VPN

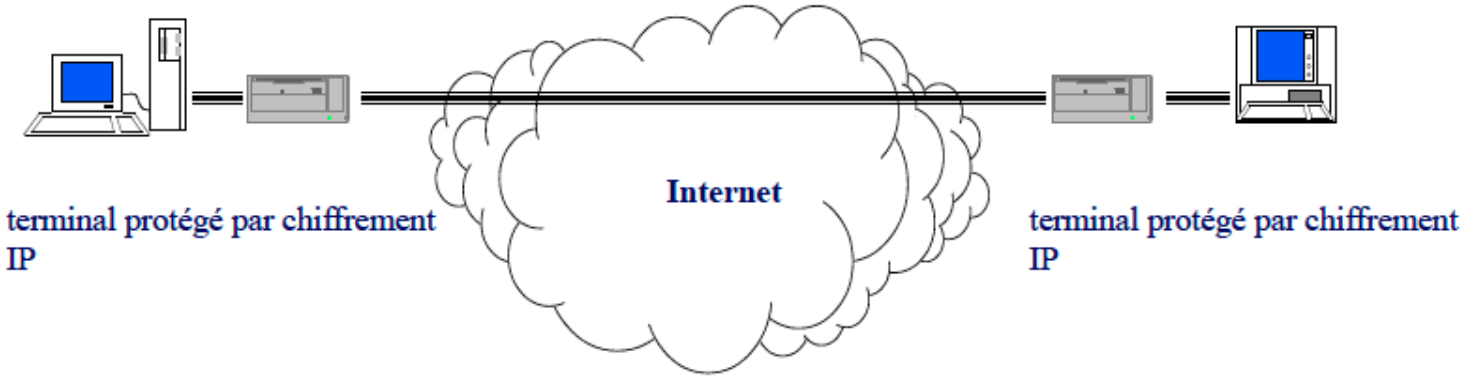
Outline

- Réseaux Privés Virtuels(VPN)
- Tunnels de niveau 3—Ipsec
- Tunnels de niveau 4—SSL/TLS
- Tunnels de niveau 7—SSH

Réseaux Privés Virtuels
Virtual Private Networks

Introduction VPN(1/3)

- ***Réseau Virtuel Privé***



- Un VPN (Virtual Private Network ou réseau virtuel privé) est un moyen de simuler un réseau privé sur un réseau public comme Internet.
- Un VPN crée des connexions temporaires ou tunnels entre 2 machines, ou une machine et un réseau, ou 2 réseaux.
- Protection du transfert de données

Introduction VPN(2/3)

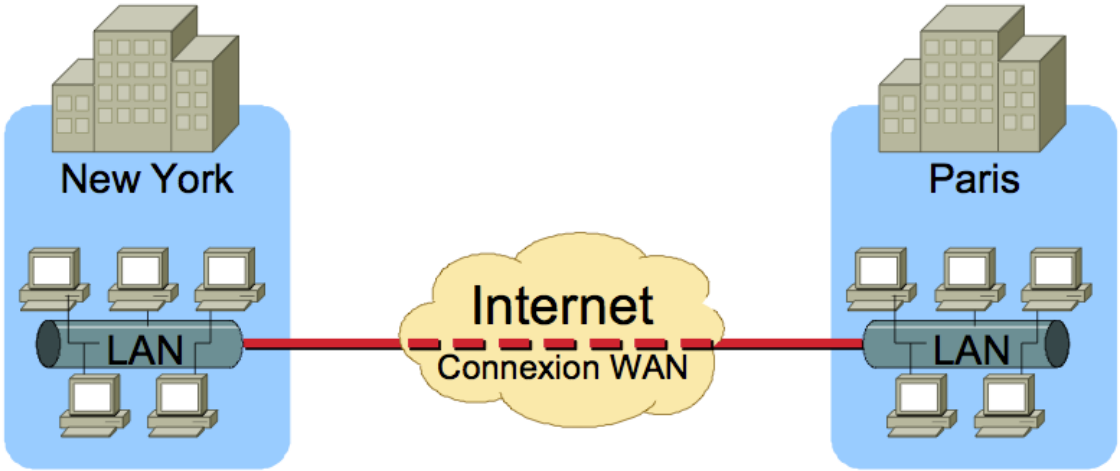
- Objectifs des réseaux privés virtuels
  - Relier deux réseaux locaux à travers un réseau non sécurisé public tel que Internet
    - Extension de la zone de confiance du réseau local
    - Permettre aux utilisateurs nomades d'accéder au réseau local
  - Sécuriser les communications
    - Remplacer ou sécuriser les protocoles ne chiffrant pas l'authentification
    - Si besoin, chiffrer les données
  - Créer une connexion chiffrée entre les clients et les serveurs
    - Accès distants (tunnels applicatifs, VPN....)

Introduction(3/3)

- Un VPN doit assurer :
  - Authentification
  - Intégrité
  - Confidentialité
  - Gestion des clés
  - Éventuellement affecter une adresse IP au client
  - Éventuellement la compression
- Utilisations
  - Accès
  - Intranet
  - Extranet

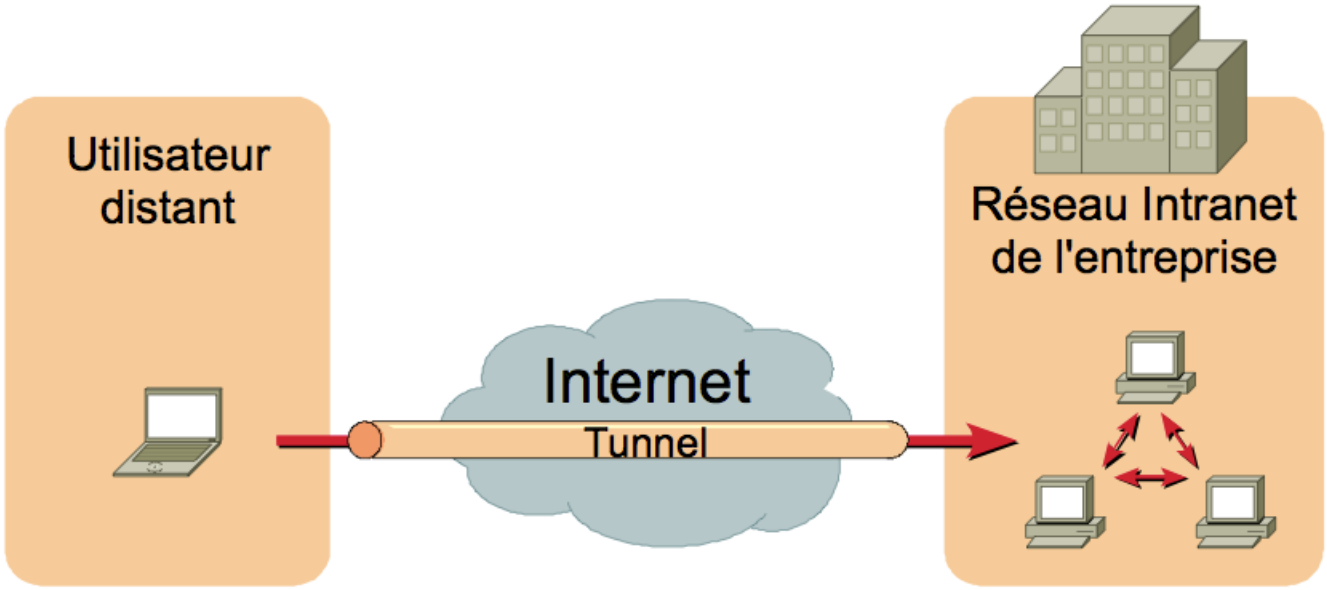
Tunnels VPN

- Tunnels VPN (*Virtual Private Network*)
- Réseau privé virtuel
- Consiste à faire transiter un protocole par l'intermédiaire d'un autre
- Aussi appelé protocole de *tunneling* (tunnel)
- Cela consiste à créer un chemin virtuel du client vers le serveur au travers un réseau public en chiffrant les données



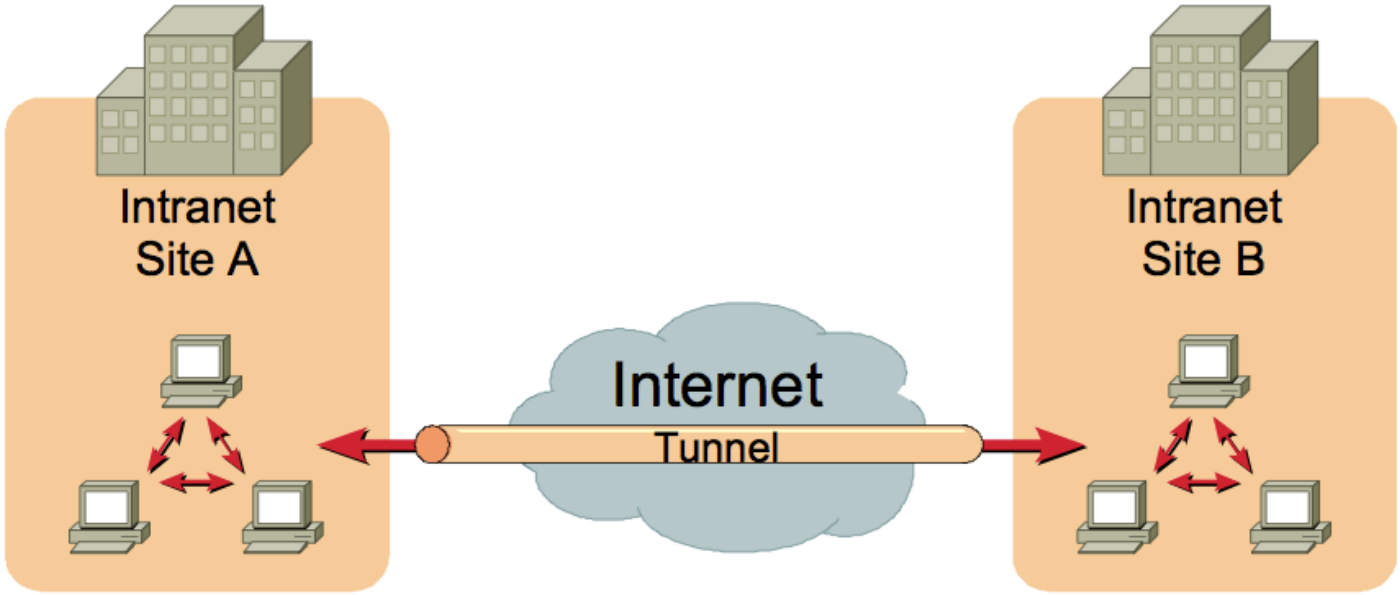
Fonctionnalité des VPN(1/3)

- VPN d'accès
  - Permettre aux utilisateurs nomades d'accéder au réseau local (*roadwarrior*)



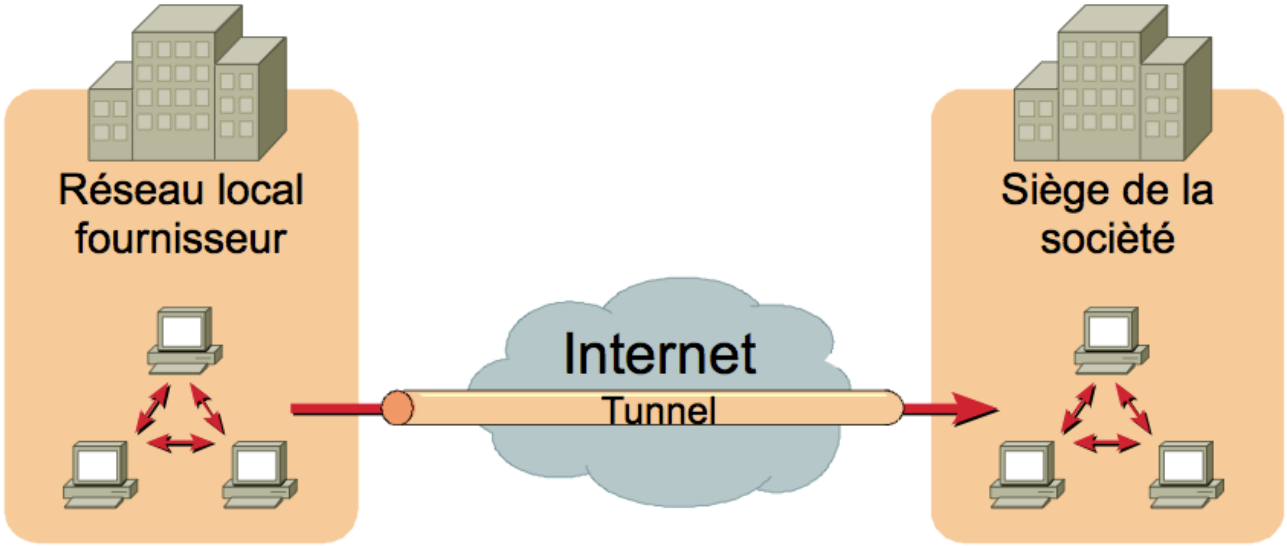
Fonctionnalité des VPN(2/3)

