Virtual Private Network

Ramzi Ouafi
Assistant Technologue
ESPRIT
e-mail : ouafiramzi@gmail.com

Qu’est ce qu’un VPN

- Abréviation de l’anglais Virtual Private Network ou encore Réseau Privé Virtuel (RPV) en français

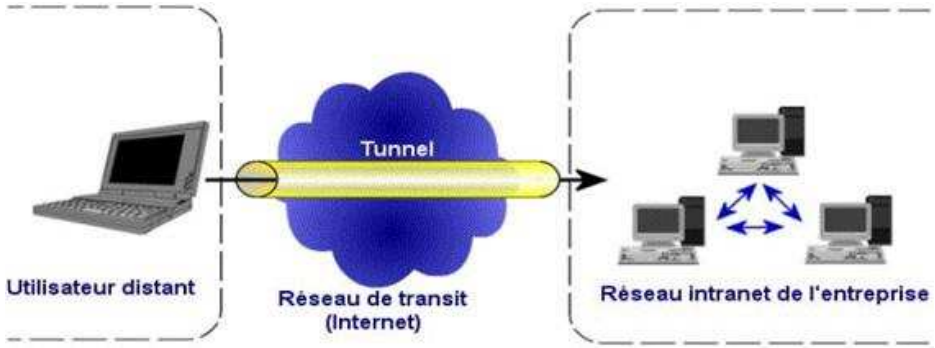
- Les VPNs permettent de créer un chemin virtuel sécurisé entre une source et une destination grâce à un principe de tunnel (**tunnelling**) dont chaque extrémité est identifiée, les données transitent après avoir été chiffrées.

- De manière succincte, les propriétés générales des tunnels destinés aux VPNs :
  - Les données transitant sont **chiffrées** (confidentialité) et protégées (intégrité)
  - Les 2 extrémités sont **authentifiées**
  - Les adresses sources et destinations sont chiffrées, avec IPSec (IP dans IPSec).
  - Ils peuvent présenter, suivant le protocole, des qualités **anti-rejeux** ou empêcher les attaques type **man-in-the-middl**e.

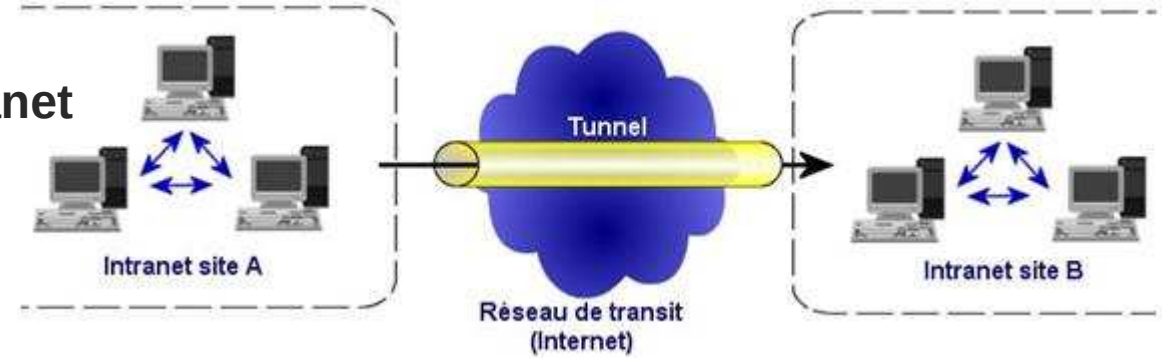
- Utilisation ciblée
  - Relier deux réseaux privés à travers un réseau « public ».
  - Permettre des accès distants aux utilisateurs nomades

Fonctionnalités des VPN

Le VPN d'accès



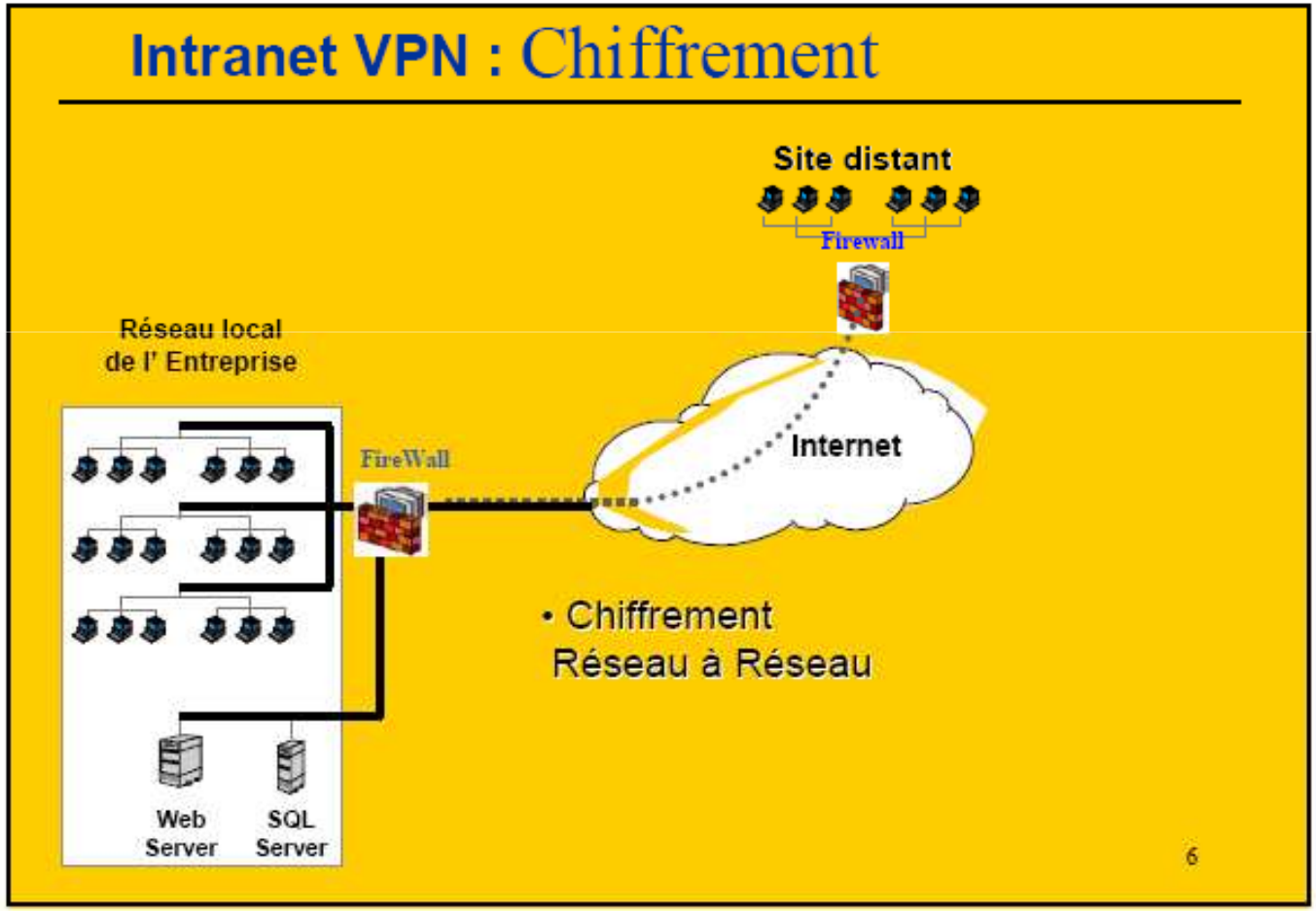
Le VPN intranet



Objectifs et services communs des VPNs

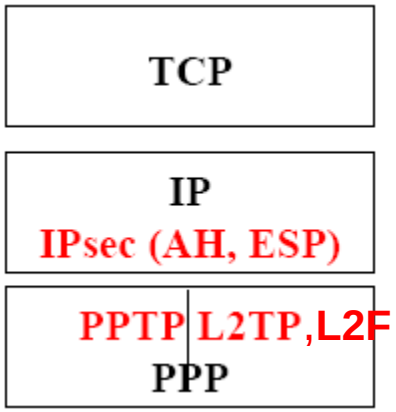
- Objectifs des VPNs : mise en oeuvre les fonctionnalités suivantes :
  - Authentification d'utilisateur. Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.
  - Gestion d'adresses. Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pouvoir se connecter facilement au réseau et recevoir une adresse.
  - Cryptage des données. Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.
  - Gestion de clés. Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.
  - Prise en charge multiprotocole. La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP

Intranet VPN : chiffrement



Comment ?

