

La sécurité d'IP

IPsec

Bernard Cousin



UNIVERSITE DE RENNES 1

Sécurité des réseaux informatiques

1

Plan

- Présentation d'IP Security
- L'architecture d'IPsec
- "Authentication Header"
- "Encapsulating Security Payload"
- Les associations de sécurité
- Politique de sécurité et gestion des clefs

Sécurité des réseaux informatiques

2

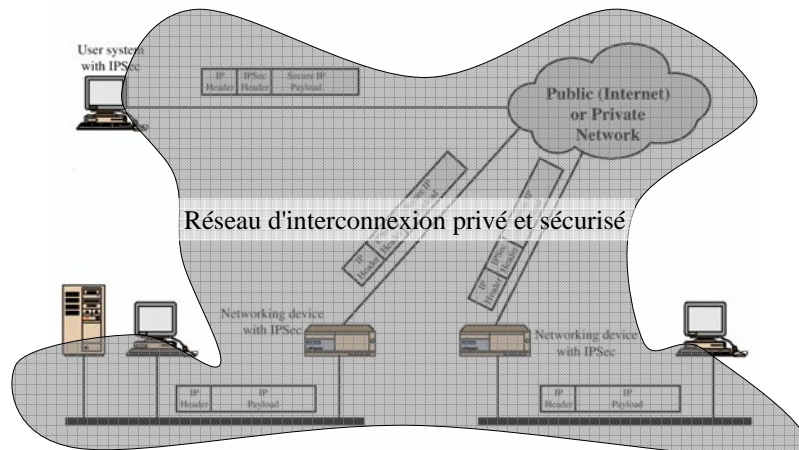
Présentation d'IPsec

- IPsec n'est pas un protocole : IPv4 ou IPv6.
- IPsec offre des services d'authentification, d'intégrité et de confidentialité
- IPsec offre un cadre général qui permet à une paire d'entités d'établir une communication sécurisée
- Les services et algorithmes utilisés sont paramétrables.

Utilisation d'IPsec

- Pour les applications :
 - Echanges sécurisés entre les sites d'une même entreprise
 - Accès sécurisés distants utilisant l'Internet
 - Etablissement d'un extranet ou d'un intranet sécurisé avec des entreprises partenaires
 - Commerce électronique sécurisé
- Pour le réseau, certifie que :
 - Les messages proviennent d'un routeur autorisé
 - Les messages de redirection proviennent d'un routeur qui a reçu le message
 - Les messages de routage ne sont pas modifiés
- IPsec est le principal procédé utilisé pour construire un VPN ("Virtual private network")

Un scénario d'utilisation d'IPsec



Sécurité des réseaux informatiques

5

Les avantages d'IPsec

- Les avantages d'IPsec
 - Transparent vis-à-vis des applications, des utilisateurs (c-à-d. de n'importe quel protocole de couche supérieure)
 - Adaptable/Paramétrable
 - Différents services
 - Différents algorithmes
 - Protège aussi bien un utilisateur individuel qu'un domaine entier

Sécurité des réseaux informatiques

6

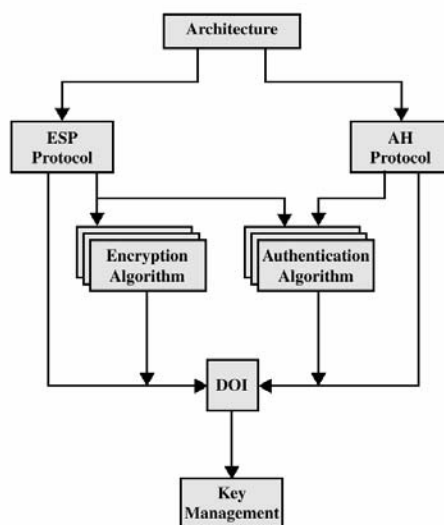
L'architecture d'IPsec

- Les normes d'IPsec :
 - RFC 2401: "An overview of security architecture"
 - RFC 2402: "Description of a packet authentication extension to IPv4 and IPv6"
 - RFC 2406: "Description of a packet encryption extension to IPv4 and IPv6"
 - RFC 2408: "Specification of key management capabilities"
 - RFC 2409 : PKI

Sécurité des réseaux informatiques

7

L'architecture d'IPsec



8

Les services d'IPSec

- Contrôle d'accès
- Intégrité des communications ("Connectionless")
- Authentification de l'origine des données
- Détection des paquets répétés (rejeu)
- Confidentialité (chiffrement)
- Confidentialité limitée du volume de trafic