- Intranet VPN
  - Relier plusieurs sites distants entre eux



Fonctionnalité des VPN(3/3)

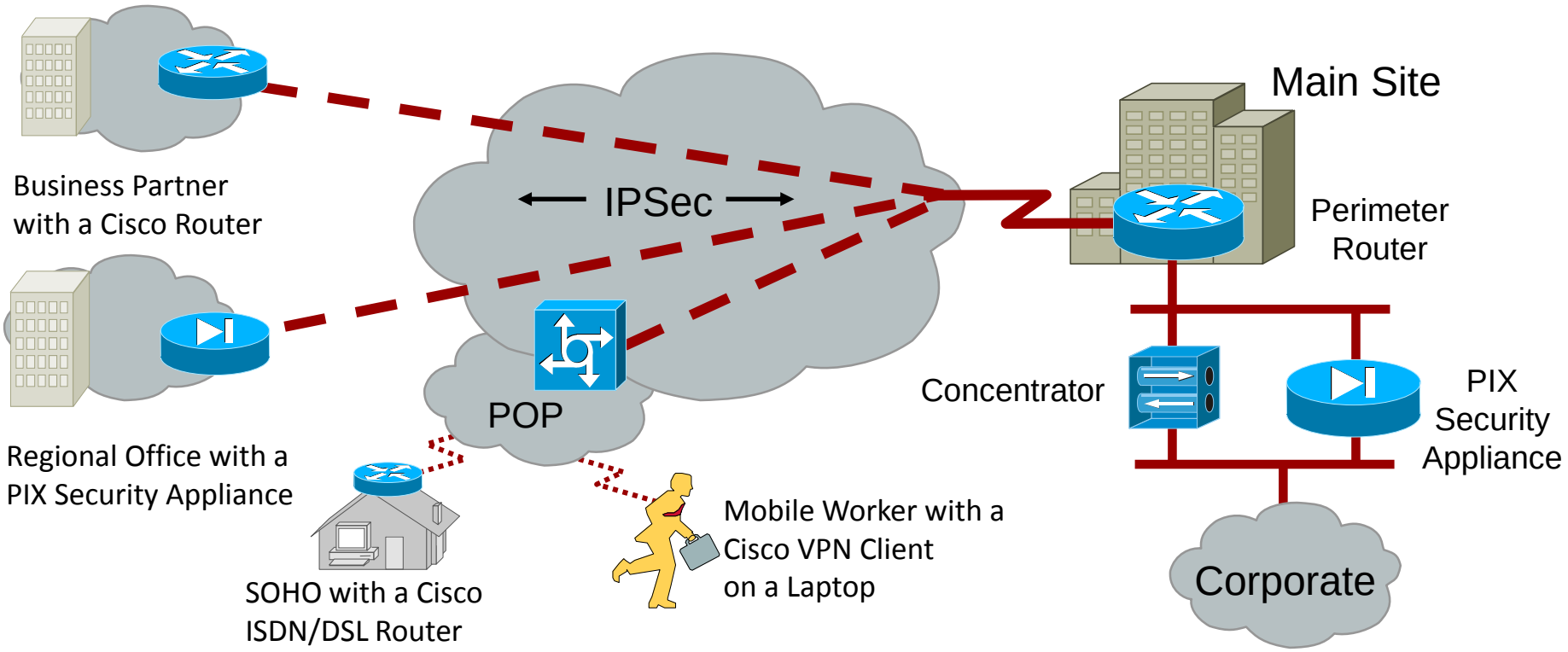
- Extranet VPN
  - Ouvrir son réseau local à ses partenaires



Tunnels de niveau 3

IPsec

What Is IPSec?(1/2)



- IPSec acts at the network layer protecting and authenticating IP packets:
- Based on a framework of open standards and is algorithm independent
- Provides data confidentiality, data integrity, and origin authentication
- Spells out the rules for secure communications
- Relies on existing algorithms to implement the encryption, authentication, and key exchange

What Is IPSec?(2/2)

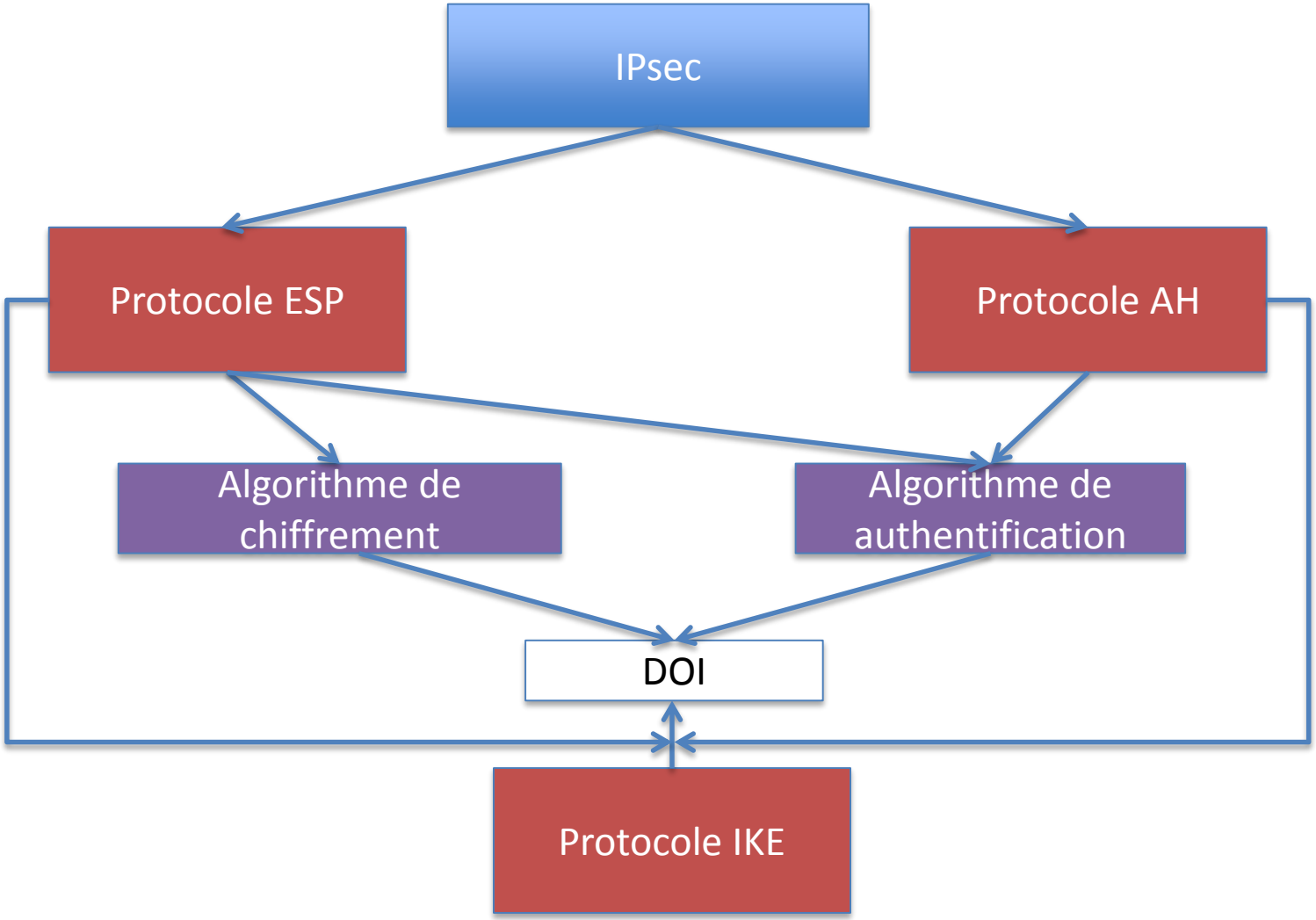
- défini par l'IETF pour assurer des communications privées et protégés de bout en bout sur des réseaux IP(couche 3), par l'utilisation des cryptographies.
- compléter par une tribu de RFC
- Obligatoire dans la pile IPv6, facultatif(en option) dans IPv4

- RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec
- RFC 2451: The ESP CBC-Mode Cipher Algorithms
- RFC 2857: The Use of HMAC-RIPEMD-160-96 within ESP and AH
- RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3686: Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)
- RFC 3947: Negotiation of NAT-Traversal in the IKE
- RFC 3948: UDP Encapsulation of IPsec ESP Packets
- RFC 4106: The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
- RFC 4301: Security Architecture for the Internet Protocol
- RFC 4302: IP Authentication Header
- RFC 4303: IP Encapsulating Security Payload
- RFC 4304: Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 4307: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4308: Cryptographic Suites for IPsec
- RFC 4309: Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)
- RFC 4543: The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH
- RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE)
- RFC 4806: Online Certificate Status Protocol (OCSP) Extensions to IKEv2
- RFC 4835: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)

IPSec Security Functions

Function	Benefit
Confidentiality	**Encryption prevents eavesdropping and reading of intercepted data.**
Data integrity	**Receiver can verify data was transmitted unchanged or altered.**
Origin authentication	**Receiver can guarantee and certify the data source.**
Anti-replay protection	**Each packet is verified as unique. Late and duplicate packets are dropped.**

Architecture de IPsec



AH(Authentication Header)

- Assure l'intégrité et l'authenticité des paquets IP
  - ✓ Intégrité: par fonction de hachage(ex:MD5)
  - ✓ Authenticité: par ajouter une clé partagé en calculant le code de vérification
- Anti Attaque par rejeu(*replay attack*)
  - ✓ Par numéro de séquence dans l'entête
- RFC 4302

ESP（Encapsulating Security Payload）

- Permet l’anthentification et la protection des données
  - pour Paquet de donnée
  - pour Stream de donnée
- Principalement utilisé pour le cryptage des informations
- RFC 4303

IKE（Internet Key Exchange）

- Prend en charge la gestion des clé de cryptographie
- Port UDP 500
- RFC 4306

DOI, SA

- **DOI（Domain of Interpretation）**
  - **utilisé pour relier les RFCs de IPsec .**
- **Security Association(SA)**
  - **Communication sécurisée avec Ipsec**
  - **Identifiée par destination/ numéro de série/ prorocole(AH, ESP)**
  - **Structure de donnée comprenant tous les paramètres**
    - ✓ **Clé, durée des clés, algorithmes, hotes…**
    - ✓ **Unidirectionnel: un flux 2 SA**
  - ➢ **IPSec SA**
  - ➢ **ISAKMP SA(ou IKE SA)**
    - ✧ **Uniquement pour le trafic de controle**
    - ✧ **Plus grande durée de vie que les Ipsec SA**

❑ Échange des clés

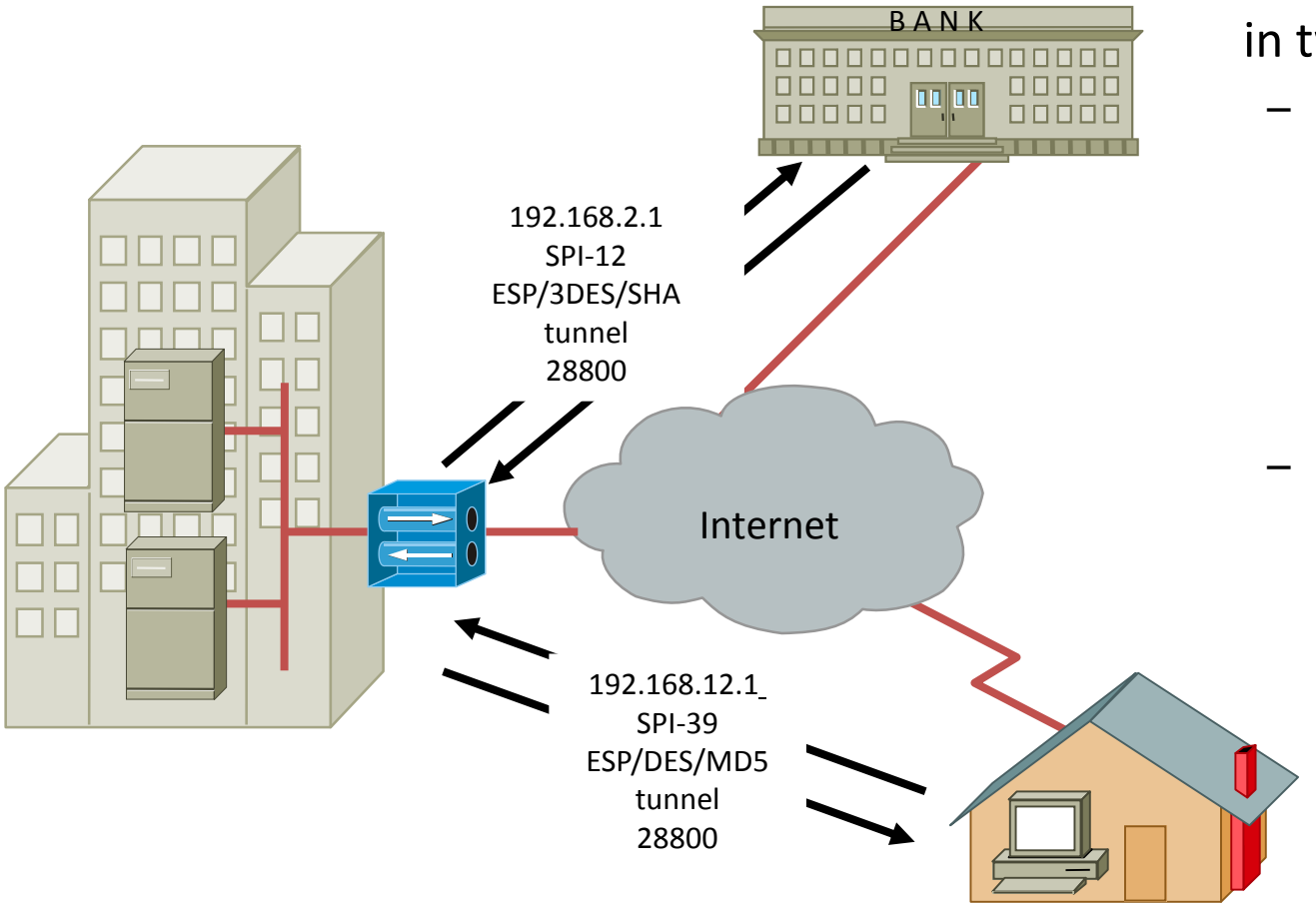
—ISAKMP (Internet Security Association and Key Management Protocol)