- Le VPN fait appel à deux moyens:
  - L'encapsulation
  - La cryptage
- Utilisation de la techniques de chiffrement symétrique et asymétrique
  - Pour l'authentification des parties
  - Pour la confidentialité et intégrité de données
- Travail au niveau des couches 2 et 3 pour simuler une connexion réseau et rendre le VPN transparent aux services qui l'utilisent



Les principaux protocoles VPN

- Les principaux protocoles de tunneling VPN sont les suivants :
  - **PPTP** (Point-to-Point Tunneling Protocol) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
  - **L2F** (Layer Two Forwarding) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais **quasi-obsolète**
  - **L2TP** (Layer Two Tunneling Protocol) est l'aboutissement des travaux de l'IETF (RFC 2661) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
  - **IPSec** est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP.

Implémentations des VPNs

- **Le VPN est avant tout un concept** : il ne décrit pas l'implémentation effective de ces caractéristiques. C'est pourquoi il existe plusieurs produits différents sur le marché dont certains sont devenus standard, et même considérés comme des normes.

- Plusieurs implémentations possibles
  - VPN SSL, IPsec, etc…

- Une initiative fédérée: le Consortium VPN gère l'interopérabilité des solutions existantes
  - http://www.vpnc.org

- Solutions logicelles
  - Microsoft, Linux FreeS/WAN, openvpn

- Solution complètes intégrant le matériel et le logiciel
  - Cisco, Nokia/CheckPoint, Fortiguard

VPN niveau 3 : IPSEC

- IPSec (Internet Protocol Security) RFC 2401 est un protocole de la couche 3 de l'OSI:
  - Est un ensemble de mécanismes destinés à protéger le trafic au niveau d'IP (**IPv4 ou IPv6**).
    - Optionnel dans IPv4, IPsec est obligatoire pour toute implémentation de IPv6.
  - Développé par le groupe de travail l'**IETF** (Internet Engineering Task Force), **RFC 2401** : Security Architecture for the Internet Protocol.
  - Les services IPSec sont fournis au niveau de la couche IP, offrant donc une protection pour IP et tous les protocoles de niveau supérieur.
    - Au niveau couches protocolaires, IPSEC se place entre IP et TCP/UDP
  - Avantages par rapport aux solutions existantes : interopérabilité, cryptage au niveau 3 (niv 2 : dépendance par rapport au réseau, niv 7: dépendance par rapport à l'application)
  - Fait appel à plusieurs notions à la fois:
    - Echange des clefs
    - Cryptage
    - Authentification
    - Type du tunnel.

Les services offerts par IPSec

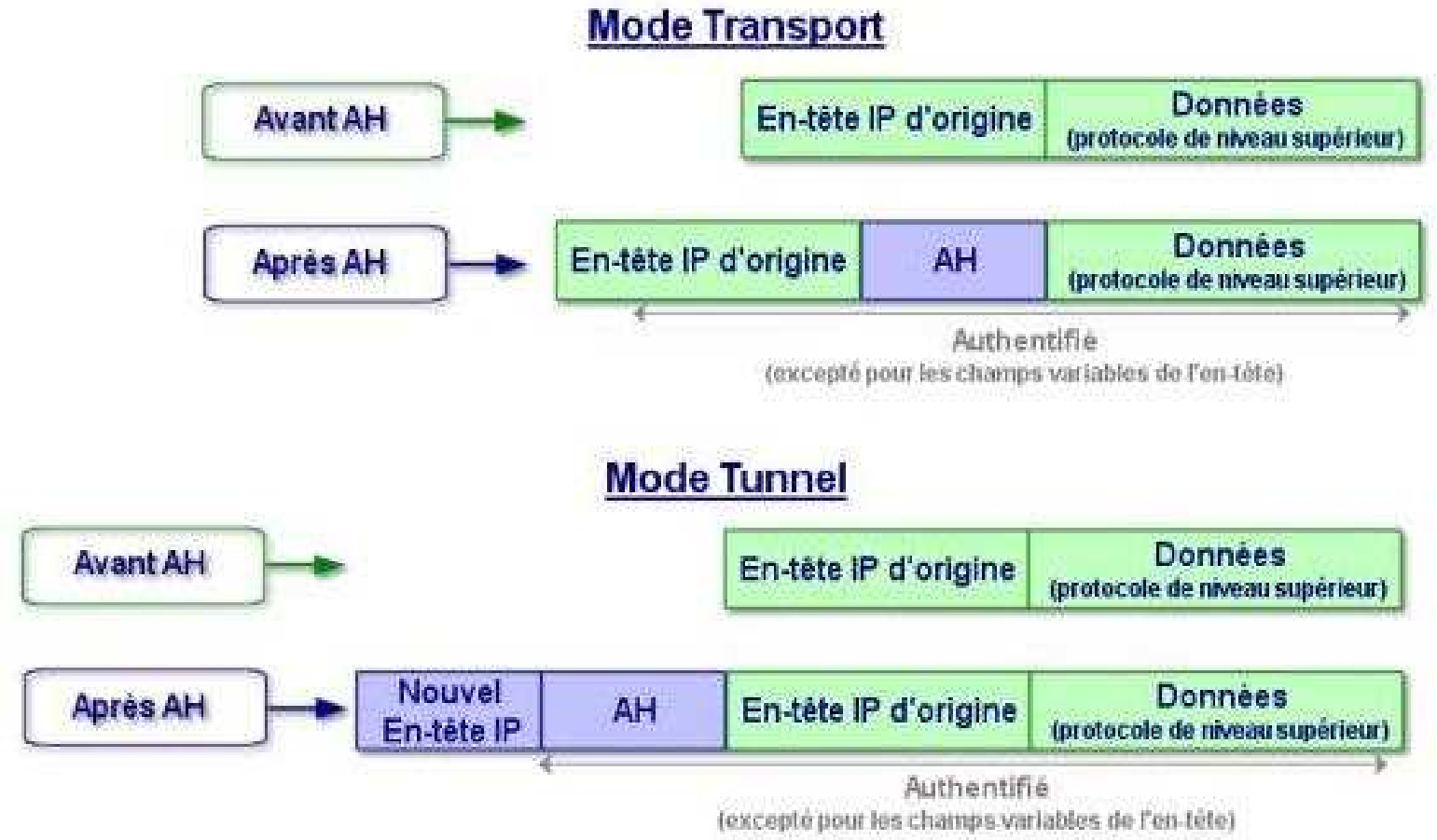
- Comme tout type de VPN, IPSec offre les propriétés basiques des tunnels de chiffrement. Particularités de l'IPSec par rapport aux autres types de VPN
  - **Authentification mutuelles des extrémités :**
    - Remarque : IPSec est un protocole de niveau 3 et qu'il ne fournit donc qu'une authentification de niveau égal, c'est-à-dire une authentification des machines mettant en œuvre le protocole plutôt que des personnes utilisant réellement la machine.
  - **Confidentialité des données échangées :** IPSec permet **si on le désire** de chiffrer le contenu de chaque paquet IP pour éviter que quiconque ne le lise.
  - **Authenticité des données :** IPSec permet de s'assurer, pour chaque paquet échangé, qu'il a bien été émis par la bonne machine et qu'il est bien à destination de la seconde machine.
  - **Intégrité des données échangées :** IPSec permet de s'assurer qu'aucun paquet n'a subit de modification quelconque (attaque dite active) durant son trajet.
  - **Protection contre les écoutes et analyses de trafic :**
    - IPSec permet de chiffrer les adresses IP réelles de la source et de la destination, ainsi que tout l'en-tête IP correspondant.
    - C'est le mode **de tunneling**, qui empêche tout attaquant à l'écoute d'inférer des informations sur les identités réelles des extrémités du tunnel, sur les protocoles utilisés au-dessus d'IPSec, sur l'application utilisant le tunnel (timing-attacks et autres)...
  - **Protection contre le rejeu :**
    - IPSec permet de se prémunir contre les attaques consistant à capturer un ou plusieurs paquets dans le but de les envoyer à nouveau (sans pour autant les avoir déchiffrés) pour bénéficier des même avantages que l'envoyeur initial.

Les différents modes IPSec

- IPSec supporte deux modes:
  - **Le mode transport:**
    - Le mode transport permet de protéger principalement les protocoles de niveaux supérieurs:
      - ne modifie pas l'en-tête initial; il s'intercale entre le protocole réseau (IP) et le protocole de transport (TCP, UDP...)
  - **Le mode tunnel:**
    - permet d'encapsuler des datagrammes IP dans des datagrammes IP:
      - Il y a donc une entête IP encapsulée dans les données IPSec et une entête IP réelle pour le transport sur le réseau public

- Le mode transport : En mode transport, la session IPSec est établie entre deux hosts.
  - **Avantages**: la session est sécurisée de bout en bout
  - **Inconvénients**: nécessité d'une implémentation de IPSec sur tous les hosts; autant de sessions IPSec que de couples de hosts
- En mode tunnel, la session IPSec est établie entre deux passerelles IPSec, ou un host et une passerelle
  - **Avantages**:
    - l'ensemble des communications traversant les passerelles VPN peuvent être sécurisées; pas de modification des hosts
    - On a le contrôle total sur l'entête IP produite par IPSec pour encapsuler ses données et son entête IPSec
  - **Inconvénients**:
    - nécessite des passerelles VPN
    - Latence : application des services cryptographiques sur tout le paquet IP

Mode de protection IPSEC



Les composants d'IPSec

- Le protocole IPSec est basé sur quatre modules :
  - Le type du protocole :
    - IP Authentification Header (**AH**) gère:
    - Encapsulating Security Payload (**ESP**)
  - Security Association (**SA**) définit l'échange des clés et des paramètres de sécurité.
  - La SAD (Security Association Database) stocke les SA afin de savoir comment traiter les paquets arrivant ou partant.
  - La SPD (Security Policy Database) est la base de configuration de IPSec..

