La sécurité réseau avec IPSec

Plan de la présentation

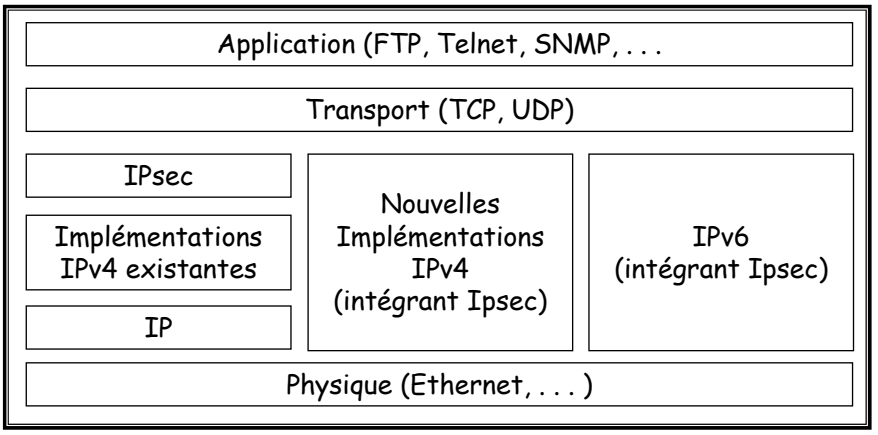
- Principes de fonctionnement
- Mécanismes AH et ESP
- Modes Transport et Tunnel
- Association Sécurité (SA)
- Internet Key Exchange (IKE)
- Déploiement et utilisation pratique

Introduction

- IPsec : architecture sécurisée pour IP
  - Permet de sécuriser les échanges sur un réseau TCP/IP au niveau réseau
  - Services de sécurité totalement transparents pour les applications
  - Commun à IPv4 et IPv6
  - Exemple d'utilisation : VPN, accès distant, ...
- IPSec (IP Security Protocol) fournit :
  - Confidentialité et protection contre l'analyse du trafic
  - Authentification des données (et de leur origine)
  - Intégrité des données
  - Contrôle d'accès
- Le support de ces facilités est obligatoire dans la version 6 du protocole IP et sont implantées comme des en-têtes d'extension à la suite de l'en-tête IP principal.

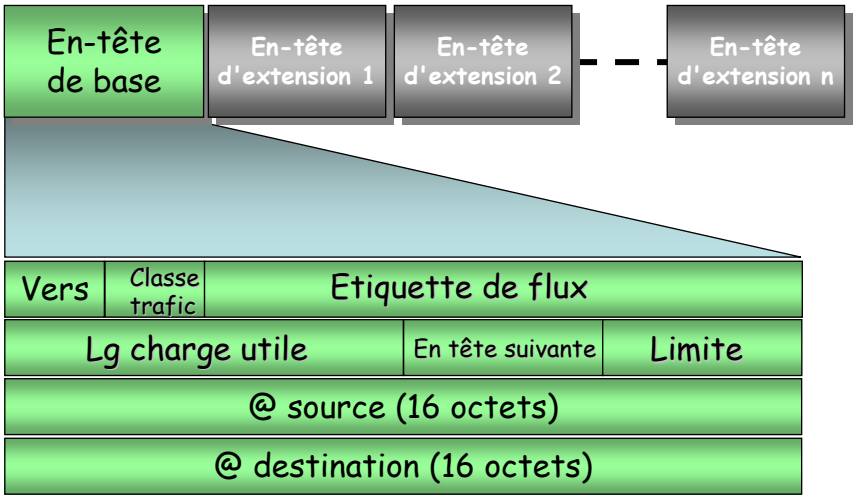
IPSEC - Architecture

- Architecture protocolaire :



IPSEC - Architecture

- Architecture IPv6



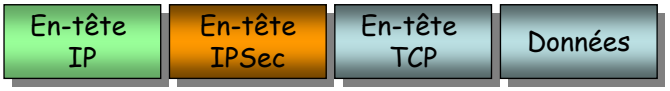
Sécurité et IP

- Mécanismes cryptographiques :
  - Authenticité = Code d'authentification de message (MAC)
  - Confidentialité = Chiffrement
  - Protection contre le rejeu = Numéro de séquence
- Deux en-tête d'extension :
  - En-tête d'extension d'authentification (Authentification Header, **AH**)
  - En-tête d'extension de confidentialité (Encapsulating Security Playload Header, **ESP**)
- Mécanismes ci-dessus font appel à la cryptographie et utilisent donc un certain nombre de paramètres (algorithmes utilisés, clefs, mécanismes sélectionnés …).