- Stockage des SA, construction des messages, phases obligatoires

—IKE (Internet Key Exchange)

- Comment l'échange de clés se fait réellement, utilisant le framework ISAKMP

Security Association



- Security Association occurs in two databases:
  - Security Policy Database
    - Encryption Algorithm
    - Authentication Algorithm
    - Mode
    - Key lifetime
  - SA Database
    - Destination IP address
    - SPI
    - Protocol (ESP or AH)

SA Lifetime

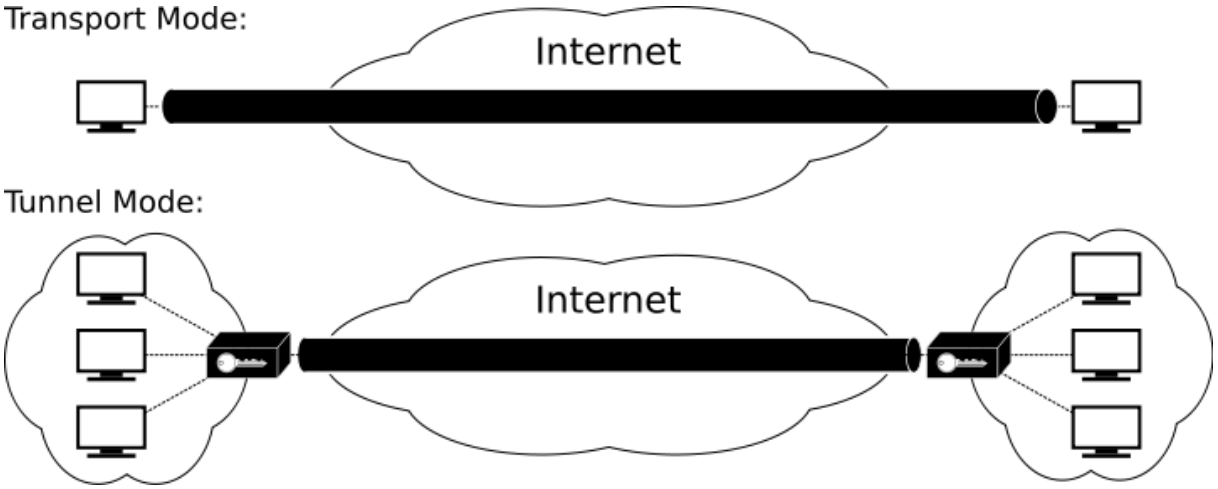
There are two parameters:

Data-Based

Time-Based

Mode d’opération IPsec

- Transport Mode et Tunnel Mode
- AH et ESP supporte touts les deux modes :
  - AH en mode Transport
  - AH en mode Tunnel
  - ESP en mode Transport
  - ESP en mode Tunnel

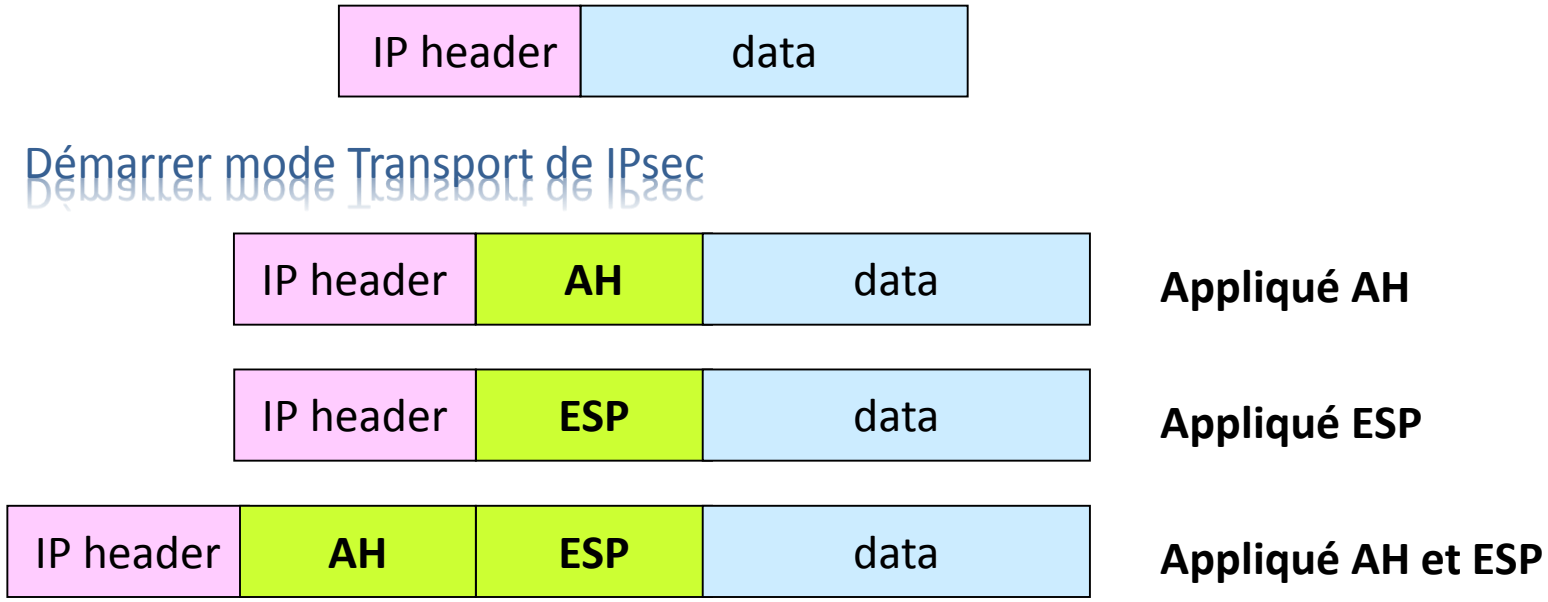


Mode d'opération IPsec

- Mode transport
  - Seules les données du paquet IP sont chiffrées
  - Entièrement routable car l'entête IP est en clair
  - Ne peut pas traverser un NAT, qui invaliderait la valeur de hash
  - Utilisé pour les communications d'hôtes à hôtes
  - Il est possible de traverser les NAT en utilisant une encapsulation UDP des paquets Ipsec ESP

Mode Transport

Protéger que les payloads

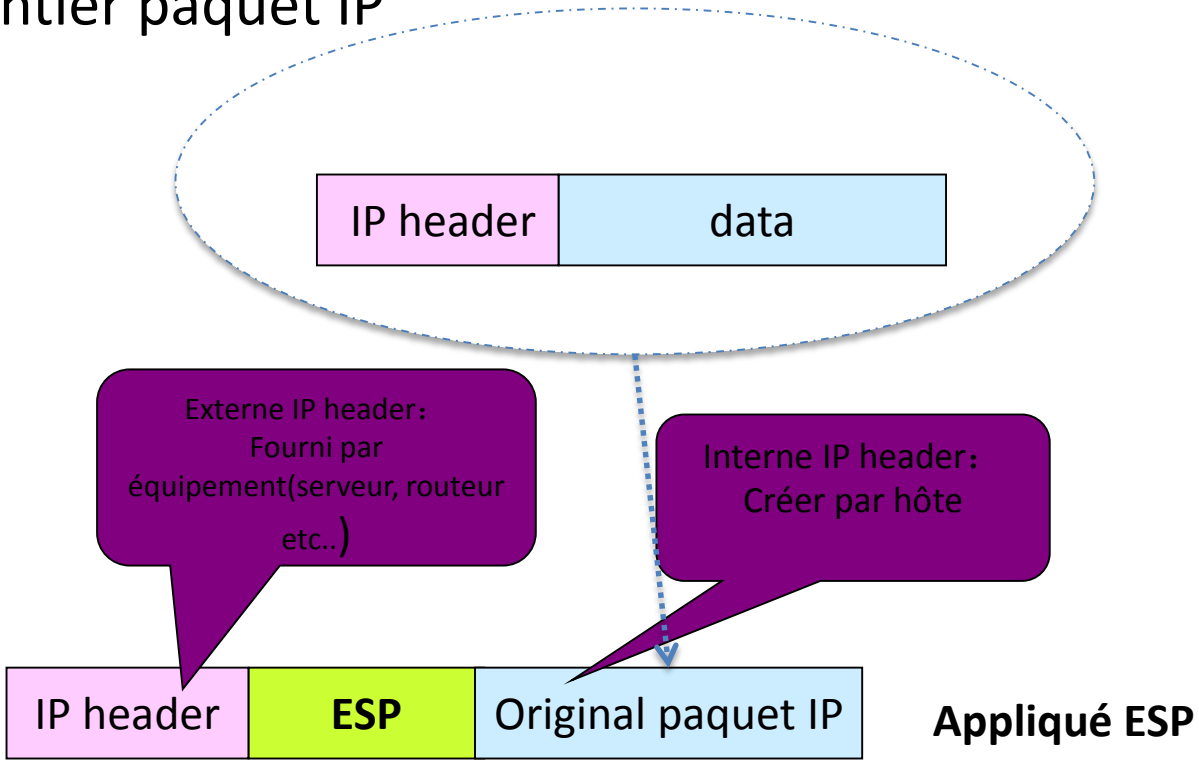


Modes d’opération IPsec

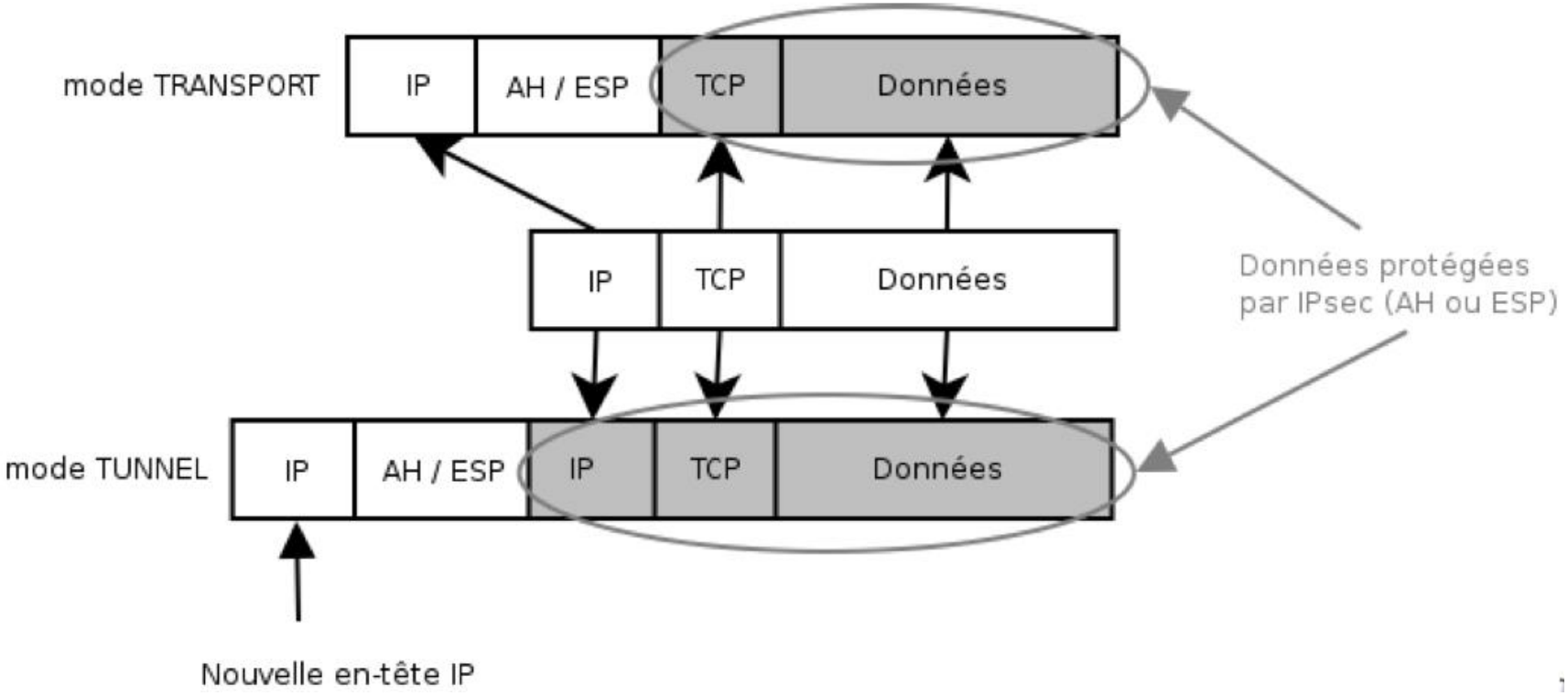
- Mode tunnel
- Doit être en capsulé dans un nouveau paquet IP pour permettre le routage
- Utilisé pour tout type de communications sécurisées à travers Internet
  - Réseau à réseau(Tunnels sécurisés entre routeurs)
  - Hôte à réseau
  - Hôte à hôte