IPSec/AH

- **l'Authentication Header (AH)** Le principe de AH est d'adjoindre au datagramme IP classique un champ supplémentaire permettant au récepteur de vérifier l'authenticité des données incluses dans le datagramme (hash signé)

- L'AH gère
  - **L'intégrité** : on s'assure que les champs 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 cryptée.

- Il supporte les deux modes transport / tunnel

IPSec/AH mode transport

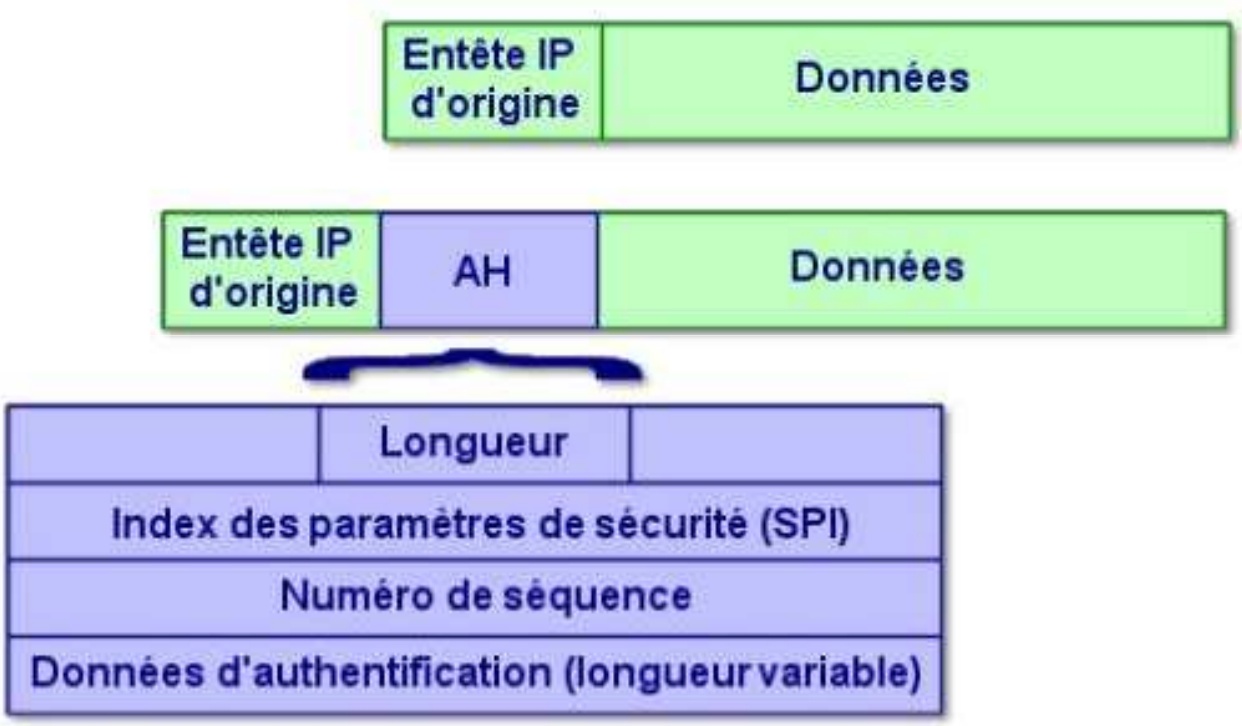
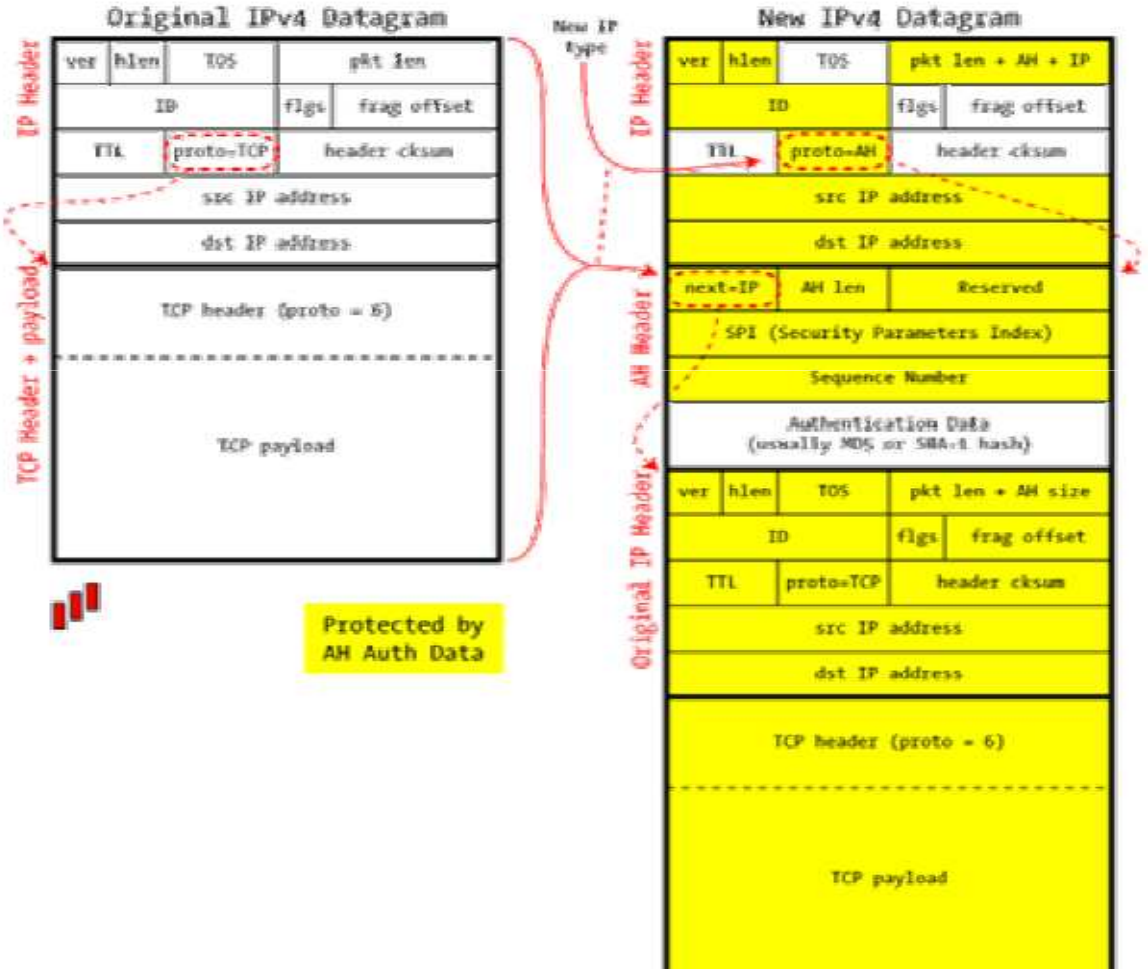


