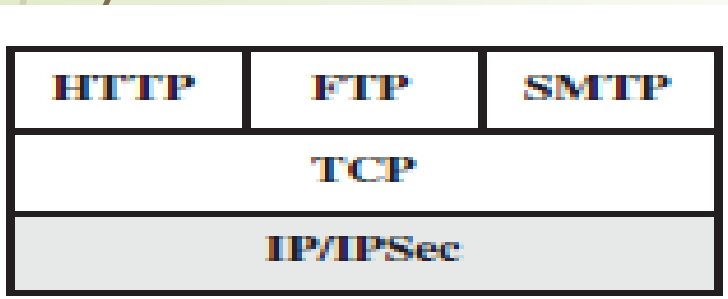
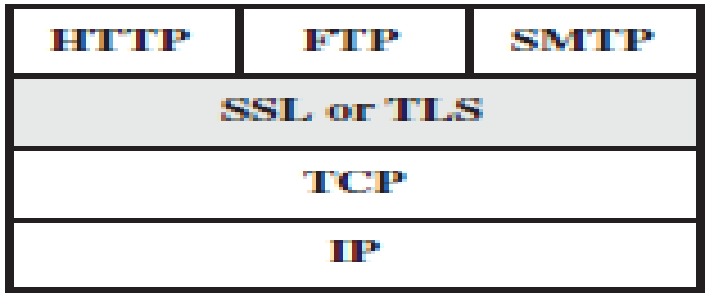
Emplacement relatif de la sécurité dans la pile de protocoles TCP / IP

Approches de sécurité du trafic Web

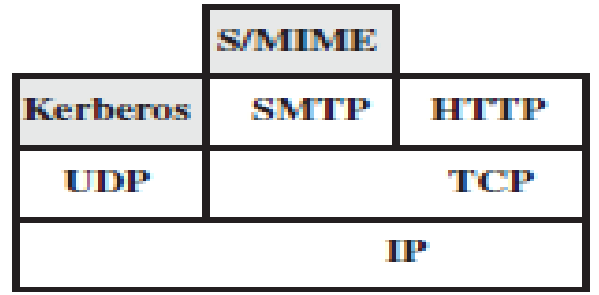
- Couche réseau : IPSec
- Couche transport: SSL-TLS
- Couche application : PGP, HTTPS



(a) Network level



(b) Transport level



(c) Application level

HTTPS (HTTP sur SSL)

- HTTPS est la combinaison de HTTP et SSL pour implémenter une communication sécurisée entre un navigateur Web et un serveur Web.
- les adresses URL commencent par https: // plutôt que par http: //.
- Une connexion HTTP normale utilise le port 80.
- Si HTTPS est spécifié, le port 443 est utilisé, ce qui appelle SSL.

HTTPS

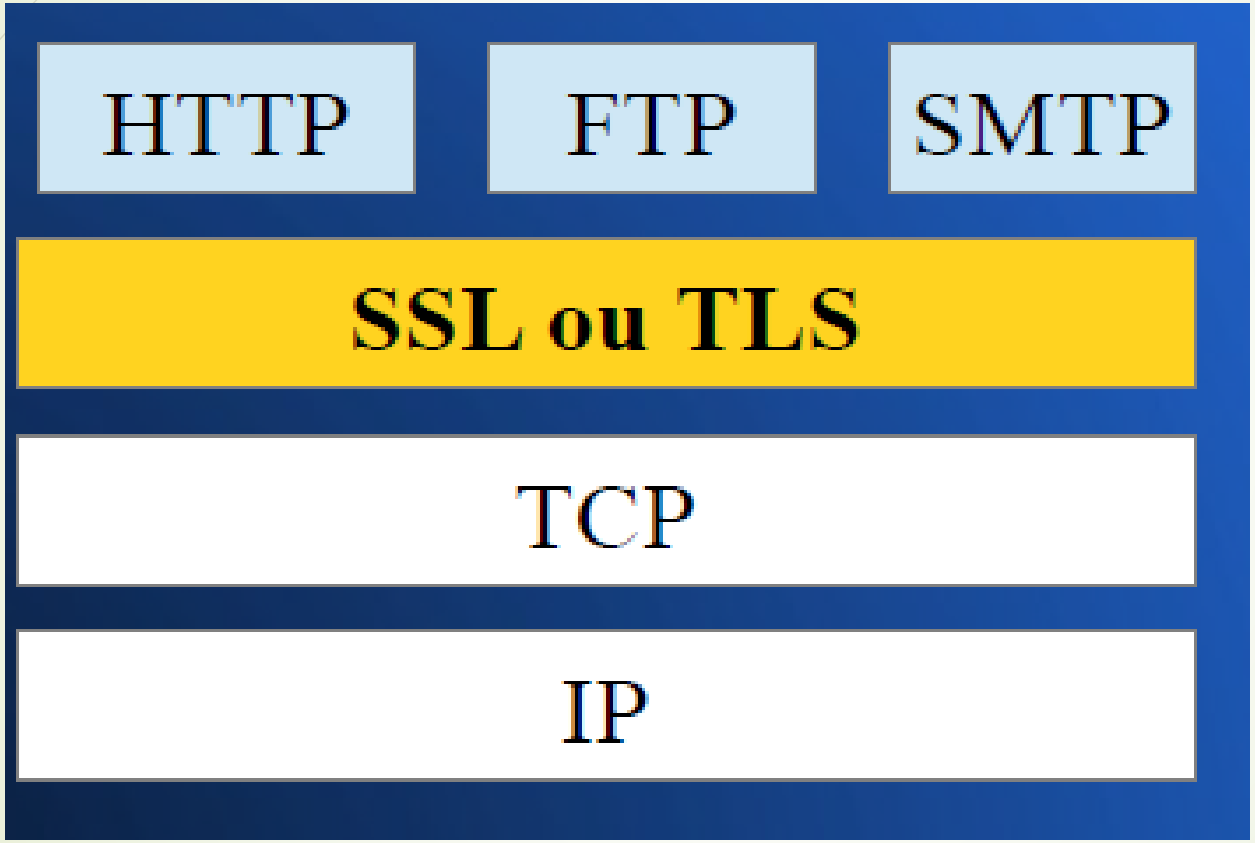
- Dans HTTPS les éléments suivants de la communication sont cryptés:
  - URL du document demandé
  - Contenu du document
  - Contenu des formulaires du navigateur
  - Cookies envoyés de navigateur à serveur et de serveur à navigateur
  - Contenu de l'en-tête HTTP
- HTTPS est documenté dans RFC 2818, HTTP sur TLS.
- Il n'y a pas de changement fondamental dans l'utilisation de HTTP sur SSL ou TLS, et les deux implémentations sont appelées HTTPS.

