Réseaux - TP
Sécurité de la couche 3 dans les réseaux

La sécurité des communications IP est un enjeu majeur, en particulier pour les connexions inter-sites ou entre dispositifs sur des réseaux non sécurisés. IPsec (*Internet Protocol Security*) est un protocole de sécurité réseau qui permet de protéger les communications au niveau de la couche réseau. Il permet de garantir l'authentification, l'intégrité, et la confidentialité des données échangées.

1 Objectifs

— Comprendre le fonctionnement d'IPsec.

— Configurer et de tester un tunnel sécurisé IPsec entre deux routeurs.

2 Consignes

Le temps de TP en salle réseau est limité. Je vous suggère donc de faire une fiche technique que vous construirez tout au long des TP avec toutes les commandes que vous jugerez pertinentes. Afin d'optimiser votre travail :

— Travaillez en groupe de deux binôme.

— Laissez votre poste dans l'état initial à la fin du TP.

3 IPsec

IPsec propose deux modes principaux pour assurer la sécurité des données : **AH** (*Authentication Header*) et **ESP** (*Encapsulating Security Payload*). AH garantit l'intégrité et l'authenticité des paquets IP, tandis qu'ESP offre des fonctionnalités supplémentaires de chiffrement pour assurer la confidentialité des données.

IPsec peut fonctionner en deux modes : le mode **transport** et le mode **tunnel** (ou VPN). Dans le mode transport, seul le contenu du paquet IP est protégé, tandis que dans le mode tunnel, l'intégralité du paquet IP est encapsulée dans un nouveau paquet IP, ce qui permet de créer des communications VPN (*Virtual Private Network*). Le mode tunnel peut être appliqué de deux manières : par **routage** (où le trafic est redirigé via les interfaces appropriées) ou par **politique** (où l'ACL spécifie explicitement les flux à protéger).

L'activation d'IPsec repose sur trois étapes essentielles :

1. **Choix du mode d'authentification :** IPsec offre plusieurs modes d'authentification pour la phase 1 de l'échange IKE (*Internet Key Exchange*). Ce TP utilise une clé pré-partagée pour l'authentification mutuelle, un mode sûr et recommandé. Le mode basé sur une clé publique non certifiée est obsolète et n'est pas pris en charge par IKEv2.
2. **Établissement des SA IKE (Phase 1) :** La phase 1 crée un canal sécurisé entre les deux pairs IPsec à l'aide du protocole IKE, en utilisant soit le *Main Mode*, soit l'*Aggressive Mode*[1].
3. **Établissement des SA IPsec (Phase 2) :** Dans cette phase, les paramètres de sécurité (algorithmes de chiffrement, d'authentification, etc.) sont définis pour protéger les flux de données spécifiés.

Dans ce TP, l'objectif est de mettre en œuvre une communication IPsec utilisant ESP, en mode tunnel, avec une authentification par clé pré-partagée et en appliquant des politiques de sécurité spécifiques aux flux à protéger.

1. Le Main Mode effectue un échange sécurisé en six messages, garantissant la confidentialité des identités des pairs et une négociation robuste des paramètres de sécurité. Bien que plus lent, il est idéal pour les scénarios nécessitant une sécurité renforcée. En revanche, l'Aggressive Mode, plus rapide avec seulement trois messages échangés, combine plusieurs étapes en une seule, mais expose les identités des pairs avant que le canal sécurisé soit établi, le rendant plus vulnérable aux attaques.

4 Mise en place du réseau

Branchez les équipements conformément au plan d'adressage suivant :

TABLE 1 – Plan d'adressage

Équipement	Interface	Adresse IP/Préf.	Description
VM1	net1	192.168.X.2/24	VM du groupe X
Routeur R1 (LAN)	GigabitEthernet0/1	192.168.X.1/24	Interface LAN du groupe X
Routeur R1 (WAN)	GigabitEthernet0/0	10.0.0.1/30	Interface WAN (vers SW1)
Switch SW1	GigabitEthernet1/0/1	N/A	Lien SW1 vers R1
Switch SW1	GigabitEthernet1/0/2	N/A	Lien SW1 vers R2
Switch SW1	GigabitEthernet1/0/3	N/A	Port mirroring vers poste 1 (net2)
Routeur R2 (WAN)	GigabitEthernet0/0	10.0.0.2/30	Interface WAN (vers SW1)
Routeur R2 (LAN)	GigabitEthernet0/1	192.168.Y.1/24	Interface LAN du groupe Y
VM2	net2	192.168.Y.2/24	VM du groupe Y

Configuration des VMs

— Ajoutez les adresses IP.

— Mettez l'interface correspondante en `up`.

