TP N°4 Réseaux 2A - Sécurisation des réseaux IP avec IPSec
Module TR-C8

1. Présentation d'IPSec

Selon la RFC de IETF : IPSec est un protocole de sécurité au sein de la couche réseau, qui a été développé pour fournir un service de sécurité à base de cryptographie, permettant de garantir *l'authentification*, *l'intégrité*, le contrôle d'accès et la *confidentialité* des données.

D'une manière plus commune : IPSec = ***formatage de trame permettant le chiffrement des données au niveau IP***.

Il existe deux types de transformations de données pour IPSec :

- **Authentification Header (AH):**

  Paquet origine : IP Header + le reste du paquet (autres headers + payloads) = A

  A l'aide de l'algorithme MD5, la clef secrète (connue des deux parties) + A on obtient :

  IP Header + AH + reste du paquet (autres headers + payloads)

  ⇒ Avec AH : pas de confidentialité = pas de chiffrement

- **Encapsulating Security Payload (ESP):**

  Paquet origine : IP Header + le reste du paquet (autres headers + payloads) = A

  1. Si on est en *mode transport* (mode de bout en bout, entre hosts ⇒ pas de routeur ni firewall entre les hosts) :

     On chiffre le "reste du paquet (autres headers + payloads)" avec la clef secrète, et on ajoute au paquet un header ESP.

     Le paquet devient donc :

     IP Header + Header ESP + reste du paquet (autres headers + payloads) crypté

  2. Si on est en *mode tunnel* (avec des routeurs + des firewalls entre hosts ⇔ Internet) :

     De nouveaux IP headers sont rajoutés lors du routage des paquets, mais le paquet origine est crypté avec la clef secrète ⇒ Le IP header d'origine est conservé intacte dans la partie cryptée.

     Le paquet devient donc :

     New Ip Header + Header ESP + Crypté [Ip Header origine + reste du paquet (autres headers + payloads)]

  ⇒ Avec ESP : confidentialité car on a chiffrement des données.

Les associations de sécurité (SA) :
Une SA est une relation à sens unique (unilatérale) entre un émetteur et un destinataire. Elle définit l'ensemble des opérations IPSec devant être appliquées aux paquets. Une SA doit être définie dans chaque direction.

IKE (Internet Key Exchange): (RFC 2409)

IKE négocie les IPSec associations de sécurité (SAs). Ce processus nécessite que les systèmes IPSec *s'authentifient* entre eux et *établissent les clefs* IKE (= ISAKMP) partagées.

En d'autres termes, IKE = Schéma de chiffrement ⇔ ***comment va se faire l'échange des informations entre les différents peers d'un VPN***.

Schématiquement :

IKE = ISAKMP (RFC 2408) + Oakley (RFC 2412)

→ ISAKMP = protocole pour la négociation préalable à l'établissement des associations de sécurité.

→ Oakley = détermine le mécanisme pour l'échange automatique des clefs, le partage, de façon sûre entre les tiers, d'un ensemble d'informations relatives au chiffrement.

→ IKE démarre donc avant IPSec.

- On a un *tunnel IKE* en premier,
- Puis un *tunnel IPSec* ensuite (ce dernier étant issu des négociations IKE préalables).

ISAKMP = IKE phase 1 :

Les sessions ISAKMP utilisent UDP (source & destination port = 500)

Les résultats de l'établissement d'une session ISAKMP sont des SAs ISAKMP bidirectionnelles.

Une session ISAKMP est authentifiée :
- soit par une clef partagée (*pre-shared key*)
- soit par RSA signature et chiffrement.

Oakley = IKE phase 2 :

Définit le mécanisme d'échange de clefs dans les SAs ISAKMP

Détermine les clefs AH/ESP nécessaires pour chaque IPSec SA

Utilise l'algorithme Diffie-Hellman pour ses générations de clefs.

IKE, en résumé :

Phase 1 d'IKE, il y a authentification des peers + établissement de la politique IKE (= IKE SA). L'algorithme principal de cette phase est Diffie-Hellman.

Phase 2, d'IKE, il y a négociation des SA IPSec, et génération des clefs pour IPSec, L'émetteur offre une ou plusieurs *transform-sets* qui sont utilisés pour spécifier les différents algorithmes utilisés au sein du tunnel IPSec. ***En d'autres termes, une SA IPSec c'est ce qui définit un VPN.***

IKE, en détails :

- Phase 1 d'IKE :
  - Méthode d'échange des clefs ;
  - Méthode d'authentification des peers : pre-shared Key ou certificats numérique authentifié par une signature RSA ;
  - Détermination de la politique ISAKMP ⇔ *IPSEc SA* : Pour qu'il y ait communication IPSec possible, il faut que les 2 peers trouvent un accord sur une politique ISAKMP commune. Une politique ISAKM contient :
    - Algorithme d'encryption : DES/3-DES
    - Algorithme de hachage : MD5/SHA-1
    - IKE SA Life time = durée de vie des SA IKE : 86400 secondes au moins.

