

# VPN

## IP security Protocol

### Architectures VPN

Communication layers	Security protocols
Application layer	ssh, S/MIME, PGP
Transport layer	SSL, TLS, WTLS
Network layer	IPsec <b>MPLS</b>
Data Link layer	PPTP, L2TP
Physical layer	Scrambling, Hopping, Quantum Communications

© Ahmed Mehaoua - 2

# **Sécurisation des communications IP**

- Pour sécuriser les échanges ayant lieu sur un réseau TCP/IP, il existe plusieurs approches :
  - niveau applicatif (PGP)
  - niveau transport (protocoles TLS/SSL, SSH)
  - niveau physique (boîtiers chiffrant).
- IPsec vise à sécuriser les échanges au niveau de la couche réseau.
- IPsec veut dire IP Security Protocols : ensemble de mécanismes de sécurité commun à IPv4 et IPv6.

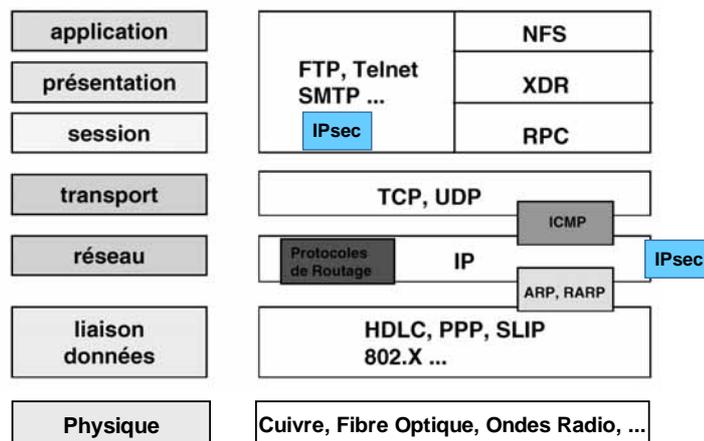
- **I. Normalisation d'IPsec**
- **II. Modes d'IPsec**
- **III. Protocoles de sécurité AH**
- **IV. Protocole de sécurité ESP**
- **V. Fonctionnement SA, SAD, SPD**
- **VI. Gestion, distribution des clefs – IKE / ISAKMP**
- **VII. Faiblesses d'IPsec**
- **VIII. Application et solutions IPsec : les VPN**

## IPSec : le standard

- Norme prévue pour IPv6
- Adaptée à IPv4, vu la lenteur de déploiement IPv6 et les besoins forts des entreprises
- Série de RFC : 2401, 2402, 2406, 2408
- Très nombreuses pages !!

© Ahmed Mehaoua - 5

## IPsec et l'architecture TCP/IP



## I. Normalisation d'IPsec

- ☞ l'IETF (Internet Engineering Task Force) débute la normalisation de IPv6 en 1994.
- ☞ Introduction des services de sécurité: IPsec (Internet Protocol Security) 1995.
- ☞ IPsec natif sur IPv6 et optionnel sur IPv4.
- ☞ 1998 IPsec intègre son protocole d'échange de clés (IKE - Internet Key Exchange).
- ☞ Publication des RFC du protocole IPsec en 1995 puis 1998.
- ☞ A la fin de l'année 1999 IPsec s'impose sur le marché.

## Les services IPsec

- **Services de sécurités offerts par IPsec :**
  - **Authentification des extrémités**
  - **Confidentialité des données échangées**
  - **Authenticité des données**
  - **Intégrité des données échangées**
  - **Protection contre les écoutes et analyses de trafic**
  - **Protection contre le rejeu**
- **2 modes d'exploitation d'IPsec :**
  - **Transport : Protège juste les données transportées (LAN)**
  - **Tunnel : Protège en plus l'en-tête IP (VPN)**
- **IPsec permet :**
  - **La mise en place de VPN**
  - **Sécuriser les accès distants (Utilisation nomade)**
  - **Protection d'un serveur sensible**

## Composants d'IPsec

- Protocoles de sécurité :
  - Authentication Header (AH)
  - Encapsulation Security Payload (ESP)
- Protocole d'échange de clefs :
  - Internet Key Exchange (IKE)
- Bases de données internes :
  - Security Policy Database (SPD)
  - Security Association Database (SAD)

## I. Normalisation d'IPsec par l'IETF

RFC 2401	Security Architecture for the Internet Protocol			
RFC 2402	IP Authentication Header	S. Kent, R. Atkinson	Novembre 1998	STANDARD
RFC 2406	IP Encapsulating Security Payload (ESP)			

## Quel protocole pour quel service de sécurité ?

Table 16.1 IPSec Services

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	✓	✓	✓
Connectionless integrity	✓		✓
Data origin authentication	✓		✓
Rejection of replayed packets	✓	✓	✓
Confidentiality		✓	✓
Limited traffic flow confidentiality		✓	✓