Sécurité et IP

- Deux modes :

IPSec en mode transport



IPSec en mode tunnel

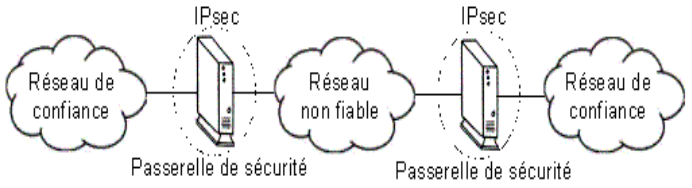
Modes transport et tunnel

- En mode transport, on chiffre/authentifie la partie data d'un paquet IP excepté les champs variables de l'en-tête (TTL, ….)

- En mode tunnel, on protège le paquet complet (y compris l'en-tête IP) et on l'encapsule dans un nouveau paquet, avec un nouvel en-tête IP qui sert à transporter le paquet jusqu'à la fin du tunnel, où l'en-tête d'origine est rétablie.
  - Offre une protection plus importante contre l'analyse du trafic, car il masque les adresses de la source et de la destination finale.

Transport, tunnel

- En mode tunnel la sécurité peut être faite par des passerelles



- En mode transport elle peut être faite de bout en bout; IPSec utilisé au niveau **d'équipements terminaux**

Authentification Header (1)

- Cette transformation authentifie, protége en intégrité les datagrammes IP et assure une protection anti-replay (chaque paquet est numéroté par le champ "Sequence Number" de l'en-tête AH), et les paquets rejoués ne sont pas pris en compte.

- L'authentification est basé sur l'utilisation d'un code d'authentification de message ou MAC (Message Autentication Code).

- Elle n'apporte pas confidentialité mais assure une parade aux attaques basés sur le leurre d'adresses IP (IP Spoofing) et sur celles utilisant le re-jeu de paquets IP (replay attack).

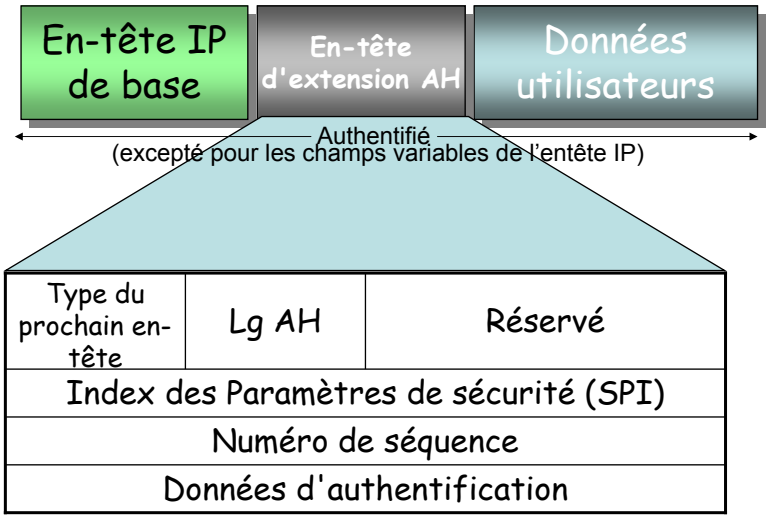
Authentification Header (2)

- L'authentification est faite sur les données qui suivent l'en-tête AH, sur l'en-tête AH ET sur les champs importants de l'en-tête IP (source, destination, protocole, longueur, version).