- Phase 2 d'IKE :
  - Négociation des algorithmes IPSec = transform-set : ESP-DES, …

    → Cette négociation est protégée grâce à la SA IKE prédéfinie
  - Identification des peers par adresse IP ou nom ;
  - Détermination des adresses IP des hôtes qui doivent communiquer en crypté ;
  - Etablissement des IPSec SA soit de manière manuelle (pas conseillé), soit via IKE (conseillé). Dans ce dernier cas, il faut spécifier ***ipsec-isakmp***.
    - Ces IPSec SA sont périodiquement renégociées afin d'augmenter le niveau de sécurité ;
    - On peut forcer le fait que les clefs de sessions IPSec seront novelles à chaque fois, ou simplement dérivées des clefs négociées en IKE Phase 1.
  - Le contenu d'une IPSec SA est le suivant :
    - Adresse IP du peer d'en face ;
    - Identifiant du VPN (SPI = Security Parameter Index)
    - Algorithme IPSec : AH / ESP + rien ou HMAC-MD5/HMC-SHA1 ;
    - Mode (Tunnel ou Transport) :
      1. Transport : PC à serveur de bout en bout
      2. Tunnel : via Internet (c'est-à-dire via des routeurs)
    - Clef de session

2. Objectifs du TP

Le TP à pour objectif de mettre en œuvre les différentes phases de configuration d'un routeur Cisco pour la mise en place d'un tunnel IPSec entre deux réseaux locaux via deux routeurs Cisco.

IPSec sera paramétré en **mode de gestion automatique** (avec *un secret pré-partagé*) des clefs basé sur le protocole ISAKMP.

2.1. Travail à réaliser

Considérant la topologie donnée ci-dessous. Le trafic à sécuriser correspond aux données échangées entre les deux sous-réseaux 10.0.1.0 et 10.0.2.0, les hôtes IPSec (**peer**) restant les deux interfaces des routeurs en 192.168.1.1 et 192.168.1.2.

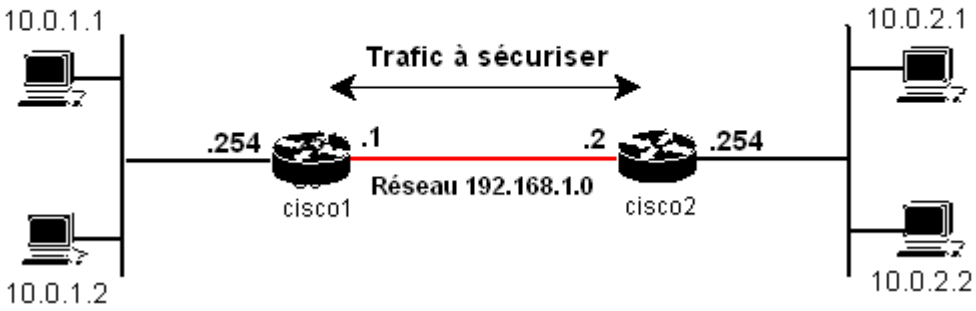
Réalisez la configuration d'IPSec sur les deux routeurs :

a) en mode automatique avec un secret pré-partagé via le protocole ISAKMP.

Les critères de configuration d'IPSec à mettre en place sont :

- Chiffrement et authentification avec le protocole ESP,
- Mode tunnel,
- Les algorithmes de chiffrement et d'authentification sont DES et MD5.

Une fois le tunnel IPSec mis en place, lancez un ping entre les deux machines et visualisez les SA établies ainsi que certaines informations de l'échange.



3. Configuration

La configuration d'IPSec s'effectue généralement en suivant les étapes ci-dessous :

1. **Configuration de la politique d'ISAKMP** de la phase 1 (algorithmes, clés, durée de vie du tunnel ISAKMP) se trouveront à la suite de la ligne de configuration commençant par ***crypto isakmp*** ;
2. **Configuration de la SA IPSec** de la phase 2 (protocoles AH/ESP, algorithmes, durée de vie du tunnel IPSec) se trouveront à la suite de la ligne de configuration commençant par ***crypto ipsec*** ;
3. **Description d'une carte de cryptage (crypto map)** rassemblant les paramètres des deux phases, l'extrémité du tunnel et la définition du trafic à sécuriser se trouvera à la suite de la ligne de configuration commençant par ***crypto map***.