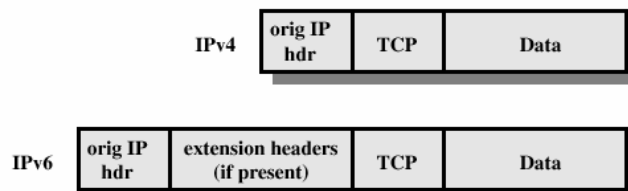
Association de sécurité (SA)

- Une relation unidirectionnelle entre un émetteur et un récepteur.
- Identifiée par 3 paramètres:
 - Security Parameter Index (SPI)
 - IP Destination address
 - Security Protocol Identifier

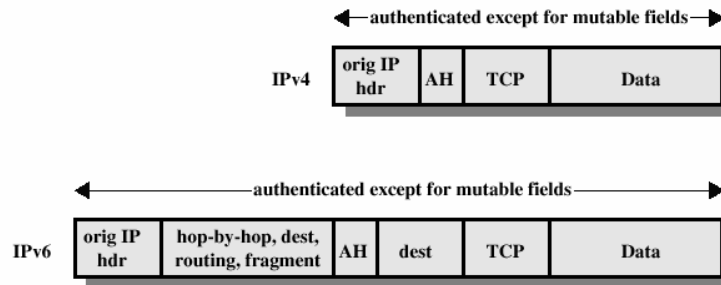
Les différents modes de sécurité d'IPsec

	Transport Mode	Tunnel Mode
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers	Authenticates entire inner IP packet plus selected portions of outer IP header
ESP	Encrypts IP payload and any IPv6 extension header	Encrypts inner IP packet
ESP with authentication	Encrypts IP payload and any IPv6 extension header. Authenticates IP payload but no IP header	Encrypts inner IP packet. Authenticates inner IP packet.

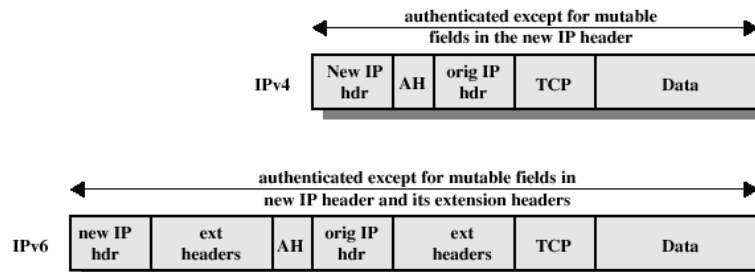
Les paquets avant transformation



Transport Mode (AH Authentication)



Tunnel Mode (AH Authentication)



L'entête d'authentification

- Offre les service d'intégrité et d'authentification (MAC code) des paquets IP.
- Protège contre le rejeu.

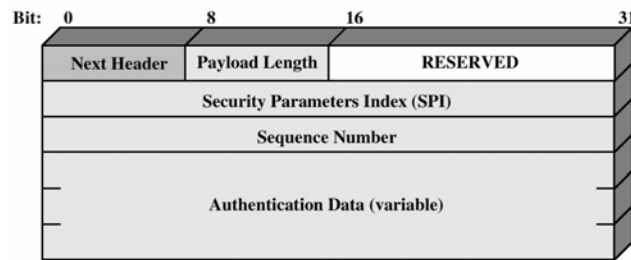
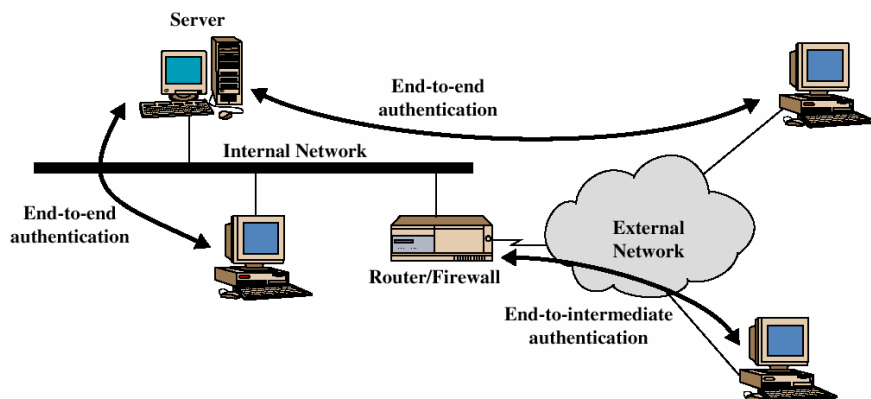


