IPSEC en mode Transport

M. Szpieg

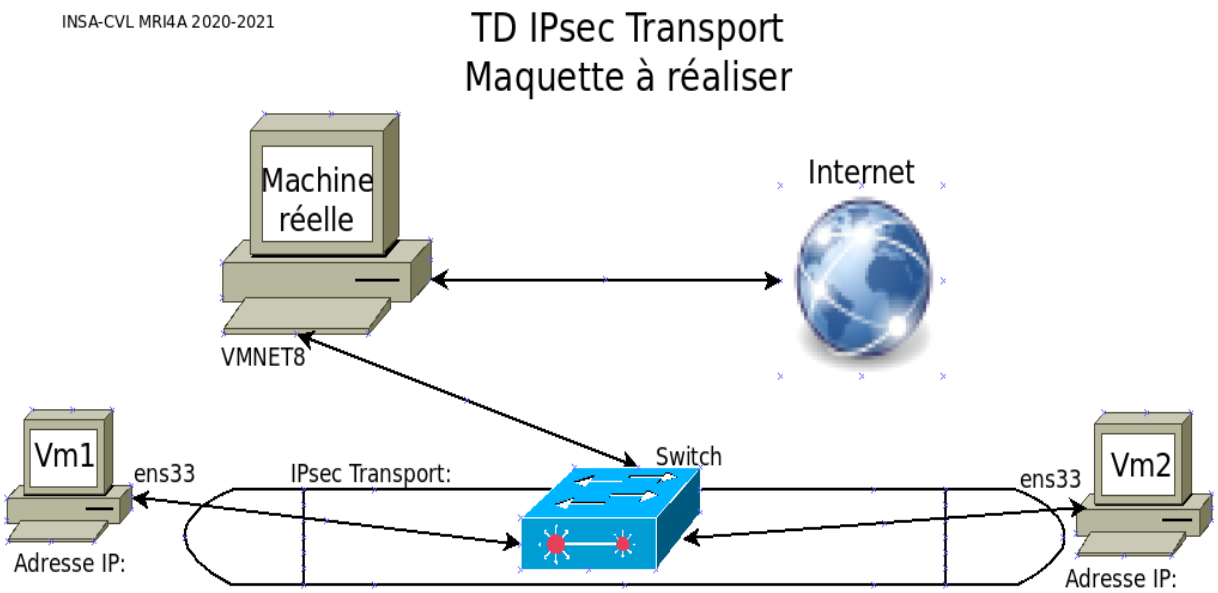
STI4A Année 2020-2021. Module : Sécurité du système d'information

Table des matières

I.Mise en place d'IPSec en mode transport avec clés statiques.....1
II.Préparation :.....2
III.Configuration de la machine « VM1 ».....2
IV.Création du réseau de test.....2
V.Configuration IPsec des machines VM1 et VM2.....2
1.Modifier le fichier de configuration de VM1.....2
2.Appliquer le fichier de configuration.....3
3.Vérifier les résultats.....4
4.Modifier le fichier de configuration de VM2.....4
VI.Vérifier le réseau.....4
VII.Authentifier et déchiffrer les paquets à la volée.....4
VIII.Installer un serveur ftp sur VM1.....5

I. Mise en place d'IPSec en mode transport avec clés statiques.

But : Créer une connexion sécurisée et authentifiée entre deux machines « VM1 » et « VM2 » avec des paquets IPSec de type ESP en mode Transport .



II. Préparation :

Récupérez une VM Linux Bodhi (https://filesender.renater.fr/?s=download&token=29662024-897f-405e-9ac2-cab794b9e307) et nommez-la « VM1 ». Pour des raisons d'homogénéité dans les résultats partez tous de cette VM !!
Faites-en un clone que vous appellerez « VM2 ».

III. Configuration de la machine « VM1 »

Chargez le paquet « ipsect-tools » dans la machine ainsi obtenue :
N'oubliez pas de passer « root » ou commande « sudo » !