Note importante : Les configurations des deux routeurs doivent être cohérentes et symétriques l'une par rapport à l'autre.

3.1. Configuration d'IKE

Pour configurer IKE, il faut réaliser les taches ci-dessous.

- Activation ou désactivation d'IKE ;
- Configuration de la politique d'IKE (phase 1) ;
- Configuration de l'authentification mutuelle par clé pré-partagée .

3.1.1 Activation ou désactivation d'IKE

IKE est activé par défaut. Il est activé globalement pour toutes les interfaces sur le routeur. Si IKE est désactivé, vous devrez faire les configurations suivantes sur les hôtes IPSec :

Router (config)# **no crypto isakmp enable** → désactive IKE.
Router (config)# **crypto isakmp enable** → active IKE.

3.1.2 Configuration des paramètres de la SA ISAKMP

Vous devez créer une politique d'IKE à chaque hôte IPSec : une combinaison des paramètres de sécurité à employer ; le tableau ci-dessous indique la liste de ces paramètres. Elle indique quels paramètres de sécurité seront employés pour protéger les négociations suivantes et précise également comment les deux hôtes IPSec seront authentifiés.

Paramètre	Valeurs acceptées	Key Word	Valeurs par défaut
algorithme d'encryption	56-bit DES-CBC 168-bit DES	**Des** **3des**	56-bit DES-CBC 168-bit DES
algorithme de hachage	SHA-1 (HMAC variant) MD5 (HMAC variant)	**Sha** **md5**	SHA-1
méthode d'authentification	Signatures RSA Chiffrement RSA Clés pré-partagées	**rsa-sig** **rsa-encr** **pre-share**	RSA signatures
groupe Diffie-Hellman	768-bit Diffie-Hellman 1024-bit Diffie-Hellman	**1** **2**	768-bit Diffie-Hellman
durée de vie de la SA	Spécifier une valeur	-	86400 seconds

Ci-dessous les étapes nécessaires à la configuration des paramètres de SA IKE :

	Commande	Description
étape 1	Router (config)# **crypto isakmp policy** priority	Identifies the policy to create.
étape 2	Router (config-isakmp)# **encryption** {**des** | **3des**}	Specifies the encryption algorithm.
étape 3	Router (config-isakmp)# **hash** {**sha** | **md5**}	Specifies the hash algorithm.
étape 4	Router (config-isakmp)# **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}	Specifies the authentication method.
étape 5	`Router (config-isakmp)#group {1|2}`	Specifies the Diffie-Hellman group.
étape 6	Router (config-isakmp)# **lifetime** seconds	Specifies the SA's lifetime.
étape 7	Router (config-isakmp)# **exit**	Exits the config-isakmp command mode.
étape 8	Router (config)# **exit**	Exits the global configuration mode.
étape 9	Router# **show crypto isakmp policy**	(Optional) Displays all existing IKE policies.

A l'issue de cette négociation, un tunnel sécurisé (phase 1 du protocole IKE) est établi. Désormais, la politique de sécurité de phase 2 (SA IPSec) sera négocié à travers ce tunnel ISAKMP.

3.1.3 Configuration de l'authentification par clé pré-partagée

Pour configurer les clés pré-partagées, vous devez suivre les étapes ci-dessous sur chaque hôte IPSec qui utilise des clés pré-partagées dans sa politique d'IKE en mode de configuration globale :

	Commande	Description
étape 1	Router-local-peer (config)# **crypto isakmp key** keystring **address** peer-address	**At the local peer**: Specifies the shared key to be used with a particular remote peer. If the remote peer specified their ISAKMP identity with an address, use the **address** keyword in this step;
étape 2	Router-remote-peer (config)# **crypto isakmp key** keystring **address** peer-address	**At the remote peer**: Specifies the shared key to be used with the local peer. This is the same key you just specified at the local peer. If the local peer specified their ISAKMP identity with an address, use the **address** keyword in this step;

3.2. Configuration des paramètres IPSec (transform-set)

Une fois la négociation de la phase 1 faite, vous devez configurer les paramètres de négociation pour la phase 2. Il s'agit de définir une transformation qui explicite les algorithmes IPSec (AH et/ou ESP) nécessaires pour la mise en œuvre du tunnel IPSec. Le tableau ci-dessous définit la liste des transformations disponibles. Le nom de la transformation est suivi de la commande **crypto ipsec transform-set**. Les transform-sets doivent être identiques aux deux paires.