Mode tunnel

- Protéger l'entier paquet IP



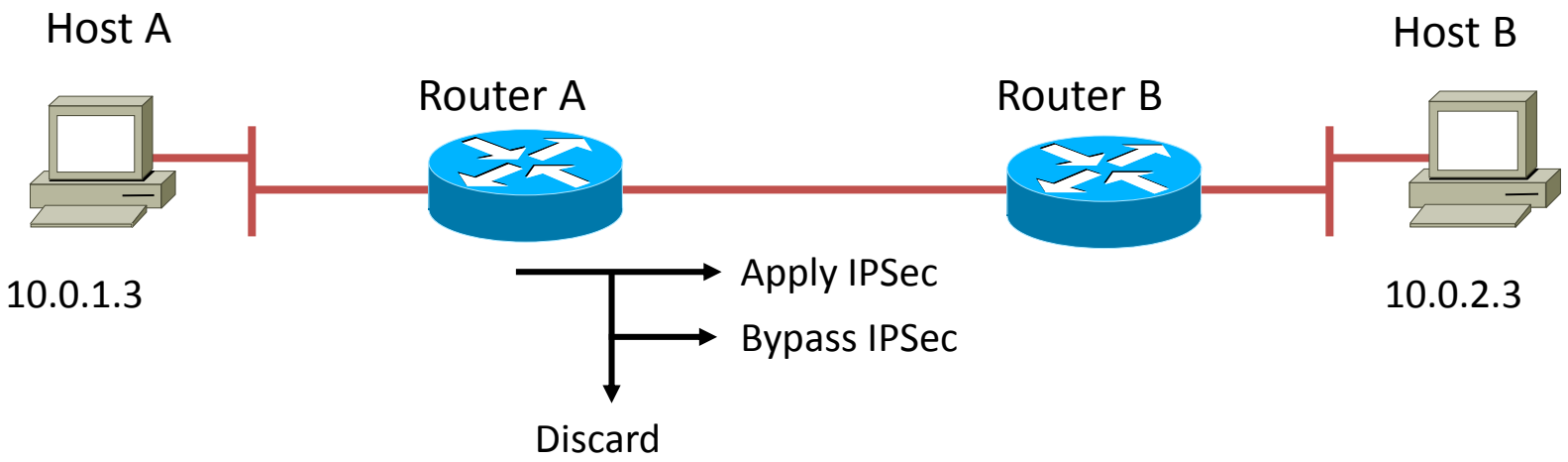
Comparaison les deux modes



IPSec Operation

- Step 1 Interesting Traffic: The VPN devices recognize the traffic to protect.
- Step 2 IKE Phase 1: The VPN devices negotiate an IKE security policy and establish a secure channel.
- Step 3 IKE Phase 2: The VPN devices negotiate the IPSec security policy used to protect IPSec data.
- Step 4 Data transfer: The VPN devices apply security services to traffic and then transmit the traffic.
- Step 5 Tunnel terminated: The tunnel is torn down.

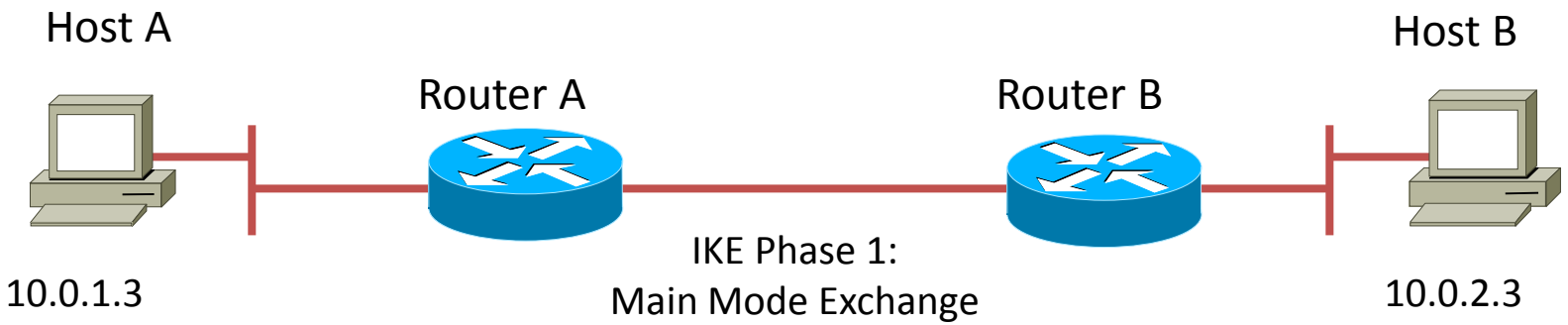
Step 1: Interesting Traffic

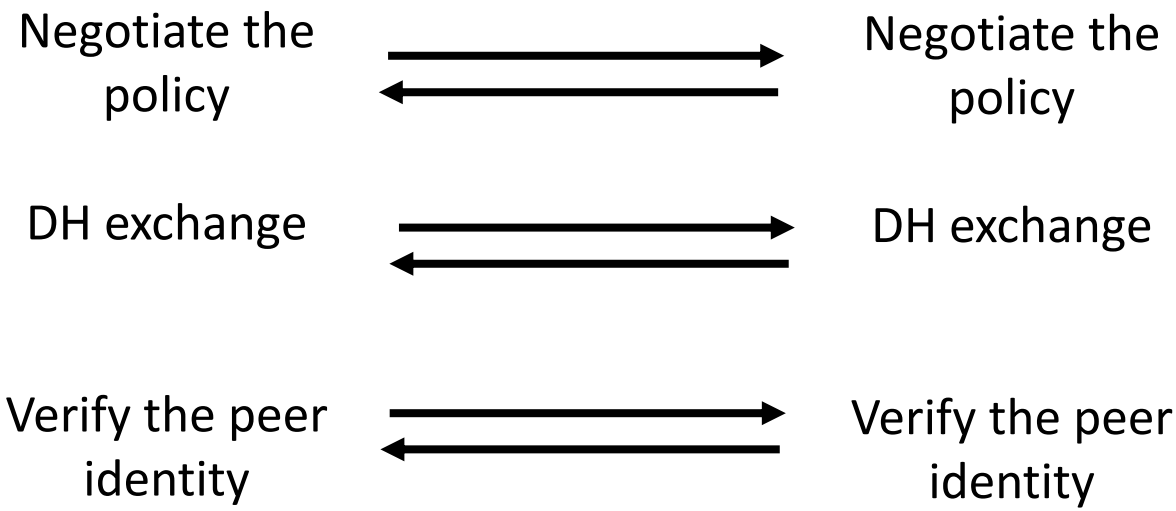


There are three choices for every inbound and outbound datagram:

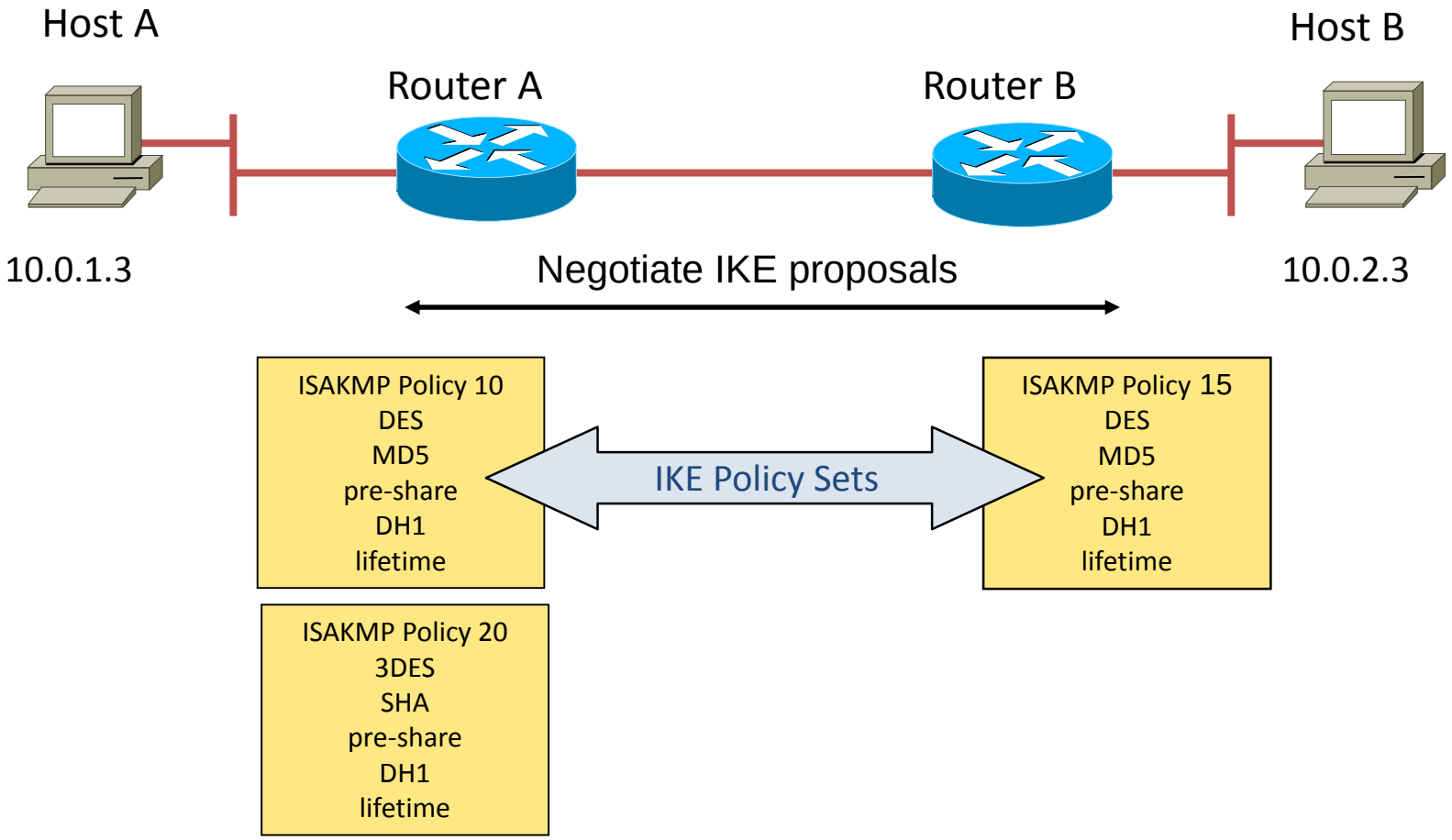
- Apply IPSec
- Bypass IPSec
- Discard the datagram

