VPN
IP security Protocol

Plan

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

Architectures VPN

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

MPLS

© Ahmed Mehaoua - 3

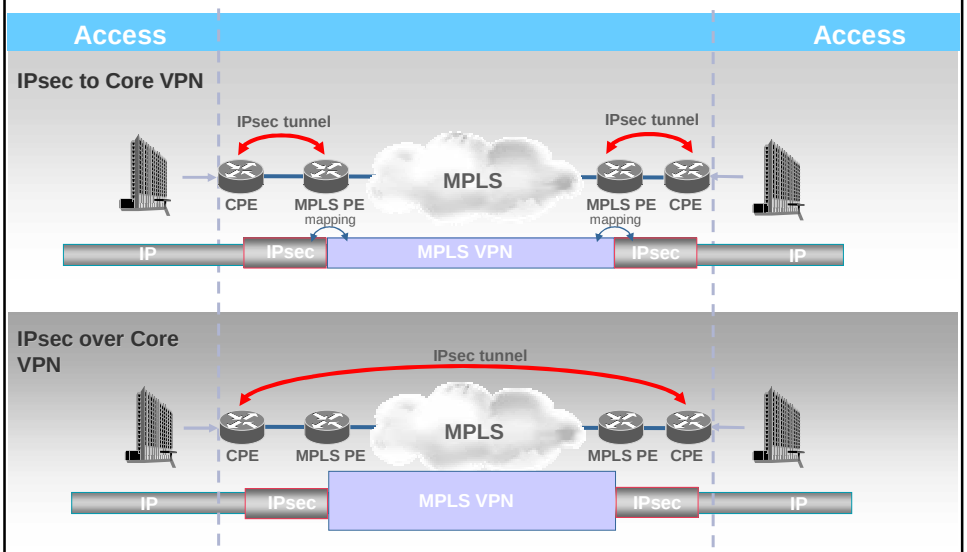
➢ VIII. Application de IPsec : les VPN

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

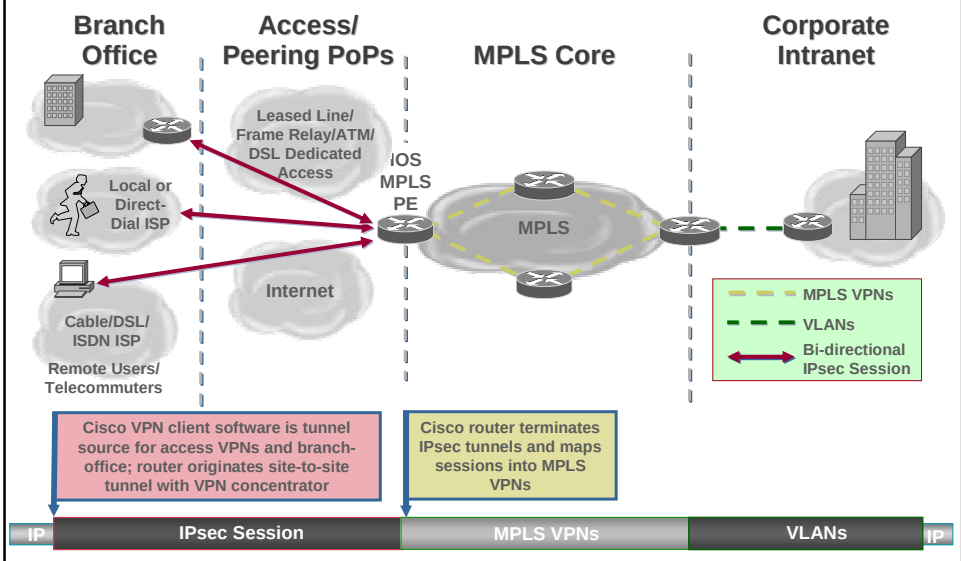
Typologie des technologies VPN

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

➢ VIII. Application de IPsec : les VPN

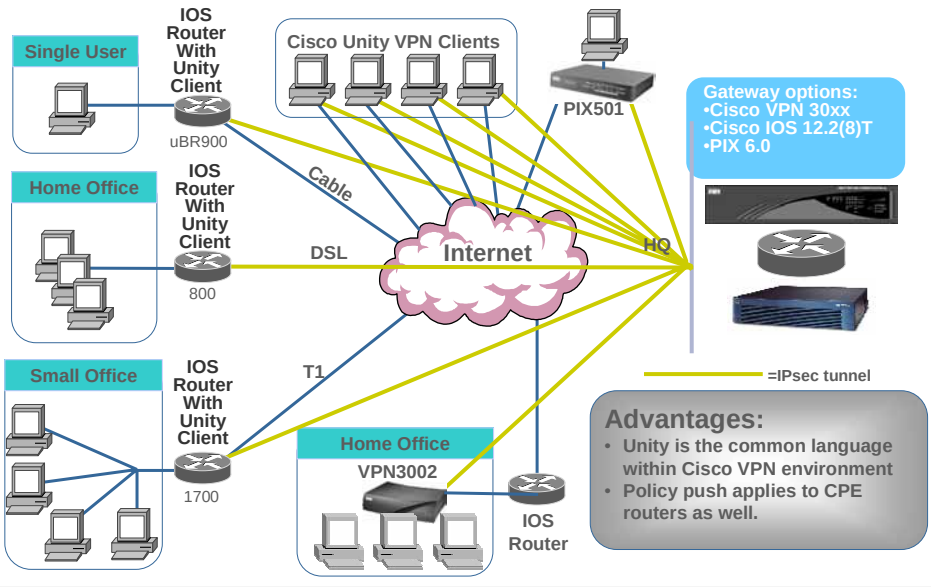


Extranet VPN : IPsec to MPLS to VLAN



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

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.