FIG. – Authentification Header

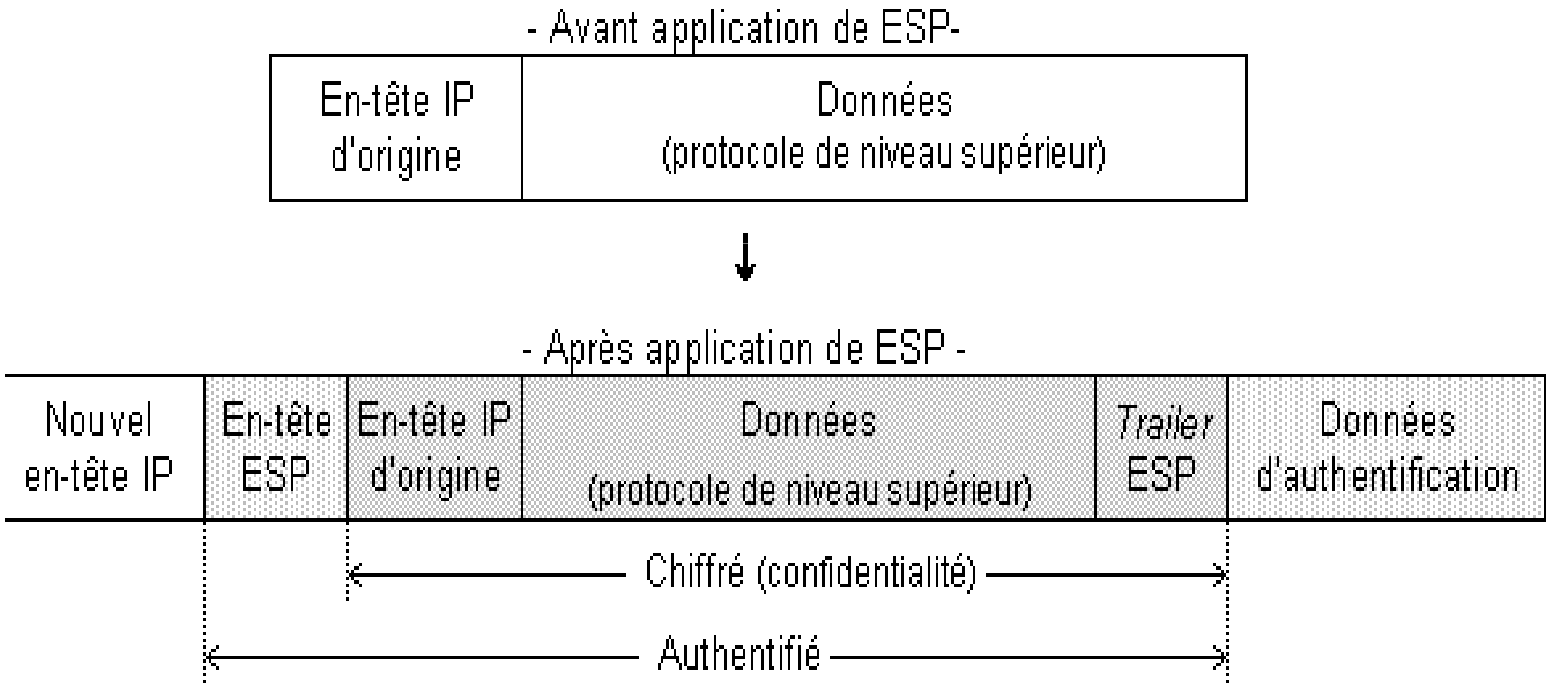
IPSec/AH mode Tunnel



IPSec/ESP

- **l'Encapsulating Security Payload (ESP)**.
  - Le principe de ESP est de générer, à partir d'un datagramme IP classique, un nouveau datagramme dans lequel les données et éventuellement l'en-tête originale sont chiffrés.
  - code d 'authentification de message (hash signé) et chiffrement des données
- 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 les vérifications de

IPSec/ESP


- Avant application de ESP-
En-tête IP d'origine
Données (protocole de niveau supérieur)
- Après application de ESP -
Nouvel en-tête IP
En-tête ESP
En-tête IP d'origine
Données (protocole de niveau supérieur)
Trailer ESP
Données d'authentification
Chiffré (confidentialité)
Authentifié

IPSec/ESP

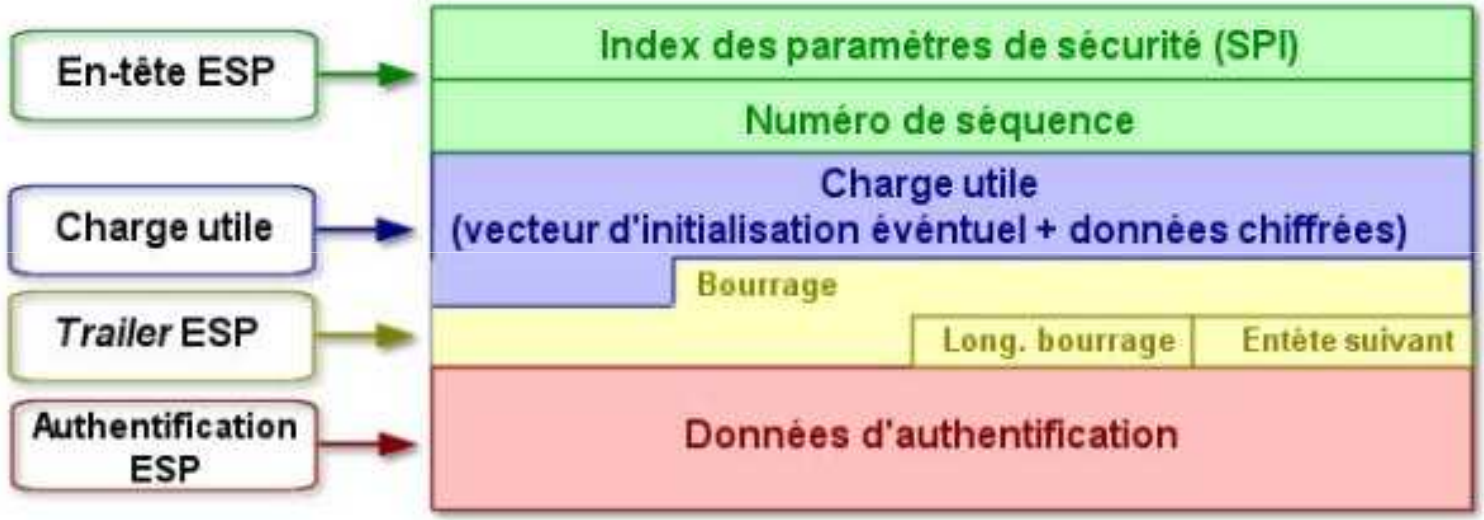
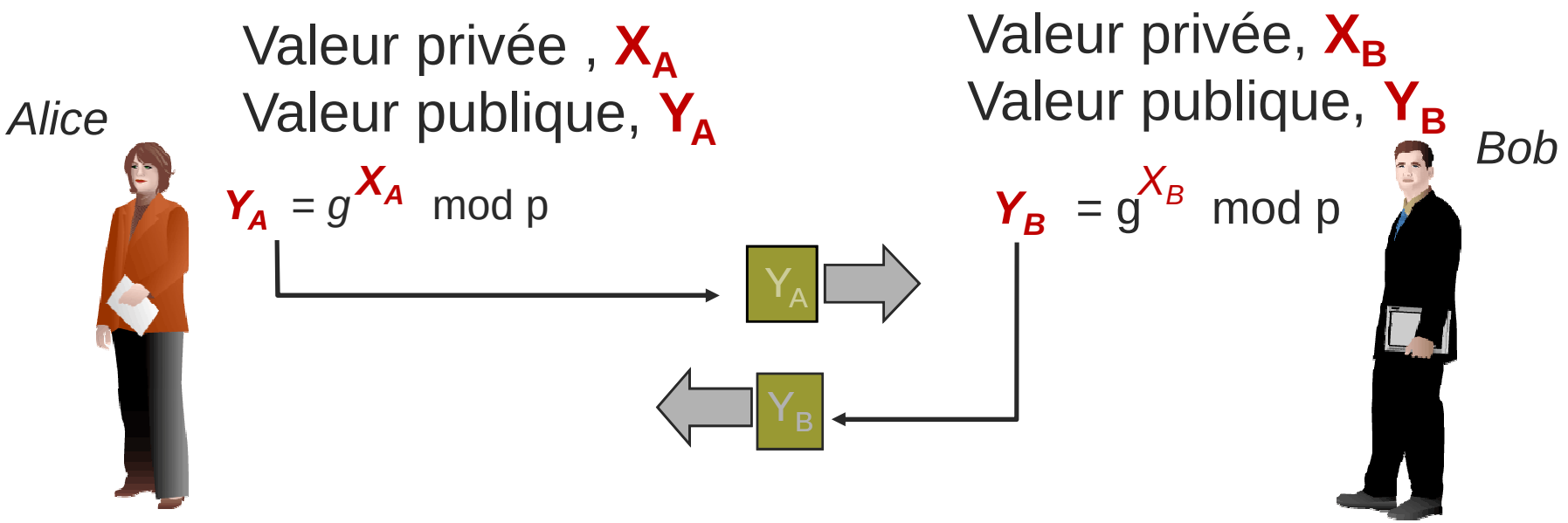


FIG. – Encapsulating Security Payload

IPsec Services

- **Algorithmes cryptographiques :**
  - AH et ESP sont utilisables avec de nombreux algorithmes cryptographiques : les RFCs n'imposent pas d'algorithme particulier.
  - Chaque produit comportant IPsec sera donc livré avec un ensemble d'algorithmes, parmi lesquels l'utilisateur ou l'administrateur du réseau pourront choisir.
  - Chiffrement : NULL, CAST-128 (clef de 40 à 128 bits), Blowfish (40-448 bits), RC5(40-2040 bits), DES (56 bits), DES triple (168 bits)....
  - DH: partage de clés symétriques.
  - Authenticité : HMAC-MD5, HMAC-SHA-1…