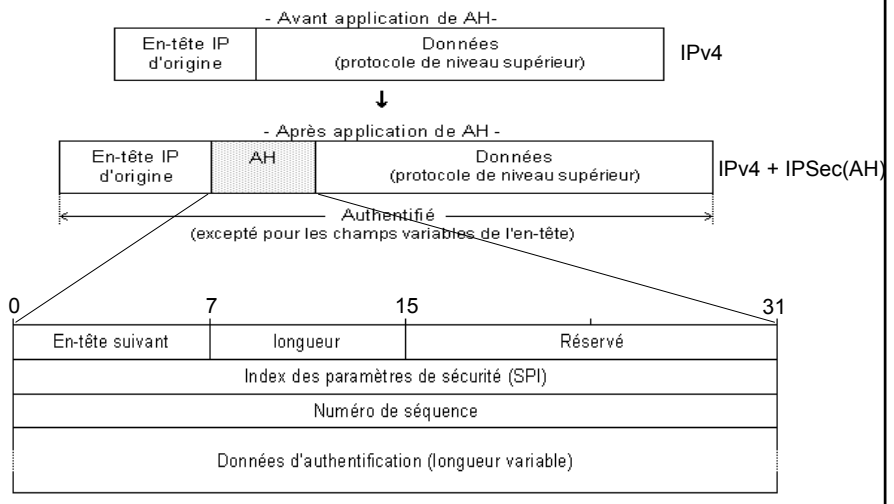
- Deux MAC (hash impliquant une clé symétrique) standard doivent être disponibles: HMAC-SHA-1 et HMAC-MD5.

- Pour calculer l'information d'authentification, on met le champ qui doit la contenir et les champs variables (TTL, routage...) à zéro.

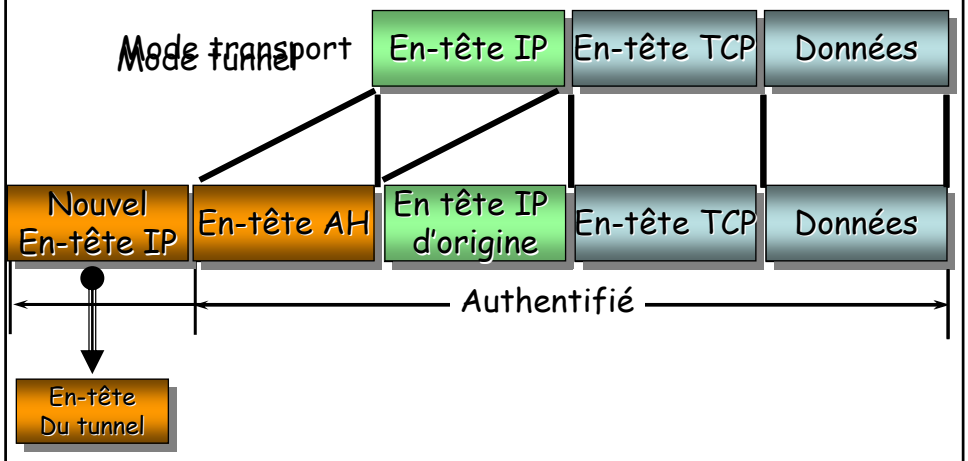
Authentification Header (3)



Authentification Header (4)



Utilisation d'AH



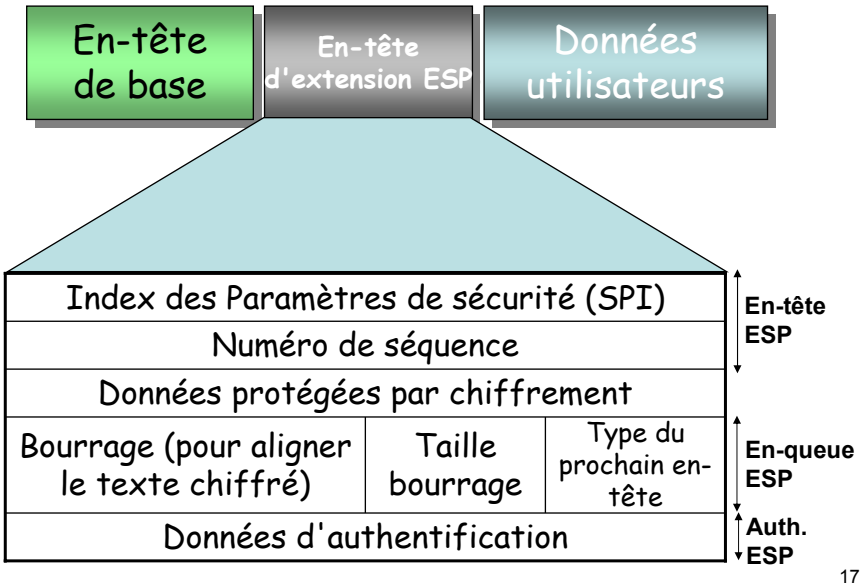
Encapsulated Security Payload (1)