© Ahmed Mehaoua - 11

## I. Normalisation d'IPsec Problèmes IP

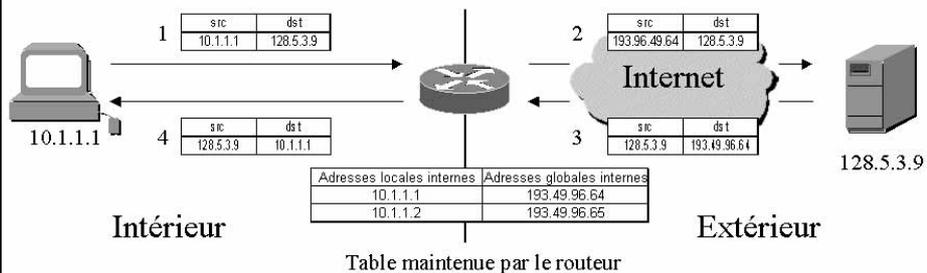
1. saturation de l'espace d'adressage prévue pour 2010
  - a. Utiliser les adresses IP privées avec un protocole de translation d'adresse (NAT: Network Address Translation)
  - b. Augmenter la taille du champ adresse (IP version 6 avec champ adresse de 128 bits -> incompatibilité)
2. Lacunes en sécurisation des communications
  - a. Réseaux Privés IP virtuels ou Virtual Private Network IP (VPN)
  - b. IP security (IPsec)

# Adresses IP Privées

- Classe A : 10.0.0.0 - 10.255.255.255
- Classe B : 172.16.0.0 - 172.31.255.255
- Classe C : 192.168.0.0 - 192.168.255.255

## « NAT »

- Network Address Translation :



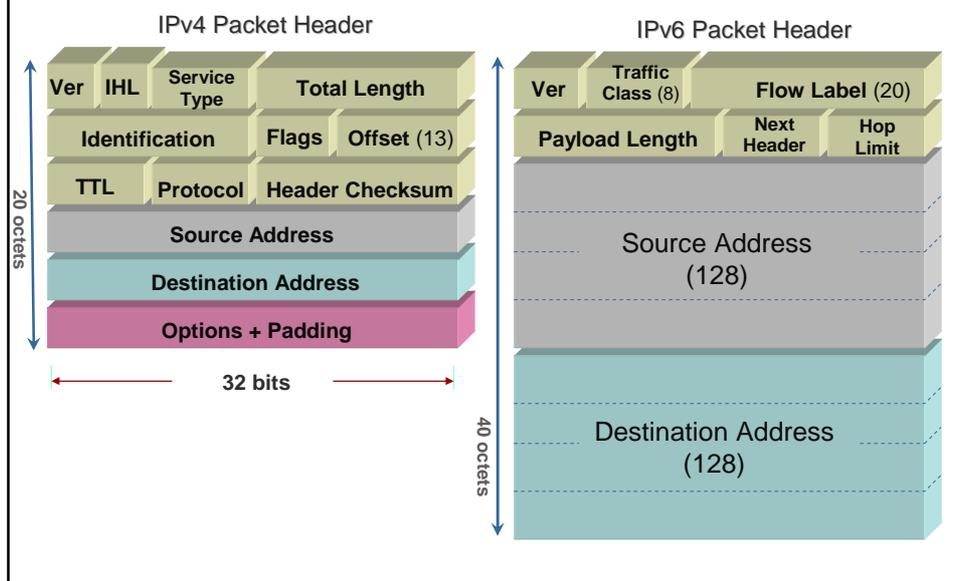
# IPv6 : Objectifs

1. Résoudre le problème de pénurie d'adresses d'IPv4 :
  - 4.3 Milliards IPv4 disponibles – 240 Millions réellement utilisables
  - 172 millions de hosts IPv4 actifs (Janv. 2003)
  - 73 % des adresses IPv4 sont octoyées aux organismes nord-américains
    - Vietnam (100 Millions d'hab. – 4 classes C)
    - Sénégal (10 millions d'hab. - 16 adresses de classe C)
    - Tunisie (8 millions d'hab. – 16 classes C pour l'administration)
2. Résoudre les problèmes de dimensionnement des tables de routage :
  - Mars 2002: 150 000 routes IP4 + 400 routes IP6 ds les routeurs backbones BGP
  - Accroissement de 20% par an
  - L'horizon de l'Internet est de 40 routeurs
  - Route moyenne traverse 25 routeurs;
3. Inclure de nouvelles fonctionnalités :
  - La sécurité, La mobilité,
  - La configuration automatique des stations
  - La qualité de service, etc...

# Solutions IPsec avec IPv6

- CISCO IOS 12.2 et supérieure
- JUNIPER JUNOS 5.1 et supérieure
  
- Windows NT et Windows 2000 avec l'installation d'un patch
  - [Research.microsoft.com/msripv6/](http://Research.microsoft.com/msripv6/)
  - [www.microsoft.com/Windows2000/technologies/communications/ipv6/](http://www.microsoft.com/Windows2000/technologies/communications/ipv6/)
- Windows XP en natif
  - Taper la commande « ipv6 install » puis vérifier avec « ipv6 if »
  - Applications IPv6 livrées : ping6, traceroute, ftp, telnet, IE, IPsec,
- MacOS 10.1 et MacOS X
  
- IBM AIX 4.3 et supérieure
- Solaris 8 et supérieure
- Compaq True64 UNIX et OpenVMS v5.1 et supérieure,
- HP-UX 11i et supérieure
- Linux 2.4 et supérieure (RedHat 7.1 – Mandrake 8.0)
- FreeBSD 4.0 et supérieure