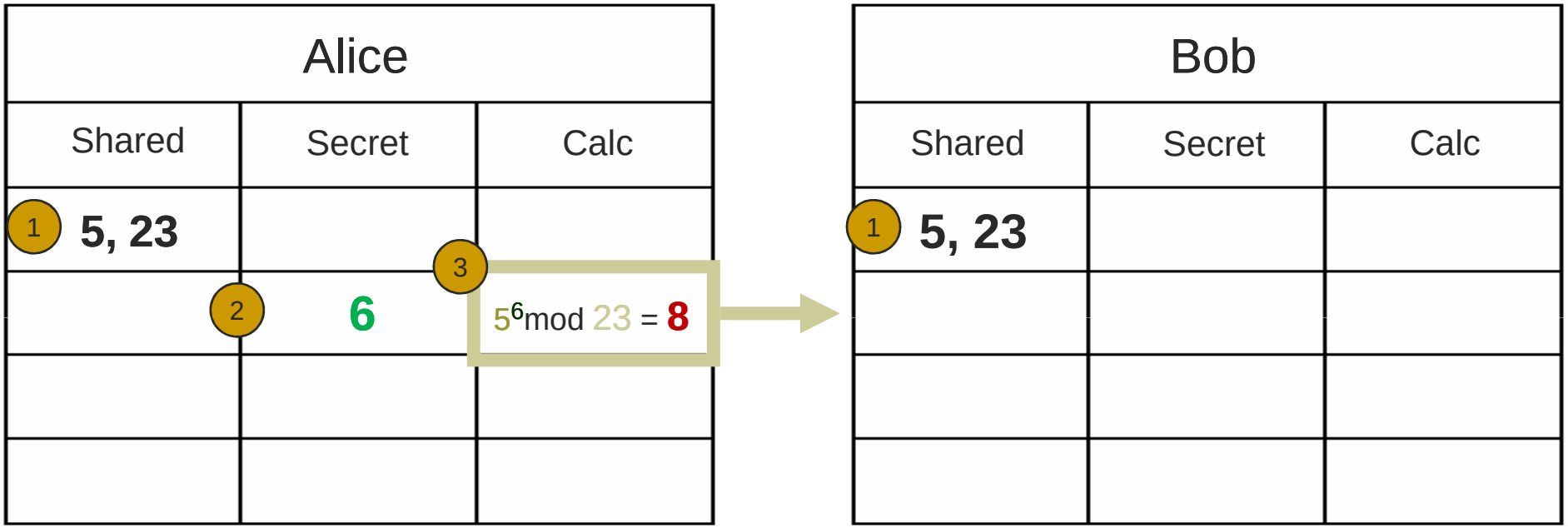
Diffie-Hellman



$(Y_B^{X_A}) \bmod p = K$

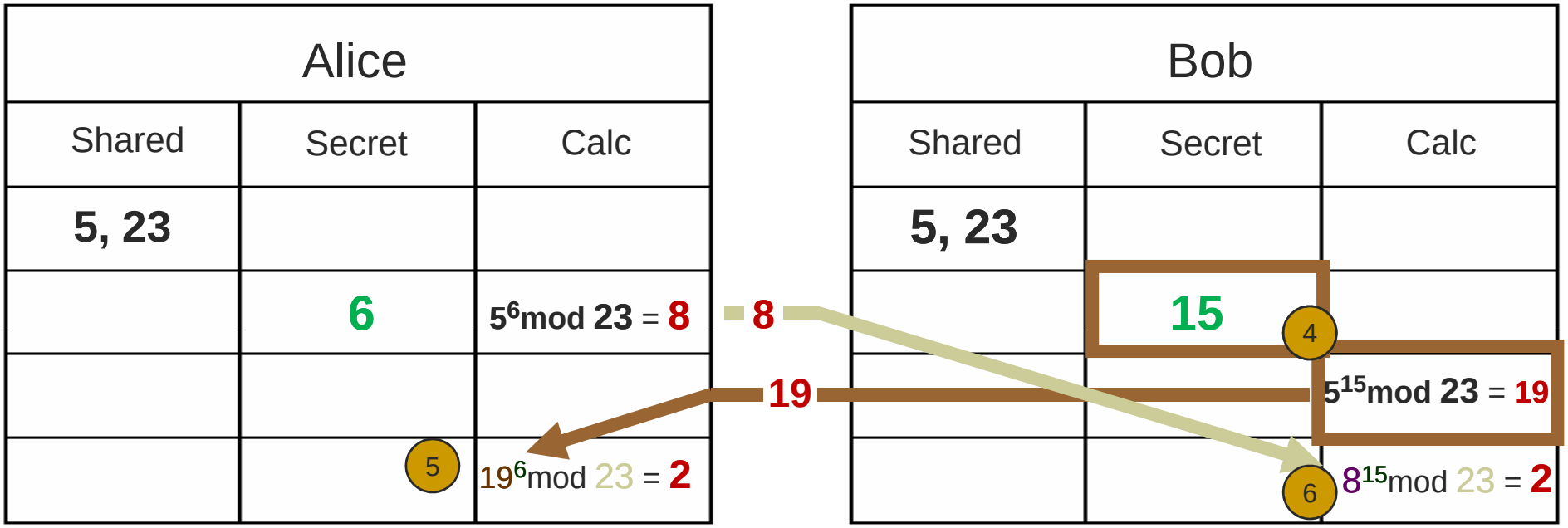
$(Y_A^{X_B}) \bmod p = K$

Diffie-Hellman



1. Alice et Bob choisissent **g=5** et un nombre premier **p=23**
2. Alice choisit une valeur secrète **x=6.**
3. Alice applique la formule de DH : g^x modulo **p = (5^6** modulo **23) = 8** (Y).
4. Envoi cette valeur (**8**) vers Bob.

Diffie-Hellman



4. Bob choisit une valeur secrète x=**15,** fait le calcul : g^x modulo **p = (5^{15} modulo 23) = 19** (Y).
5. Alice calcule **Y^x modulo p = (19^6 modulo 23)** = 2.
6. Bob calcule **Y^x modulo p = (8^{15} modulo 23)** = 2.

Le résultat (**2**) est la clé partagée utilisée pour le chiffrement symétrique des données.

Security Association

- Afin de gérer ces paramètres, IPsec a recours à la notion d'association de sécurité (**Security Association, SA**).

- **Une association de sécurité IPsec est une "connexion" simplexe qui fournit des services de sécurité au trafic qu'elle transporte.**

- *La 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 algo de sécurité utiliser pour crypter, vérifier l'intégrité
  - Les clés utilisées

- De fait, chaque association est identifiée de manière unique à l'aide d'un triplet composé de :
  - L'adresse de destination des paquets.
  - L'identifiant d'un protocole de sécurité (AH ou ESP).
  - Un index des paramètres de sécurité (**Security Parameter Index, SPI**). Un SPI est un bloc de 32 bits inscrit en clair dans l'en-tête de chaque paquet échangé ; il est choisi par le récepteur.

SAD / SPD

- **La SAD : Security Association Database:**
  - Pour gérer les associations de sécurité actives, on utilise une ”base de données des associations de sécurité (Security Association Database, SAD).
  - Elle stocke les SA afin de savoir comment traiter les paquets arrivant ou partant
  - Chaque SA est identifiée par les 3 paramètres cités ci-dessus

- **La SPD (Security Policy Database):**
  - Elle est la base de configuration de IPSec.
  - C’est une liste ordonnée d'entrées contenant des critères de contrôle d'accès similaire aux règles d’un pare-feu
  - Il y a 2 SPDs par interfaces, une pour le trafic entrant, l'autre pour le trafic sortant
  - Les traitements possible par une SPD sont :
    - **DROP** (jette),
    - **BYPASS** (laisse passer)
    - **IPSec PROCESS** (traitement avec IPSec). Ce dernier cas précise en outre les paramètres propres à IPSec tel que l'algorithme, etc...

ISAKMP

- Une SA peut être configurée manuellement dans le cas d'une situation simple, mais la règle générale est d'utiliser un protocole spécifique qui permet la négociation dynamique des SA et notamment l'échange des clefs de session.