- ESP peut assurer au choix un ou plusieurs des services suivants :
  - Confidentialité des données et protection partielle contre l'analyse du trafic si l'on utilise le mode tunnel.
  - Intégrité des données et authentification de l'origine des données, protection partielle contre le re-jeu.
- Contrairement à AH, ou l'on se contente d'ajouter un en-tête supplémentaire au paquet IP, ESP fonctionne suivant le principe de l'encapsulation : les données originales sont chiffrées puis encapsulées.

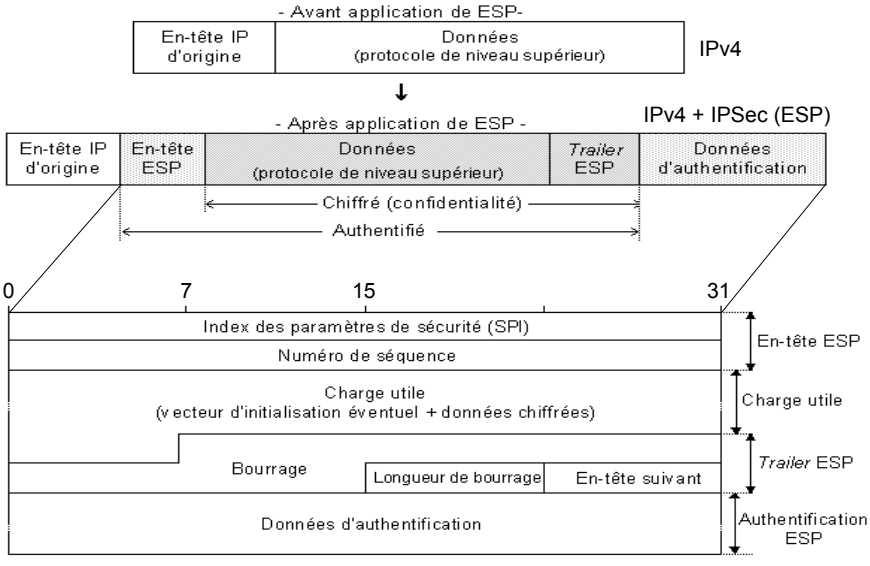
Encapsulated Security Payload (2)

- Le chiffrement ne porte que sur les données encapsulées et l'en-queue ESP, elle n'inclut pas les champs de l'en-tête IP (sauf en mode tunnel) et les données d'authentification.
- L'authentification ESP porte uniquement sur le paquet (en-tête + charge utile + en-queue) ESP et n'inclut ni en-tête IP ni le champ d'authentification.
- Les algorithmes obligatoires sont :
  - **Cryptage**: DES triple, NULL (pas de chiffrement).
  - **Auth**: HMAC-SHA-1, HMAC-MD5 et NULL (pas d'authentification).

Encapsulated Security Payload (3)

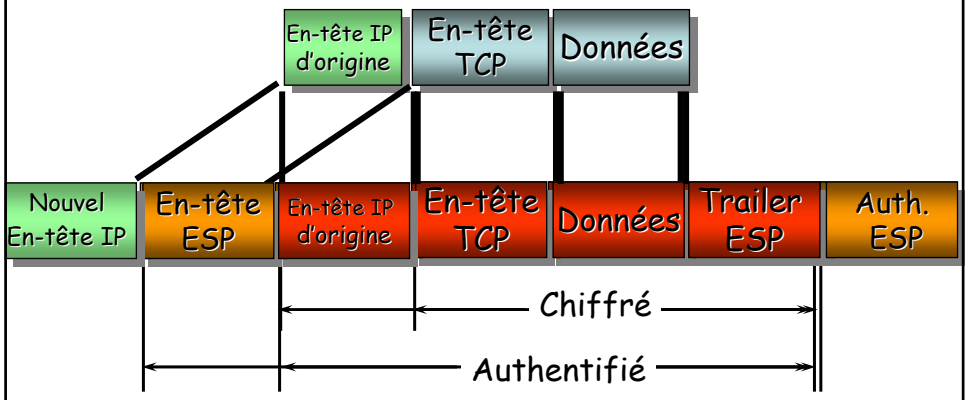


Encapsulated Security Payload (4)



Utilisation d'ESP

Mode transport



Associations de sécurité

- Les mécanismes précédents nécessitent un certain nombre de paramètres (algorithmes de chiffrement, clés…) sur lesquels les tiers communicants doivent se mettre d'accord.