Transform Type	Transform	Description
AH Transform	**ah-md5-hmac**	AH with the MD5 authentication algorithm
	ah-sha-hmac	AH with the SHA authentication algorithm
ESP Encryption Transform	**esp-des**	ESP with the 56-bit DES encryption algorithm
	esp-3des	ESP with the 168-bit DES encryption algorithm
	esp-null	Null encryption algorithm
ESP Authentication Transform	**esp-md5-hmac**	ESP with the MD5 authentication algorithm
	esp-sha-hmac	ESP with the SHA authentication algorithm

	Commande	Description
étape 1	Router (config)# **crypto ipsec transform-set** transform-set-name transform1 [transform2 [transform3]]	Defines a transform set. .
étape 2	Router (cfg-crypto-tran)# **mode** [**tunnel** | **transport**]	(Optional) Changes the mode associated with the transform set.
étape 3	Router (cfg-crypto-tran)# **exit**	Exits the crypto transform configuration mode.
étape 4	Router (config)# **clear crypto sa** or Router (config)# **clear crypto sa peer** { ip-address | peer-name} or Router (config)# **clear crypto sa map** map-name or Router (config)# **clear crypto sa entry** destination-address protocol spi	Clears existing IPSec security associations so that any changes to a transform set will take effect on subsequently established security associations.(Manually established SAs are reestablished immediately.) Using the **clear crypto sa** command without parameters will clear out the full SA database, which will clear out active security sessions. You may also specify the **peer**, **map**, or **entry** keywords to clear out only a subset of the SA database.

3.3. Configuration de la crypto map

La carte de cryptage (ou crypto map) permet de lier les SA négociées et la politique de sécurité (SP : Security Policy). En d'autres termes, elle permet de renseigner :

- Quel trafic devrait être protégé par IPSec ;
  → Utiliser les listes d'accès
- L'autre extrémité du tunnel vers lequel le trafic IPSec devrait être envoyé ;
- L'adresse locale à employer pour le trafic d'IPSec ;
  → Lier la carte de cryptage à une interface du routeur
- Quelle sécurité d'IPSec devrait être appliquée à ce trafic (transform-sets) ;

Pour créer les différentes entrées de la carte de cryptage, qui emploieront IKE pour établir les associations de sécurité, procédez comme suit en suivant les étapes du tableau ci-dessous.

	Commande	Description
étape 1	Router (config)# **crypto map** map-name seq-num **ipsec-isakpm**	Indique la crypto map à créer.
étape 2	Router (config-crypto-m)# **match address** access-list-id	Spécifie le trafic à sécuriser.
étape 3	Router (config-crypto-m)# **set peer** {hostname | ip-address}	Spécifie l'autre extrémité du tunnel IPSec.
étape 4	Router (config-crypto-m)# **set transform-set** transform-set-name1[transform-set-name2...transform-set-name6]	Applique le modèle de transformation a la carte de cryptage.
étape 5	Router (config-crypto-m)# **set security-association lifetime seconds** seconds	Durée de vie de du tunnel IPSec (optionnel).
étape 7	Router (config-crypto-m)# **exit**	

Configuration des listes d'accès

Il faut configurer une liste d'accès qui définit le trafic à sécuriser. Ces listes d'accès sont différentes des ACL qui déterminent quel trafic à expédier ou bloquer sur une interface. C'est l'entrée de la crypto

map référençant la liste d'accès qui décide si le traitement d'IPSec est appliqué au trafic en fonction de l'action (**permit** et/ou **deny**) définie dans la liste d'accès.

Remarque : *Si vous voulez définir divers traitement d'IPSec (par exemple, uniquement de l'authentification pour un certain trafic, authentification et chiffrement pour tout autre trafic), vous devez créer deux listes d'accès différentes associés aux deux types de trafic. Ces différentes listes d'accès sont alors employées dans différentes cryptos map qui indiquent différentes politiques d'IPSec.*

Application des crypto map aux interfaces :

Il faut lier la crypto map ainsi définie à une interface du routeur par laquelle le trafic d'IPSec passera. Tout trafic arrivant ou sortant de cette interface est comparé avec le trafic à sécuriser défini dans une liste d'accès: s'il y a correspondance ce dernier est chiffré.

Pour appliquer une crypto map à une interface: Router (config-if) # **crypto map** map-name