- Le protocole de négociation des SA développé pour IPsec s'appelle protocole de gestion des clefs et des associations de sécurité pour Internet "(Internet Security Association and Key Management Protocol, **ISAKMP**).Il comporte trois aspects principaux :

  - Il définit une façon de procéder, en deux étapes appelées **phase 1** et **phase 2** :
    - Dans la première, un certain nombre de paramètres de sécurité propres à ISAKMP sont mis en place, afin d'établir entre les deux tiers un canal protégé ;
    - Dans un second temps, Ce canal est utilisé pour négocier les associations de sécurité pour les mécanismes de sécurité que l'on souhaite utiliser (AH et ESP par exemple).
  - Il définit des formats de messages, par l'intermédiaire de blocs ayant chacun un rôle précis et permettant de former des messages clairs.

  - Il présente un certain nombre d'échanges types, composés de tels messages, qui permettant des négociations présentant des propriétés différentes : protection ou non de l'identité,

IKE (Internet Key Exchange)

- IKE utilise ISAKMP pour construire un protocole pratique.
- Avant l ’échange des données sécurisé par AH ou ESP, les deux peers utilisent le protocole IKE (500/UDP) pour :
  - négocier les algorithmes utilisés et la longueur des clés
  - générer la clé asymétrique de chiffrement par Diffie-Hellman
  - spécifier la durée de vie des clés
  - spécifier la durée de vie de la SA (Security Association ~ tunnel) principale
- Il comprend quatre modes :
  - Le mode principal (Main mode):
  - Le mode agressif (Aggressive Mode)
  - Le mode rapide (Quick Mode)
  - Le mode nouveau groupe (New Groupe Mode)
- Main Mode et Aggressive Mode sont utilisés durant la **phase 1**, Quick Mode est un échange de **phase 2**. New Group Mode se mettre d'accord sur un nouveau groupe pour de futurs échanges Diffie-Hellman une fois qu'une SA ISAKMP est établie
- IKE n ’est pas obligatoire (manual IPSEC) mais fortement conseillé

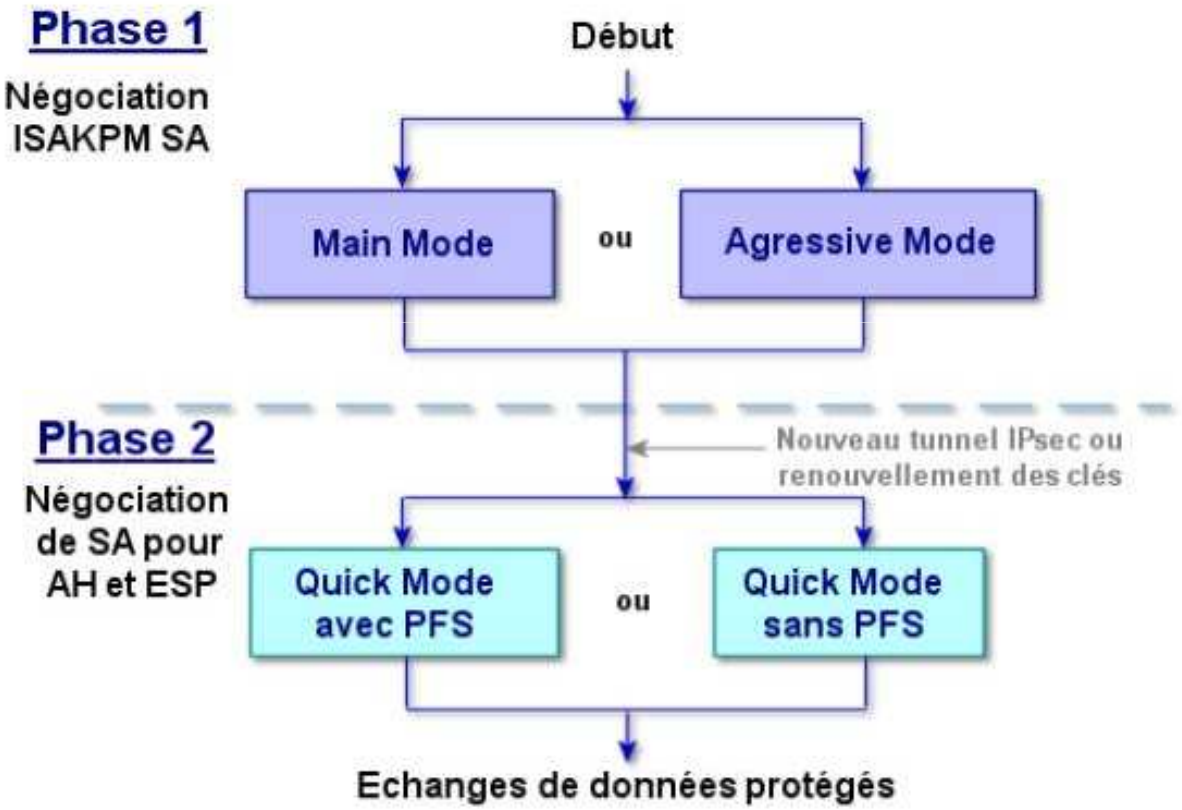
IKE (Internet Key Exchange)

- Phase 1 : **Main Mode et Aggressive Mode**
  - Les attributs suivants sont utilisés par Ike et négociés durant la phase 1 **:**
    - **un algorithme de chiffrement**,
    - **une fonction de hachage**,
    - **une méthode d'authentification (PSK** ou **RSA)**
    - et **un groupe pour Diffie-Hellman**. (Si la méthode d'authentification est PSK)

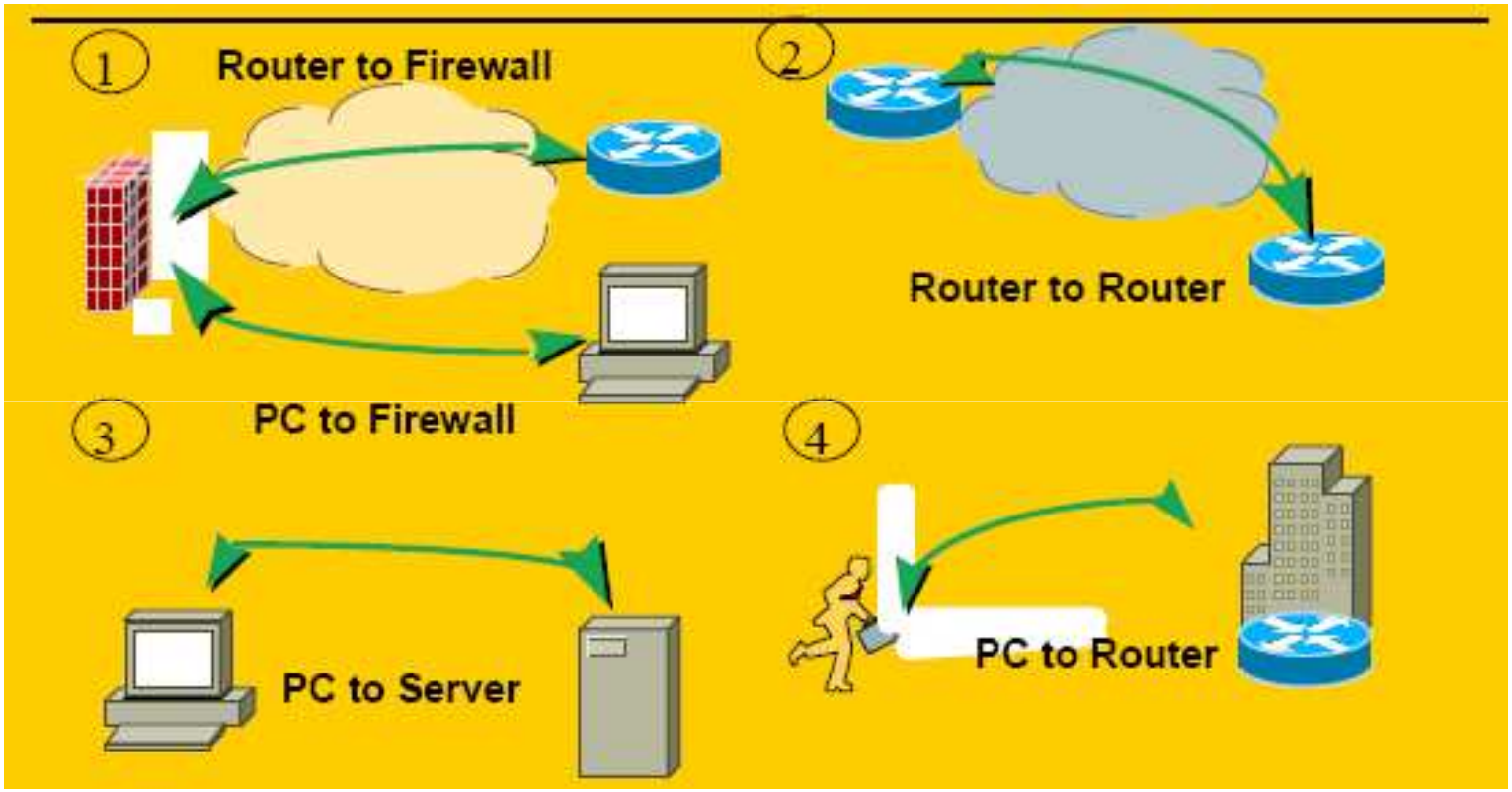
- Phase 2 : **Quick Mode**
  - Les messages échangés durant la phase 2 sont protégés en authenticité et en confidentialité grâce aux éléments négociés durant la phase 1.