- 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 **pour chaque flux unidirectionnel** (dans chaque direction).

Les paramètres

Paramètre	Valeurs acceptées	keyword	Valeurs par défaut
encryption algorithm	56-bit DES-CBC 168-bit Triple DES	**des** **3des**	56-bit DES-CBC
hash algorithm	SHA-1 (HMAC) MD5 (HMAC)	**sha** **md5**	SHA-1
authentication method	RSA signatures pre-shared keys	**rsa-sig** **pre-share**	RSA signatures
Diffie-Hellman group identifier	768-bit Diffie-Hellman 1024-bit Diffie-Hellman	**1** **2**	768-bit Diffie-Hellman
security association's lifetime	Un nombre en secondes		Une journée

Gestion des clés et des SA

- Un des problèmes cruciaux d'utilisation de la cryptographie est la gestion de clés.
  - Le terme "gestion" recouvre la génération, la distribution, le stockage et la suppression des clefs.
- Les SA contiennent tous les paramètres nécessaires à IPsec, notamment les clés utilisées.
  - Comment se mettre d'accord sur les paramètres à utiliser pour les SA ?
- Deux solutions :
  - **Configuration manuelle** : l'administrateur définit le contenu de la SA, y compris les clés.
  - **Négociation dynamique des SA** et notamment l'échange des clés de session, au moyen d'un protocole spécifique.

Internet Key Exchange (1)

• 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.

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

• Plusieurs éléments composent IKE :

- ISAKMP (Internet Security Association and Key Management Protocol)
- Oakley

Internet Key Exchange (2)

- **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.

Négociation IKE

- Première phase : **SA ISAKMP**
  - Négociation d'un ensemble d'attributs relatifs à la sécurité,
  - Une session ISAKMP est authentifiée :
    - soit par une clef partagée (*pre-shared key*)
    - soit par RSA signature et chiffrement
  - SA ISAKMP pour sécuriser l'ensemble des échanges futurs.
- Seconde phase : **SA IPSec**
  - SA à établir pour le compte d'un mécanisme de sécurité donné (par exemple AH ou ESP).
  - Échanges de cette phase sont sécurisés (confidentialité, authenticité...) grâce à la SA ISAKMP.

Négociation IKE

- 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 phase 1

Phase 1 d'IKE :

- Méthode d'échange des clefs :
- Méthode d'authentification des peers :
  - pre-shared Key
  - 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 :
  - 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

IKE phase 2

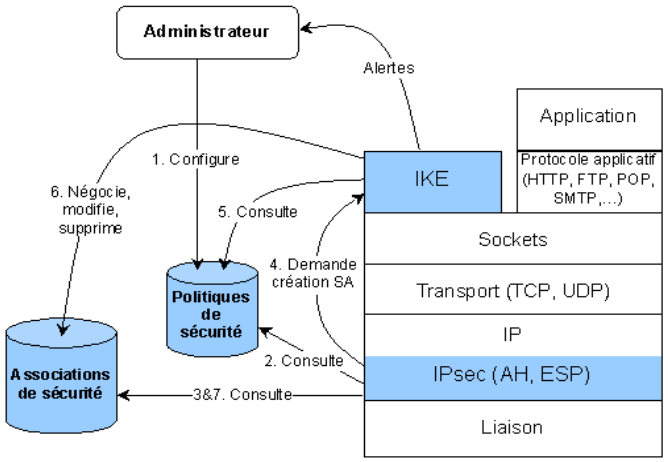
Phase 2 d'IKE :

- 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
- Établissement des IPSec SA soit de manière manuelle (pas conseillé), soit via IKE (conseillé).