Figure 6.3 IPSec Authentication Header
Sécurité des réseaux informatiques

15

Authentification "End-to-end" ou "End-to-intermediate"



Sécurité des réseaux informatiques

16

Encapsulating Security Payload

- ESP offre un service de confidentialité et d'authentification

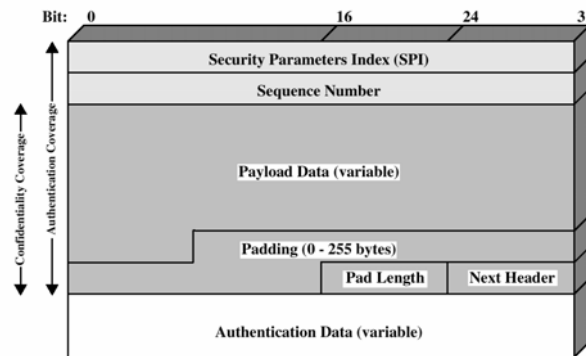


Figure 6.7 IPsec ESP Format
Sécurité des réseaux informatiques

17

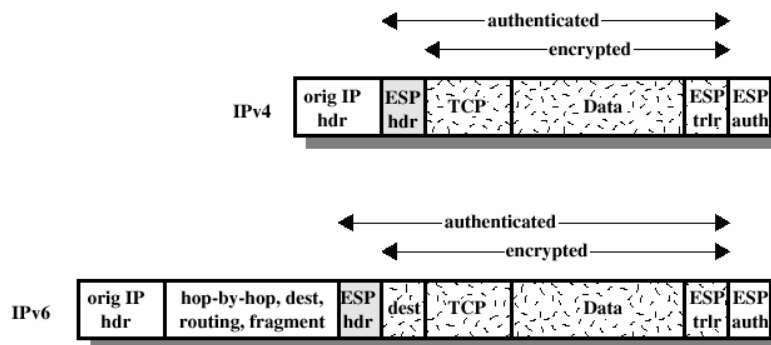
Les algorithmes de chiffrement et d'authentification

- Chiffrement :
 - Three-key triple DES
 - RC5
 - IDEA
 - Three-key triple IDEA
 - CAST
 - Blowfish
- Authentification:
 - HMAC-MD5-96
 - HMAC-SHA-1-96