Protocole SSL/TLS
(Securre Socket Layer/Transport Layer Security)

SSL/TLS : Introduction

- Le Protocole SSL est développé en 1994 par Netscape.
- Permet la mise en œuvre de tunnels au niveau 4 du modèle OSI (transport).
- N'est utilisable que pour la sécurisation du flux TCP.
- La dernière version de SSL est 3. Ses fonctionnalités sont très similaires à celles du protocole TLS (Transport Layer Security) version 1. On dit souvent que SSLv3=TLSv1

SSL/TLS: Architecture



Ports au dessus de SSL

Protocole sécurisé	Port	Protocole non sécurisé	Application
FTP-DATA	889	FTP	Transfert de fichiers
FTPS	990	FTP	Contrôle du transfert de fichiers
IMAPS	991	IMAP4	Accès distant à la boîte aux lettres avec ou sans rapatriement des messages
TELNETS	992	Telnet	Protocole d'accès distant à un système informatique
IRCS	993	IRC	Protocole de conférence par l'écrit

Protocole sécurisé	Port	Protocole non sécurisé	Application
HTTPS	443	HTTP	Transactions requête-réponse sécurisées
SSMTP	465	SMTP	Messagerie électronique
SNNTP	563	NNTP	News sur le réseau Internet
SSL-LDAP	636	LDAP	Annuaire X.500 allégé
SPOP3	995	POP3	Accès distant à la boîte aux lettres avec rapatriement des messages

Fonction de SSL

1. La confidentialité des données => algorithme de chiffrement
2. L'intégrité des données => fonction de hachage
3. Authentification (serveur, client) => certificat numérique

TRANSPORT LAYER SECURITY TLS

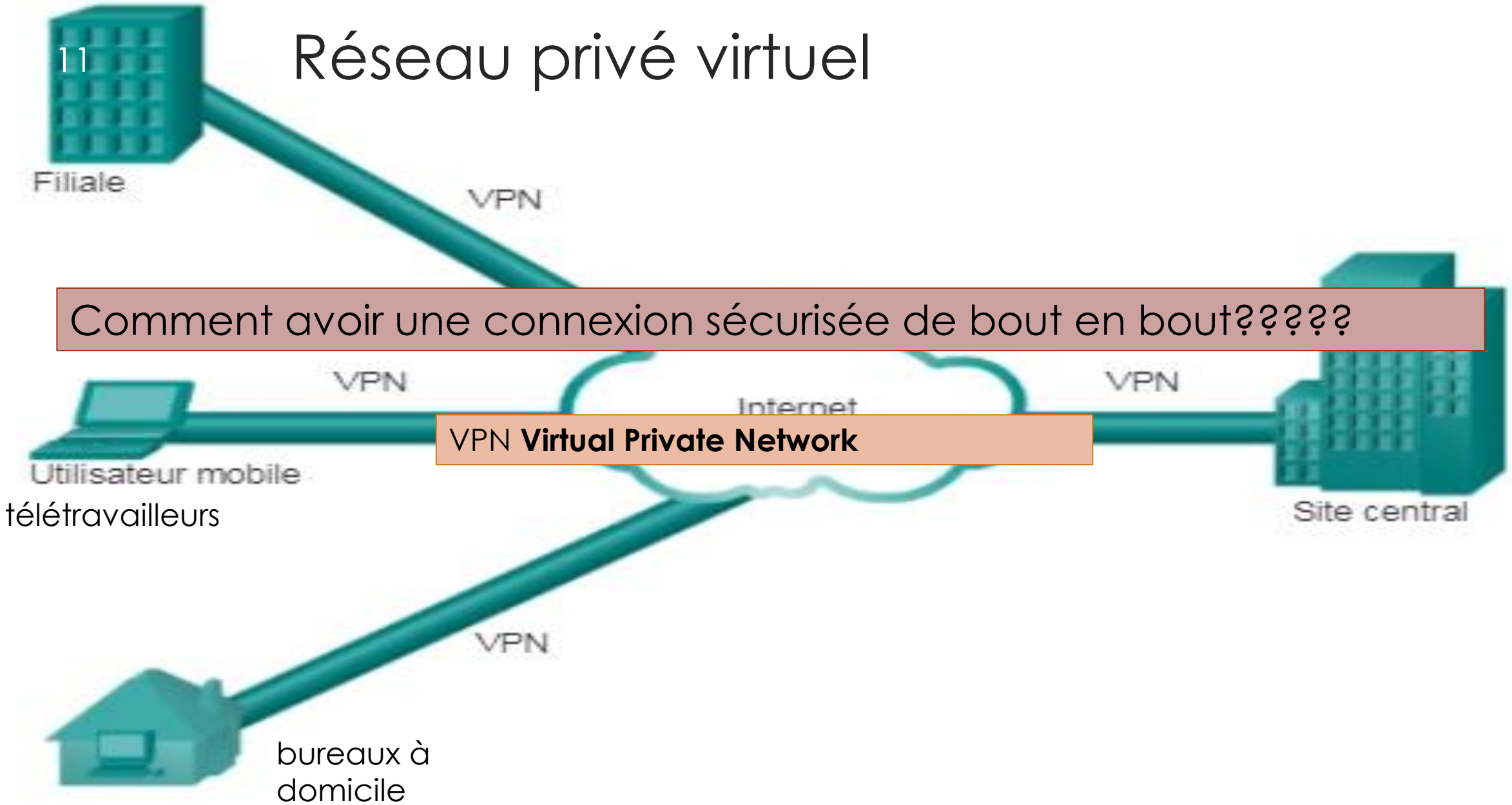
- TLS est une initiative de normalisation de l'IETF dont le but est de produire une version Internet standard de SSL. TLS est défini comme une norme Internet proposée dans la RFC 5246. La RFC 5246 est très similaire à SSLv3.