Step 2: IKE Phase 1



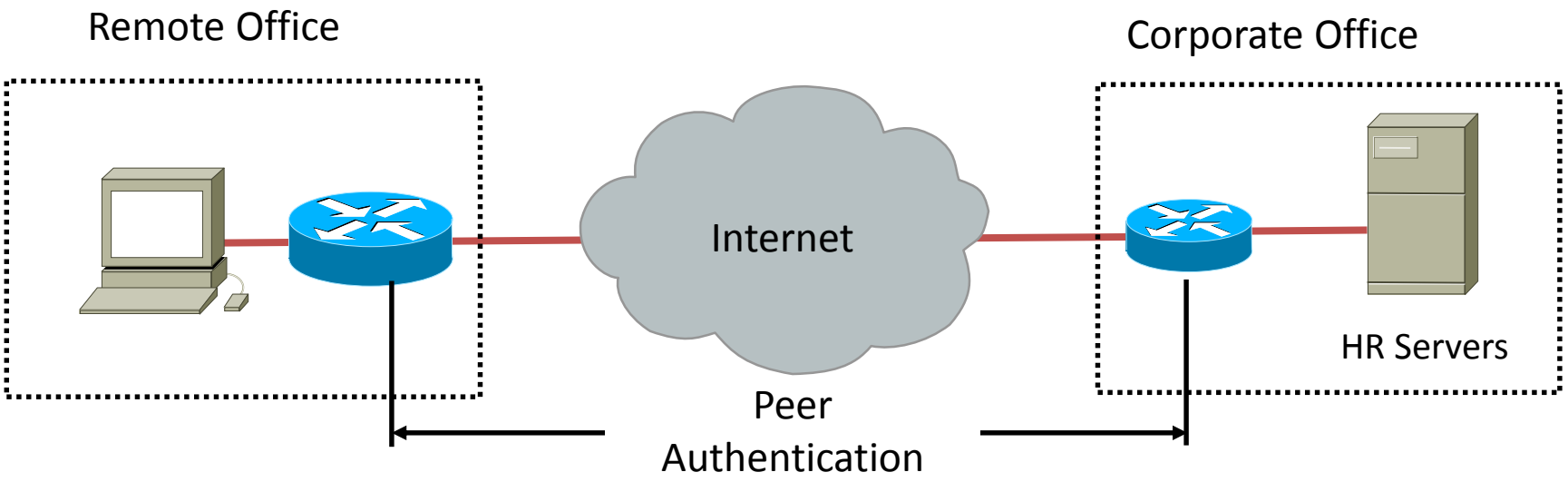


First and Second Exchange—IKE Policy Sets and Establishing a Shared Secret



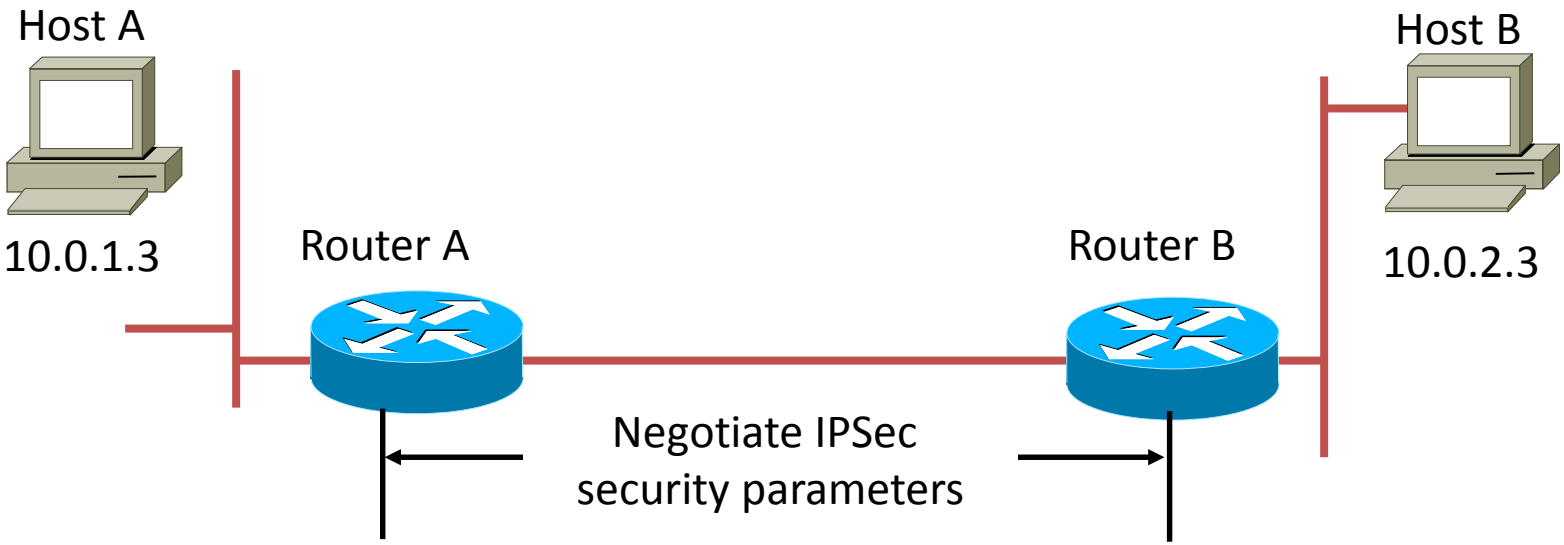
- Negotiates matching IKE transform sets to protect IKE exchange.
- A DH exchange is performed to establish a shared secret.

Third Exchange—Authenticate Peer Identity

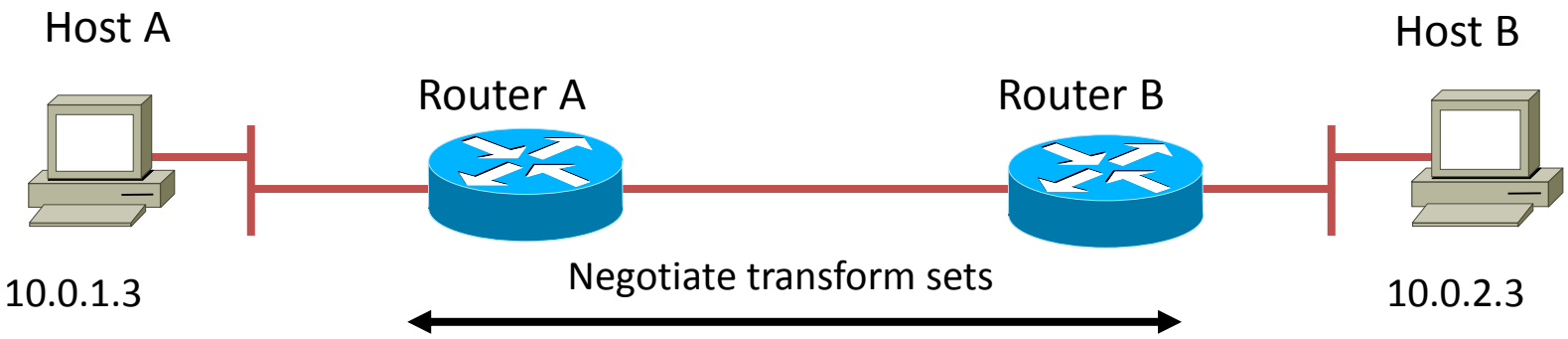


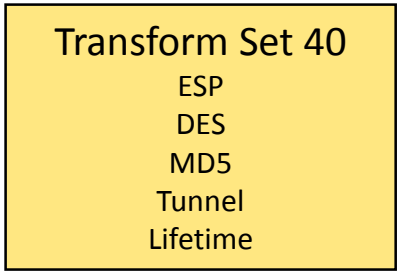
- Peer authentication methods are follows:
  - Pre-shared keys
  - RSA signatures
  - RSA encrypted nonces

Step 3: IKE Phase 2



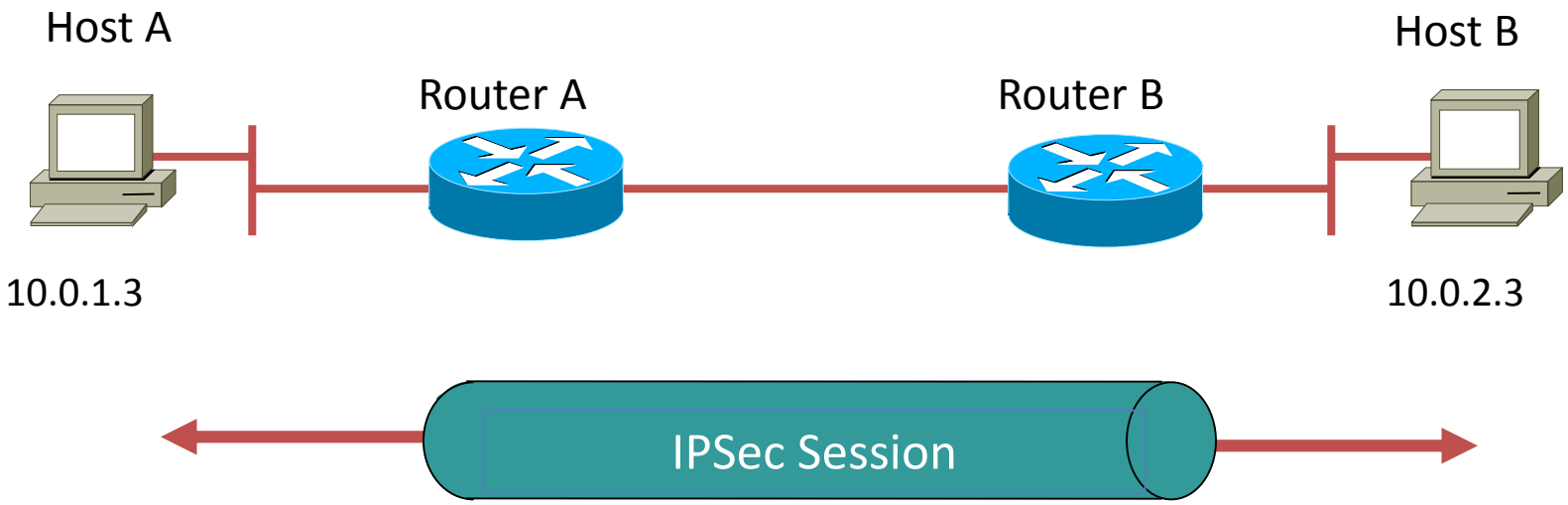
IPSec Transform Sets





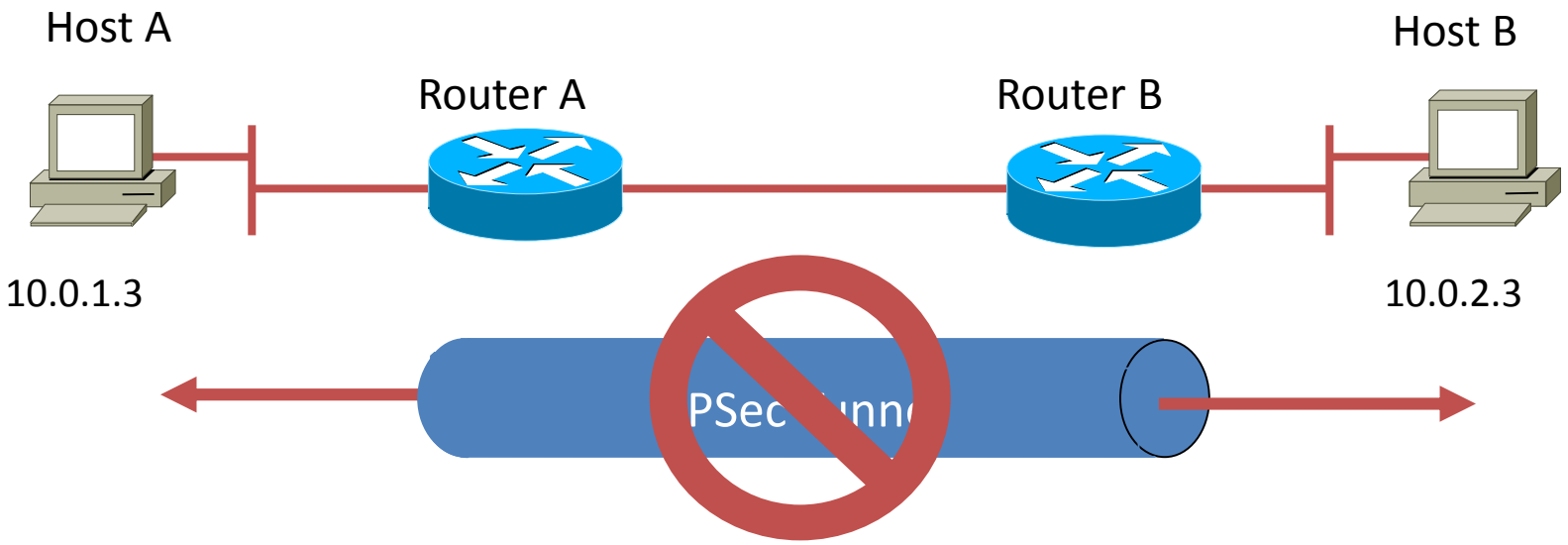
A transform set is a combination of algorithms and protocols that enact a security policy for traffic.

