IPSEC

VPN's (Virtual Private Networks) :

Connexions sécurisées reliant 2 réseaux privés (ou 2 end-users) via un réseau public (p. e. Internet)

Étendent le concept d'Intranet au-delà d'un réseau privé en préservant la sécurité des communications

Reposent sur le concept de base du TUNNELING ou ENCAPSULATION de paquets de la couche réseau (ou IP selon le modèle réseau employé)

Tunneling

Encapsulation de paquets chiffrés dans de nouveaux paquets en vue de leur transmission à travers un réseau public

Intérêt

Implémenter la sécurité au niveau IP permet de protéger toutes les communications réseaux qu'elles soient initiées par des applications disposant de mécanismes de sécurité ou pas.

Assure l'authentification, l'intégrité, la confidentialité et la gestion des clé

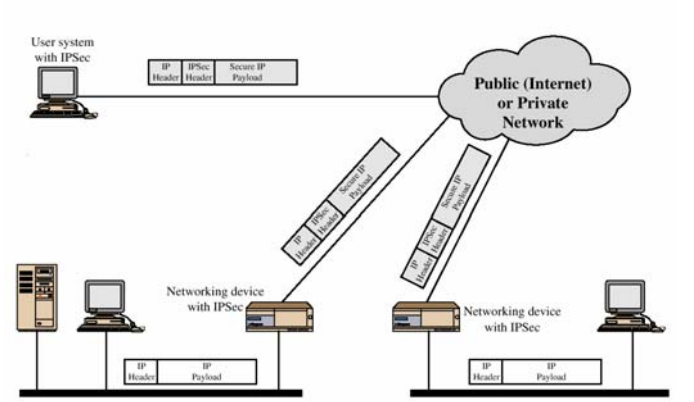
Vue générale

- IPSec n'est pas un protocole simple. Il fournit un ensemble d'algorithmes de sécurité ainsi qu'un cadre général qui permet à une paire d'entités communicantes d'employer n'importe quels algorithmes fournissant la sécurité appropriée pour la communication
- Services fournis
  - authentification
  - confidentialité
  - gestion des clés

Utilisation d'IPSEC

- applicable dans les LANs , à travers les WAN publics et privés, et pour l'Internet
- Exemples d'applications d'IPSec
  - protéger la connectivité de succursale au travers de l'Internet
  - protéger l'accès à distance via l'Internet
  - établir la connectivité Intranet et extranet avec des partenaires
  - augmenter la sécurité du commerce électronique

Scénario de sécurité IP



Vue générale

- Avantages d'IPSec
  - Transparent aux applications (au dessous de couche transport (TCP, UDP))
  - Fournir la sécurité pour différents utilisateurs
- IPSec permet d'assurer que :
  - Une annonce de routeur vient d'un routeur autorisé
  - Un message réorienté vient du routeur auquel le paquet initial a été envoyé
  - Une mise à jour de routage n'est pas forgée

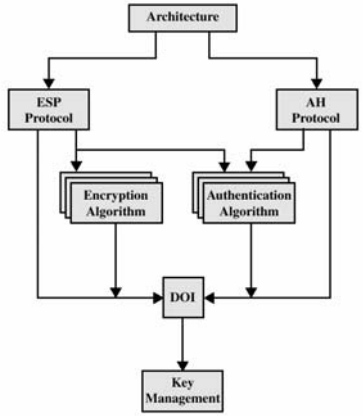
IPSEC

Architecture

Architecture

- Architecture : voir RFC 2401, 2402, 2046, 2408
- Éléments de travail
  - Architecture
  - ESP (Encapsulating Security Payload)
  - AH (authentification header)
  - Algorithme de chiffrement
  - Algorithme d'authentification
  - DOI (Domaine d'interprétation)
  - Gestion des clés

Éléments de l'architecture 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		✔	✔

SA (security association)

- relation à sens unique entre un expéditeur et un récepteur.
- Identifiée par trois paramètres :
  - Index de Paramètre de Sécurité (SPI)
  - Adresse de destination IP
  - Identifiant du protocole de sécurité : AH ou ESP
- a un certain nombre d'autres paramètres
  - N° seq, informations sur AH et ESP, durée de vie, etc..