SSL/TLS résumé

- **Échange sécurisé de clés de chiffrement**
- **Authentification du serveur** (optionnelle mais souvent utilisée)
- **Authentification du client** (optionnelle et très peu utilisée)
- **Confidentialité et Intégrité des messages**

- SSL est conçu pour utiliser TCP pour fournir un service sécurisé et fiable de bout en bout.
- La version standard Internet est appelée Transport Layer Service (TLS).

Réseau privé virtuel



Présentation des VPN

- Un VPN est un réseau privé créé par tunnel ' **tunneling'** sur un réseau public, généralement Internet. tunnel = canal sécurisé
- Un VPN est un environnement de communication dans lequel l'accès est strictement **contrôlé**
- Les premiers VPN étaient des tunnels IP , pas de sécurité (GRE crée une liaison point à point)
- l'implémentation sécurisée de VPN avec chiffrement, tels que des VPN IP sec
- Une passerelle VPN est requise pour l'implémentation de VPN (routeur, un pare-feu)
- Points de terminaison = La fin du tunnel entre les périphériques VPN
- Peut être un **logiciel** sur un ordinateur local ou un **concentrateur VPN**
- **Concentrateur VPN - un périphérique matériel dédié qui regroupe des centaines ou des milliers de connexions VPN**

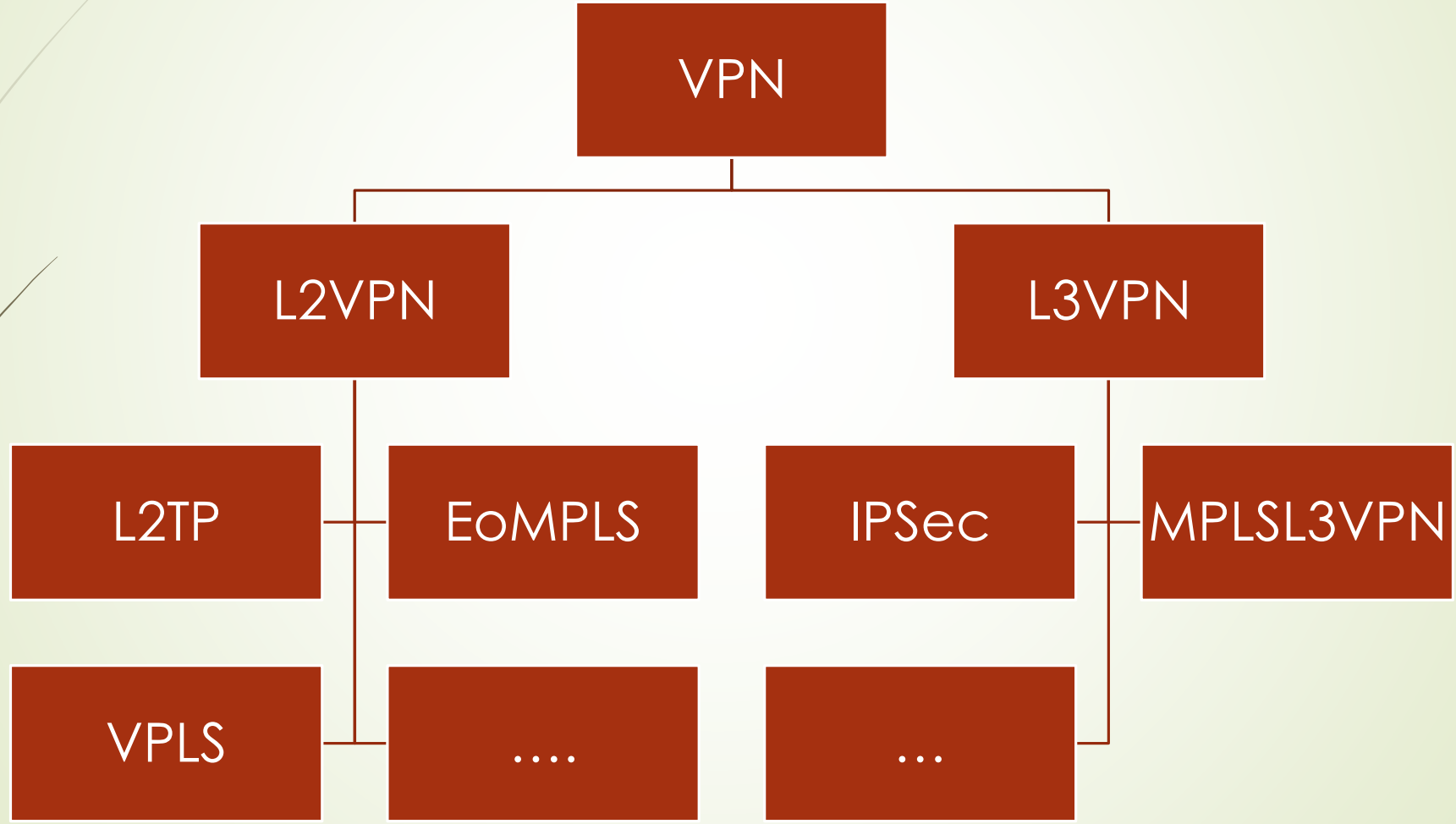
Avantages des réseaux privés virtuels

- **Réductions des coûts :** wan technologie
- **Évolutivité :** ajouter facilement de nouveaux utilisateurs
- **Compatibilité avec la technologie haut débit** : Permet au travailleurs mobiles et aux télétravailleurs d'avoir une connectivité haut débit rapide,
- **Sécurité :** protocoles de chiffrement et d'authentification avancés qui protègent les données