Step 4: IPSec Session



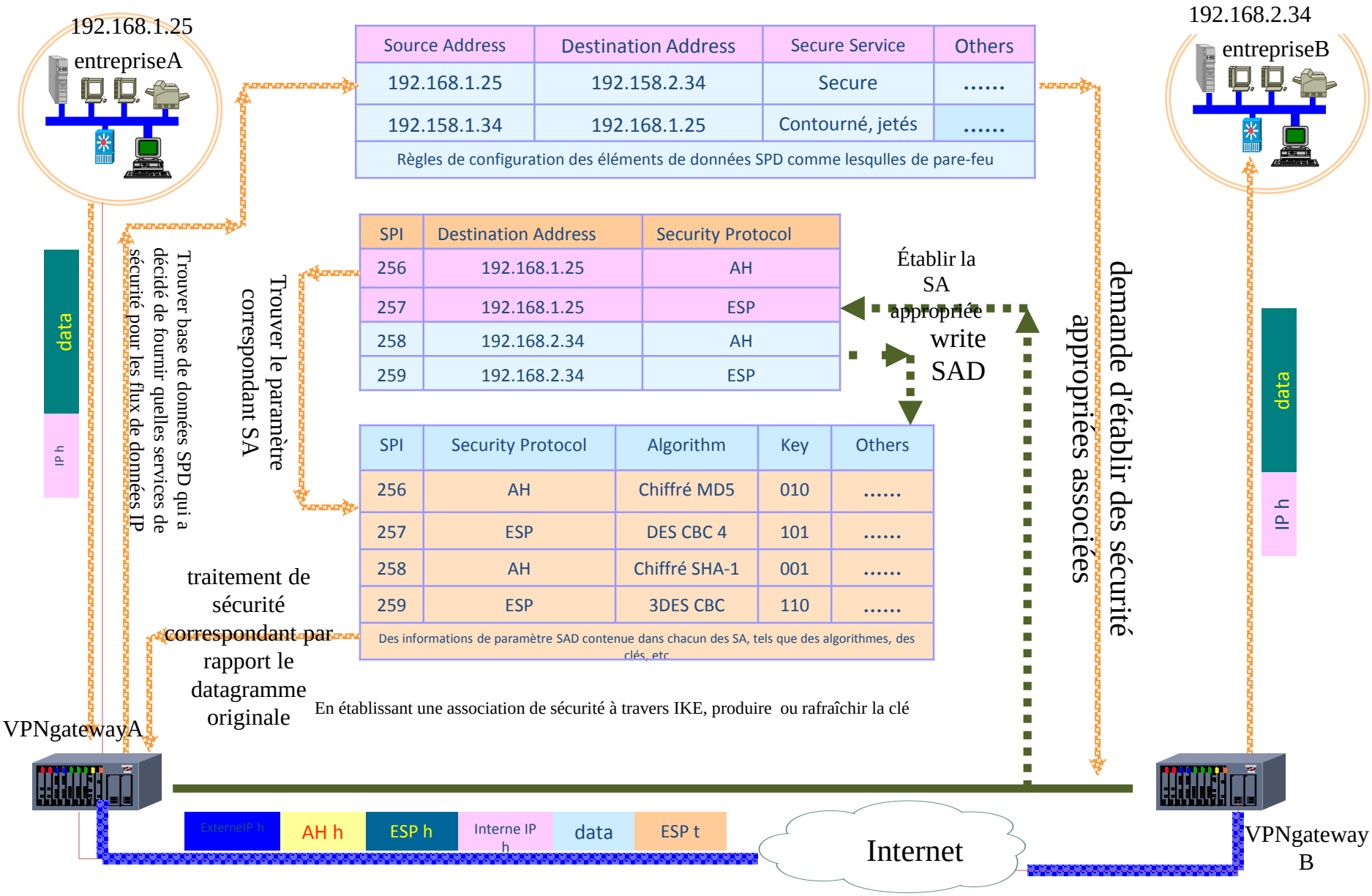
- SAs are exchanged between peers.
- The negotiated security services are applied to the traffic.

Step 5: Tunnel Termination

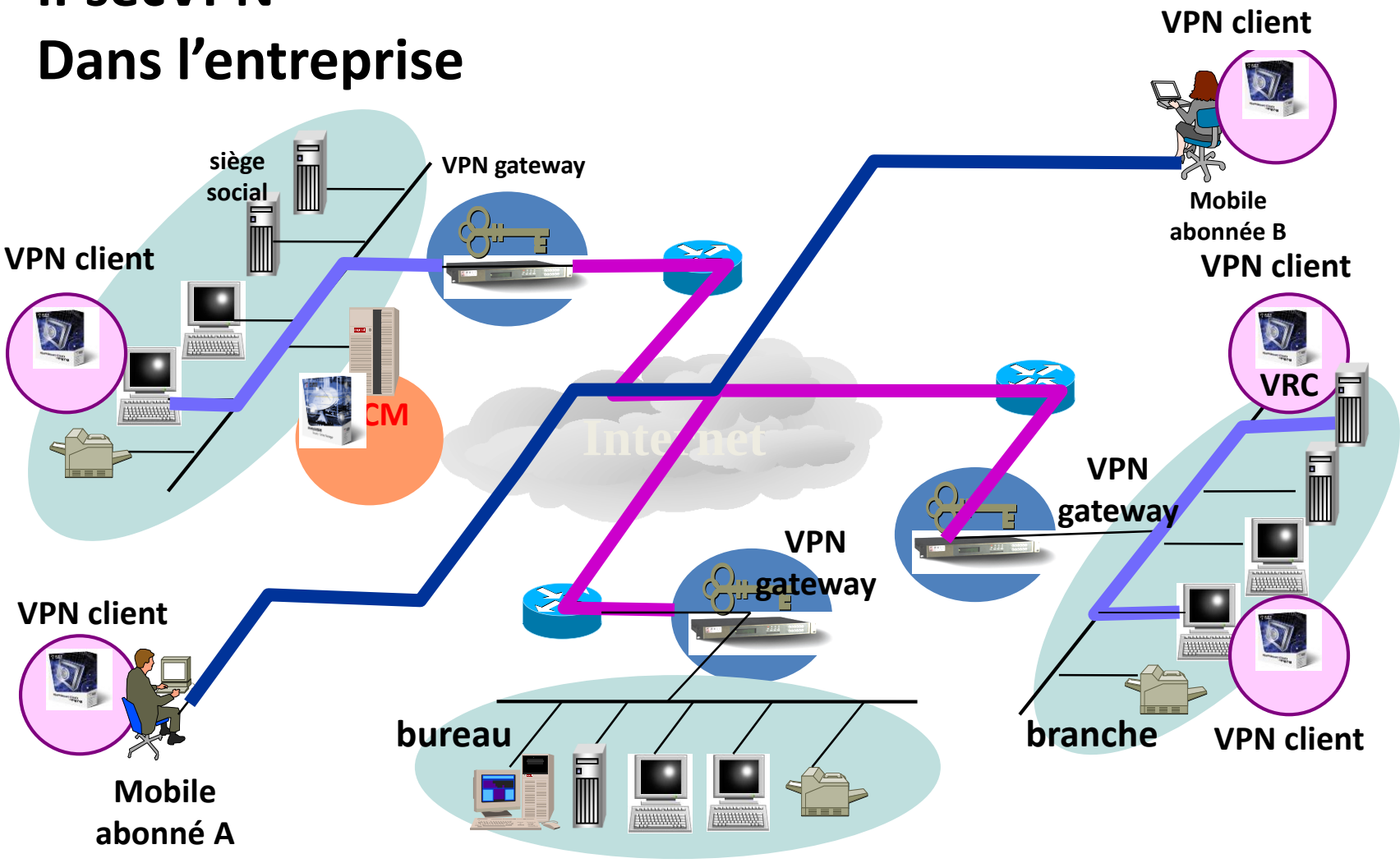


- Tunnel termination occurs as follows:
  - By an SA lifetime timeout
  - If the byte counter is exceeded
- It removes IPSec SA

Un complet fonctionne IPsecVPN



Ex: Déploiement IPsecVPN Dans l'entreprise



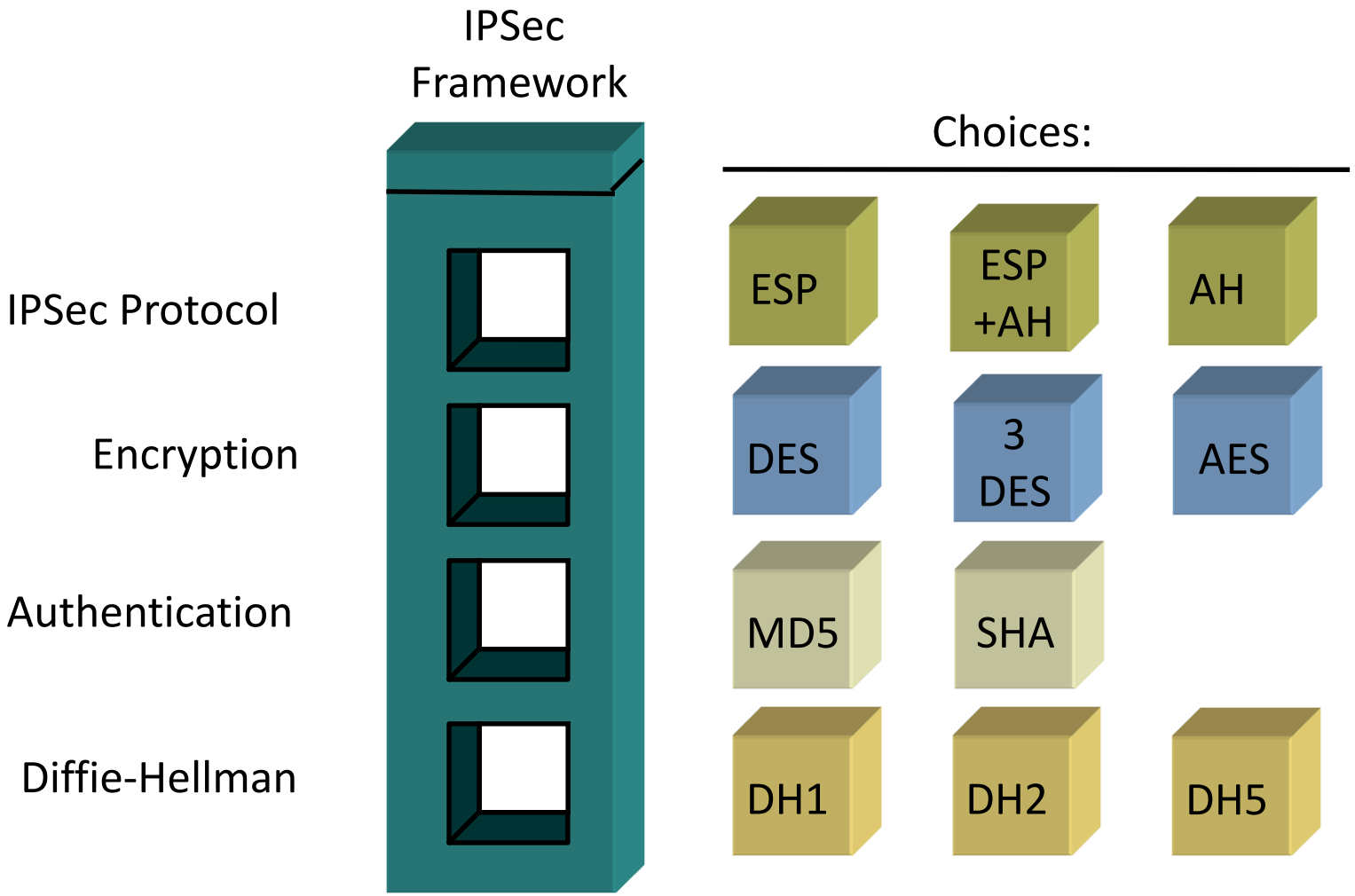
La Disponibilité de IPsec

—En théorie, IPsec peut être implémenté dans n'importe quel appareil utilisant la pile TPC/IP
—Obligatoire dans IPv6 – Optionnel dans IPv4
—Unix / Linux
    Implémentations natives (OpenBSD, Solaris, AIX)
    KAME, FreeS/WAN (Linux)
—Windows
    Implémentation native avec L2TP(Windows 2000, XP, 2003)
    VPN+, PGPnet,...
—Firewall
—Routeurs
    Cisco
    3Com
—Concentrateur VPN

Bilan:IPSec Building Blocks

Component	Role
Authenication Header (AH)	• **IP header that provides a cryptographic checksum on the packet** • **Used to achieve data authentication and integrity** • **Separate from the ESP header**
Encapculating Security Payload (ESP)	• **Header applied after the packet has been encrypted** • **Provides data confidentiality in transit** • **Provides for data authentication and integrity**
Security Association (SA)	• **Specifies cryptographic parameters needed before any two devices can communicate using IPSec**

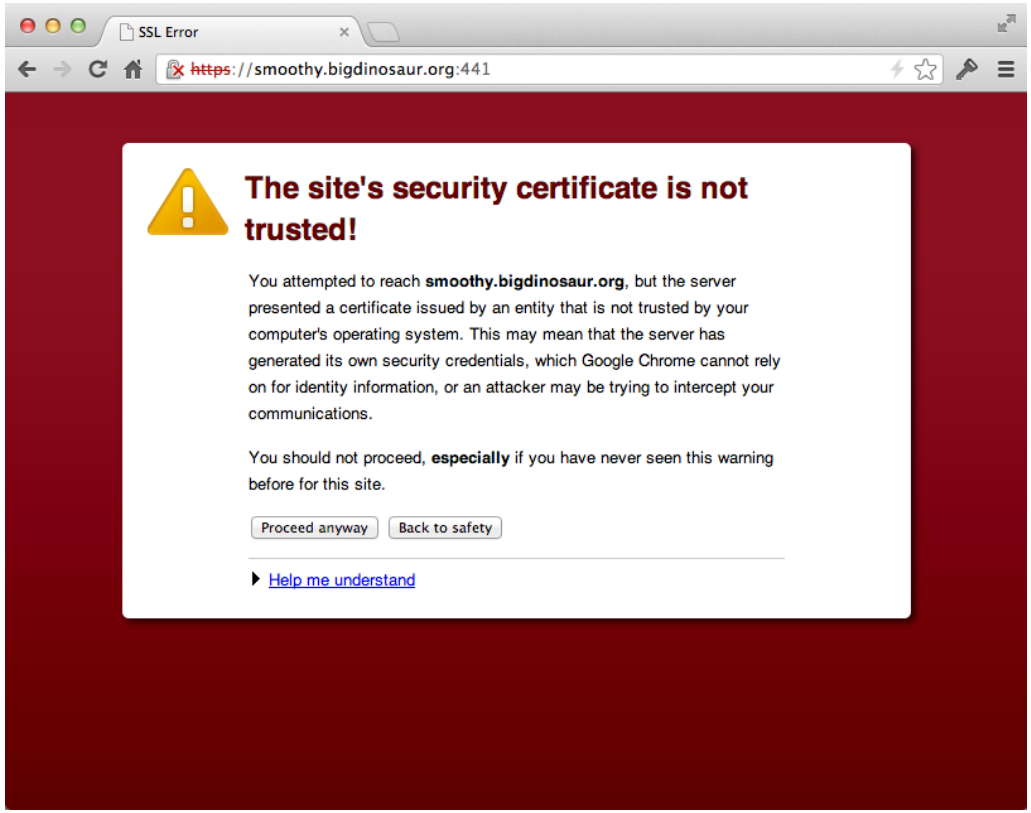
Bilan:IPSec Implementation Framework



Bilan:IPSec Services

Services IPSec	AH	ESP (chiffrement seul)	ESP (chiffrement et authentification)
intégrité	x		x
authentification de l'origine des données	x		x
détection du rejeu	x	x	x
confidentialité		x	x