Sécurité des réseaux informatiques

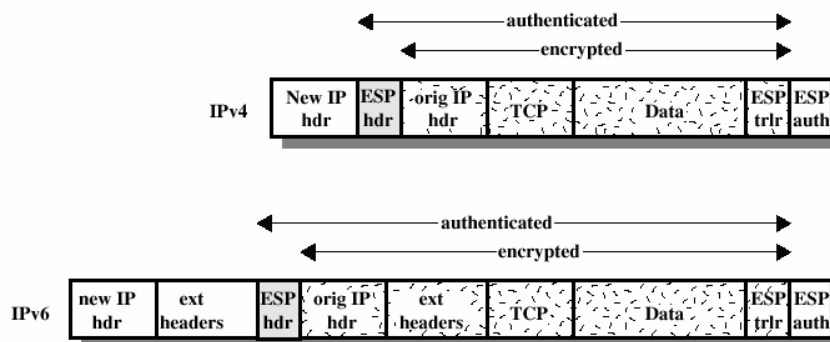
18

Chiffrement et authentification grâce à ESP



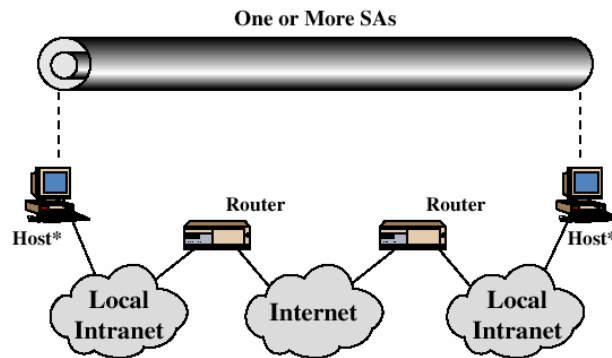
(a) Transport Mode

Chiffrement et authentification grâce à ESP



(b) Tunnel Mode

Organisation des associations de sécurité

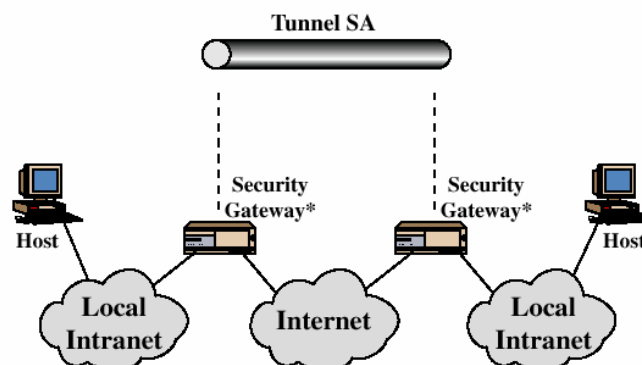


(a) Case 1

Sécurité des réseaux informatiques

21

Organisation des associations de sécurité : partielle

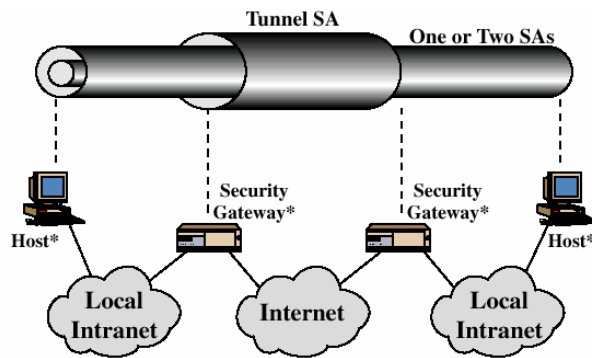


(b) Case 2

Sécurité des réseaux informatiques

22

Organisation des associations de sécurité : hiérachique

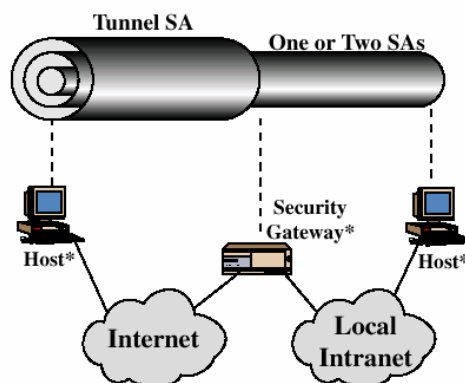


(c) Case 3

Sécurité des réseaux informatiques

23

Organisation des associations de sécurité : asymétrique



(d) Case 4

Sécurité des réseaux informatiques

24

Les services d'IPsec

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	0	0	0
Connectionless integrity	0		0
Data origin authentication	0		0
Rejection of replayed packets	0	0	0
Confidentiality		0	0
Limited traffic flow confidentiality		0	0

Politique de sécurité et IPsec

- IPsec est utilisé dans le cadre d'une politique
 - IPsec a besoin d'être paramétré
 - Pour être adapté aux services de sécurité qu'il doit rendre
 - Pour effectuer les opérations nécessaires aux traitements sécurisés
 - IPsec a besoin d'une SPD et utilise une SADB

SADB

- SADB : "Security Association DataBase"
 - Ensemble des SA établies
 - SPI + règles nécessaires au fonctionnement de cette SA :
 - Mode de sécurisation du transport
 - Algorithmes,
 - Paramètres d'IPsec

SPD

- SPD "Security Policy Database"
 - Définit la politique de sécurité associée à chaque type de paquet
 - Nom de la politique
 - Définition des sélecteurs de ce type de paquet
 - Adresse source, adresse destination, type de protocole, port, etc.
 - Traitement associé à ce type de paquet :
 - élimination,
 - "by-pass",
 - à sécuriser :
 - Définition des règles IPsec à appliquer
 - Si c'est le premier paquet de ce type alors création d'une SA

La gestion des clefs

- Pour utiliser une communication sécurisée :
 - Une SA doit exister
 - Les clés doivent avoir été échangées
 - La SADB doit être renseignée avec cette SA
- 2 types de gestion des clefs :
 - Manuel
 - Pour les environnements petits et statiques
 - Automatique
 - Création des clefs de SA à la volée (" on demand")
 - Utilisation d'un système réparti et dynamique