types de réseaux privés virtuels

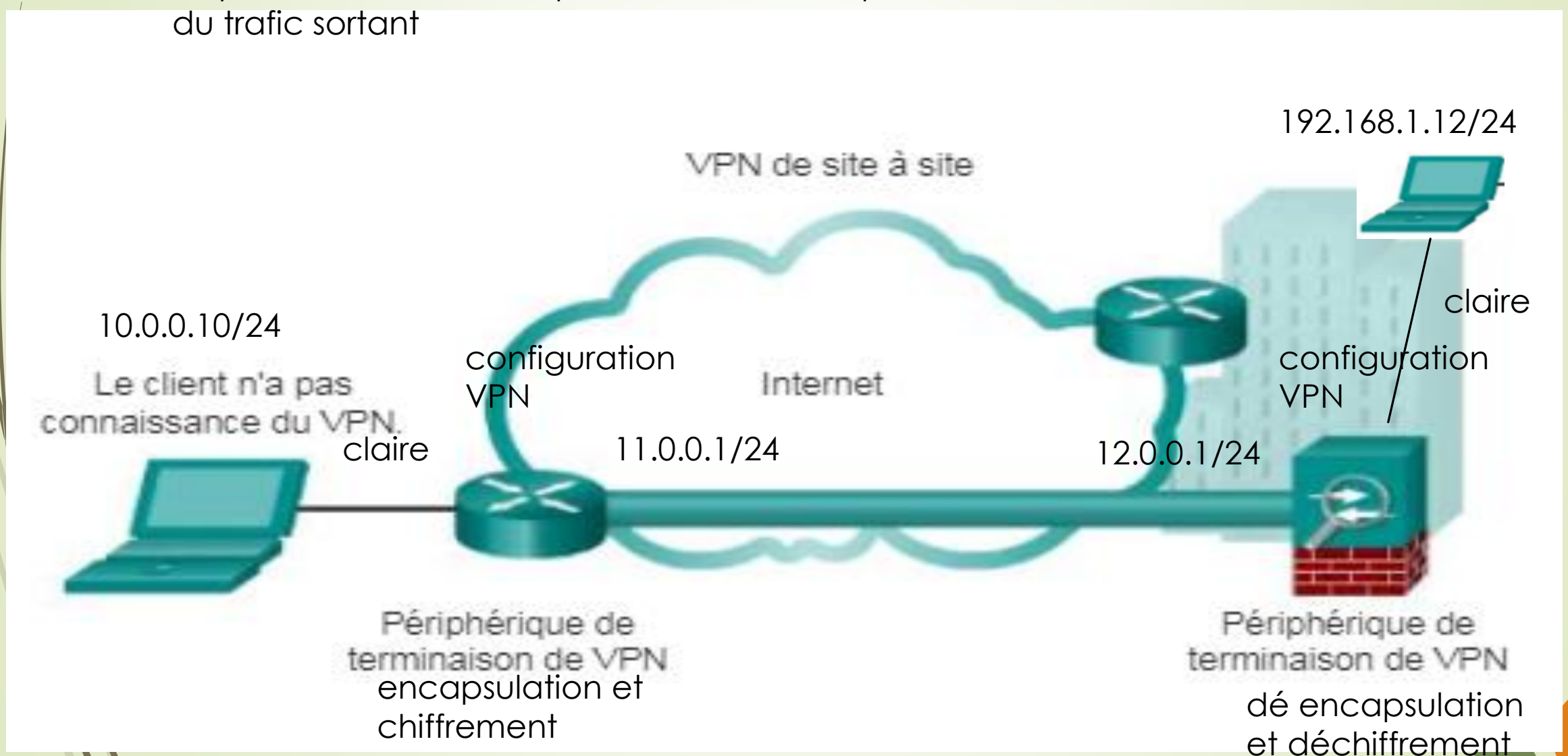
Il existe deux types de réseaux privés virtuels :

- Site à site : R-R , FW-FW , R-FW
- Accès à distance : PC-R , PC-FW


VPN
L2VPN
L3VPN
L2TP
EoMPLS
IPSec
MPLSL3VPN
VPLS
....
...