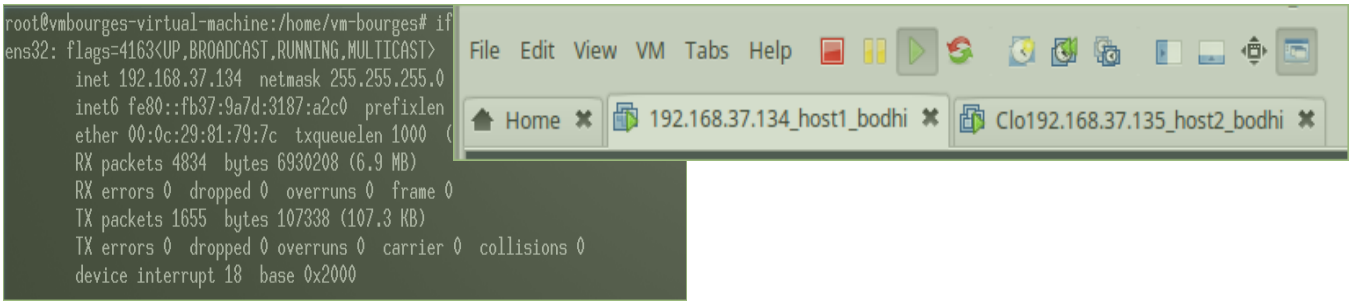
```
insacvl-vm insacvl # apt-get install ipsec-tools
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  ipsec-tools
0 mis à jour, 1 nouvellement installés, 0 à enlever et 17 non mis à jour.
Il est nécessaire de prendre 60,4 ko dans les archives.
```

Vérifiez le bon fonctionnement.

```
insacvl-vm insacvl # setkey -D
No SAD entries.
insacvl-vm insacvl # setkey -DP
No SPD entries.
```

IV. Création du réseau de test

Arrêtez la machine virtuelle et créez un clone linké appelé VM2 comme sur la maquette du paragraphe I.
Démarrez les deux machines et notez les adresses IP sur l'énoncé du TD sur le dessin du paragraphe I.



V. Configuration IPsec des machines VM1 et VM2

1.Modifier le fichier de configuration de VM1

Copiez le fichier /etc/ipsec-tools.conf dans /etc/ipsec-tools.conf.org

```
root@vmbourges-virtual-machine:/home/vm-bourges# cp /etc/ipsec-tools.conf /etc/ipsec-tools.conf.org
```

En vous inspirant des réglages ci-dessous, configurez « Vm1 » et « Vm2 » de manière à bénéficier d'une connexion Ipsec sécurisée entre « Vm1 » et « Vm2 »:
Réglez le fichier /etc/ipsec-tools.conf de la manière suivante :

Attention :

- Pour la valeur du SPI vous mettrez votre mois et année de naissance, en décimale, dans le sens A vers B
  Exemple si vous êtes né en février 1980 (;-)) vous écrirez pour les lignes commençant par « add » :
  ```
  add 192.168.190.128 192.168.190.129 esp 021980 -E des-cbc "12345678" -A hmac-md5 "1234567890123456";
  ```
- Pour la valeur du SPI vous mettrez votre mois et année de naissance, en héxadécimale, dans le sens B vers A
  Exemple si vous êtes né en février 1980 (;-)) vous écrirez pour les lignes commençant par « add » :
  ```
  add 192.168.190.129 192.168.190.128 esp 0X021980 -E des-cbc "12345678" -A hmac-md5 "1234567890123456";
  ```

```
spdadd 192.168.190.128 192.168.190.129 any -P out ipsec esp/transport//require;
add 192.168.190.128 192.168.190.129 esp 021980 -E des-cbc "12345678" -A hmac-md5 "1234567890123456";
spdadd 192.168.190.129 192.168.190.128 any -P in ipsec esp/transport//require;
add 192.168.190.129 192.168.190.128 esp 0X021980 -E des-cbc "12345678" -A hmac-md5 "1234567890123456";
```

```
flush;
spdflush;
spdadd 192.168.37.134 192.168.37.135 any -P out ipsec esp/transport//require;
add 192.168.37.134 192.168.37.135 esp 021980 -E des-cbc "12345678" -A hmac-md5 "1234567890123456";
spdadd 192.168.37.135 192.168.37.134 any -P in ipsec esp/transport//require;
add 192.168.37.135 192.168.37.134  esp 0X021980 -E des-cbc "12345678" -A hmac-md5 "1234567890123456";
```

2.Appliquer le fichier de configuration

```
root@vmbourges-virtual-machine:/home/vm-bourges# systemctl restart setkey
```