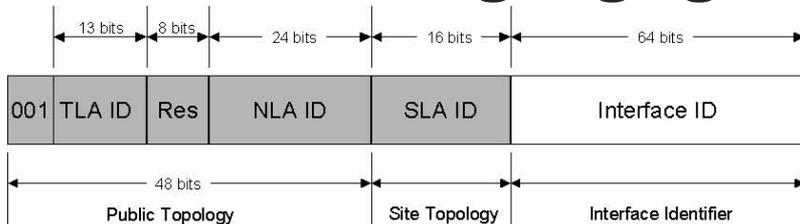
## IPv4 vs IPv6



## IPv6 : adressage

- **Passage de 4 à 16 octets pour l'adressage (RFC 3513):**
  - $2^{128} \cong 3 \times 10^{38}$  équipements adressables
  - $6 \times 10^{22}$  adresses au m<sup>2</sup> sur terre
- **Plan d'adressage agrégé : Adressage hiérarchique (RFC 2374)**
  - Diminution taille des tables de routage / temps de traitement des paquets
  - En pratique :
    - $10^{33}$  adresses (dû à la hiérarchie)
    - $3 \times 10^{18}$  adresses par mètre carré sur la terre
- **3 niveaux de hiérarchie :**
  1. Une topologie publique (48 bits) : TLA Top Level Aggregator
  2. Une topologie de site (16 bits) : SLA Site Level Aggregator
  3. Un identifiant d'interface (64 bits) : IID Interface Identifier
- **3 types d'adresse IPv6 :**
  1. globales (utilisation du plan agrégée),
  2. site local ou link local, etc... (adresses privées)
  3. compatible IPv4 ou adresse "mappée" (tunneling)

## Plan d'adressage Agrégé



- **Format Prefix (3 bits)** Type de Plan d'adressage
  - 001 : plan agrégé
  - 010 : plan de test
- **Top Level Aggregator (13 bits)** identifie les fournisseurs/opérateurs internat.
- **Reserved (8 bits)** pour utilisation future (entre TLA et NLA)
- **Next Level Aggregator (24 bits)** identifie les fournisseurs/opérateurs régionaux ainsi que l'identifiant du site (décomposition et allocation sous la responsabilité du TLA)
- **Site Level Aggregator (16 bits)** identifie les sous-réseaux dans le site (sous la responsabilité de l'administrateur du site)

## Allocation des Adresses



Internet Corporation  
For Assigned Names  
and Numbers



RIR  
Regional Internet  
Registries



NIR  
National Internet  
Registries



LIR  
Local Internet  
Registries

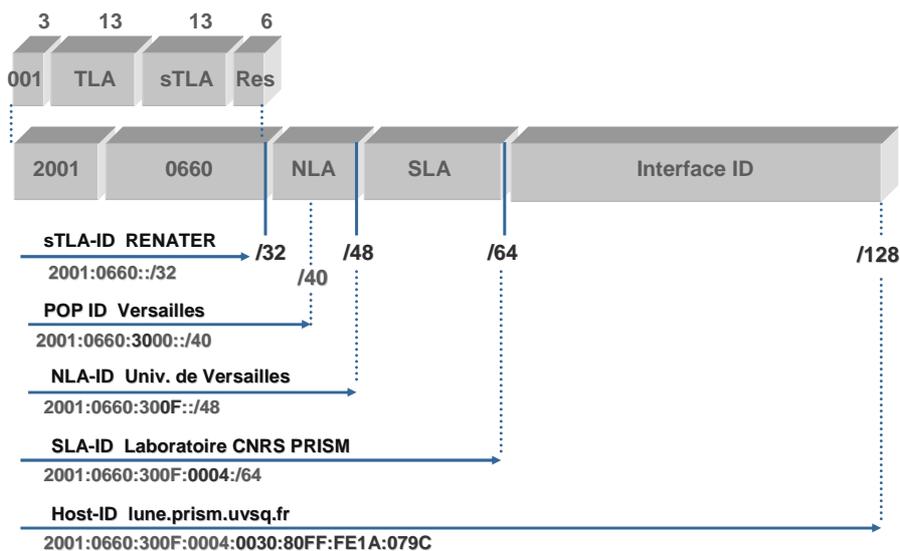


End Users

# Attribution des Adresses

- Pour obtenir un préfixe sub-TLA de 32 bits en Europe (délais 48h):
  - Être membre du RIPE-NCC (Réseaux IP Européen-Network Coordination Centre)
    - Abonnementt annuel : 2750-3750-5250 Euros (dépend du nbre @ utilisés)
  - Remplir le formulaire RIPE-195 sur [www.ripe.net](http://www.ripe.net) puis l'envoyer à [hostmaster@ripe.net](mailto:hostmaster@ripe.net)
    - France Telecom                    2001:0688::/32    (depuis juin 2000)
    - Renater                                2001:0660::/32
    - Nerim                                    2001:07A8::/32
    - Tiscali                                  2001:BC8::/32
  
- 4 Conditions d'attribution à vérifier (Phase de BootStrap):
  1. Être un opérateur IPv4 avec au moins 3 peering actifs avec d'autres AS
  2. Avoir au moins 40 clients IPv4 ou une expérience sur le réseau test 6bone (pTLA)
  3. Envisager d'offrir des services IPv6 dans les 12 prochains mois
  4. Maintenir un service DNS forward (AAAA) et reverse (ip6.int)

# Allocation des Adresses



## II. Modes d'IPsec

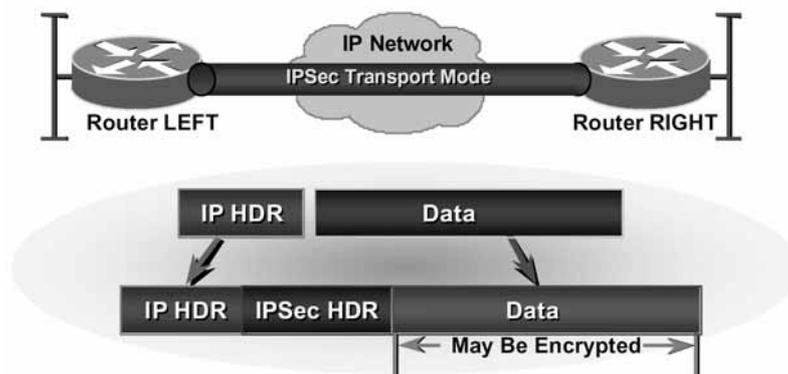
- mode transport

- insertion transparente entre TCP et IP
- pas de masquage d'adresse
- facilité de mise en œuvre
- ⇒ sécurise de bout en bout les échanges entre deux utilisateurs.