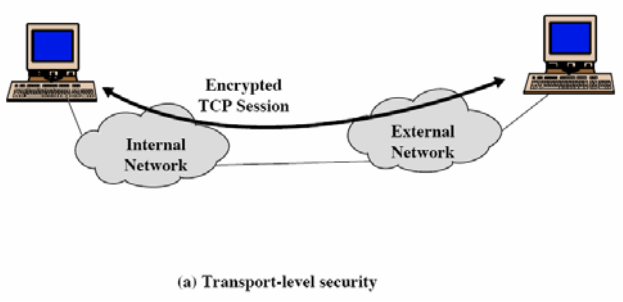
Sélecteurs de SA

- La SPD (Security Policy Database) associée définit le comportement à appliquer à un certain trafic
- Il y a trois possibilités
  - Appliquer les paramètres IPSec (via une SA)
  - Laisser passer le trafic
  - Rejeter le trafic
- Les sélecteurs permettent de retrouver les SAs associées à un type de trafic.
- Pour envoyer un paquet, il faut dans l'ordre :
  - Rechercher la politique de sécurité grâce aux sélecteurs
  - Déterminer la SA associée et son SPI
  - Appliquer le traitement IPSEC défini

Transport vs tunnel

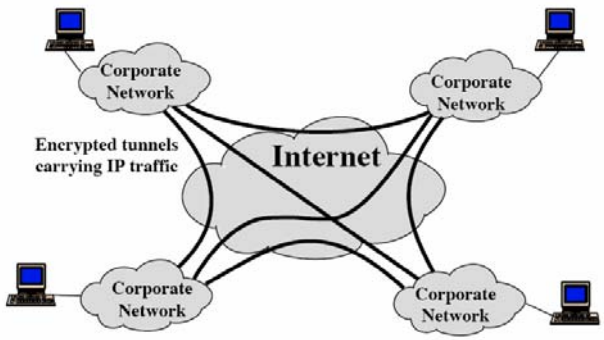
- le mode de transport est employé pour chiffrer et authentifier sur option des données d'IP
  - Peut être utilisé entre deux end users
  - Protège uniquement la zone de données du paquet
  - Utilisation ponctuelle et dans des cas précis
- le mode de tunnel chiffre le paquet IP entier
  - Permet la transparence
  - Habituellement utilisé entre des routeurs

Transports vs Tunnel



(a) Transport-level security

Transports vs Tunnel



(b) A virtual private network via Tunnel Mode

Comparaison des fonctionnalités

	Transport Mode SA	**Tunnel Mode SA**
AH	Authentifie la payload du paquet IP et des parties choisies de l'en-tête IP	Authentifie le paquet IP intérieur entier plus des parties choisies de l'en-tête IP externe
ESP	Chiffre la payload du paquet IP	Chiffre le paquet IP intérieur
ESP + authentification	Chiffre la charge utile du paquet IP. Authentifie la charge utile du paquet IP mais aucun en-tête.	Chiffre et authentifie le paquet IP intérieur

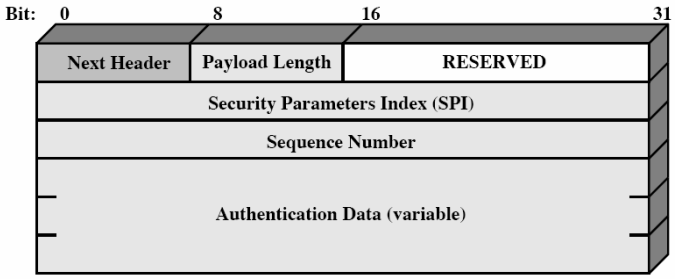
IPSEC

AH

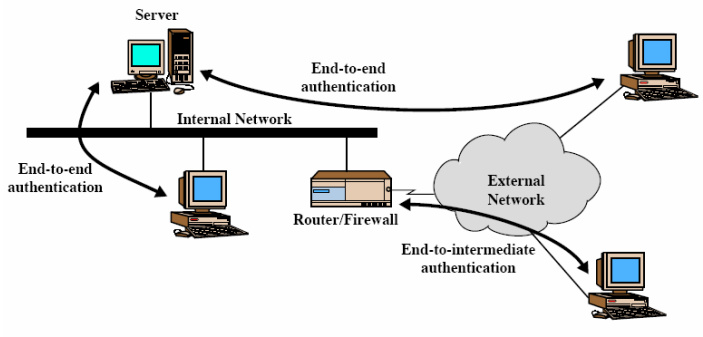
Protocole d'authentification (AH)