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 - 13

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	S. Kent, R. Atkinson	Novembre 1998	STANDARD
RFC 2402	IP Authentication Header			
RFC 2406	IP Encapsulating Security Payload (ESP)			

© Ahmed Mehaoua - 16

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		✔	✔

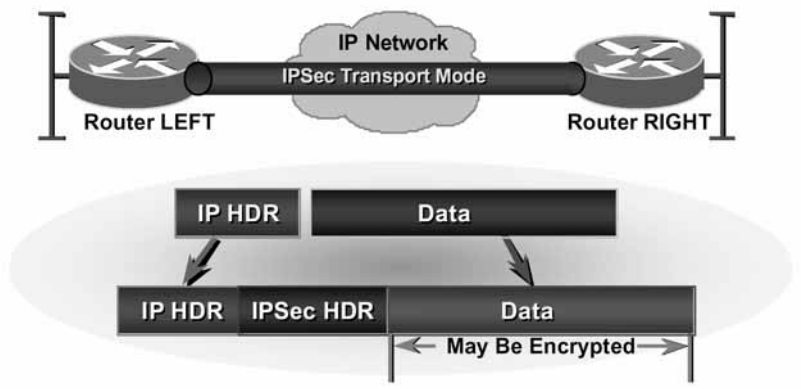
© Ahmed Mehaoua - 17

II. Modes d'IPsec

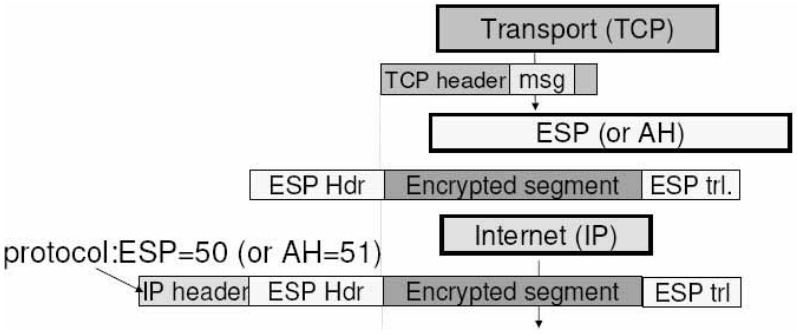
• mode transport
- insertion transparente entre TCP et IP
- pas de masquage d'adresse
- facilité de mise en œuvre
⇨ sécurise de bout en bout les échanges entre deux utilisateurs.