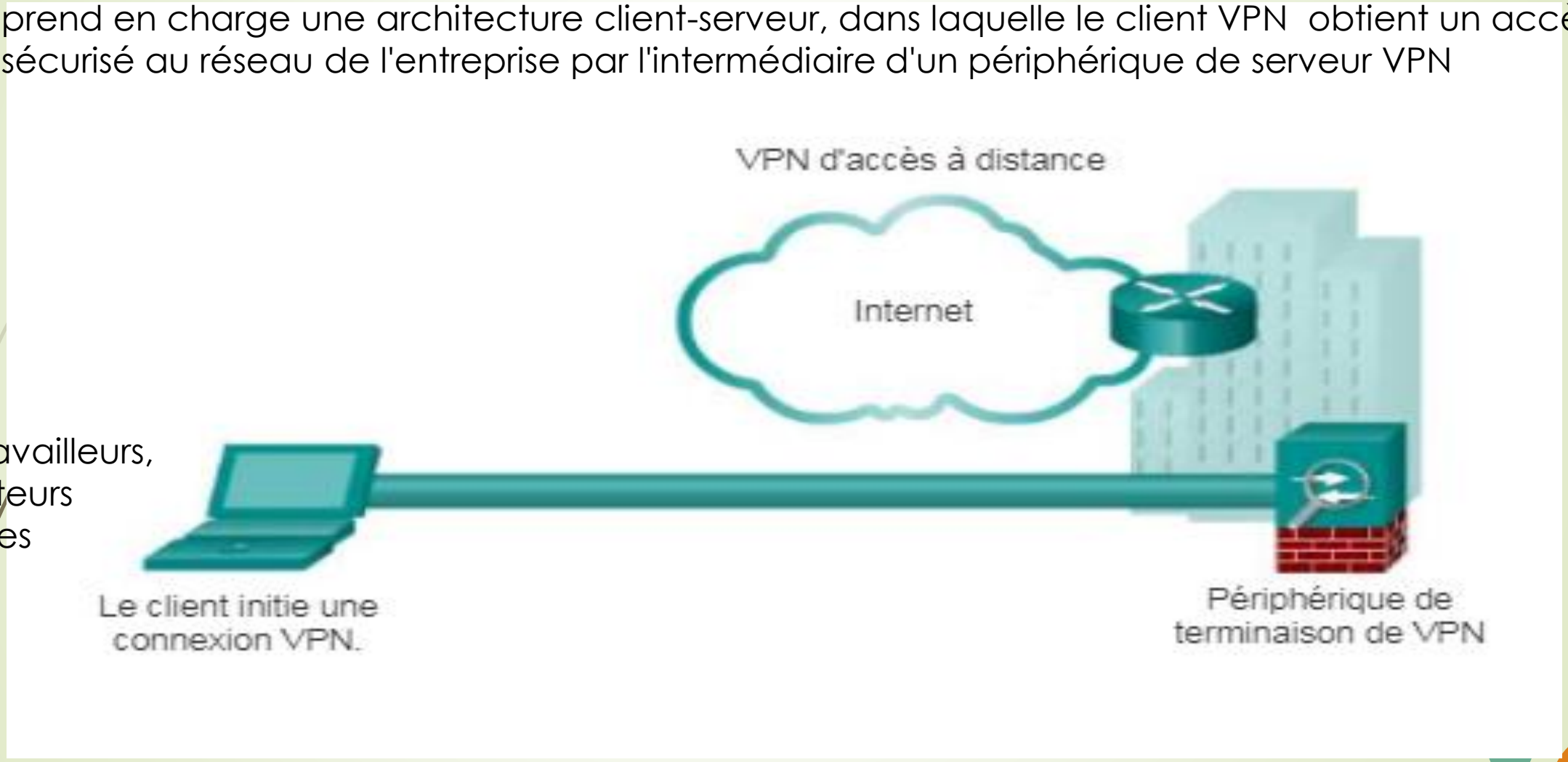
VPN de site à site = VPN statique

l'architecture est statique
La passerelle VPN est responsable de l'encapsulation et du chiffrement de la totalité du trafic sortant



VPN d'accès à distance = VPN dynamique

- l'architecture n'est pas statique @ IP dynamique
- prend en charge une architecture client-serveur, dans laquelle le client VPN obtient un accès sécurisé au réseau de l'entreprise par l'intermédiaire d'un périphérique de serveur VPN