SA IPSec

- Le contenu d'une SA IPSec est le suivant:
  - Adresse IP du peer d'en face
  - Identifiant du VPN (SPI = Security Parameter Index)
  - Protocole de sécurité (AH ou ESP)
  - Mode (Tunnel ou Transport)
  - Durée de vie de la SA
- Les SA sont regroupées dans une "base de données des associations de sécurité" (SAD).
  - Contient tous les paramètres relatifs à chaque SA et sera consultée pour savoir comment traiter chaque paquet reçu ou à émettre.

IPsec / IKE



Relation entre IPSec, SAD, SPD
(Trafic sortant et entrant)

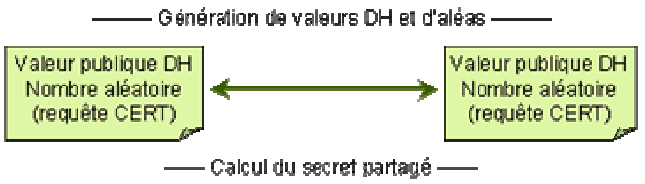
IKE phase 1

- Deux modes :
  - Main mode (mode normal) :
    - requiert six messages,
    - protège l'identité de l'initiant.
  - Agressive mode (mode agressif) :
    - ne comprend que trois messages,
    - révèle l'identité,
    - plus rapide (pas de DH).

Phase 1 – Main Mode (1)

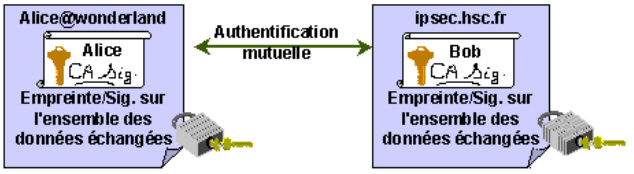
- Les deux premiers messages, **pour négocier les paramètres IKE :**
  - Algorithme de chiffrement (3DES, DES …),
  - Fonction de hachage (MD5, SHA),
  - Méthode d'authentification des tiers :
    - signature numérique (HMAC)
    - utilisation d'un secret partagé préalable
    - authentification par chiffrement à clé publique
  - Groupe pour Diffie-Hellman.

Phase 1 – Main Mode (2)



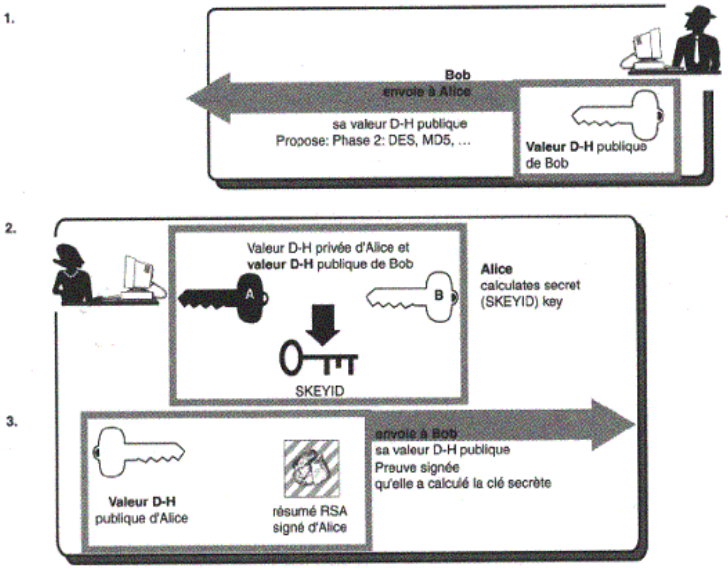
- Les deux seconds messages, **pour établir un secret partagé et dériver les clés de sessions :**
  - Utilisation de DIFFIE-HELLMAN avec le groupe négocié précédemment,
  - Deux des clés de sessions seront utilisées pour protéger la suite des échanges avec les algorithmes de chiffrement et de hachage négociés précédemment.