3.Vérifier les résultats.

```
root@vmbourges-virtual-machine:/home/vm-bourges# setkey -D
192.168.37.135 192.168.37.134
        esp mode=transport spi=137600(0x00021980) reqid=0(0x00000000)
        E: des-cbc  31323334 35363738
        A: hmac-md5  31323334 35363738 39303132 33343536
        seq=0x00000000 replay=0 flags=0x00000000 state=mature
        created: Nov 18 08:17:44 2020   current: Nov 18 08:25:03 2020
        diff: 439(s)    hard: 0(s)      soft: 0(s)
        last:                           hard: 0(s)      soft: 0(s)
        current: 0(bytes)       hard: 0(bytes)  soft: 0(bytes)
        allocated: 0    hard: 0 soft: 0
        sadb_seq=1 pid=2347 refcnt=0
192.168.37.134 192.168.37.135
        esp mode=transport spi=21980(0x000055dc) reqid=0(0x00000000)
        E: des-cbc  31323334 35363738
        A: hmac-md5  31323334 35363738 39303132 33343536
        seq=0x00000000 replay=0 flags=0x00000000 state=mature
        created: Nov 18 08:17:44 2020   current: Nov 18 08:25:03 2020
        diff: 439(s)    hard: 0(s)      soft: 0(s)
        last:                           hard: 0(s)      soft: 0(s)
        current: 0(bytes)       hard: 0(bytes)  soft: 0(bytes)
        allocated: 0    hard: 0 soft: 0
        sadb_seq=0 pid=2347 refcnt=0
```

```
root@vmbourges-virtual-machine:/home/vm-bourges# setkey -DP
192.168.37.135[any] 192.168.37.134[any] 255
        fwd prio def ipsec
        esp/transport//require
        created: Nov 18 08:17:44 2020  lastused:
        lifetime: 0(s) validtime: 0(s)
        spid=18 seq=1 pid=2349
        refcnt=1
192.168.37.135[any] 192.168.37.134[any] 255
        in prio def ipsec
        esp/transport//require
        created: Nov 18 08:17:44 2020  lastused:
        lifetime: 0(s) validtime: 0(s)
        spid=8 seq=2 pid=2349
        refcnt=1
192.168.37.134[any] 192.168.37.135[any] 255
        out prio def ipsec
        esp/transport//require
        created: Nov 18 08:17:44 2020  lastused:
        lifetime: 0(s) validtime: 0(s)
        spid=1 seq=0 pid=2349
        refcnt=1
root@vmbourges-virtual-machine:/home/vm-bourges#
```

D'abord la base des associations de sécurité (SA Security Association) « setkey -D ». Ensuite la base des politiques de sécurité (SP Security Policies) « setkey -DP ».
Que dit le service « setkey ».
Cela paraît correcte !

```
root@vmbourges-virtual-machine:/home/vm-bourges# systemctl status setkey
● setkey.service - option to manually manipulate the IPsec SA/SP database
     Loaded: loaded (/lib/systemd/system/setkey.service; disabled; vendor preset: enabled)
     Active: active (exited) since Tue 2020-11-17 13:43:41 CET; 33s ago
    Process: 1618 ExecStart=/etc/init.d/setkey start (code=exited, status=0/SUCCESS)
   Main PID: 1618 (code=exited, status=0/SUCCESS)

nov. 17 13:43:40 vmbourges-virtual-machine systemd[1]: Starting option to manually manipulate the IPsec SA/SP database...
nov. 17 13:43:40 vmbourges-virtual-machine setkey[1618]:  * Loading IPsec SA/SP database:
nov. 17 13:43:41 vmbourges-virtual-machine setkey[1618]:    ...done.
nov. 17 13:43:41 vmbourges-virtual-machine systemd[1]: Started option to manually manipulate the IPsec SA/SP database.
```

4.Modifier le fichier de configuration de VM2

Recommencez du paragraphe V.1 jusqu'au paragraphe V.3 mais pour VM2.

Attention aux paramètres « in » et « out » du fichier de configuration.

VI. Vérifier le réseau

Faites un ping de « VM1 » à « VM2 » en capturant les paquets réseaux.
Pour capturer les paquets, allez sur la machine réelle. Lancez « Wireshark » en capturant sur l'interface « VMNET8 »
Vérifiez qu'ils sont bien authentifiés et chiffrés entre « Vm1 » et « Vm2 ».