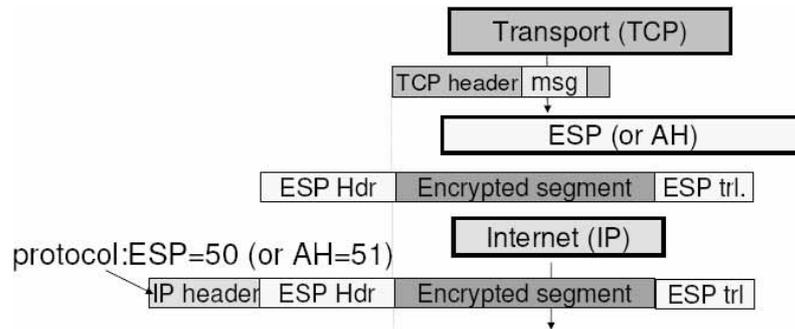
- mode tunnel

- insertion après IP
- encapsulation des datagrammes IP dans d'autres datagrammes IP
- masquage d'adresse
- ⇒ sécurise lien par lien les segments de réseau.
- ⇒ utilisé quand au moins une des deux extrémités d'IPsec se comporte comme une passerelle

### IPsec : Mode Transport

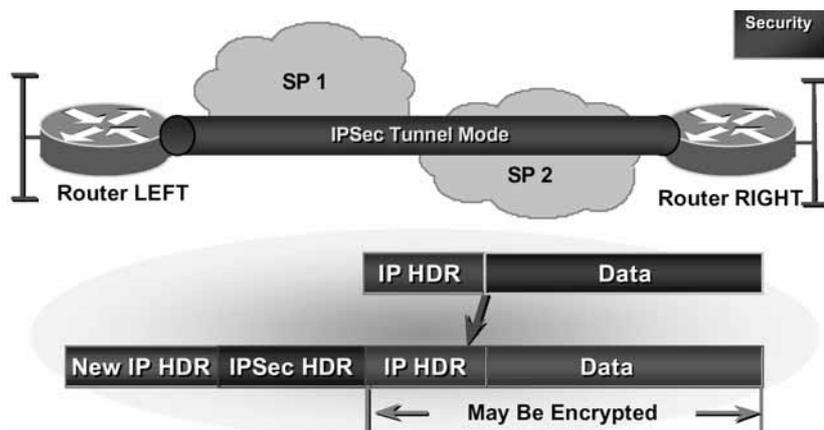


# Transport Mode Encapsulation

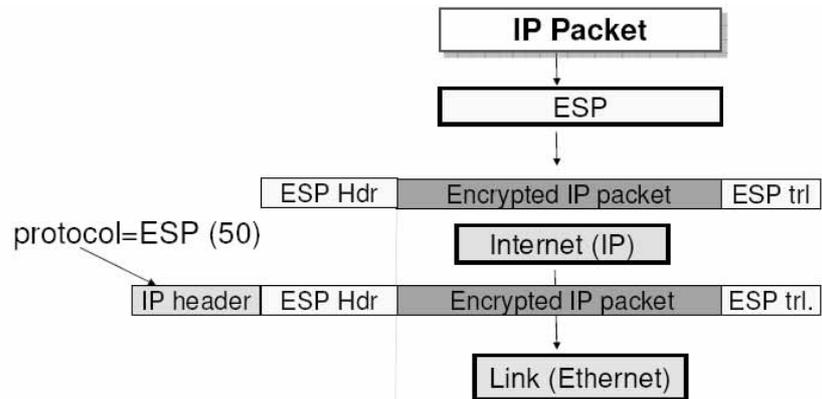


© Ahmed Mehaoua - 25

# IPsec : Mode Tunnel



## Tunnel Mode Encapsulation



© Ahmed Mehaoua - 27

### III. Protocole de sécurité AH

- AH = Authentication Header : 1er protocole et aussi le plus simple
- définit dans le RFC 2402
- Garantit :
  - l'authentification.
  - l'unicité (anti-rejeu)
  - l'intégrité

! Pas de confidentialité !

=> les données sont seulement signées mais pas chiffrées  
support des algorithmes MD5 (128 bits) et SHA-1

# IPSec protocols – AH protocol

- **AH - Authentication Header**

- Defined in RFC 1826
- Integrity: Yes, including IP header
- Authentication: Yes
- Non-repudiation: Depends on cryptography algorithm.
- Encryption: No
- Replay Protection: Yes

