Protocole IPSec

Introduction: Le protocole IP Sec, développé par l'IETF (**Internet Engineering Task Force)**,
il a pour but de:

'Sécuriser TCP/IP par **l'authentification** et le **chiffrement** des paquets IP afin de protéger les transmissions de données'

Motivation: Les utilisateurs ont des problèmes de sécurité transversaux aux couches de protocoles.
La communauté Internet a développé des mécanismes de sécurité dans:
Courrier électronique, Client/Serveur (Kerberos), les accès web (SSL)

Solution: Sécurité au niveau IP avec le protocole **IPSec**

- Elle concerne 3 zones fonctionnelles:
- **Authentification**
- **Confidentialité**
- **Gestion des clés**

IPSec fournit la possibilité de sécuriser les transmissions de: réseaux LAN, et WAN

Exemples d'utilisation

- Sécuriser une connexion de succursale sur Internet
- Accès à distance sécurisé sur Internet
- Etablir des liens Intranet et Extranet aves des partenaires
- Améliorer la sécurité du e-commerce

Avantages d'IPSec

- IPSec est associé à un pare-feu ou à un routeur
- Il fournit une sécurité forte qui peut être appliquée à tout le trafic traversant le périmètre
- IPSec dans un pare-feu résistera aux tentatives de contournement
- IPSec est au dessous de la couche transport TCP, UDP
- Il est transparent aux applications & aux utilisateurs

IPSEC a pour vocation d'établir des canaux communications sécurisés garantissant l'**intégrité** et la **confidentialité** des données véhiculées au niveau de la couche IP.

Ses principales implémentations se retrouvent dans les logiciels et les matériels créant des VPN.

Utilité en pratique:

Sécuriser une liaison entre deux réseaux locaux, en passant par un réseau non sécurisé.

Le moyen utilisé était du créer un **tunnel VPN** en utilisant IP Sec.

Fonctionnement

1. Mode de transport

Il existe deux modes pour IPSec :

- Le mode transport qui permet de protéger principalement les protocoles de niveaux supérieurs :

  – IPSec récupère les données venant de la couche 4 (**TCP/transport**), les signe et les crypte puis les envoie à la couche 3 (**IP/réseau**).

  Cela permet d'être transparent entre la couche TCP et la couche IP et d'être relativement facile à mettre en place.

  – Il y a des inconvénients :

  l'entête IP est produite par la couche IP et donc IPSec ne peut pas la contrôler.

2. Le mode tunnel

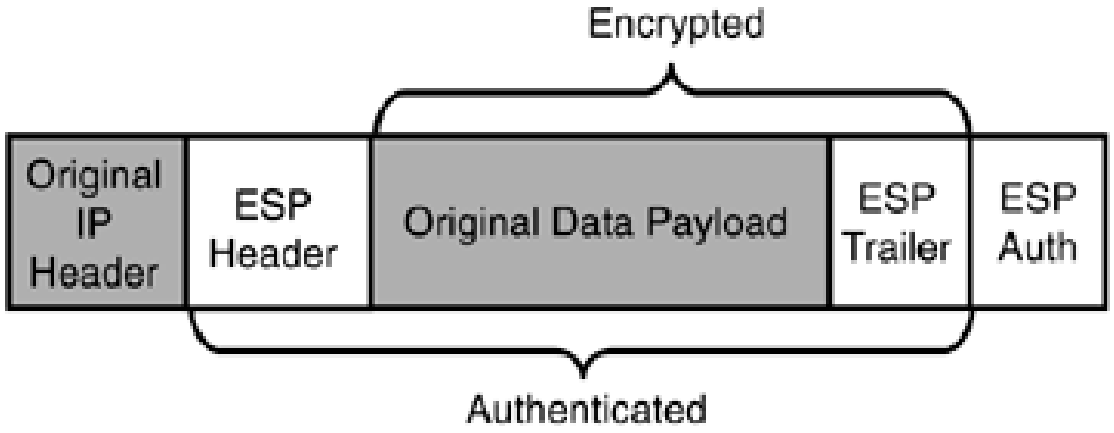
Il permet d'encapsuler des datagrammes IP dans des datagrammes IP

- les paquets descendent dans la pile jusqu'à la couche IP et c'est la couche IP qui passe ses données à la couche IPSec.
- Il y a donc une entête IP encapsulée dans les données IPSec et une entête IP réelle pour le transport sur Internet
- Aavantages :
  - l'entête IP réelle est produite par la couche IPSec.
    Cela permet d'encapsuler une entête IP avec des adresses relatives au réseau virtuel et en plus de les crypter de façon à être sûr qu'elles ne sont pas modifiées.
  - On a des adresses IP virtuelles tirant partie au mieux du concept de VPN
  - On a le contrôle total sur l'entête IP produite par IPSec pour encapsuler ses données et son entête IPSec.