No.	Source	Destination	Protocol	Info
2	00:0c:29:70:e9:e4	00:0c:29:81:79…	ARP	192.168.37.135 is at 00:0c:29:70:e9:e4
3	192.168.37.134	192.168.37.135	ESP	ESP (SPI=0x000055dc)
4	192.168.37.135	192.168.37.134	ESP	ESP (SPI=0x00021980)
5	192.168.37.134	192.168.37.135	ESP	ESP (SPI=0x000055dc)

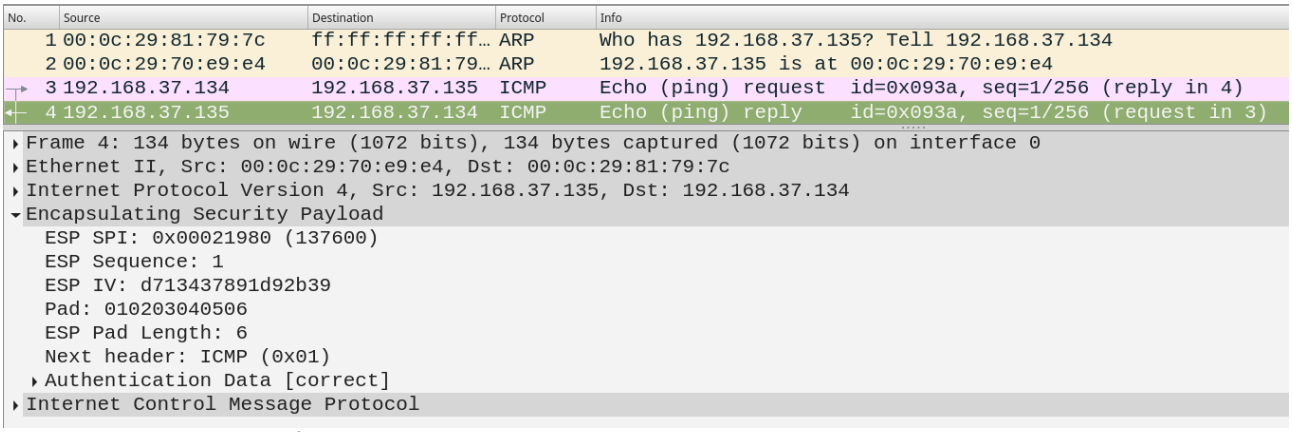
```
▸ Frame 4: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
▸ Ethernet II, Src: 00:0c:29:70:e9:e4, Dst: 00:0c:29:81:79:7c
▸ Internet Protocol Version 4, Src: 192.168.37.135, Dst: 192.168.37.134
▾ Encapsulating Security Payload
    ESP SPI: 0x00021980 (137600)
    ESP Sequence: 1
```

On voit que la charge utile « Payload » au dessus de IP est chiffrée en utilisant ESP.
Nommez votre fichier de capture « 001_crytpEspPing.pcapng » et déposez le sur « celene » dans le devoir à cet effet.
Faites une capture d'écran comme ci-dessus. Nommez-la « 002_cryptEspPing.png » et déposez-la sur « celene ».

VII. Authentifier et déchiffrer les paquets à la volée.

En utilisant les capacités de « Wireshark », (menu « Edit » → « Préférences »→

« Protocoles »→ « ESP »→ « Edit... »), donnez à « Wireshark » les moyens de déchiffrer vos paquets à la volée.
Ce que vous devez obtenir après déchiffrement :



Faites une capture d'écran comme ci-dessus.
Nommez-la « 003_deCryptEspPing.png » et déposez-la sur « celene ». On doit voir sur votre capture d'écran l'entête ESP suivi de ICMP.
Faites un fichier « 004_espPAD.docx » dans lequel vous expliquerez ce que signifie dans la capture « Wireshark » le champ « Pad : 010203040506 » et « ESP Pad Length ».
Vous expliquerez aussi pourquoi les trames « ARP » ne sont pas chiffrées.
Déposez le fichier « 004_espPAD.docx » sur « celene ».

VIII. Installer un serveur ftp sur VM1.

Sur la machine « VM1 », installez le serveur « ftpd » : apt install ftpd.
Modifiez le fichier « /etc/ipsec-tools.conf » de manière à ne chiffrer et authentifier que les paquets relatifs à la connexion cliente à partir de VM2 vers le serveur « ftp » sur VM1.
Les « pings » doivent pouvoir passer non chiffrés alors que les paquets ftp non « ftp-data » doivent être chiffrés par « ESP ».
Installez les outils « FTP » sur « VM2 », **« apt install ftp »** et configurez « /etc/ipsec-tools.conf » de VM2 en conséquence.
Lancez « Wireshark » sur « vmnet8 » de la machine réelle, faites une connexion ftp de VM2 vers le serveur ftp de VM1, et vérifiez que votre réglage est conforme.
Copier votre fichier « /etc/ipsec-tools.conf » **de la VM1** sur « Celene » sous le nom « 005_ipsecConfVm1.conf » .