Phase 1 – Main Mode (3)

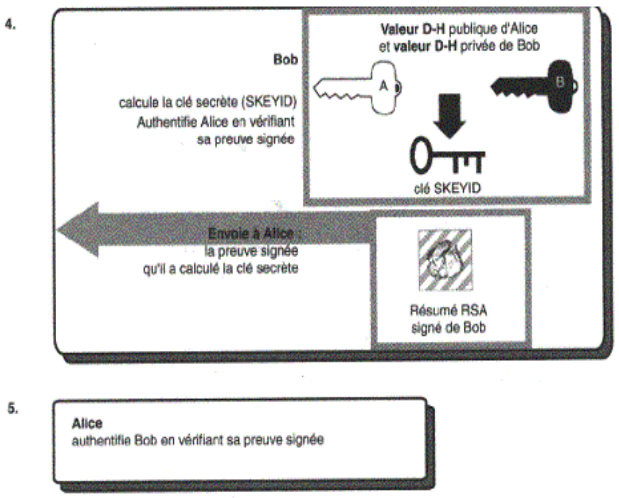


- Les deux derniers messages, **pour l'authentification des échanges et notamment des valeurs publiques :**
  - Utilisation de la méthode d'authentification négociée lors des deux premiers messages (secret partagé, chiffrement à clé publique ou signature numérique)

IKE phase 1 – Illustration



IKE phase 1 – Illustration



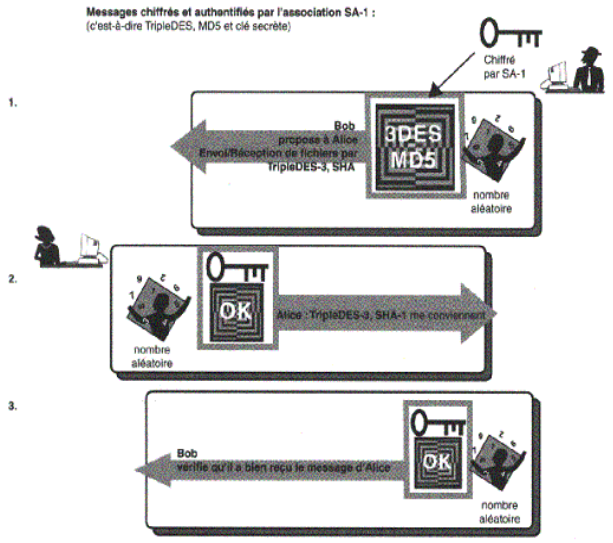
IKE phase 1 – Illustration

1. Bob initie l'échange et envoie sa valeur DH publique et une valeur aléatoire ainsi que ses propositions de paramètres cryptographiques pour la SA IKE.
2. Alice utilise la valeur DH publique de Bob ainsi que sa propre valeur DH privée et sa valeur aléatoire pour calculer la clé secrète partagée SKEYID.
3. Alice envoie à Bob sa valeur DH publique et un "hash" signé de SKEYID, générée par Alice.
4. Bob emploie la valeur DH publique d'Alice et la sienne pour calculer à son tour SKEYID. Bob vérifie la preuve signée d'Alice et vérifie que la clé secrète d'Alice est bien la même que la sienne, c'est-à-dire SKEYID. Bob envoie une preuve signée qu'il a calculé la clé SKEYID.
5. Alice vérifie la preuve signée de Bob et s'assure qu'il a bien calculé la même clé SKEYID.

IKE phase 2

- Mode Quick :
  - Phase 2 plus rapide car elle utilise la cryptographie à clés secrètes et non celle à clés publiques qui est beaucoup plus lente et coûteuse.
  - L'authenticité des messages est assurée par l'ajout d'un bloc HASH après l'en-tête ISAKMP,
  - La confidentialité est assurée par le chiffrement de l'ensemble des blocs du message.

IKE phase 2 – Illustration



IKE phase 2 – Illustration

1. Bob envoie à Alice une proposition pour les paramètres des SAs IPsec. Bob génère un nouveau nombre aléatoire pour identifier le message de façon unique.

2. Alice répond pour le choix des paramètres et envoie son nouveau nombre aléatoire. Elle prouve aussi qu'elle a bien reçu le précédent message de Bob grâce au nombre aléatoire de Bob.