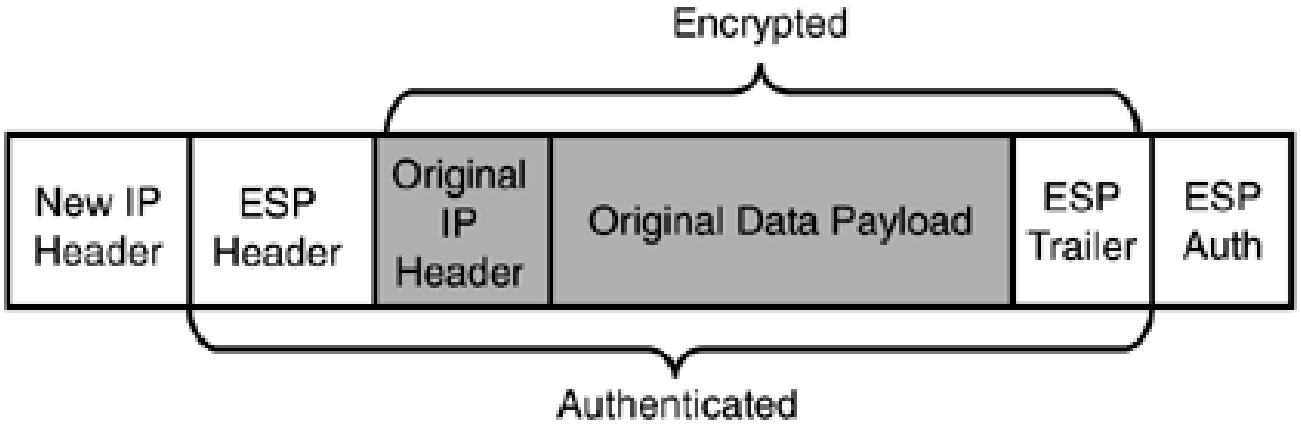
Le protocole IPSec est basé sur **différents modules** :