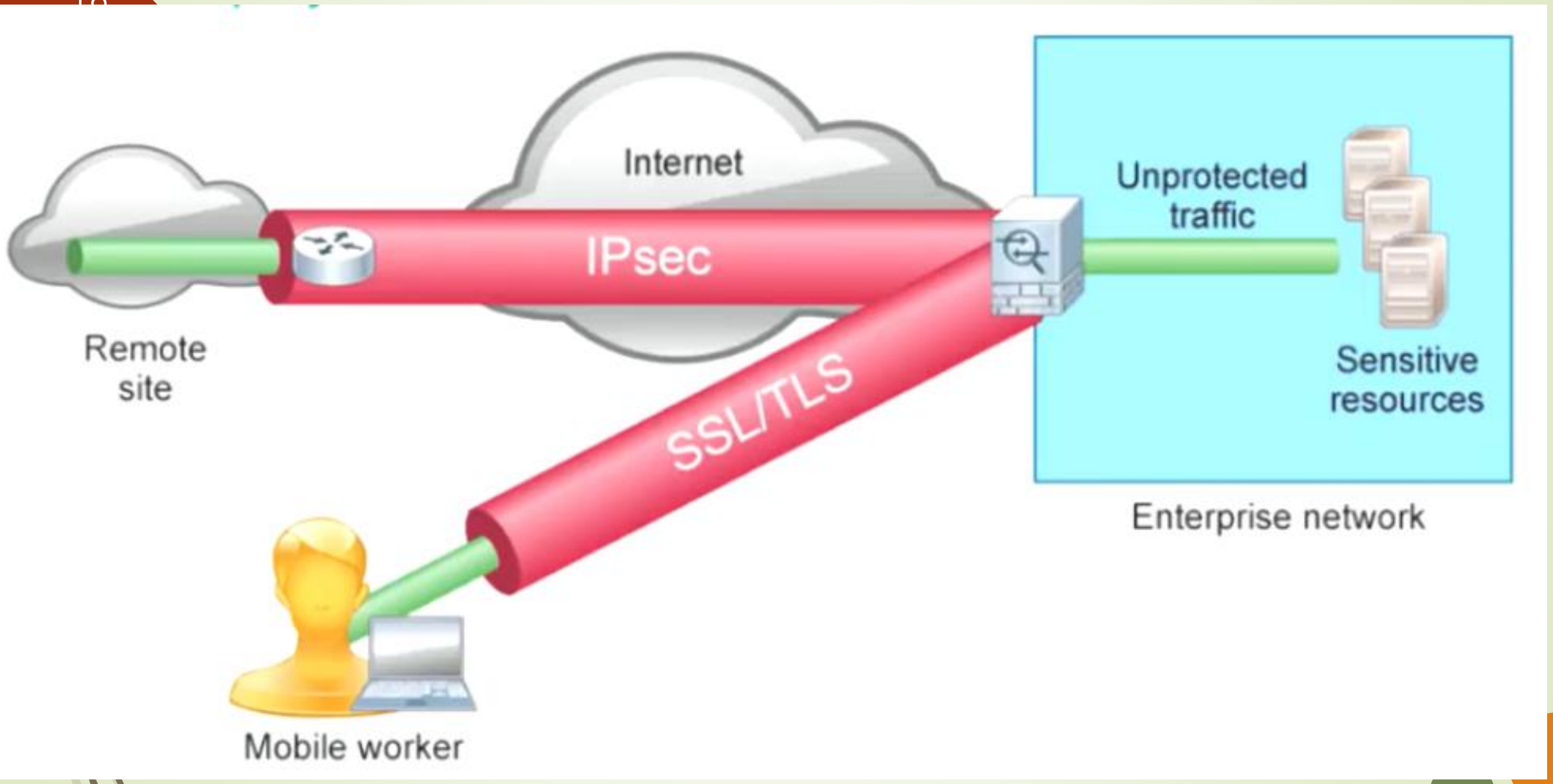
télétravailleurs, utilisateurs mobiles

logiciel client VPN doive être installé sur le périphérique final de l'utilisateur mobile

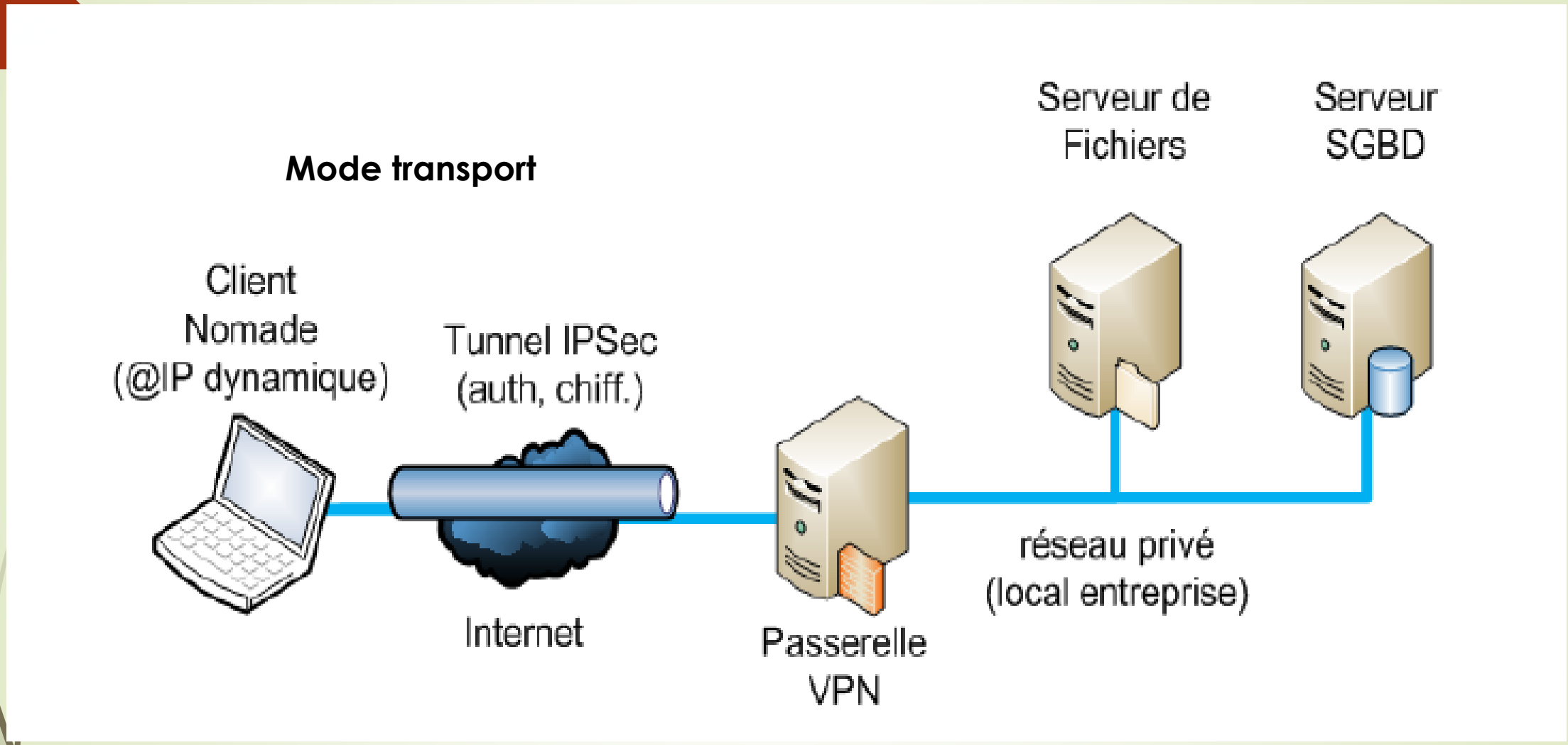
types de réseaux privés virtuels

Il existe deux types de réseaux privés virtuels :

- Site à site utilise mode tunnel
- Accès à distance utilise mode transport.