3. Bob accuse réception du message d'Alice comme Alice vient de le faire à l'étape précédente.

IPSec – La Synthèse

- Bilan des composants IPsec :
  - AH et ESP = mécanismes de sécurisation au niveau IP qui protègent les données transférées.
  - Les paramètres relatifs à ces mécanismes sont stockés dans des associations de sécurité (SA).
  - IKE = protocole utilisé par les équipements IPSec pour gérer les associations de sécurité.
  - Un ensemble de Politiques de sécurité qui sont des règles à appliquer au trafic traversant un équipement donné. C'est par elles que l'administrateur du réseau configure IPsec et notamment indique à IKE quels sont les tunnels sécurisés à créer.

Déploiement et utilisation pratique

Où trouver IPSec ?

- Passerelle de sécurité : routeur, garde-barrire…
- Exemples :
  - Module FreeS/WAN pour Linux
  - Firewall-1 de Check Point à partir de la version 4.0
  - CISCO IOS à partir de la version 11.3.(3)T
- Utilisé principalement pour la création de réseaux privés virtuels (VPN).

Où trouver IPSec ?

- Équipements terminaux : serveurs, postes utilisateurs
- Différents types d'implémentations :
  - Re-compilation du noyau du système (FreeS/WAN pour Linux)
  - Simple module à ajouter sur la machine et qui va s'interfacer avec la pile TCP/IP
- Principales utilisations :
  - Lorsque IPsec est installé sur un serveur sensible, il peut être utilisé pour protéger l'accès à ce serveur.
  - Installé sur une machine utilisateur, il permet d'accéder aux serveurs ou aux réseaux protégés par IPsec.

Déployer IPsec: planification

- Les étapes du déploiement :
  - Identification des besoins = établir un plan du réseau et **identifier les communications à sécuriser**.
  - **Choix du type de sécurisation souhaité** : chiffrement et/ou authentification des données, mode d'authentification des tiers, algorithmes à utiliser …
  - Identification des équipements concernés par la mise en œuvre de la politique de sécurité retenue et **définition des règles à faire appliquer par chaque équipement**.

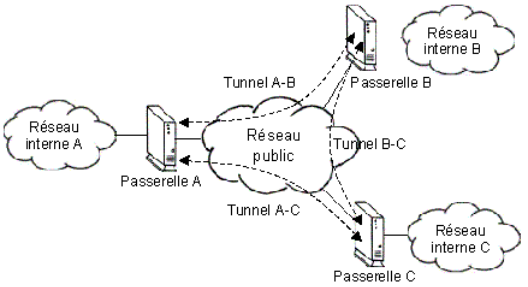
Déployer IPsec: configuration

- La méthode de configuration d'IPsec varie fortement d'un produit à l'autre :
  - Tous les fournisseurs ne font généralement de distinction claire entre la politique de sécurité et les associations de sécurité telles qu'elles ont été présentées précédemment.
- Point important :
  - Pour que deux équipements puissent s'entendre, ils doivent être configurés avec des paramètres similaires.
  - D'où, une nécessité de concertation lors d'une configuration entre deux réseaux gérés par des personnes différents.

Exemple 1: réseaux privés virtuels

- But : protection des échanges entre différents réseaux privés, séparés par un réseau non fiable.

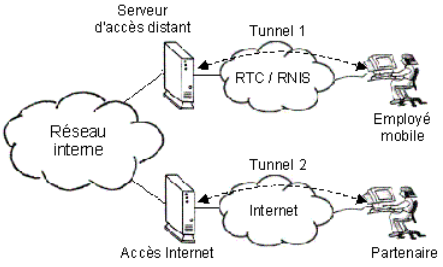
- Équipements impliqués : passerelle de sécurité en entrée/sortie des différents réseaux.



Exemple 2: extranet

- But : sécuriser les accès distants (partenaires, employés) au réseau de l'entreprise.

- Équipements impliqués : portes d'entrées du réseau (serveurs d'accès distant, liaison Internet …) et machines utilisées par les employés ou partenaires.



Quelques Liens

- IPsec : présentation technique
(http://www.hsc.fr/ressources/articles/ipsec-tech/index.html.fr)

- Sécurité des Réseaux (transparents PH. Oechslin, 2003)

- Vue conceptuelle "réduite" du protocole IKE
(http://benoit-joseph.mine.nu/tfe/)

- http://www.hsc.fr/ressources/presentations/