• 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

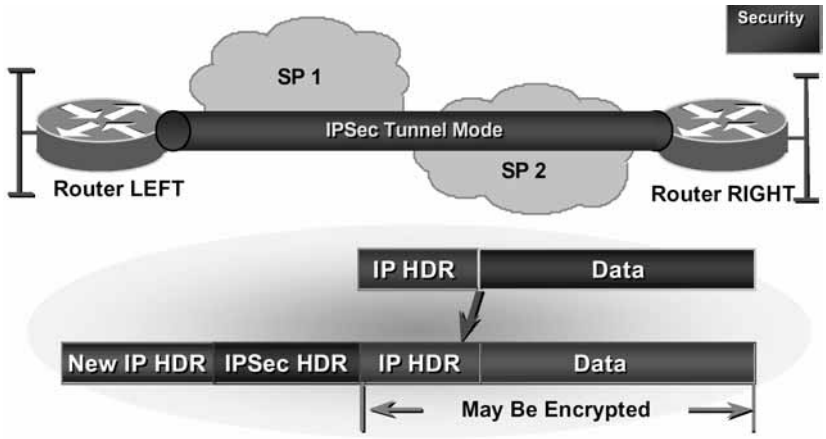


Transport Mode Encapsulation

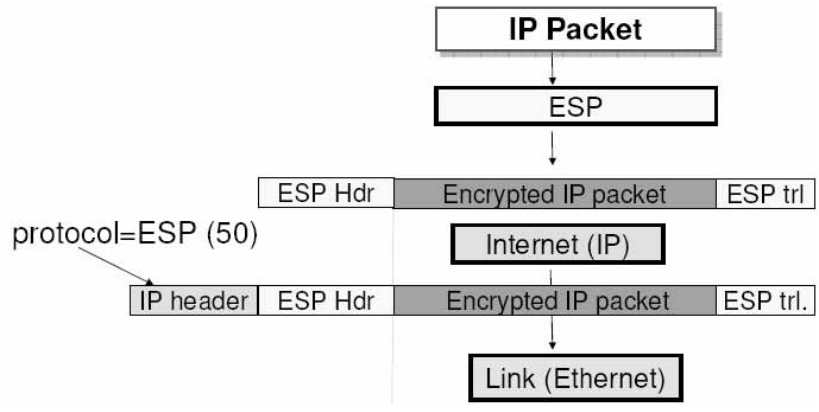


© Ahmed Mehaoua - 20

IPsec : Mode Tunnel



Tunnel Mode Encapsulation



© Ahmed Mehaoua - 22

III. Protocole de sécurité AH

- AH = Authentication Header : 1er protocole et aussi le plus simple
- définit dans le RFC 2402
- Garantit :

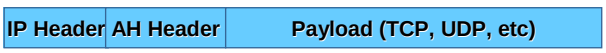
- l'authentification.
- l'unicité (anti-rejeu)
- l'intégrité

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

IPSec protocols – AH protocol

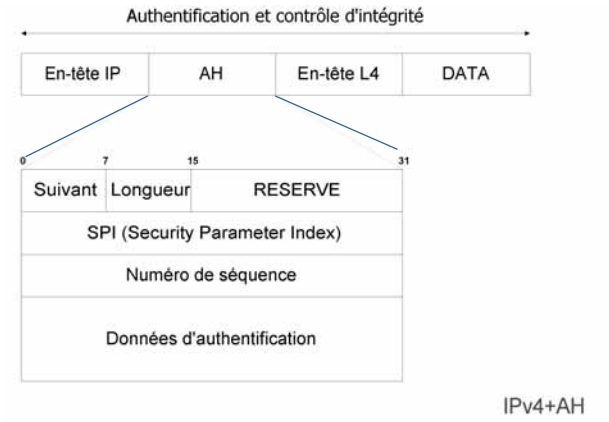
- **AH - Authentication Header**
  - **Defined in RFC 1826**
  - **Integrity: Yes, including IP header**
  - **Authentication: Yes**
  - **Non-repudiation: Depends on cryptography algorithm.**
  - **Encryption: No**
  - **Replay Protection: Yes**

Transport Packet layout



Tunnel Packet layout

III. Protocole de sécurité AH



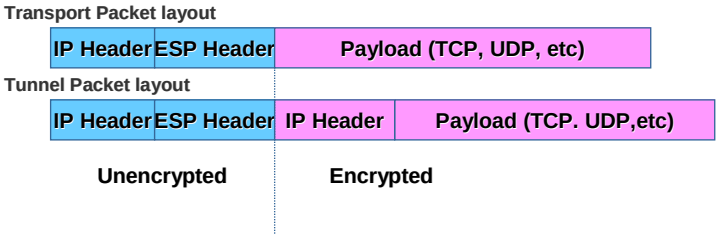
IV. Protocole de sécurité ESP

- ESP = Encapsulating Security Payload
- définit dans le RFC 2406
- Seules les données sont protégées (pas de protection en-tête)
- Garantit:

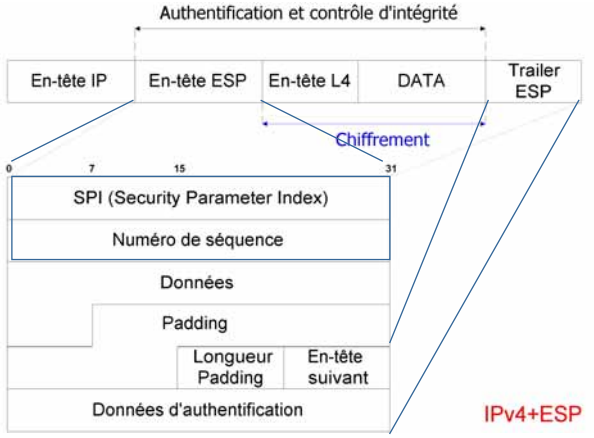
- l'authentification.
- l'unicité (anti-rejeu)
- l'intégrité
- la confidentialité

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**



IV. Protocole de sécurité ESP



V. Fonctionnement SA, SAD, SPD

❶ 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)

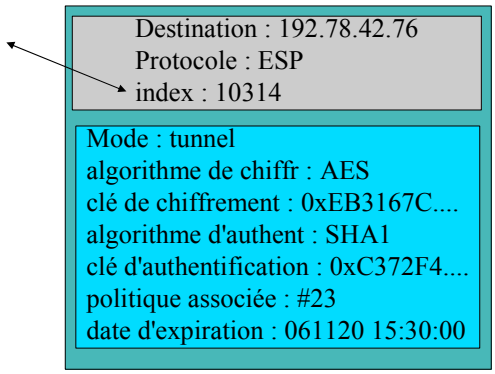
V. Fonctionnement SA, SAD, SPD

❶ 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 - 31

V. Fonctionnement SA, SAD, SPD

❷ **SAD : Security Association Database**

- base de données des SA pour la gestion des associations de sécurité actives

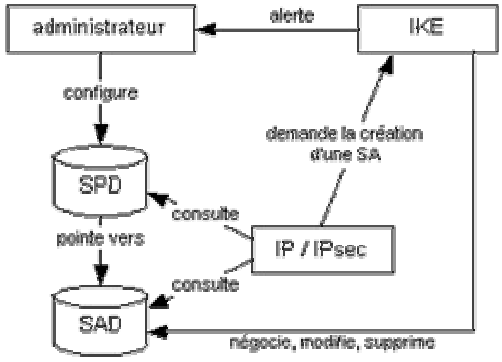
- consultée pour savoir quels mécanismes il faut appliquer à chaque paquet reçu ou à émettre.

❸ **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 clefs – IKE / ISAKMP

- Problèmatique : 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 clefs 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 creation 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 clefs 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 amélioration des protocoles ISAKMP/Oakley (dont la sécurité et la "scalabilité" étaient limitées)

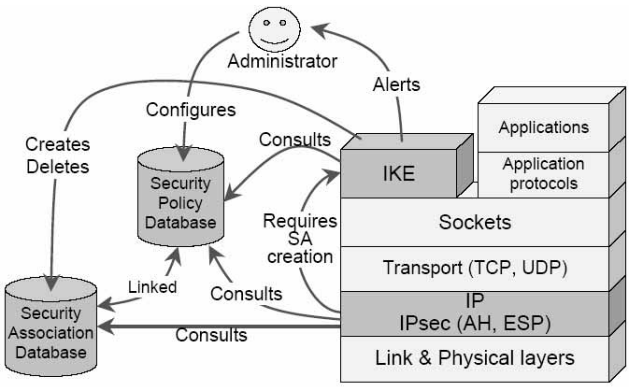
➢ RFC 2409

➢ Deux manières d'échanger des clefs :

- clefs pré-partagées
- certificats X.509

VI. Gestion, distribution des clefs – IKE / ISAKMP

❶ IKE : Internet Key Exchange



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 ≈ 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 (2)

➢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 3)

- 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.

Conclusion: IPSec-IKE-SA

- IPsec ensemble de protocoles et mécanismes pour le chiffrement de paquets IP
- SA->traitement à mettre en oeuvre sur un paquet IP quand il faut appliquer IPSec
- IKE->gestionnaire de SA
- IPSec->utilisateur de SA

© Ahmed Mehaoua - 42