  - Quick Mode est utilisé pour la négociation de SA pour des protocoles de sécurité donnés comme Ipsec. Chaque négociation aboutit en fait à deux SA, une dans chaque sens de la communication.:
    - **AH ou ESP.**
    - **Adresse destination**

IKE (Internet Key Exchange)



Où tourne IPsec



- **2 modes :**
  - **mode transport (de host à host seulement) : seul le champ data est chiffré**
  - **mode tunnel : tout le paquet IP d'origine est chiffré, ajout d'une entête IP de tunnel**

IPSEC : configuration

- L'administrateur du réseau définit, par le biais de politiques de sécurité configurées dans chaque élément IPSEC du VPN, comment le trafic va être sécurisé (notion de « SA selectors », « SPD »).

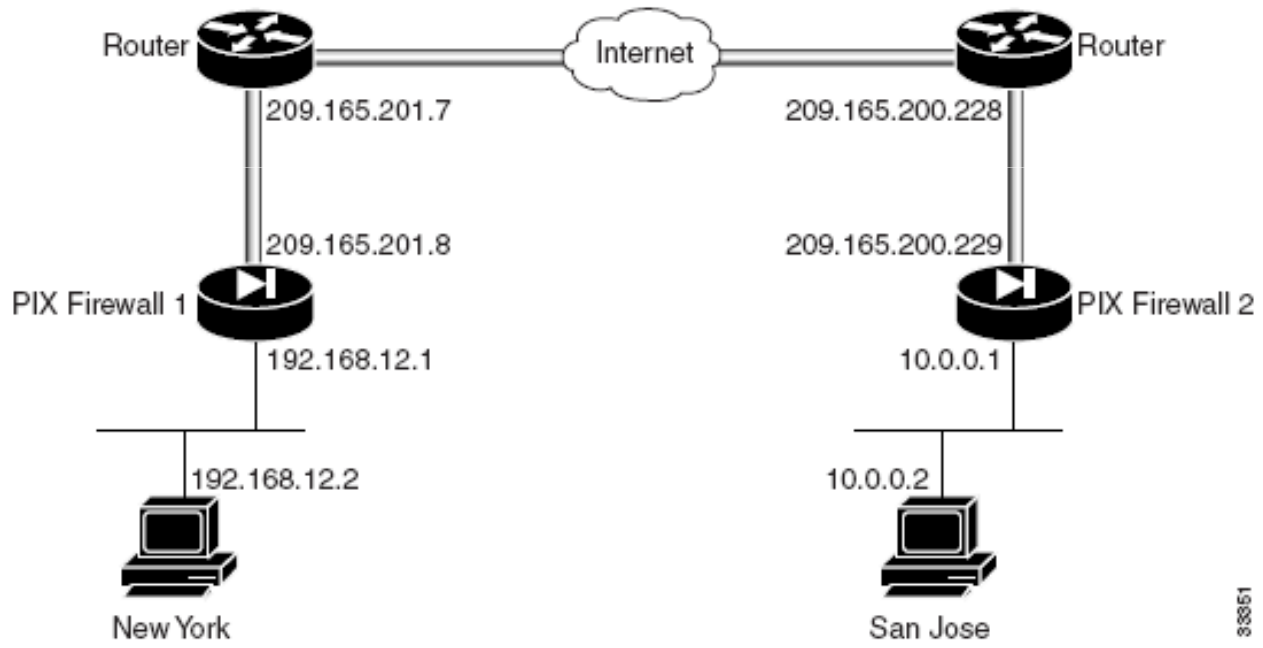
- Politiques = ensemble de règles qui :
  - permettent, pour chaque paquet IP, de décider s'il se verra apporter des services de sécurité, sera autorisé à passer outre ou sera rejeté.
  - indiquent à IKE quelles associations de sécurité il doit négocier, et, en particulier, quels tunnels sécurisés il doit établir.

- Configuration des équipements IPsec = configuration manuelle des politiques de sécurité sur chaque équipement (sur CISCO, équivalent des access-lists)

- Des systèmes de gestion centralisée et dynamique de ces politiques («policy servers») sont en cours d'élaboration.

Exemple de configuration cisco

Figure 7-1 VPN Tunnel Network



Exemple de configuration cisco

- **L'exemple de cette configuration sur le firewall 1**
  - Using Pre-Shared Keys, (on peut avoir recours à une CA vois le dernier slite)
- **Step 1** : Define a host name:
  - **hostname NewYork**
- **Step 2** : Configure an ISAKMP policy:
  - **isakmp enable outside**
  - **isakmp policy 9 authentication pre-share**
  - **isakmp policy 9 encrypt 3des**
- **Step 3** :Configure a pre-shared key and associate with the peer:
  - **crypto isakmp key cisco1234 address 209.165.200.229**
- **Step 4** Configure the supported IPSec transforms:
  - **crypto ipsec transform-set strong esp-3des esp-sha-hmac**

Exemple de configuration cisco

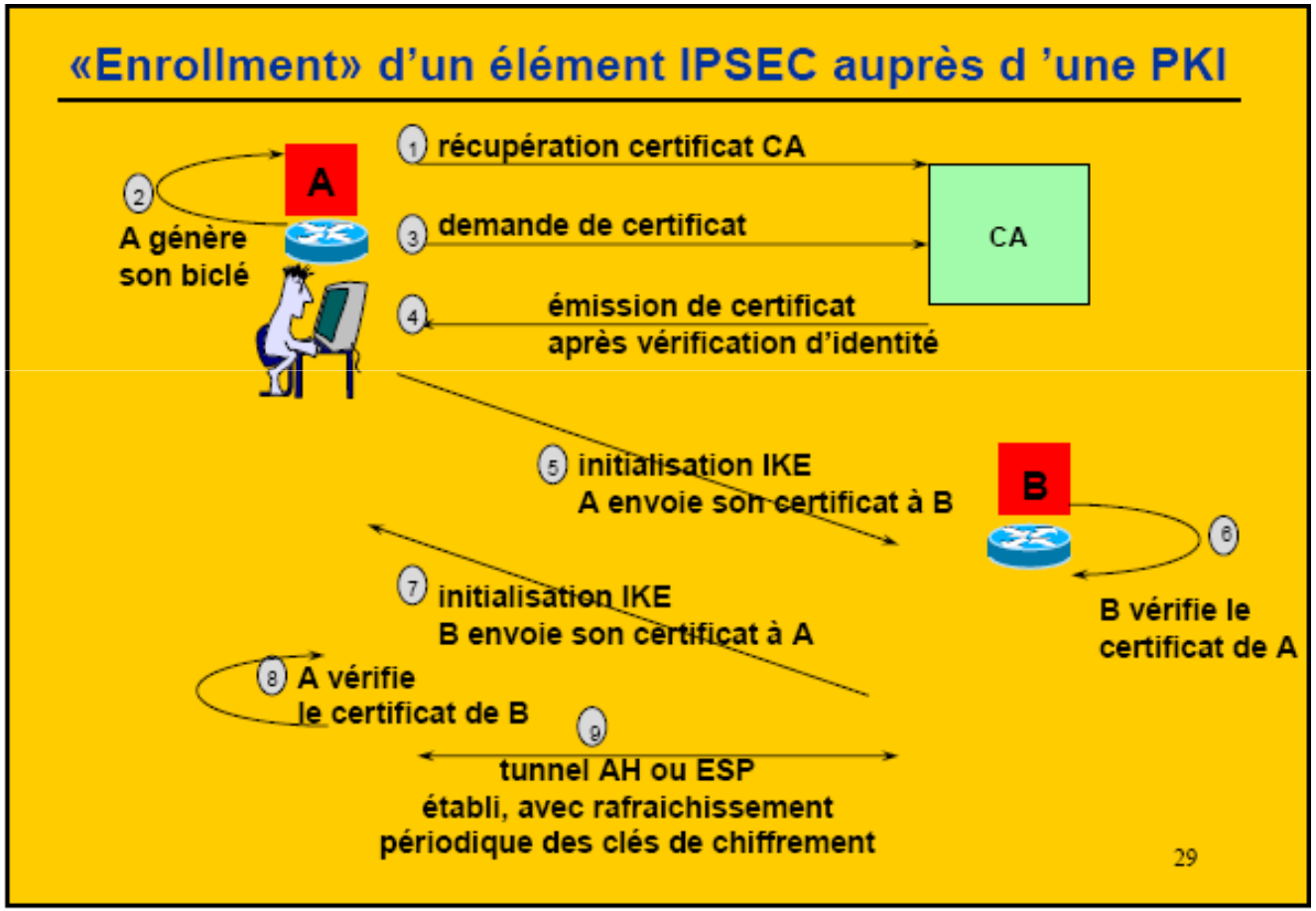
- **Step 5** Create an access list:
  - **access-list 90 permit ip 192.168.12.0 255.255.255.0 10.0.0.0 255.0.0.0**
- **Step 6** Exclude traffic between the intranets from NAT:
  - **nat 0 access-list 90**
  - This excludes traffic matching access list 90 from NAT. The **nat 0 command is always processed before** any other **nat commands.**
- **Step 7** Enable NAT for all other traffic:
  - **nat (inside) 1 0 0**
- **Step 8** Assign a pool of global addresses for NAT and PAT:
  - **global (outside) 1 209.165.201.9-209.165.201.30**
  - **global (outside) 1 209.165.201.7**
  - The pool of registered addresses are only used for connections to the public Internet.