— Ajoutez une route vers le LAN de vos voisins.

```
# Sur VM1 (Groupe X)
vm1@groupX:$ ip addr add 192.168.X.2/24 dev net1
vm1@groupX:$ ip link set net1 up
vm1@groupX:$ ip route add 192.168.Y.0/24 via 192.168.X.1

# Sur VM2 (Groupe Y)
vm2@groupY:$ ip addr add 192.168.Y.2/24 dev net2
vm2@groupY:$ ip link set net2 up
vm2@groupY:$ ip route add 192.168.X.0/24 via 192.168.Y.1
```

Configuration des routeurs

— Ajoutez les adresses IP.

— Mettez l'interface en `no shutdown`.

— Ajoutez les routes statiques pour les LANs.

```
# Sur R1 (Routeur du Groupe X)
Routeur> enable
Routeur# configure terminal
Routeur(config)# interface GigabitEthernet0/1
Routeur(config-if)# ip address 192.168.X.1 255.255.255.0
Routeur(config-if)# no shutdown
Routeur(config-if)# exit
Routeur(config)# interface GigabitEthernet0/0
Routeur(config-if)# ip address 10.0.0.1 255.255.255.252
Routeur(config-if)# no shutdown
Routeur(config-if)# exit
Routeur(config)# ip route 192.168.Y.0 255.255.255.0 10.0.0.2
Routeur(config)# exit

# Sur R2 (Routeur du Groupe Y)
Routeur> enable
Routeur# configure terminal
Routeur(config)# interface GigabitEthernet0/0
Routeur(config-if)# ip address 10.0.0.2 255.255.255.252
Routeur(config-if)# no shutdown
Routeur(config-if)# exit
Routeur(config)# interface GigabitEthernet0/1
Routeur(config-if)# ip address 192.168.Y.1 255.255.255.0
Routeur(config-if)# no shutdown
Routeur(config-if)# exit
Routeur(config)# ip route 192.168.X.0 255.255.255.0 10.0.0.1
Routeur(config)# exit
```

Configuration du switch

— Configurez le port mirroring pour observer le trafic (Wireshark, depuis le poste X).

```
# Sur SW1
Switch> enable
Switch# configure terminal

# Configuration du port mirroring (SPAN)
Switch(config)# monitor session 1 source interface
GigabitEthernet1/0/1
Switch(config)# monitor session 1 destination interface
GigabitEthernet1/0/3
```

Q.4.1 : Assurez-vous de la connectivité entre VM1 et VM2.

Q.4.2 : Assurez-vous de pouvoir observer le trafic entre VM1 et VM2 via le port mirroring (utiliser Wireshark).

5 Tunnel IPsec avec ESP

Q.5.1 : Quelle taille minimale doit avoir une clé symétrique chiffrant sur un réseau ?

Q.5.2 : Quelle taille minimale doit avoir une clé asymétrique RSA utilisée pour une procédure d'authentification mutuelle ?

Q.5.3 : Quelle taille minimale doit avoir une empreinte (haché) utilisée pour une procédure de signature ?

Configuration ISAKMP (Phase 1)

La phase 1 d'IPsec utilise le protocole IKE (*Internet Key Exchange*) pour établir un canal sécurisé entre les deux routeurs. Cette étape configure les paramètres de chiffrement, d'authentification et d'échange de clés. **ISAKMP (*Internet Security Association and Key Management Protocol*)** est le protocole sous-jacent utilisé par IKE pour la négociation et la gestion des clés de sécurité. Il fournit un cadre standardisé permettant d'établir, de négocier, de modifier et de supprimer les associations de sécurité (**Security Associations, SA**). Ces associations définissent les paramètres de sécurité (algorithmes de chiffrement, de hachage, etc.) utilisés pour protéger les communications entre les pairs IPsec.

Lorsque la méthode de clé partagée est utilisée pour configurer IPsec entre deux routeurs, il est essentiel de s'assurer que les deux routeurs possèdent la même clé. Cette clé symétrique, saisie manuellement sur chaque routeur, doit être gardée secrète et ne doit être utilisée que pour une paire de routeurs. Ce type de configuration est particulièrement adapté aux petits réseaux ou aux environnements expérimentaux, où les besoins de simplicité et de contrôle direct priment sur les mécanismes plus complexes comme les certificats.