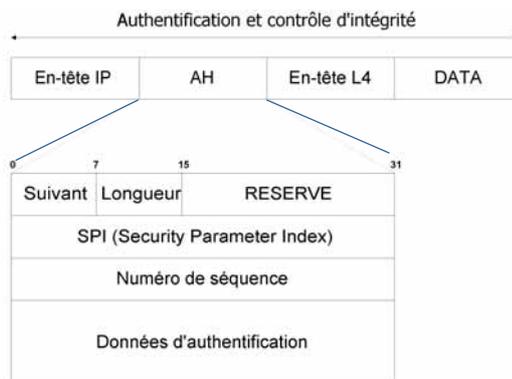
Transport Packet layout



Tunnel Packet layout



## III. Protocole de sécurité AH



IPv4+AH

## IV. Protocole de sécurité ESP

- ESP = Encapsulating Security Payload
- définit dans le RFC 2406
- Seules les données sont protégées (pas de protection en-tête)
- Garantit:
  - l'authentification.
  - l'unicité (anti-rejeu)
  - l'intégrité
  - la confidentialité

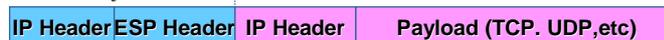
## IPSec protocols – ESP protocol

- **ESP – Encapsulating Security Payload**
  - Defined in RFC 1827
  - Integrity: Yes
  - Authentication: Depends on cryptography algorithm.
  - Non-repudiation: No
  - Encryption: Yes
  - Replay Protection: Yes

Transport Packet layout



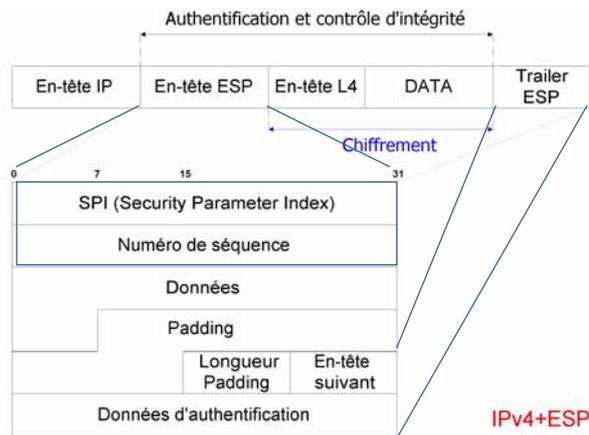
Tunnel Packet layout



Unencrypted

Encrypted

## IV. Protocole de sécurité ESP



## V. Fonctionnement SA, SAD, SPD

### ① SA : 'Security Association'

- Les Associations de sécurité (SA) définissent les paramètres des divers mécanismes utilisés pour la sécurisation des flux sur le réseau privé virtuel
- A chaque SA correspond un bloc de données identifié par un index et contenant les informations correspondantes
- Plus précisément, chaque association est identifiée de manière unique à l'aide d'un triplet composé de :
  - le SPI (Security Parameter Index) : index de la SA défini par le récepteur
  - l'adresse de destination des paquets
  - l'identifiant du protocole de sécurité (AH ou ESP)

## V. Fonctionnement SA, SAD, SPD

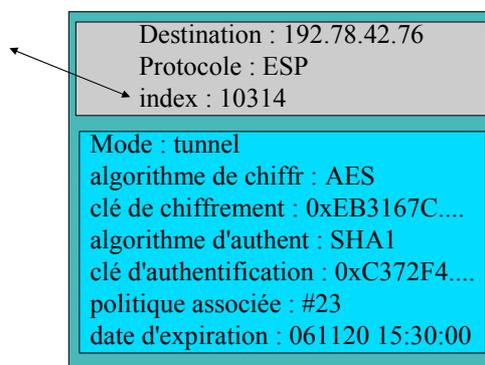
### ① SA : 'Security Association' (suite)

Les informations échangées sont :

- index de la SA appelé SPI (pour Security Parameter Index)
- un numéro de séquence, indicateur utilisé pour le service d'anti-rejeu
- une fenêtre d'anti-rejeu : compteur 32 bits
- dépassement de séquence
- paramètres d'authentification (algorithmes et clés)
- paramètres de chiffrement (idem)
- temps de vie de la SA
- mode du protocole IPsec (tunnel ou transport)

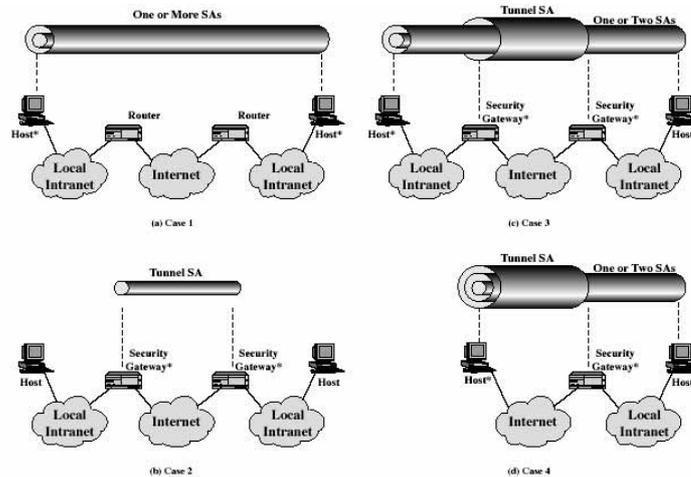
**Attention : un SA est Unidirectionnelle: protéger les deux sens d'une communication classique requiert deux associations.**

## SA : exemple



© Ahmed Mehaoua - 36

## Combinaison des SA



\* = implements IPSec

iaoua - 37

## V. Fonctionnement SA, SAD, SPD

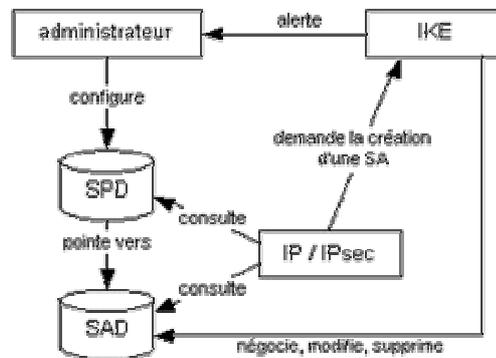
### ② SAD : Security Association Database

- base de données des SA pour la gestion des associations de sécurité actives
- consultée pour savoir quels mécanismes il faut appliquer à chaque paquet reçu ou à émettre.