- fournit le support pour l'intégrité des données et l'authentification des paquets d'IP
- authentification : l'extrémité du système/routeur peut authentifier l'utilisateur/application
- empêche les attaques par spoofing d'adresse
- basé sur l'utilisation d'un MAC (nécessite le partage d'un secret)
  - Hmac_md5_96 ou Hmac_sha-1_96

En-tête AH



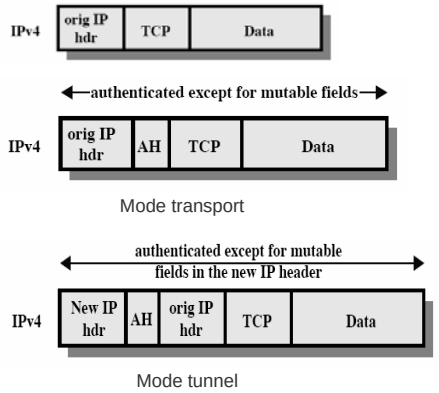
Authentification directe ou indirecte



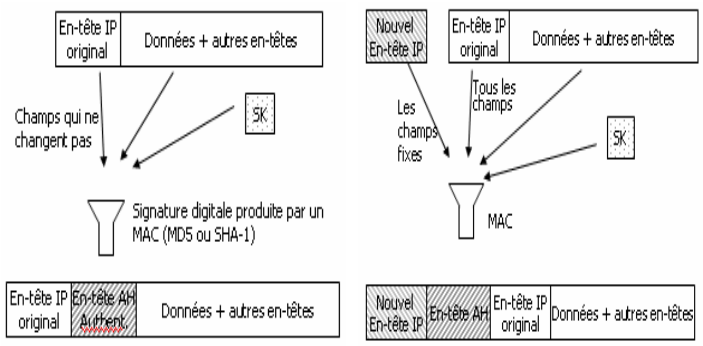
End to end : transport

End to intermediate : tunnel

AH + modes



AH + modes transport ou tunnel



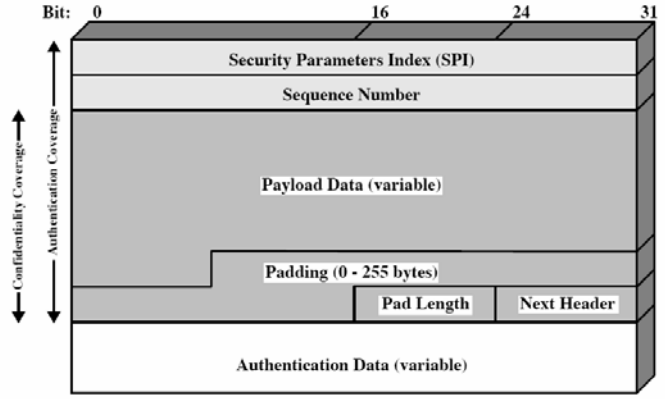
IPSEC

ESP

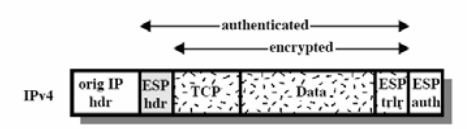
Encapsulating Security Payload (ESP)

- fournit la confidentialité du contenu du message
- peut fournir en option les mêmes services d'authentification que AH
- supporte les chiffres, modes, padding :
  - DES, Triple DES, RC5, IDEA, CAST, etc..
  - CBC
  - Padding pour obtenir la taille d'un bloc- > trafic