Explication des commandes de configuration de phase 1 :

- `crypto isakmp enable` : Active le protocole IKE (Internet Key Exchange), permettant aux deux routeurs de négocier automatiquement les paramètres de sécurité nécessaires pour établir un canal sécurisé.
- `crypto isakmp policy 4` : Définit une politique ISAKMP avec une priorité (ici, 4). Les politiques avec la priorité la plus basse sont préférées.
- `encryption aes 128` : Spécifie l'algorithme de chiffrement utilisé pour protéger les données.
- `hash sha` : Définit l'algorithme de hachage utilisé.
- `authentication pre-share` : Indique que l'authentification mutuelle se fera à l'aide d'une clé pré-partagée.
- `group 5` : Configure le groupe Diffie-Hellman utilisé pour l'échange de clés. Le groupe 5 correspond à une taille de clé de 1536 bits.
- `lifetime 300` : Définit la durée de vie de l'association de sécurité IKE (SA IKE) à 300 secondes. Les deux routeurs doivent avoir la même valeur pour garantir la compatibilité.

— `crypto isakmp identity address` : Configure l'identification des pairs basée sur leur adresse IP plutôt que sur leur nom.

— `crypto isakmp key 0 0123abcd address 10.0.0.1 (ou 10.0.0.2)` : Configure une clé pré-partagée pour l'authentification mutuelle. Cette clé doit être identique sur les deux routeurs. L'adresse IP correspond à celle du pair avec lequel établir la connexion sécurisée.

```
Routeur> enable
Routeur# configure terminal
Routeur(config)# crypto isakmp enable
Routeur(config)# crypto isakmp policy 4
Routeur(config-isakmp)# encryption aes 128
Routeur(config-isakmp)# hash sha
Routeur(config-isakmp)# authentication pre-share
Routeur(config-isakmp)# group 5
Routeur(config-isakmp)# lifetime 300
Routeur(config-isakmp)# exit
Routeur(config)# crypto isakmp identity address
Routeur(config)# crypto isakmp key 0 0123abcd address 10.0.0.1 (ou
10.0.0.2)
```

Pour visualiser vos configurations, vous pouvez utiliser :

```
Routeur# show crypto isakmp policy
Routeur# show crypto isakmp key
```

Q.5.4 : Visualisez vos configurations. Qu'observez-vous ?

Pour vérifier la configuration de la phase 1, vous pouvez utiliser :

```
Routeur# show crypto isakmp sa
```

Q.5.5 : Qu'observez-vous en visualisant les SA ?

Il est possible de résoudre les problèmes pour la configuration d'ISAKMP en observant les messages :

```
Routeur# debug crypto isakmp
```

Vous pouvez également supprimer les anciennes SA en cas de reconfiguration :

```
Routeur# clear crypto sa Routeur# clear crypto isakmp
```

Configuration de la phase 2 (flux)

La phase 2 configure les paramètres utilisés pour protéger un flux de trafic utilisateur. Les étapes à suivre sont les suivantes :

— **Définir une access-list appropriée :** Cela consiste à spécifier les types de flux sur lesquels la sécurité IPsec s'appliquera.

— **Choisir les protocoles de sécurité :** Sélectionner les protocoles de chiffrement et d'intégrité (comme ESP ou AH) pour la phase 2 d'IPsec.

— **Choisir le mode de fonctionnement :** Déterminer si IPsec fonctionnera en mode tunnel (où tout le paquet IP est encapsulé) ou en mode transport (où seule la charge utile est protégée).

— **Configurer les crypto-map :** Les crypto-maps spécifient les informations nécessaires à la création du tunnel IPsec, notamment le type de trafic à sécuriser, les politiques de sécurité et les pairs IPsec.

Configuration des ACLs

```
# Sur chaque routeur
Routeur(config)# access-list 100 permit icmp 192.168.X.0 0.0.0.255
192.168.Y.0 0.0.0.255
Routeur(config)# access-list 100 permit icmp 192.168.Y.0 0.0.0.255
192.168.X.0 0.0.0.255
```

Pour visualiser vos configurations, vous pouvez utiliser :

```
Routeur# show access-lists 100
```

Q.5.6 : Pourquoi faut-il définir deux access-lists sur chaque routeur ?

Configuration des `transform-set`

— `crypto ipsec transform-set myset esp-aes 128 ah-sha-hmac` : Définit les algorithmes de chiffrement et d'authentification utilisés. Le nom `myset` est un identifiant arbitraire pour le transform set.

— `mode tunnel` : Spécifie le mode IPSec choisi. Par défaut, sur les routeurs Cisco, il s'agit du mode tunnel, où l'intégralité du paquet IP est encapsulée.

```
# Sur chaque routeur
Routeur(config)# crypto ipsec transform-set myset esp-aes 128
ah-sha-hmac
Routeur(config-transform-set)# mode tunnel
Routeur(config-transform-set)# exit
```

Configuration de la `crypto-map`

L'ACL définit quel trafic doit être protégé par IPsec. La `crypto map` associe ces paramètres à une interface WAN, liant les paramètres définis en phase 2 aux pairs IPsec.