### ③ SPD : Security Policy Database

- base de données des politiques de sécurité (SPD).
- Pour savoir comment appliquer les mécanismes sur les paquets

## V. Fonctionnement SA, SAD, SPD



## V. Fonctionnement SA, SAD, SPD

Exemple 1 : trafic sortant

- 1) IPsec reçoit des données à envoyer
- 2) Consultation de la base de données SPD (quel traitement pour ces données ?)
- 3) Mécanismes de sécurité pour ce trafic ?
- 4) Oui ⇒ récupération des caractéristiques requises pour la SA et consultation de la base SAD
- 5) SA existe ?
- 6) Oui ⇒ utilisée pour traiter le trafic en question  
Non ⇒ appel à IKE pour établir une nouvelle SA

## V. Fonctionnement SA, SAD, SPD

Exemple 2 : trafic entrant

- 1) Réception paquet
- 2) Examen l'en-tête: services IPsec appliqués ?
- 3) Oui ⇒ références de la SA ? ⇒ consultation de la SAD
- 4) Déchiffrement
- 5) Consultation de la SPD : « SA du paquet correspond bien à celle requise par les politiques de sécurité ? »

## VI. Gestion, distribution des clés – IKE / ISAKMP

- Problématique : afin d'échanger des données de façon sécurisée, il est nécessaire de se mettre d'accord sur les paramètres à utiliser, et notamment d'échanger les clés de session
- Il faut 2 paires de clés (AH et ESP) : soit 2 par direction.
- 1er solution : configuration manuelle des équipements
  - (unique méthode proposée dans la première version d'IPSec...)
- 2eme solution : gestion dynamique des paramètres au moyen d'un protocole sécurisé adapté
  - système automatique pour la création à la demande des clés pour les SA
  - Plusieurs solutions : SKIP, Prothuris, Oakley, SKEME and ISAKMP → IKE
  - IKE est un protocole orienté connexion utilisé par les équipements IPsec pour échanger et gérer les associations de sécurité à travers l'Internet :
    - Echange de clés à l'aide de protocoles cryptographiques
    - Fournit une authentification des entités
    - Permet un établissement de SA à travers un réseau non sécurisé

## **VI. Gestion, distribution des clefs – IKE / ISAKMP**

❶ IKE : Internet Key Exchange : Qu'est ce que c'est ?

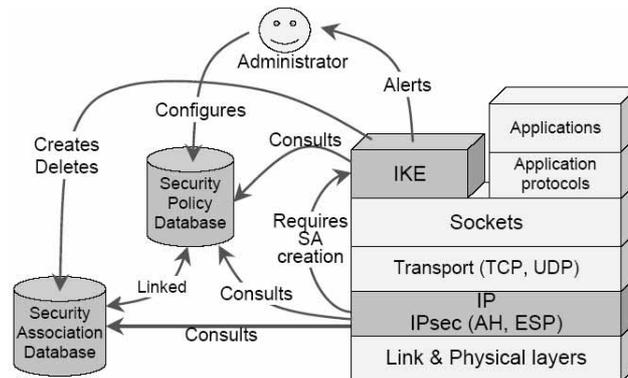
- IKE est un ensemble de protocoles et de mécanismes assurant une gestion sécurisée et dynamique des paramètres de sécurité utilisés dans IPSec
- IKE = échange de clés d'authentification + gestion des SA
  
- Basé sur des améliorations des protocoles ISAKMP/Oakley (dont la sécurité et la "scalabilité" étaient limitées)
  
- RFC 2409
- Deux manières d'échanger des clefs :
  - clefs pré-partagées
  - certificats X.509

## **relations IPSec-IKE-SA**

- SA->traitement à mettre en oeuvre sur un paquet IP quand il faut appliquer IPSec
  
- IKE->gestionnaire de SA
  
- IPSec->utilisateur de SA

## VI. Gestion, distribution des clefs – IKE / ISAKMP

### ① IKE : Internet Key Exchange



## VI. Gestion, distribution des clefs – IKE / ISAKMP

### ② ISAKMP : Internet Security Association and Key Management Protocol

- associé à une partie des protocoles SKEME et Oakley
- négociation des paramètres (algorithmes de chiffrement...)
- mécanisme de négociation découpé en deux phases:
  - Phase 1: **définition des moyens pour protéger les échanges suivants.**
    - 2 modes possibles :**
      - normal (6 messages et protection d'identité)
      - agressif (3 messages)
    - Phase 2: **négociation des paramètres des futures SA.**

## **IKE (Internet Key Exchange)**

- **Phase I: Oakley Main Mode (DH key exchange & authentication)**
  - **To negotiate bi-directional ISAKMP Security Association (SA)**  
[ISAKMP: Internet Security Association & Key Management Protocol]
    - An encryption algorithm
    - A hash algorithm
    - A Diffie-Hellman group identifier
  - **Authentication methods**
    - Pre-Shared Secret
    - Digital Signature (Digital Certificate)
    - Public Key Encryption (Encrypted Nonce)
- **Phase I: Oakley Aggressive Mode**
  - **No identity protection**
- **Phase II: Oakley Quick Mode**
  - **To negotiate IPSec Security Association (SA)**
    - <Security Parameter Index, IP Destination Address, Security Protocol>
  - **To negotiate keys to protect data traffic**