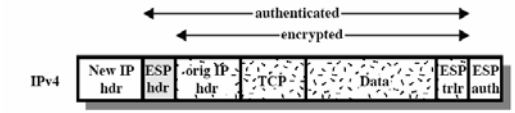
ESP



ESP

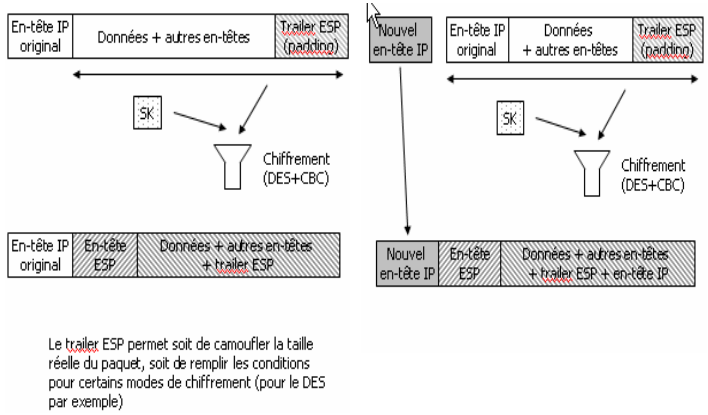


Mode transport



Mode tunnel

ESP + modes Transport - Tunnel



Le trailer ESP permet soit de camoufler la taille réelle du paquet, soit de remplir les conditions pour certains modes de chiffrement (pour le DES par exemple)

ESP avec authentification

- N'authentifie pas les parties fixes de l'en-tête IP (en mode transport) ou le nouvel en-tête IP (en mode tunnel)
- Applique le chiffrement avant l'authentification

ESP (sans authentification) puis AH

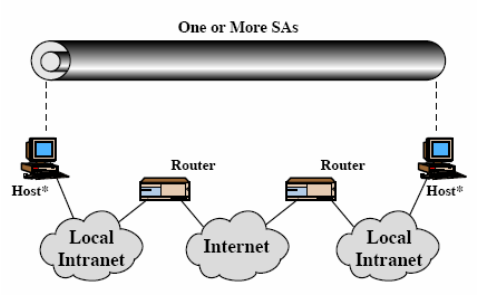
- Authentifie les parties fixes de l'en-tête IP
- Nécessite deux SA's

AH puis ESP (sans authentification)

- L'authentification s'applique directement aux données (permet de stocker les signatures sans devoir rechiffrer)
- Le header d'authentification est protégé par chiffrement
- Nécessite toujours deux SA's

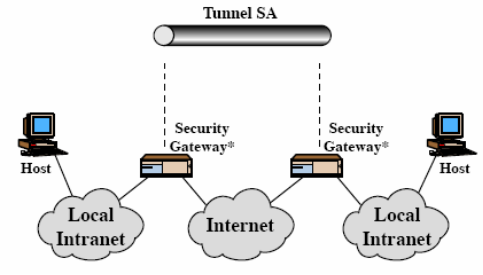
Combinaison des modes

- Toutes les protocoles et modes sont possibles, dans l'ordre souhaité



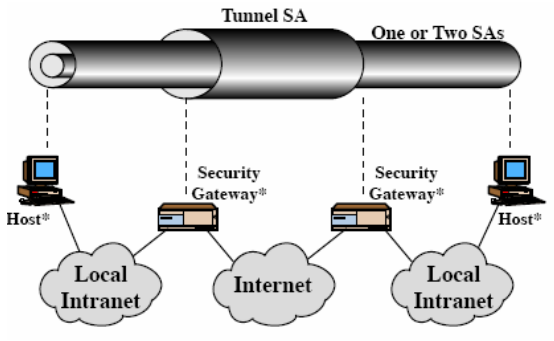
Combinaison des modes

- Sécurité uniquement entre 2 gateways (simples VPN) – mode tunnel (AH, ESP, ESP + auth)



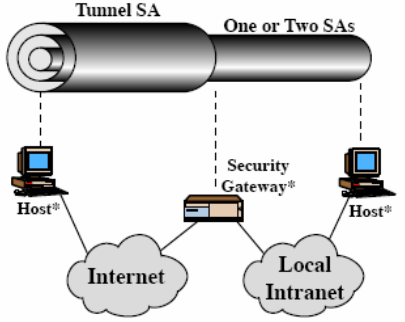
Combinaison des modes

- Idem cas précédent + sécurité end-to-end



Combinaison des modes

- Si accès à distance



IPSEC

Gestion des clés

Key Management

- Gère la génération et la distribution des clés
- typiquement le besoin 2 paires de clefs
  - 2 par direction pour AH et ESP
- Gestion de clé manuelle
  - le sysadmin configure manuellement chaque système
- Gestion principale automatisée
  - système automatisé pour la création sur demande des clefs pour SA dans de grands systèmes
  - Utilise les protocoles OAKLEY et ISAKMP