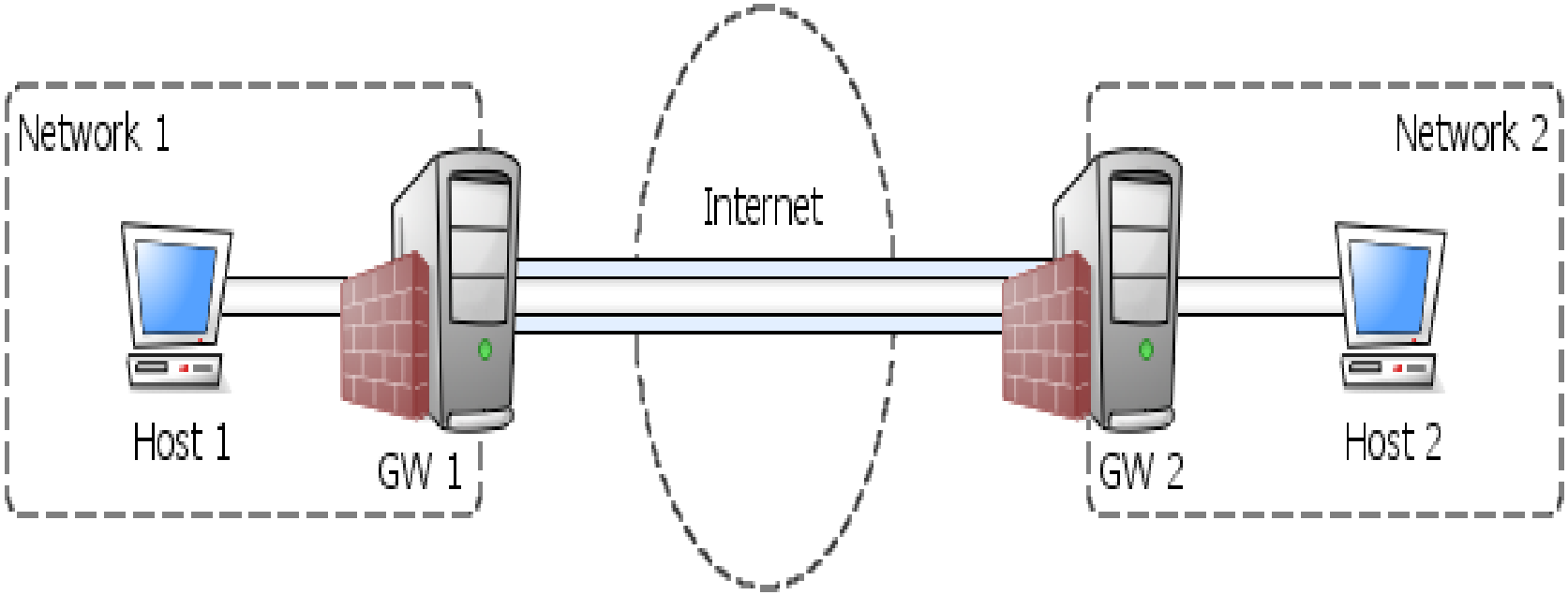
- ***IP Authentification Header*** (**AH**) gère
  - l'intégrité : on s'assure que les champs restent invariants pendant la transmission, dans l'entête IP qui précède l'entête AH et les données
  - l'authentification pour s'assurer que l'émetteur est bien celui qu'il dit être
  - la protection contre le rejeu : un paquet intercepté par un pirate ne peut pas être renvoyé
  - il ne gère pas la confidentialité : les données sont signées mais pas cryptées
- ***Encapsulating Security Payload*** (**ESP**)
  - **en mode transport**, il assure
    - confidentialité : les données du datagramme IP encapsulé sont cryptées
    - authentification : on s'assure que les paquets viennent bien de l'hôte avec lequel on communique (qui doit connaître la clé associée à la communication ESP pour s'authentifier)
    - l'unicité optionnelle contre le rejeu des paquets
    - l'intégrité des données transmises
  - **en mode tunnel**, c'est l'ensemble du datagramme IP encapsulé dans ESP qui est crypté et subit des vérifications.

Mode transport

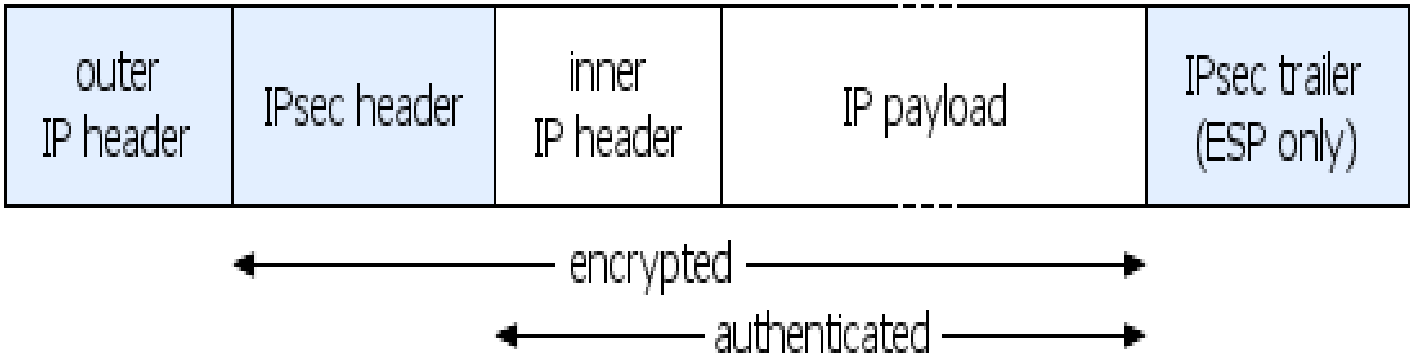


Mode tunnel





Tunnel-mode encapsulation:



Security Association (SA)

- ***Security Assocation*** (**SA**) définit l'échange des clés et des paramètres de sécurité.
- Il existe une SA par sens de communication.
- Les paramètres de sécurité sont les suivants:

  - **protocole AH et/ou ESP**
  - **mode tunnel ou transport**
  - **les algorithmes de sécurité**
  - **les clés**

La **SAD (*Security Association Database*)** stocke les SA afin de savoir comment traiter les paquets arrivant ou partant.