## **Internet Security Association and Key Management Protocol (ISAKMP)**

- Defines procedures and packet formats to establish, negotiate, modify and delete security associations
- Defines payloads for exchanging key generation and authentication data
- ISAKMP message consists of an ISAKMP header followed by one or more payloads

## VII. Faiblesses d'IPsec

- Limitations dues à la gestion manuelle des clefs
  - AH et ESP s'appuient sur des numéros de séquence initialisés à 0 lors de la création d'une SA et incrémentés lors de l'envoi de chaque datagramme.
  - Numéros de séquence sont stockés dans un entier de 32 bits  $\approx$  4 milliards
  - Passé cette limite, nécessité de créer une nouvelle SA et donc une nouvelle clef.
  - Possibilité de désactivation des numéros après la limite.
  
- Broadcast et multicast
  - Problème de performance et impossibilité de résolution par l'augmentation de la puissance.

## VII. Faiblesses d'IPsec (suite)

- Firewalls
  - Le filtrage de datagrammes IPsec est délicat pour deux raisons :
    - les RFCs ne précisent pas si, sur un système remplissant simultanément les fonctions de passerelle de sécurité et de firewall, le décodage de l'IPsec doit avoir lieu avant ou après l'application des règles de firewalling ;
    - il n'est pas possible au code de firewalling de lire certaines données, par exemple des numéros de port, dans des données chiffrées, ou transmises dans un format qu'il ne connaît pas.
  
- NATs
  - Théoriquement, aucune translation d'adresse ne devrait affecter un datagramme IPsec, car ce type d'opération modifie le contenu des datagrammes, ce qui est incompatible avec les mécanismes de protection de l'intégrité des données d'IPsec.

## VII. Faiblesses d'IPsec (suite 2)

- Non support de protocoles réseaux autres qu'IP

IPsec est un protocole qui ne prévoit que le convoyage sécurisé de datagrammes IP

Ceci n'est pas suffisant, car d'autres standards comme IPX et NetBIOS sont utilisés sur un grand nombre de réseaux. Il existe cependant une solution à ce problème : encapsuler les données à protéger dans du PPP, lui-même transporté par IPsec. Le rôle de PPP est en effet de permettre la transmission de différents protocoles au-dessus d'un lien existant.

- Partie 3 VPN IP sécurisé avec IPsec -

## ➤ VIII. Application de IPsec : les VPN

---

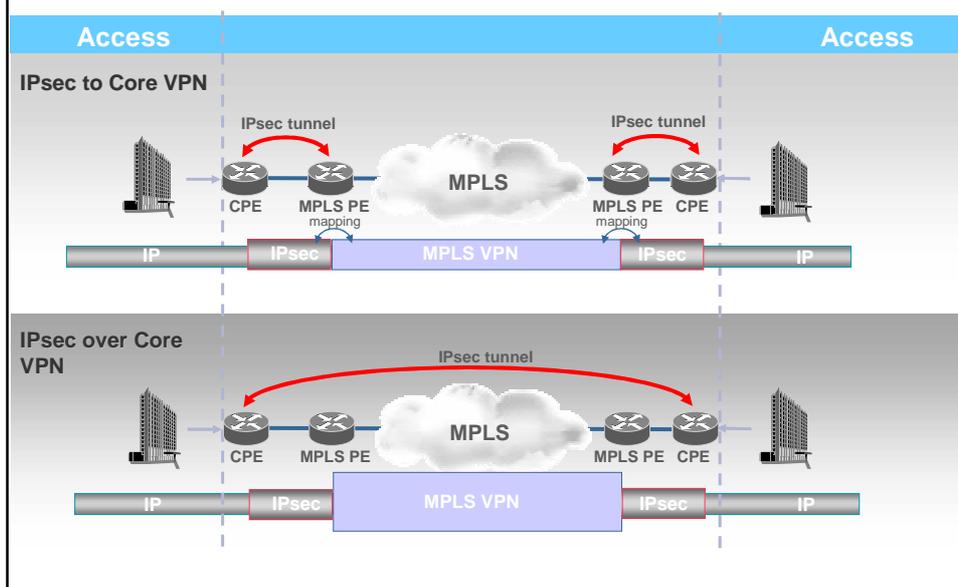
**A “VPN service” is a service which offers secure, reliable connectivity over a shared public network infrastructure such as the Internet. Because the infrastructure is “shared”, connectivity can be provided at lower cost than existing dedicated private networks**

