest any -P *direction* ipsec *protocol/mode/src-dst/level*

où :

spdadd *:* permet de définir les politiques de sécurité qui seront utilisé pour le tunnel entre les machines

@**source** : l'adresse ip source

@**dest** : l'adresse ip du routeur du site distant

any : tous les protocoles utiliserons le tunnel IPSec entre @source et @dest

-P *:* utilisé pour définir la politique

direction : indique que la politique de sécurité doit être utilisée pour les paquets sortant (*out*) ou entrant (*in*).

ipsec : indique que les opérations IPSec seront effectuées sur les paquets.

Protocol : le protocole utilisé AH ou ESP

mode : permet de spécifier tunnel ou transport. Le *mode transport* ne protège que les données de la couche supérieure (couhe 4 et +). L'application d'IPSec se fait sur les données provenant de la couche transport. Le *mode tunnel* protége le paquet IP en entier. L'application d'IPSec se fait sur les données provenant de la couche réseau par encapsulation (couche 3 et +). Avec le protocole AH, le paquet est authentifié quelque soit le mode tunnel ou transport. Alors qu'avec ESP, en mode transport seulement les champs données et *trailer esp* sont chiffrés et authentifiés. L'authentification est aussi sur les parties en-tête ESP et en-tête ip d'origine. Contrairement au mode transport, le mode tunnel chiffre aussi l'en-tête ip d'origine et authentifie les même champs du paquets avec en plus la nouvelle en-tête ip.

Src-dst :Les addresses ip des réseaux source et destination

level : *Require* est utilisé pour indiquer que la SA est obligatoire alors que la valeur *use* indique que la SA doit être utilisée si elle est disponible sinon le paquet est envoyé normalement.

La commande *spadd* permet d'ajouter une politique de sécurité dans la SPD (Security Policy Database). Une Politique de Sécurité nous permet de déterminer quels seront les éléments de sécurité à appliquer aux paquets (entrant ou sortant).

5.2 Configuration pour ESP :

Le protocole ESP permet de garantir, en plus des propriétés de AH la propriété de confidentialité.

Confidentialité : Seules les personnes autorisées ont accès aux données

La configuration pour utiliser le protocole ESP est très proche de celle pour le protocole AH. En effet, il suffit de rajouter deux lignes et d'en modifier deux autres dans les fichier setkey.conf :

Ajouter :

add @source @dest esp 0×201 -m transport -E 3des-cbc
0x9287239acedfafed294934750028abdecf2948a91e3b819a;
add @dest @source esp 0×301 -m transport -E 3des-cbc
0xabd1902becadefa194726abe294832cbad2938104657abc;

Modifier :

spdadd @source @dest any -P out ipsec
ah/transport//require;

par

spdadd @source @dest any -P out ipsec
esp/transport//require
ah/transport//require;

ce qui donne

```
#!/usr/sbin/setkey -f
flush;
spdflush;

# Associations de sécurité pour le protocole AH
add @source @dest ah 0×200 -m transport -A hmac-sha1 clef;
add @dest @source ah 0×300 -m transport -A hmac-sha1 clef;

#Associations de sécurité pour le protocole ESP
add @source @dest esp 0×201 -m transport -E 3des-cbc
0x9287239acedfafed294934750028abdecf2948a91e3b819a;
add @dest @source esp 0×301 -m transport -E 3des-cbc
0xabd1902becadefa194726abe294832cbad2938104657abc;


# Politiques de sécurité
spdadd @source @dest any -P out ipsec
esp/transport//require
```

ah/transport//require;

spdadd @dest @source any -P in ipsec
esp/transport//require
ah/transport//require;

6 Capture des paquets réseau

Pour capturer les paquets réseaux, vous allez utiliser le logiciel *tcpdump*. Pour le lancer il suffit d'exécuter la commande suivante dans le *shell* :

tcpdump -i ethX host @source and @dest -w output.cap

Cette commande exécute tcpdump pour écouter l'interface eth1 (à modifier par l'interface que vous utilisez), ne conserve que les paquets provenant de **@source** et **@dest** (**host**) et écrit dans le fichier **output.cap** (**-w**).

Pour examiner les paquets vous utiliserez le logiciel *wireshark* sur le système hôte. Pour récupérer les fichiers **output.cap** des VM *netkit* vous devez les déplacer avec la commande :

cp output.cap /hosthome

Ceci se retrouverons dans le répertoire netkit-lab-XXX. Il suffit ensuite d'ouvrir la capture avec *wireshark* et de naviguer dans les paquets. Vous utiliserez la commande ***ping*** ***@ip*** pour faire transiter des paquets. Vous devrez *pinger* les machines PC1 et PC3 depuis PC2. *tcpdump* sera exécuté sur le *switch*.

7 Exercices :

7.1 Réalisations des configurations avec AH :

Il vous faut réaliser les configurations sur routeur 1 et routeur 2 en utilisant le protocole AH avant de capturer et d'analyser les trames réseaux.

Question 1 : Donner un exemple pratique où utiliser le protocole AH suffit.

Question 2 : Décrivez les paquets *ping* vers PC1 et PC3 en exécutant la commande *ping* sur PC2. La capture des paquets se fait depuis le *switch*. A quoi correspondent les champs de ces paquets ? Quels est leur longueur ? A quoi voit-on que les paquets sont passés par le tunnel ? Dans quel cas cela n'est pas le cas?

Question 3 : A l'aide de ces trames, proposer une représentation d'un paquet AH.

7.2 Réalisations des configurations avec AH et ESP :

Même exercice que précédemment mais en ajoutant le protocole ESP pour atteindre la propriété de confidentialité des données.

Question 1 : Donner un exemple pratique où utiliser le protocole ESP suffit.

Question 2 : Décrivez les paquets *ping* vers PC1 et PC3 en exécutant la commande *ping* sur PC2. La capture des paquets se fait depuis le *switch*. A quoi correspondent les champs de ces paquets ? Quel est leurs longueurs ? A quoi voit-on que les paquets sont passés par le tunnel ? Dans quel cas cela n'est pas le cas?

Question 3 : A l'aide de ces trames, proposer une représentation d'un paquet ESP.

7.3 Questions supplémentaires

Question 1 : Quels différences y a t-il entre AH et ESP ? Vous pouvez vous aidez des trames relevées précédemment pour illustrer vos propos.

Question 2 : D'un point de vue de l'espion, quels sont les informations qu'il peut considérer comme utile dans les trames ? Tout d'abord en utilisant le protocole AH puis avec le protocole ESP ?

Question 3 : Une attaque *man-in-the-middle* est une attaque permettant d'intercepter toutes (ou partie) des communications entre deux sites sans que les sites distants ne s'en rendent compte. Est-ce qu'une tel attaque est possible avec IPSec AH, ESP sans authentification et ESP (indice : penser authentification).

Question 4 : Le chiffrement utilisé est suffisant pour l'instant. Donc un attaquant interceptant les trames du tunnel ne pourra pas les lire (chiffrement offre confidentialité). Cependant, la cryptographie utilisée aujourd'hui sera probablement inefficace dans quelques années. Est-ce que cela peut poser problème dans le cas de données confidentielles (militaire, gouvernementale, entreprise concevant de nouvelle technologie) ?