- ***Gestion des clefs : protocole ISAKMP/IKE***
  - Diffie Hellman avec une authentification, basée sur un secret partagé, ou une signature, ou un chiffrement asymétrique



Tunnel de niveau 4

protocole SSL/TLS

SSL / TLS : historique

—**07/1994** : Conception initiale du protocole (V1.0) développé par Netscape

—**12/1994** : SSL V2.0 Sortie des premiers produits

—**04/1995** : SSL Ref 2.0 - L'implémentation de référence

—**1995** : Arrivée d'une quantité importante d'implémentations au niveau international

—**07/1995** : SSL à l'IETF

—**11/1995** : SSL V3.0

—**03/1996** : le développement est repris par l'IETF au sein du groupe TLS (*Transport Layer Security*)

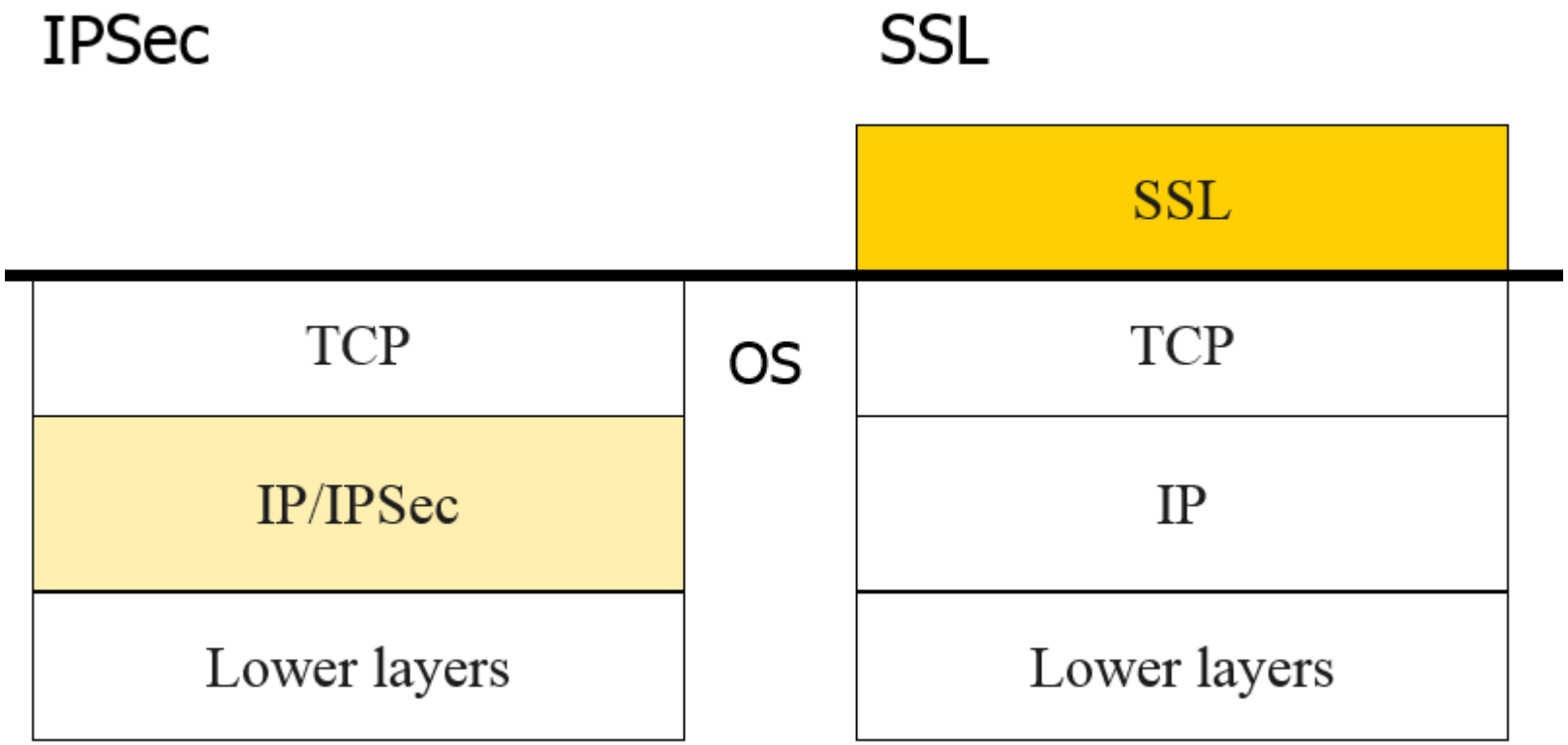
—**03/1997** : IETF TLS V1.0

—**08/2004** : TLS V1.1

caractéristiques

- SSL / TLS :
  - —Permettent le chiffrement des communications et l'authentification des clients et des serveurs
  - —Indépendants du protocole avec lequel ils sont utilisés
  - —Authentification des extrémités
  - —Confidentialité
  - —Intégrité des échanges
  - —Utilisation de certificats X509 et de clés de session
  - —Flot de données découpé en paquets signés et chiffrés

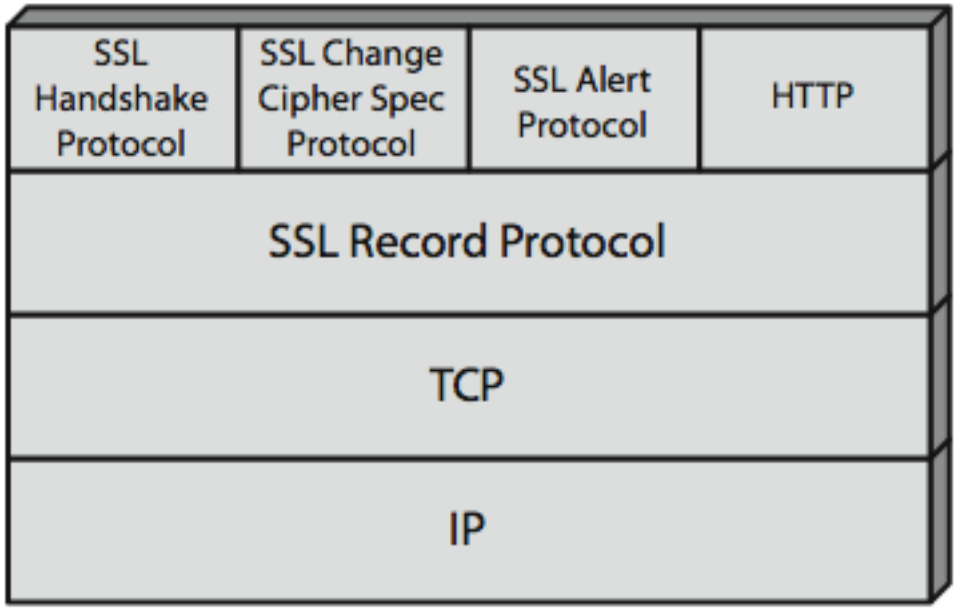
What layer?


IPSec
SSL
SSL
TCP
IP/IPSec
Lower layers
OS
TCP
IP
Lower layers

L'authentification avec SSL

- L'identification des serveurs est basée sur les DNS
- Le serveur est authentifié avec un certificat (X.509)
- Il doit y avoir identité entre le nom DNS et celui du certificat
- Attention : l'authentification du serveur ne permet pas de savoir si le serveur de la poste est poste.fr ou laposte.com
- Authentification du client :
  - par mot de passe (basic), mais dans le tunnel chiffré
  - par certificat (depuis SSL v3)

SSL Architecture



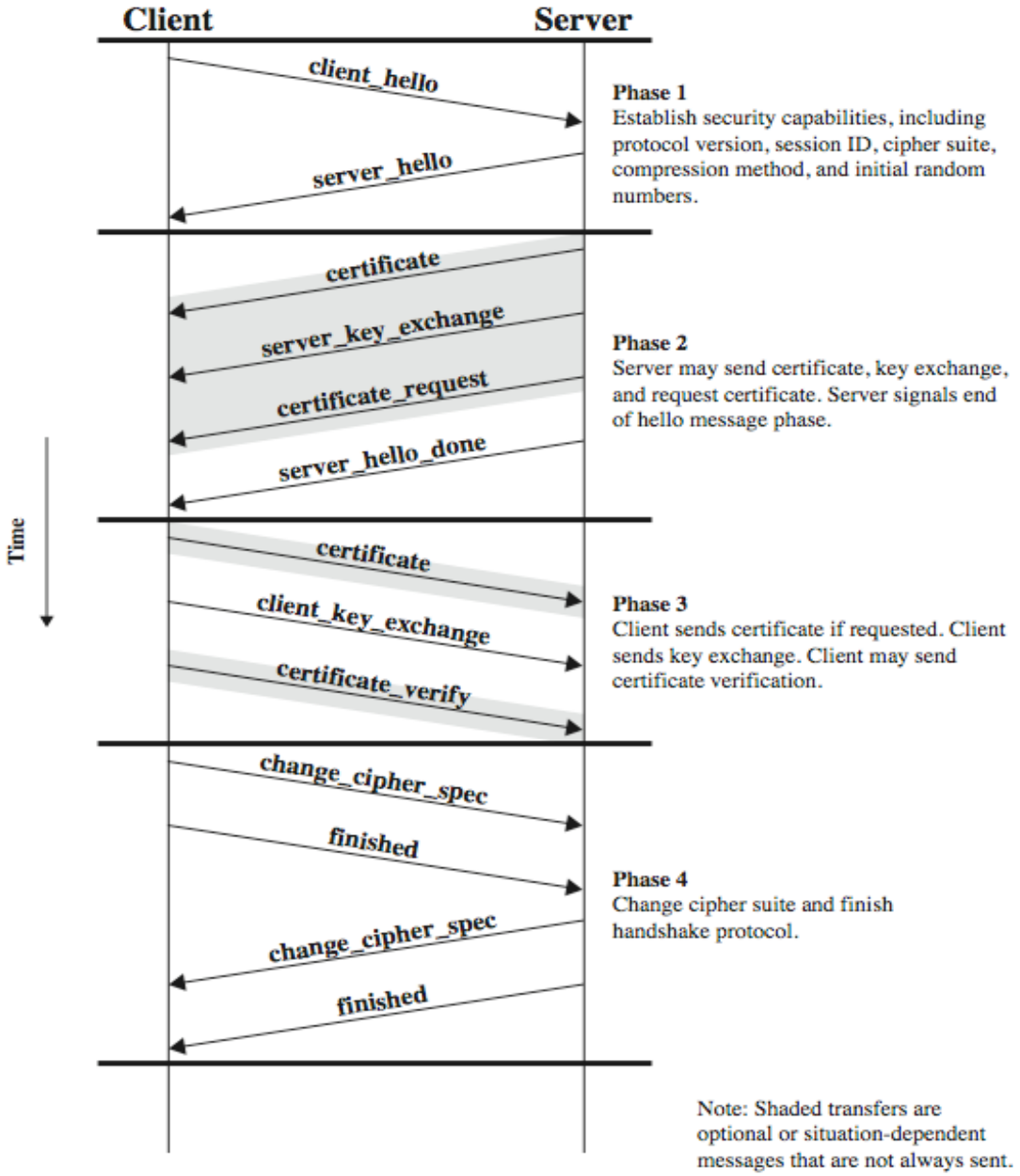
SSL Architecture

- SSL/TLS est composé :
  - d'un générateur de clés
  - de fonctions de hachage
  - d'algorithmes de chiffrement
  - de protocoles de négociation et de gestion de session
  - de certificats X509
- SLL/TLS s'appuie sur OpenSSL
- Composants :
  - SSL *Record Protocol* : protection des données
  - SSL *Handshake Protocol* : établissement de la session
  - SSL *Change Cipher Spec Protocol* : négociation des algorithmes (chiffrement, compression)
  - SSL *Alert Protocol* : messages d'erreur