---

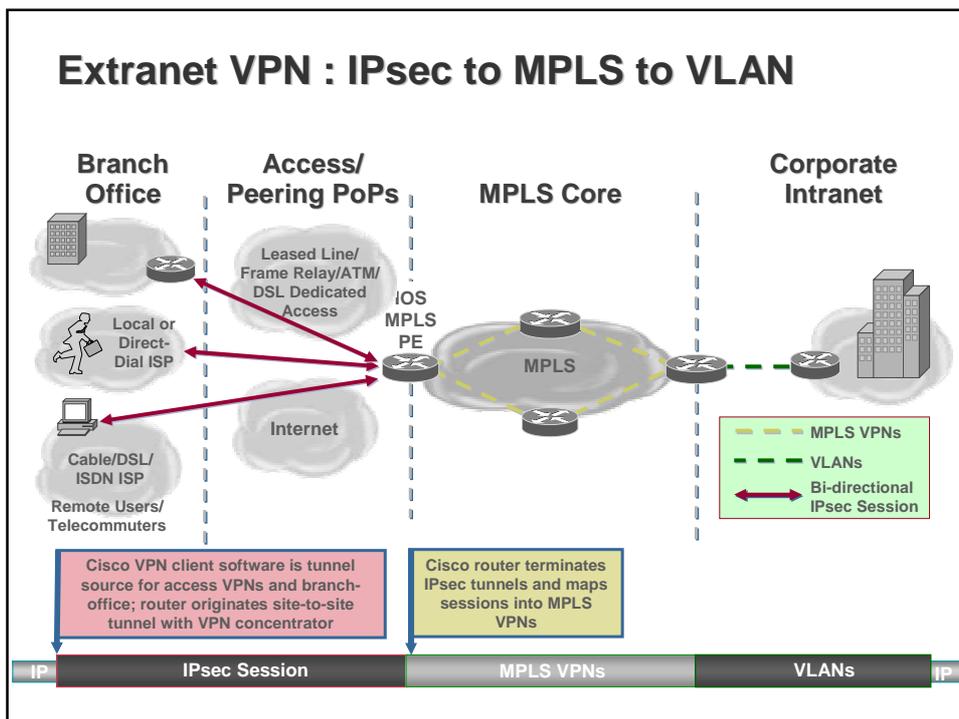
## Typologie des technologies VPN

- VPN de niveau 2
- VPN IP avec IPSEC
- VPN IP avec MPLS
- VPN SSL

### ➤ VIII. Application de IPsec : les VPN

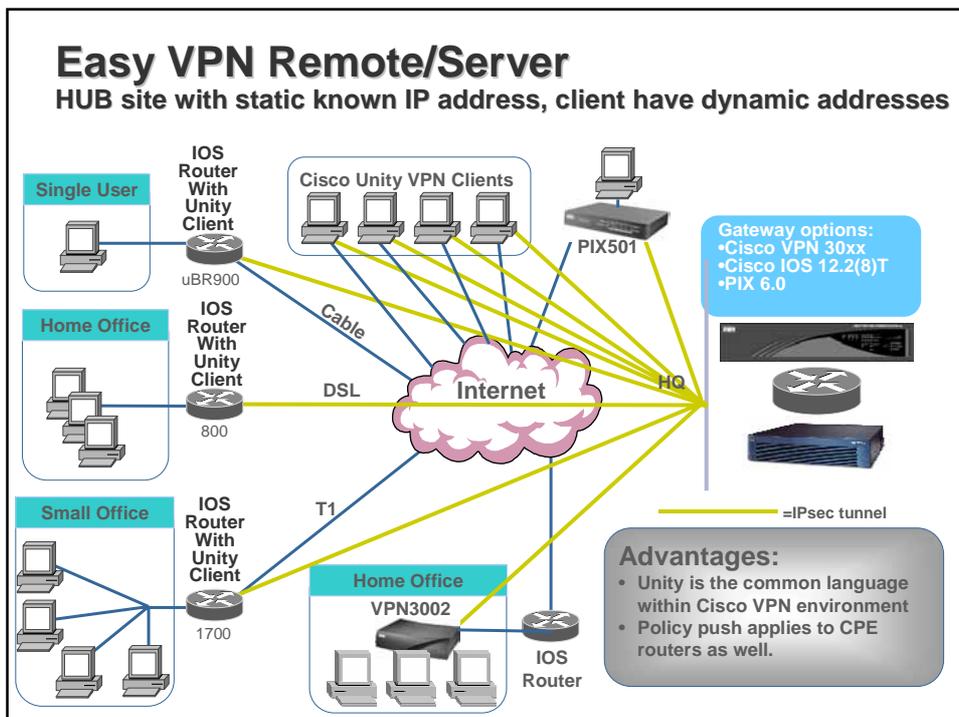


## Extranet VPN : IPsec to MPLS to VLAN



## Easy VPN Remote/Server

HUB site with static known IP address, client have dynamic addresses



## Les offres commerciales de VPN pour l'entreprise

Les grands acteurs en France et en Europe aujourd'hui:

- Level 3
- France Telecom (Oleane VPN)
- Easynet
- Qwest
- Global Crossing

## VPN IP- Offre en France -

Il existent 10 offrent de réseaux privés virtuel IP en France (01réseaux/Sept. 2002)

- |                    |  |
|--------------------|--|
| ❖ Cable & Wireless | (IPsec, aucune classe, 50 PoP nat, 49 PoP int.)      |
| ❖ Cegetel/Infonet  | (MPLS, 3 classes: Std, Data, Tps réel, 160, 55 pays) |
| ❖ Colt             | (IPsec, 4, 13, via offre IP Corporate)               |
| ❖ FT/Global One    | (MPLS, 3, 60, 140)                                   |
| ❖ KPNQwest         | (IPSec, 5 classes, 30, 300)                          |
| ❖ Maiaah           | (MPLS, 5, 7, via réseaux tiers)                      |
| ❖ QoS Networks     | (IPSec, 5 classes, 1, 9)                             |
| ❖ LDcom/Siris      | (MPLS, 4 classes, 77, 0)                             |
| ❖ Worldcom         | (MPLS)   |

## Critère des choix d'un fournisseur de VPN

- La bande passante proposée
- La qualité de service négociée (SLA)
- Gamme d'options d'accès en boucles locales
- Assistance