Elles sont identifiées par des triplets :

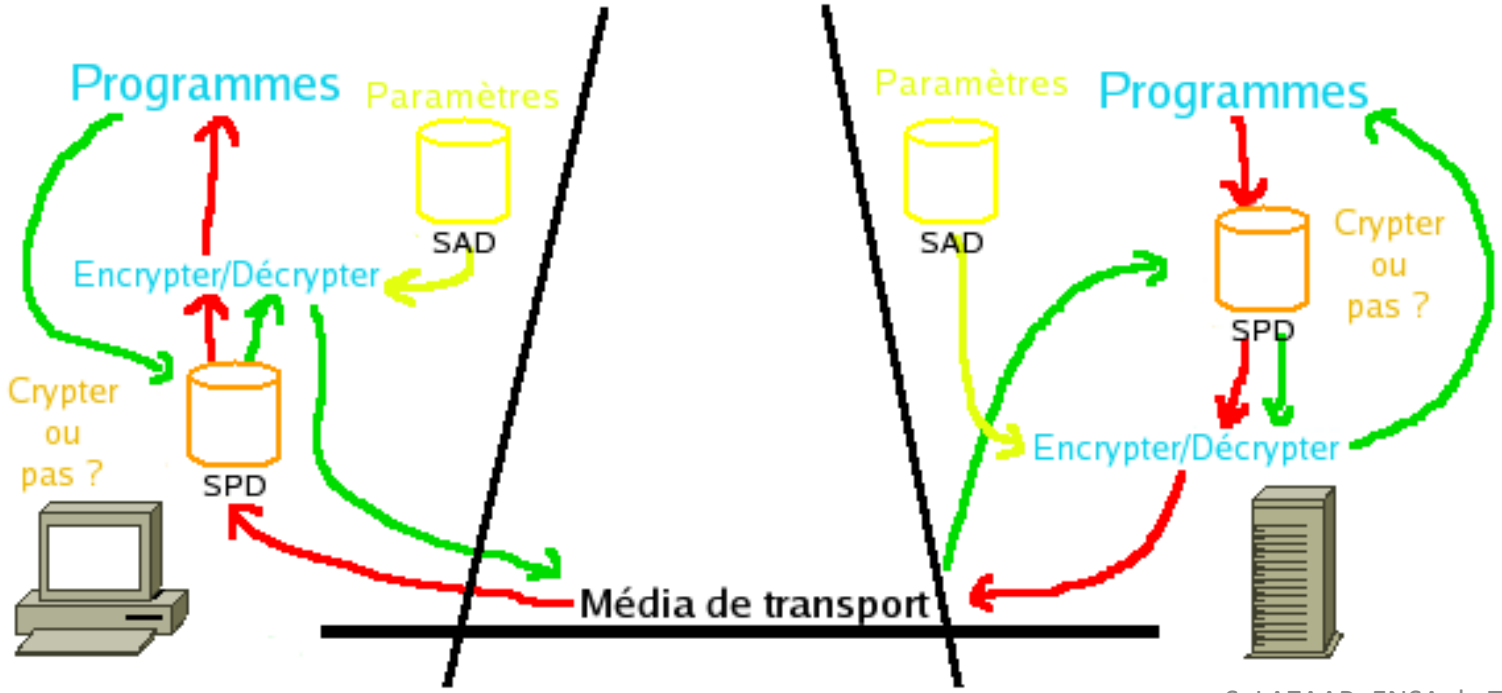
- adresse de destination des paquets
- identifiant du protocole AH ou ESP utilisé
- un index des paramètres de sécurité (Security Parameter Index) qui est un champ de 32bits envoyer en clair dans les paquets

La SPD (Security Policy Database) est la base de configuration de IPSec.

- Elle permet de dire au noyau quels paquets il doit traiter.