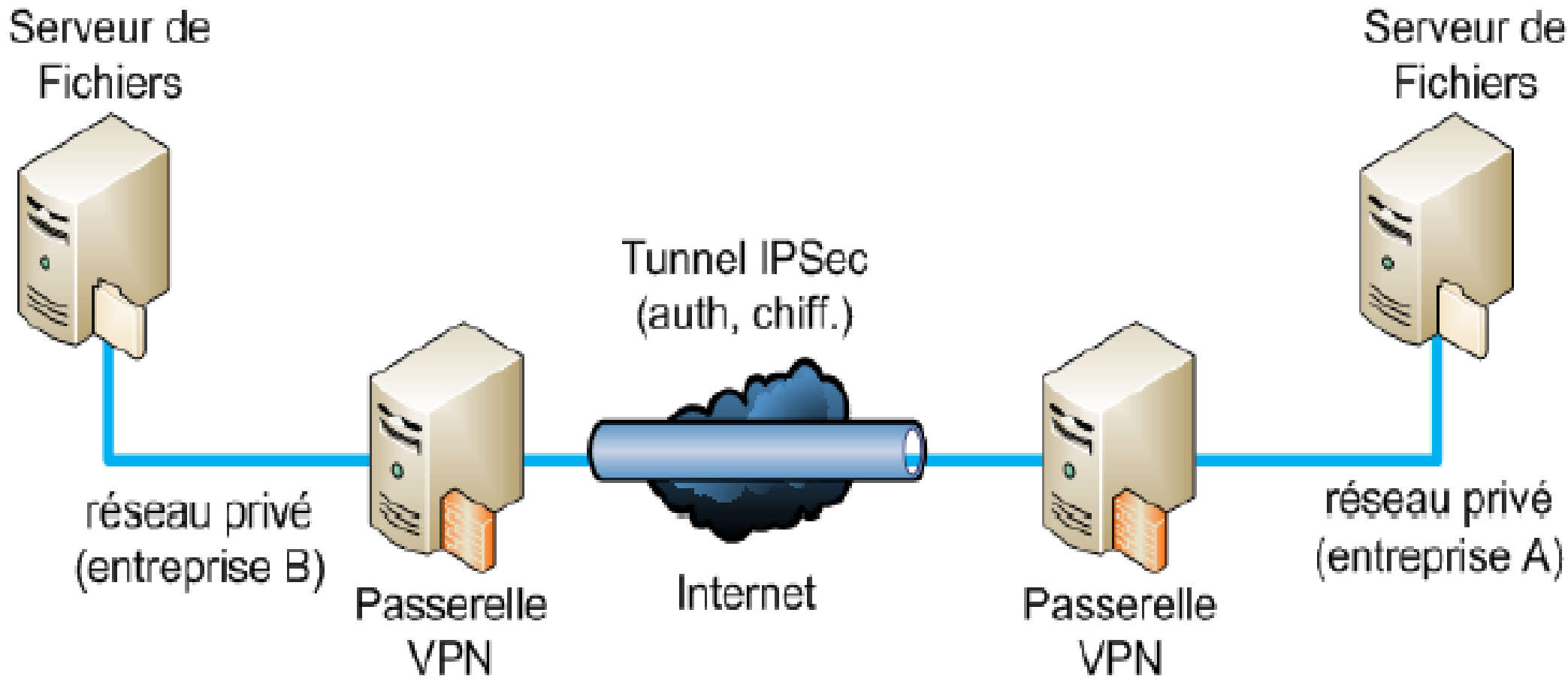

Internet
IPsec
SSL/TLS
Remote site
Unprotected traffic
Sensitive resources
Enterprise network
Mobile worker

Le chiffrement IP : IPSEC Transport



Utilisé pour offrir un accès distant sécurisé aux nomades via un réseau non sûr (Internet)
Connexion point à point non permanente (@ip dynamique)

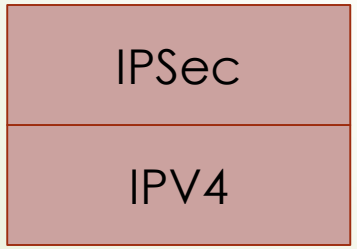
mode tunnel



connexion permanente

IP sec : **Sécurité de protocole Internet**

- Version sécurisé du Protocol IP
- Avec un VPN IPsec, les informations issues d'un réseau privé sont transportées en toute sécurité sur un réseau public.
- Le protocole IPsec est une norme IETF qui définit comment un VPN peut être configuré de manière sécurisée à l'aide du protocole Internet (IP).
- le protocole IPsec se base sur des algorithmes existants pour mettre en œuvre des communications sécurisées.
- IPsec fonctionne au niveau de la couche réseau, en protégeant et en authentifiant les paquets IP entre les équipements IPsec participants .