Oakley

- protocole d'échange de clés
- basé sur l'échange de clef de Diffie-Hellman
- ajoute des dispositifs pour contrer certaines faiblesses
  - cookies, groupes (param globaux), nonces, échange de clé DH avec authentification
- peut employer des nombres premiers ou des courbe elliptiques

Exemple d'échange de clé selon Oakley

I → R: CKY_I, OK_KEYX, GRP, g^x, EHAO, NIDP, ID_I, ID_R, N_I, $S_{KI}[ID_I \| ID_R \| N_I \| GRP \| g^x \| EHAO]$

R → I: CKY_R, CKY_I, OK_KEYX, GRP, g^y, EHAS, NIDP, ID_R, ID_I, N_R, N_I, $S_{KR}[ID_R \| ID_I \| N_R \| N_I \| GRP \| g^y \| g^x \| EHAS]$

I → R: CKY_I, CKY_R, OK_KEYX, GRP, g^x, EHAS, NIDP, ID_I, ID_R, N_I, N_R, $S_{KI}[ID_I \| ID_R \| N_I \| N_R \| GRP \| g^x \| g^y \| EHAS]$

Notation:

I	=	Initiator
R	=	Responder
CKY_I, CKY_R	=	Initiator, responder cookies
OK_KEYX	=	Key exchange message type
GRP	=	Name of Diffie-Hellman group for this exchange
g^x, g^y	=	Public key of initiator, responder; g^{xy} = session key from this exchange
EHAO, EHAS	=	Encryption, hash, authentication functions, offered and selected
NIDP	=	Indicates encryption is not used for remainder of this message
ID_I, ID_R	=	Identifier for initiator, responder
N_I, N_R	=	Random nonce supplied by initiator, responder for this exchange
$S_{KI}[X]$, $S_{KR}[X]$	=	Indicates the signature over X using the private key (signing key) of initiator, responder

ISAKMP

- Internet Security Association and Key Management Protocol
- fournit le cadre pour la gestion de clés
- définit des procédures et le format de paquet pour établir, négocier, modifier, et supprimer des SAs
- indépendant du protocole d'échange de clé, de l'algorithme de chiffrement, et de la méthode d'authentification

ISAKMP – types d'échanges

(a) Base Exchange	
(1) **I → R:** SA; NONCE	Begin ISAKMP-SA negotiation
(2) **R → I:** SA; NONCE	Basic SA agreed upon
(3) **I → R:** KE; ID_I; AUTH	Key generated; Initiator identity verified by responder
(4) **R → I:** KE; ID_R; AUTH	Responder identity verified by initiator; Key generated; SA established
(b) Identity Protection Exchange	
(1) **I → R:** SA	Begin ISAKMP-SA negotiation
(2) **R → I:** SA	Basic SA agreed upon
(3) **I → R:** KE; NONCE	Key generated
(4) **R → I:** KE; NONCE	Key generated
(5)* **I → R:** ID_I; AUTH	Initiator identity verified by responder
(6)* **R → I:** ID_R; AUTH	Responder identity verified by initiator; SA established

Notation:
I = initiator
R = responder
* = signifies payload encryption after the ISAKMP header

ISAKMP – types d'échanges

(c) Authentication Only Exchange	
(1) **I → R:** SA; NONCE	Begin ISAKMP-SA negotiation
(2) **R → I:** SA; NONCE; ID_R; AUTH	Basic SA agreed upon; Responder identity verified by initiator
(3) **I → R:** ID_I; AUTH	Initiator identity verified by responder; SA established
(d) Aggressive Exchange	
(1) **I → R:** SA; KE; NONCE; ID_I	Begin ISAKMP-SA negotiation and key exchange
(2) **R → I:** SA; KE; NONCE; ID_R; AUTH	Initiator identity verified by responder; Key generated; Basic SA agreed upon
(3)* **I → R:** AUTH	Responder identity verified by initiator; SA established
(e) Informational Exchange	
(1)* **I → R:** N/D	Error or status notification, or deletion

Notation:
I = initiator
R = responder
* = signifies payload encryption after the ISAKMP header

Références

- [Stallings] – ch 16
- http://www.hsc.fr/ressources/articles/
- http://web.mit.edu/tytso/www/ipsec/index.html

Questions

- Expliquer
  - Principe général d'IPSEC
  - Architecture IPSEC
  - Protocoles et modes
  - Gestion des clés