Ces étapes ne sont pas obligatoire : elles permettent définir du NAT puisque on traverse un réseau publique.

Exemple de configuration cisco

- **Step 9** Define a crypto map (spécifie la politique IPSec: Quel trafic à sécuriser, où doit être envoyé le trafic à sécuriser, les adresses locales (ACL) utilisées par la trafic IPsec):
  - **crypto map toSanJose 20 ipsec-isakmp**
  - **crypto map toSanJose 20 match address 90**
  - **crypto map toSanJose 20 set transform-set strong**
  - **crypto map toSanJose 20 set peer 209.165.200.229**
- **Step 10** Apply the crypto map to the outside interface:
  - **crypto map toSanJose interface outside**
- **Step 11** Specify that IPSec traffic be implicitly trusted (permitted):
  - **sysopt connection permit-ipsec**
- **La même configuration doit se faire pour l'autre PIX.**

IPsec: utilisation des certificats



Evolution du standard IPSec

- IPSec est en constante évolution afin d'intégrer entre autres les derniers standards cryptographiques (AES...). Voici une liste non-exhaustive des tendances actuelles :
  - Numéros de séquence étendus (64 bits): cela est rendu nécessaire par l'utilisation d'algorithmes beaucoup plus performants et des débits gigantesques (Gbit/s).
  - Amélioration des sélecteurs de SPD.
  - Nouveaux protocoles d'échanges de clés supportés (IKEv2, Sigma, JFK...)
  - Simplification du design et amélioration de la robustesse du protocole
  - Support d'AES en mode CBC.
  - Nouveaux modes d'intégrité seule.

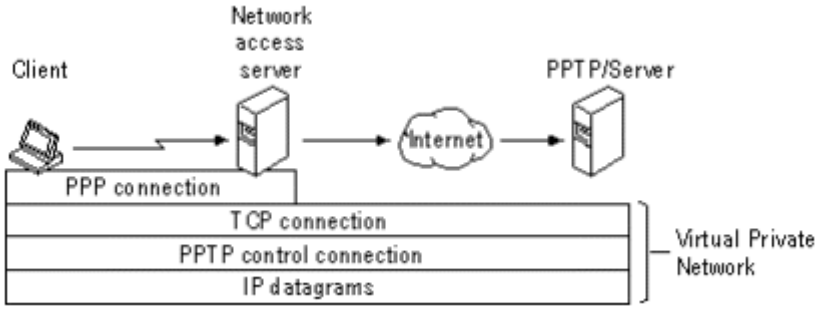
- D'autre part, de nombreux groupes (à l'IETF par exemple) travaillent actuellement sur des problèmes liés à IPSec afin d'améliorer sont intégration dans tous les environnements :
  - IPSec et NAT.
  - Langages standards de police de sécurité et négociations inter-domaines
  - Protocoles de découverte des passerelles de sécurité

Les protocoles niveau 2

- Il existe sur le marché trois principaux protocoles :
  - PPTP (Point to Point Tunnelling Protocol) de Microsoft
  - L2F (Layer Two Forwarding) de Cisco
  - L2TP (Layer Two Tunnelling Protocol) de l'IETF.

Point to Point Tunnelling Protocol (PPTP)

- La technologie réseau **PPTP** est une extension du protocole d'accès distant **Point-to-Point Protocol**.
- Une ébauche de ce document a été soumise à l'IETF en juin 1996 par les compagnies du forum PPTP, qui inclut Microsoft Corporation, Ascend Communications, 3Com/Primary Access, ECI Telematics et US Robotics.
- Le protocole PPTP est inclus dans les systèmes d'exploitation Windows NT® Server version 4.0.
- Généralement il y a 3 ordinateurs impliqués dans tout
  - un client PPTP
  - un serveur d'accès réseau
  - un serveur PPTP



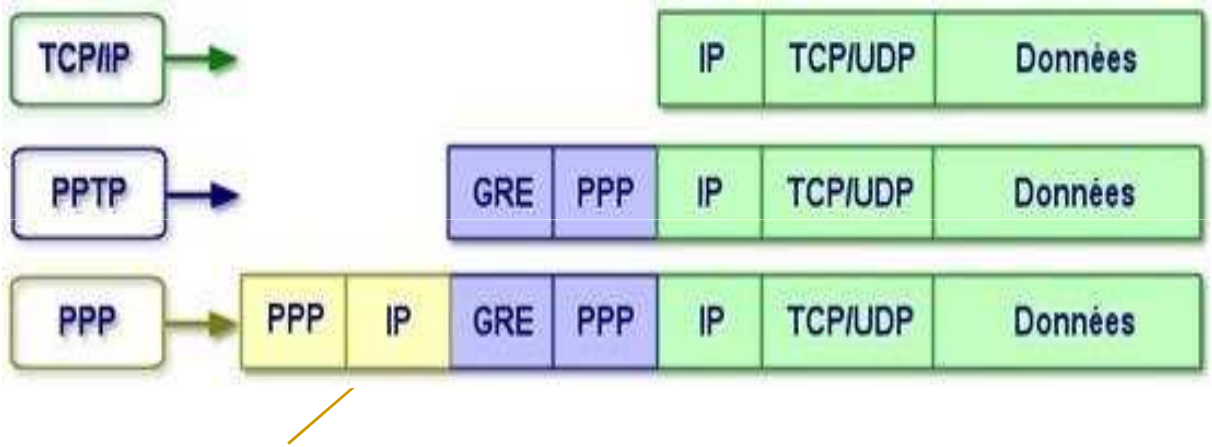
- C'est un protocole de niveau 2 qui encapsule des trames **PPP** dans des datagrammes IP afin de les transférer sur un réseau IP. PPTP permet le cryptage des données PPP encapsulées mais aussi leur compression.

Point to Point Tunnelling Protocol (PPTP)

- PPTP est un protocole de niveau 2 qui permet le cryptage des données ainsi que leur compression.
- L'authentification se fait grâce au protocole **MS-CHAP** de Microsoft :
  - Déjà cracké (version 1).
  - Microsoft a corrigé ces défaillances et propose aujourd'hui une version 2 de Ms-Chap plus sûre
- La partie chiffrement des données s'effectue grâce au protocole **MPPE** (Microsoft Point-to-Point Encryption)

Point to Point Tunnelling Protocol (PPTP)

- Le schéma suivant montre comment un paquet PPTP est assemblé avant d'être transmis par un client distant vers un réseau cible.



- L'en-tête de délivrance **IP** fournit les informations nécessaires pour que le datagramme passe par l'Internet.
- Le **GRE** (**G**eneric **R**outing **E**ncapsulation**) :** est un protocole développé par Cisco. (**RFC 2784**). L'en-tête GRE est utilisé pour encapsuler la trame PPP dans le datagramme IP.

- **Notez que le paquet PPP est juste un bloc incompréhensible car il est crypté. Même si le datagramme IP était intercepté, il serait presque impossible de décrypter les données**

L2TP (Layer Two Tunnelling Protocol)

- L2TP est un protocole réseau qui encapsule des trames **PPP** pour les envoyer sur des réseaux IP, X25, relais de trames ou ATM.

- Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunnelling sur Internet. Mais L2TP peut aussi être directement mis en œuvre sur des supports WAN (relais de trames) sans utiliser la couche de transport IP.

- On utilise souvent ce protocole pour créer des VPN sur Internet. Dans ce cas, L2TP transporte des trames PPP dans des paquets IP. Il se sert d'une série de messages L2TP pour assurer la maintenance du tunnel et d'UDP pour envoyer les trames PPP dans du L2TP