SSL Handshake

- SSL *Handshake* : négociation du chiffrement et de l'authentification
  - Sélection des algorithmes de chiffrement et de la version utilisée
  - Choix d'un identificateur de session
  - Sélection et échange des certificats
    - Le serveur envoi son certificat (et sa chaîne de certification)
    - A la demande du serveur, le client envoi son certificat (et sa chaîne de certification)
    - Authentification du client et vérification (si demandée)
    - Envoi par le client d'une chaîne chiffrée avec sa clef privée. Le serveur vérifie que le client est bien titulaire de la clef privée en déchiffrant cette chaîne avec la clef publique du client qu'il avait reçue auparavant
  - Échange d'une clef de session pour le chiffrement symétrique des communications

SSL Handshake



SSL Handshake

- Reprendre une session :
  - Pour reprendre une session déjà initialisée, le client envoie dans le *Client Hello* l'identificateur de cette session.
  - S'il retrouve cet identificateur dans son cache de session le serveur répond avec le même identificateur de session dans le *Server Hello*
  - Cet identificateur permet de restaurer le contexte de la session, en particulier la clef de chiffrement symétrique.
- Forcer la renégociation :
  - Le serveur peut forcer la renégociation en répondant avec un nouveau Session ID

- SSL *Change Cipher Spec Protocol* :
  - Permet de signaler des transitions dans les stratégies de chiffrement,
  - Envoi d'un message pour indiquer que les messages
  - suivants utilisent les nouveaux paramètres négociés
- SSL *Alert Protocol* :
  - Définit plusieurs niveaux d'alertes
  - Certaine alertes sont définies pour entraîner l'arrêt immédiat de la session
- Optimisation indispensable du réglage des paramètres des serveurs :
  - Durée de conservation des contextes de session
  - Partage du cache en processus coopérants

TLS : *Transport Layer Security*

—TLS reprend tous les concepts généraux de SSL car TLS 1.0 puis TLS 1.1 sont basés sur SSL 3.0, donc compatibles

—TLS est plus clair

—TLS est plus générique que SSL (encapsulation)

—La conception du protocole est indépendante de son utilisation

—TLS n'impose pas de méthodes de chiffrements spécifiques

Utilisation SSL/TLS

- Quelques applications et standards utilisant SSL/TLS

http	80	https	443
smtp	25	smtps	465
pop3	110	pop3s	995
imap	143	imaps	993
ssh	22		
nntp	119	nntps	563
telnet	23	telnets	992
ftp	21	ftps	990
ftp-data	20	ftps-data	989

- SSL / TLS
  - Pré-requis :
    - Utiliser des logiciels serveurs et clients SSL/TLS
  - Inconvénients :
    - Si utilisation des certificats X509 => formation obligatoire des utilisateurs
  - Avantages :
    - Authentification forte du client
    - Maintenant, de nombreuses applications utilisent SSL/TLS
    - Confidentialité et intégrité des échanges
    - L'utilisateur utilise les mêmes logiciels sur son LAN que à l'extérieur, les communications sur LAN sont également sécurisées
  - Utilisation :
    - VPN d'accès (nomades à site)
    - Intranet, extranet (Sites à sites)
    - LAN
- Les tunnels SSL/TLS de part leur moindre coût et leur facilité de mise en place par rapport à IPsec se généralisent.
- Les applications utilisant une interface web et la messagerie sont déjà largement utilisées avec SSL/TLS.

Bilan : SSL(Record Protocol)

- **confidentialité**
  - using symmetric encryption with a shared secret key defined by Handshake Protocol
  - IDEA, RC2-40, DES-40, DES, 3DES, RC4-40, RC4-128
  - message is compressed before encryption
- **message intégrité**
  - using a MAC with shared secret key
  - similar to HMAC but with different padding

HTTPS

- HTTPS (HTTP over SSL)
  - combination of HTTP & SSL/TLS to secure communications between browser & server
    - documented in RFC2818
    - no fundamental change using either SSL or TLS
- use https:// URL rather than http://
  - and port 443 rather than 80
- encrypts
  - URL, document contents, form data, cookies, HTTP headers

Niveau 7

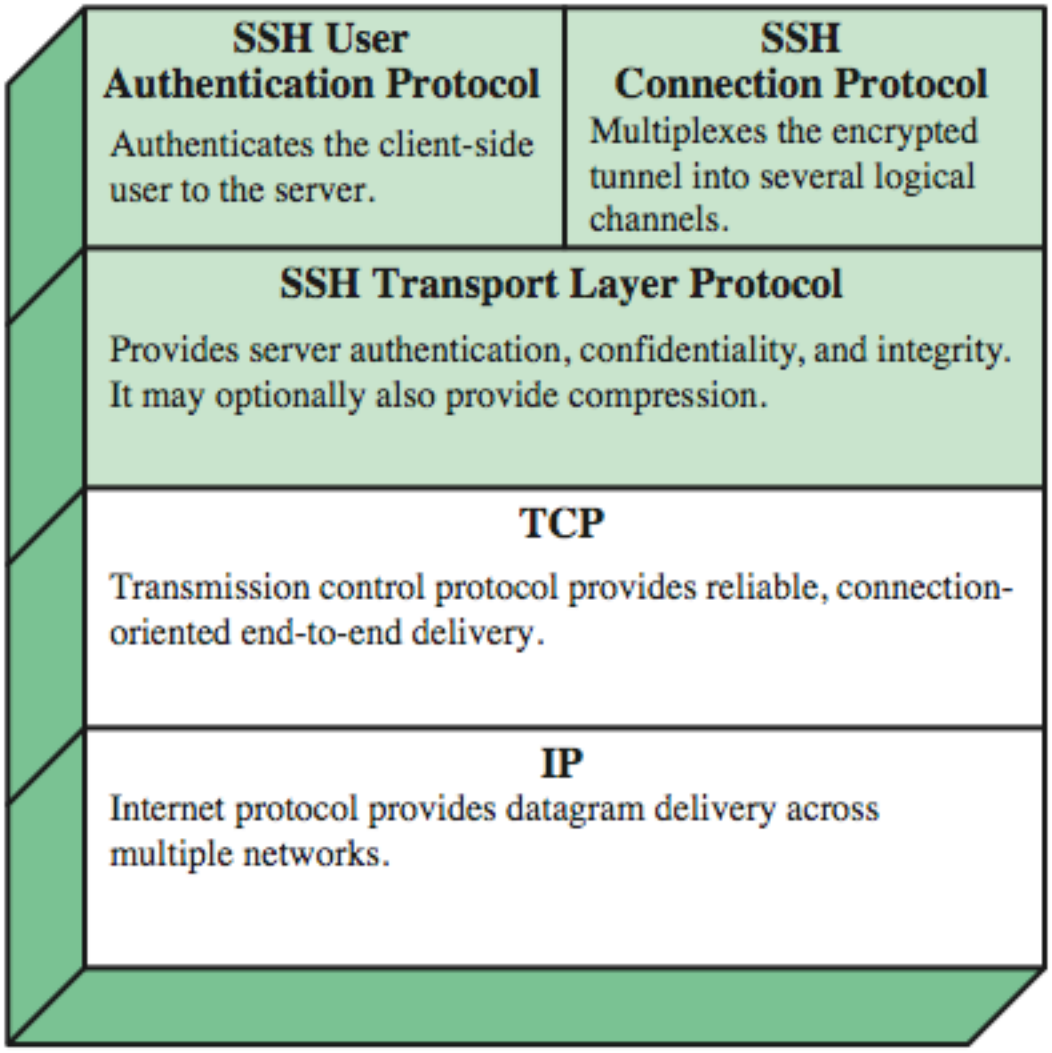
SSH


SSH!
DON'T GIVE AWAY YOUR PASSWORD TO
ANYONE WHO MIGHT BE LISTENING!
Always use SSH (Secure SHell) when connecting
to Computer Science Department hosts, instead of
telnet or rsh. For more information:
http://www.cs.umd.edu/faq/ssh.html

SSH

- SSH (*Secure Shell*)
  - Le protocole SSH comprend une suite d'outils dont l'objectif est de remplacer les commandes clientes et les services de :
    - Connections interactive : rlogin, telnet et rsh => ssh
    - Copie entre machines : rcp => scp
    - Transfert de fichiers : ftp => sftp
  - Il permet également de :
    - Transférer toutes applications TCP dans le tunnel de la session ssh
  - On peut ainsi forwarder :
    - X11 (X11 forwarding)
    - SMTP, POP, IMAP, … (redirection de port)
    - Transférer les jetons Kerberos et AFS

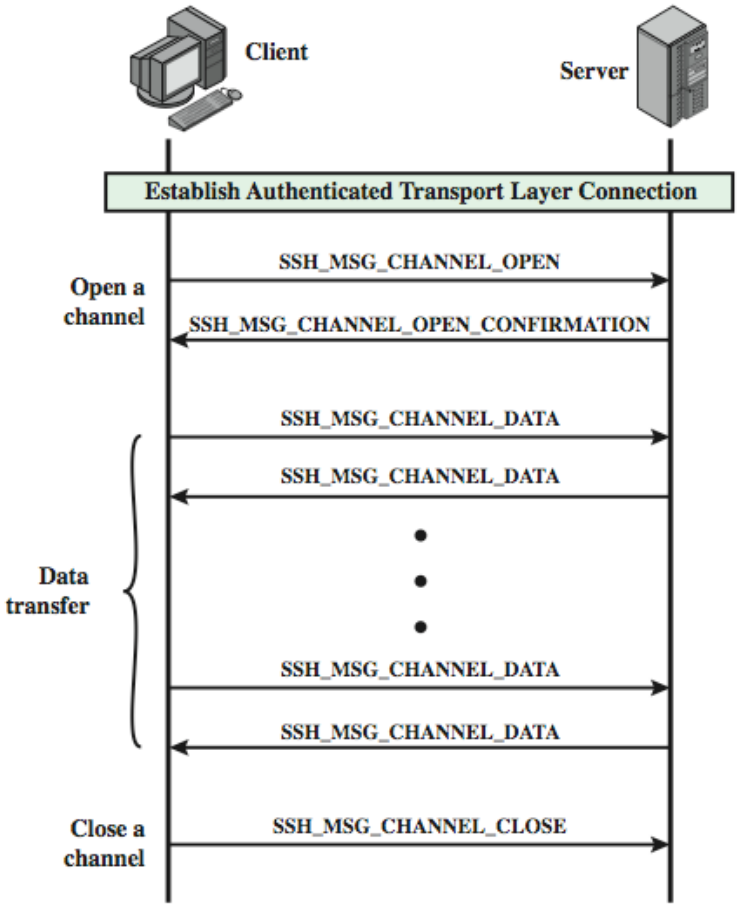
SSH Protocol Stack



SSH User Authentication Protocol

- authenticates client to server
- three message types:
  - SSH_MSG_USERAUTH_REQUEST
  - SSH_MSG_USERAUTH_FAILURE
  - SSH_MSG_USERAUTH_SUCCESS
- authentication methods used
  - public-key, password, host-based

SSH Connection Protocol Exchange



Applications SSH

- ***Applications SSH***
  - FTP anonyme pour modifier des versions de logiciels, appliquer des patchs...
    - L'authentication du client n'est pas nécessaire, mais le client veut être sûr de l'origine du logiciel.
  - FTP sécurisé.
    - Upload de pages web vers un serveur en utilisant sftp.
    - Le serveur doit authentifier les clients.
    - Une authentification Login/Mot de passe est suffisante, transmise via SSH transport layer protocol.
  - Administration à distance sécurisée
    - L'administrateur système lance un terminal sur la machine distante
    - Son mot de passe est protégé par SSH transport layer protocol.

summary

- SSH
  - Pré-requis :
    - Logiciel serveur et client, en standard sur Linux, existe en opensource pour Windows
  - Inconvénients :
    - Configuration des tunnels => former les utilisateurs
    - Possibilité d'accéder à tout le LAN => attention
  - Avantages :
    - Confidentialité et intégrité des échanges
    - Compression des communications
    - X11 forwarding, transfert de jetons Kerberos et AFS, tunnels
    - Simple d'installation et d'utilisation
  - Utilisation :
    - VPN d'accès (nomades à site) : VPNe

Fin(1/2)

- SSH permet également :
  - Authentification forte des machines et des clients
  - Utilisation possible des certificats X509
  - Chiffrer le tunnel
  - Compresser le tunnel sur demandes
- Beaucoup de produits, des solutions *Open Source* convenables
- La tendance actuelle va vers les VPN SSL moins coûteux et moins lourds pour les machines clientes
- Faites votre choix ….

Fin(1/2)

- ***Comparaison IPSec, SSL/TLS & SSH***
  - Protocoles de Distribution et gestion de clefs
    - IKE dans IPSec
    - Handshake Protocol dans SSL/TLS (éventuellement sans authentification)
    - Authentication Protocol dans SSH
  - Négotiation d'algorithmes de chiffrement protégée.
  - Opèrent à des couches différentes
    - Où doit-on mettre la sécurité ?
    - Peuvent tous être utilisés pour construire des réseaux virtuels privés (VPNs).