— `crypto map vpnge0 1 ipsec-isakmp` : Crée une crypto-map et associe le protocole ISAKMP pour l'échange automatique des paramètres de sécurité entre les routeurs. `vpnge0` est un identifiant arbitraire donné à la crypto-map.

— `set PFS` : Active le Perfect Forward Secrecy (PFS) pour une meilleure sécurité en générant une nouvelle clé Diffie-Hellman pour chaque session.

— `match address 100` : Associe la crypto-map à l'ACL 100, qui spécifie le trafic à sécuriser avec IPsec.

— `set peer 10.0.0.1 (ou 10.0.0.2)` : Indique l'adresse IP du pair (le routeur distant) avec lequel établir la connexion sécurisée. Cette adresse est celle du destinataire des paquets chiffrés.

— `set transform-set myset` : Associe le transform set `myset` à la crypto-map. Ce transform set contient les algorithmes de sécurité définis précédemment.

— `set security-association lifetime seconds 300` : Définit la durée de vie de la SA IPsec à 300 secondes. Cette valeur doit être identique sur les deux routeurs.

```
# Sur chaque routeur
Routeur(config)# crypto map vpnge0 1 ipsec-isakmp
Routeur(config-crypto-map)# set PFS
Routeur(config-crypto-map)# match address 100
Routeur(config-crypto-map)# set peer 10.0.0.1 (ou 10.0.0.2)
Routeur(config-crypto-map)# set transform-set myset
Routeur(config-crypto-map)# set security-association lifetime
seconds 300
Routeur(config-crypto-map)# exit
```

Application de la `crypto-map` sur l'Interface WAN

Cette étape active IPsec sur le lien entre les deux routeurs en appliquant la `crypto map` sur l'interface WAN.

— `crypto map vpnge0` : Applique la crypto-map `vpnge0` à l'interface WAN pour activer IPsec sur ce lien.

```
# Sur chaque routeur
Routeur(config)# interface GigabitEthernet0/0
Routeur(config-if)# crypto map vpnge0
Routeur(config-if)# exit
```

Pour vérifier la configuration de la phase 2, vous pouvez utiliser :

```
Routeur# show crypto map
```

Q.5.7 : Qu'observez-vous en visualisant la `crypto map` ?

Il est possible de résoudre les problèmes pour la configuration de phase 2 en observant les messages :

```
Routeur# debug crypto ipsec
```

Q.5.8 : Effectuez des pings entre vos VMs. Capturez le trafic sur le poste X (eth2) avec Wireshark. Qu'observez-vous ?

Q.5.9 : Effectuez des pings entre vos VMs. Capturez le trafic sur VM1 (eth1) avec Wireshark. Qu'observez-vous ?

Q.5.10 : À partir de l'analyseur, identifier les protocoles mis en jeu lors de l'établissement du VPN IPsec entre les deux routeurs.

Q.5.11 : Quel mode est choisi pour la phase 1 : agressive ou main ?

Q.5.12 : Est-ce que le trafic ping transite via le VPN IPsec ? Quels éléments permettent de vous en assurer ?

Q.5.13 : Donner les éléments de trafic permettant de vérifier le mode utilisé par IPsec (transport ou tunnel).

Une spécificité des routeurs Cisco est que chaque paquet autorisé par cette ACL 100 (permit) associée à la crypto-map est envoyé dans la transformation IPsec ; le reste du trafic est envoyé en clair.

Q.5.14 : Pourquoi le trafic web est-il toujours possible ?

6 Configuration IPsec pour HTTP

Q.6.1 : Modifiez votre configuration IPsec pour chiffrer le trafic HTTP plutôt qu'ICMP. Expliquez vos modifications.

Q.6.2 : Modifiez votre configuration IPsec pour chiffrer le trafic HTTP plutôt qu'ICMP. Expliquez vos modifications.

Q.6.3 : Illustrez vos modifications avec Wireshark.

7 Configuration IPsec avec AH

Q.7.1 : Modifiez votre configuration IPsec pour utiliser AH plutôt qu'ESP. Expliquez vos modifications.

8 Utilisation de clefs RSA pour 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.

1. Modifier la politique de la configuration précédente en spécifiant comme paramètre d'authentification "rsa-sig" (`authentication [rsa-sig | rsa-encr | pre-share]`).
2. Créer des clefs et visualiser 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.

`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. Enregistrer 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*

> Q8.1 : Après avoir modifié la configuration, vérifiez la communication entre les deux VMs (ping / HTTP).

NB : La transmission manuelle de la clef publique du routeur distant est fastidieuse. Il existe une méthode utilisant une Autorité de Certification (CA) 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.

> Q8.2 : En comparant avec l'utilisation de PSK, quels sont les avantages liés à l'utilisation d'une CA d'un point de vue sécurité ?