  C'est à sa charge de savoir avec quel SA il fait le traitement.

- La SPD indique quels paquets il faut traiter et le SAD indique comment il faut traiter un paquet sélectionné.



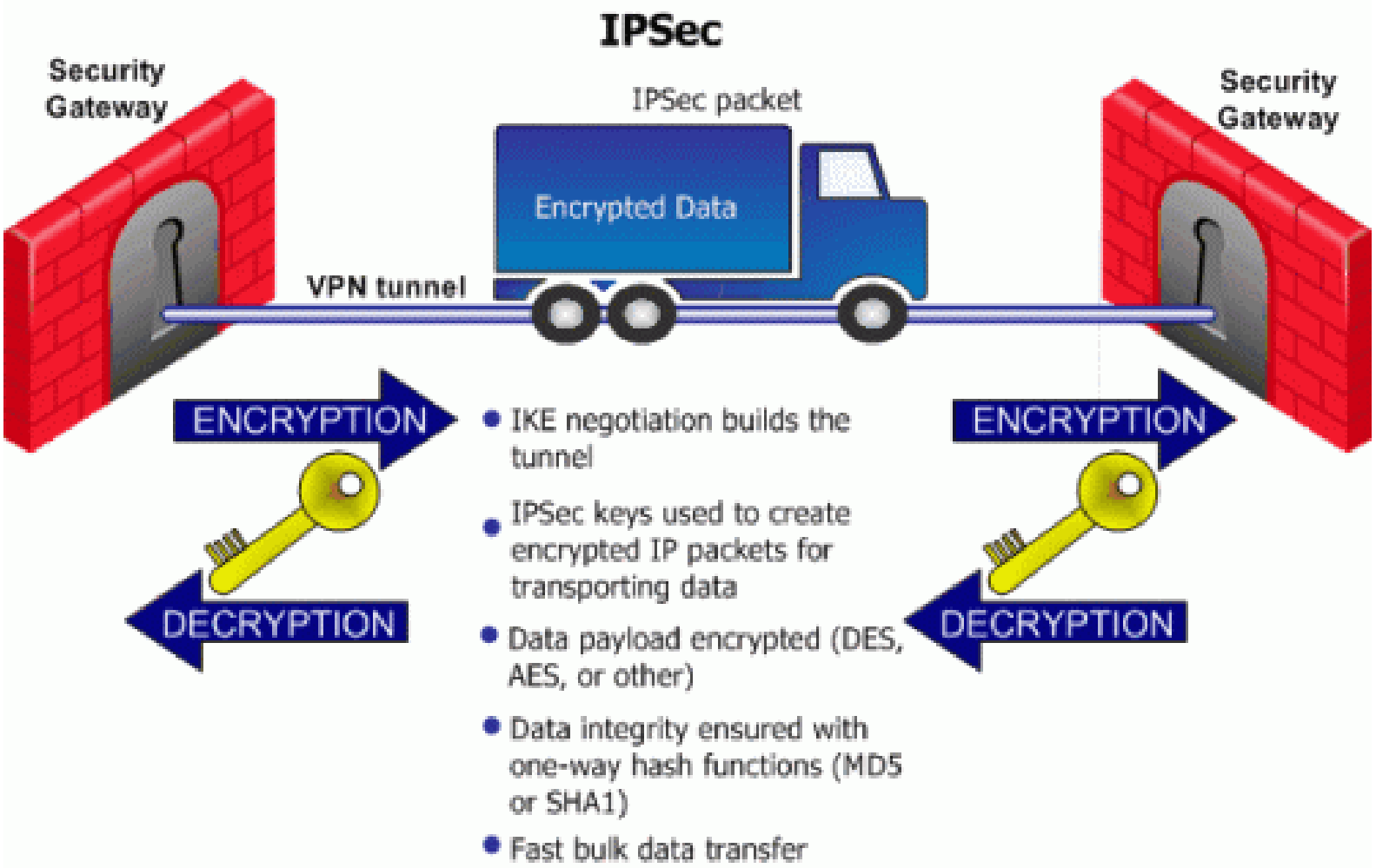
L'échange des clés:

L'échanges des clés nécessaires au cryptage des données dans IPSec peut se faire de trois façons différentes :

- à la main : pas très pratique
- IKE (Internet Key Exchange) : c'est un protocole développé pour IPSec.

ISAKMP (Internet Security Association and Key Management Protocol) en est la base et a pour rôle la création (négociation et mise en place), la modification et la suppression des SA. Elle se compose de deux phases :

- la première permet de créer un canal sécurisé (par Diffie-Hellman) et authentifié à travers duquel on échange un secret pour dériver les clés utilisées dans la phase 2.
- la seconde permet de mettre en place IPSec avec ses paramètres et une SA par sens de communication.
- Les données échangées sont protégées par le canal mis en place dans la phase 1.


IPSec
Security Gateway
IPSec packet
Encrypted Data
Security Gateway
VPN tunnel
ENCRYPTION
DECRYPTION
ENCRYPTION
DECRYPTION
IKE negotiation builds the tunnel
IPSec keys used to create encrypted IP packets for transporting data
Data payload encrypted (DES, AES, or other)
Data integrity ensured with one-way hash functions (MD5 or SHA1)
Fast bulk data transfer

Implémentation Linux:

- Il existe plusieurs implémentation de IPSec dans Linux suivant la version du noyau

- 2.4 et inférieur : FreeS/WAN (http://www.freeswan.org) et OpenSWAN (http://www.openswan.org)

- 2.6 et supérieur : support Natif (KAME-tools at http://ipsec-tools.sourceforge.net/), OpenSWAN ou isakmpd (de OpenBSD)

Configuration de base

- La configuration est assez compliquée mais peu se résumer de la façon suivante :

on crée un script pour définir les paramètres IPSec à mettre dans la SAD (Security Association Database) et dans la SPD (Security Policy Database) :

  - SAD
    - les IP source et destination
    - le mode tunnel ou transport
    - les algos de hachage, cryptage et autres
    - des clés pour AH et ESP
  - SPD
    - les IP source et destination
    - le sens du traffic
    - si AH et/ou ESP sont requis

on exécute le script avec la commande setkey -f.

Openswan est une implémentation IPsec pour Linux

- Projet FreeS/WAN (1999).
- Openswan permet la mise en place de liens IPsec entre machines, tunnels VPN, entre réseaux d'entreprises ou pour des clients nomades.
- Il est compatible avec un grand nombre de systèmes d'exploitation et de solutions propriétaires.
- OpenSwan est disponible sous licence GPL.

Installation de OpenSwan (grandes étapes**)**

sudo apt-get install openswan

- Génération des clés:

ipsec ranbits 256

- Puis édition du fichier /etc/ipsec.secrets sur le ROUTEUR VPN A:

sudo vi /etc/ipsec.secrets

PUBLIQUE_A PUBLIQUE_B
“0×02e91301_438852a5_da987f97_762d2c97_22f0b9c9_8fe399c6_49b818
58_603d90fe”

- PS: remplacer PUBLIQUE_A et PUBLIQUE_B par les adresses IP publiques de vos routeurs
- Copie de la clés sur le ROUTEUR VPN B:

scp /etc/ipsec.secrets root@PUBLIQUE_B:/etc/ipsec.secrets

- PS: si besoin, remplacer root par un compte administrateur valide

Configuration du tunnel IPSec:

- Configuration sur le ROUTEUR VPN A (exemple adresse IP réseaux PRIVEE_A=192.168.1.0/24 et PRIVEE_B=192.168.2.0/24):

- Configuration sur le ROUTEUR VPN B (exemple adresse IP réseaux PRIVEE_A=192.168.1.0/24 et PRIVEE_B=192.168.2.0/24):

Quelques commandes utiles:

Démarrer le daemon IPSec (à faire sur les deux serveurs VPN)

sudo /etc/init.d/ipsec start

Redémarrer le daemon IPSec (en cas de modification d'un des fichiers de configuration):

sudo /etc/init.d/ipsec restart

Status des tunnels VPN:

sudo ipsec whack –status

Debug:

tail -f /var/log/messages | grep pluto

Bibliographie

- William Stalings. '*Sécurité des réseaux. Application et standards'*. Editeur Vuibert Informatique, 2001
- https://sc1.checkpoint.com/
- http://www.kernel-panic.it/
- https://www.openswan.org/