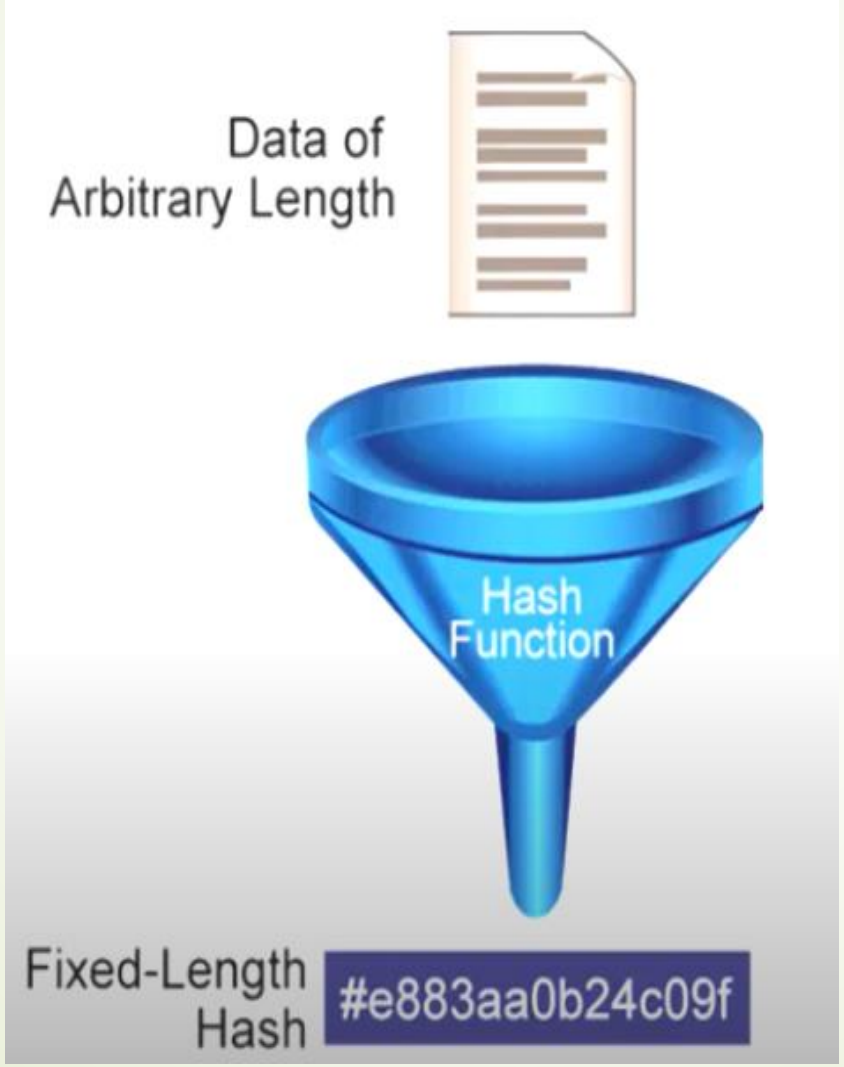


Module Ipsec intégré
il faut juste de l'activé

Hachage sans clé (MDC)

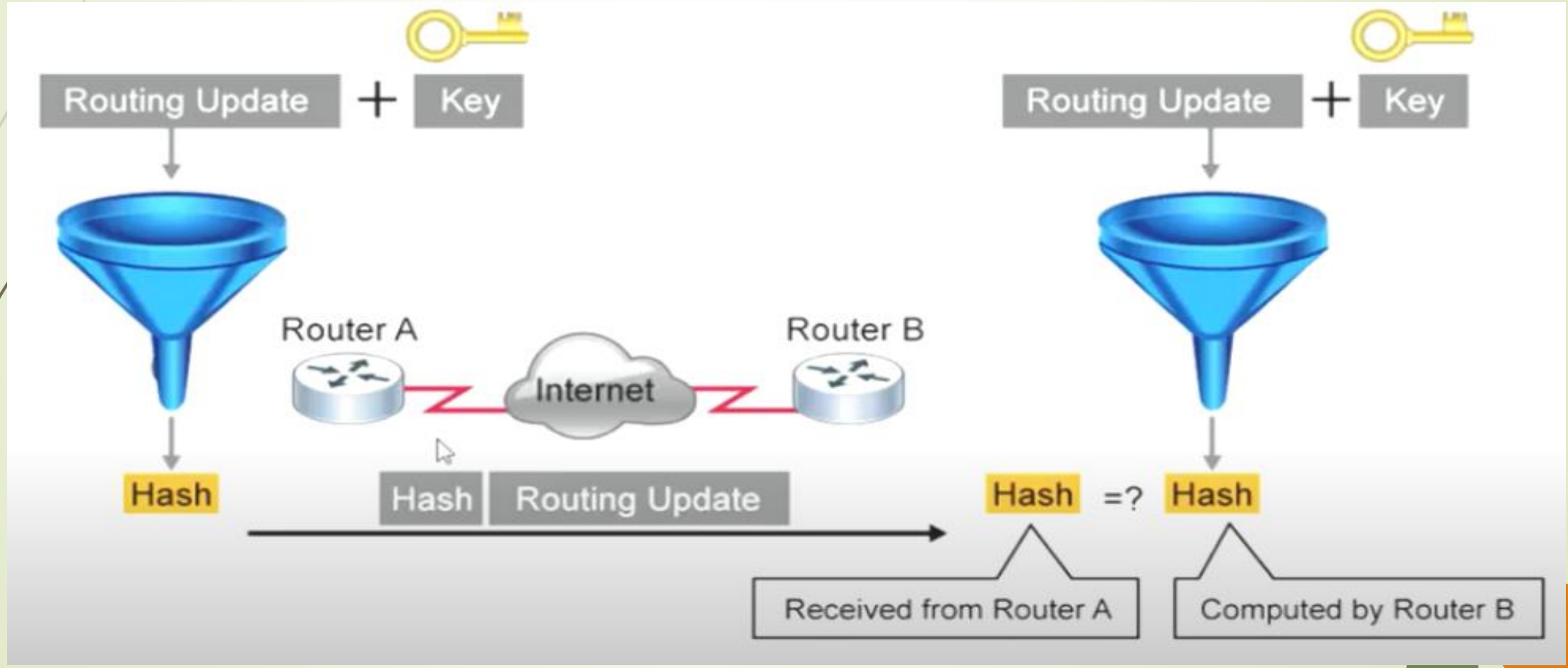
1) Fonction de hachage sécuritaire sans clé :

- **MDC** «Message Digest Code» => Empreinte de message.



MAC «Message Authentication Code»

Nombre limité =>PSK
Grand nombre => RSA



Fonctions IPsec

Confidentialité

Intégrité des données

Authentification

16	24	32 bits
SPI (Security Association Identifier)		
Numéro d'ordre		
Données utiles transportées (longueur variable)		
Remplissage (0-255 octets)		
	Longueur de remplissage	En-tête suivant
Données d'authentification (variable)		

Protection anti-reprise

Protection anti-reprise :

- la protection anti-reprise est la capacité à détecter et à rejeter des paquets rediffusés,
- vérifie que chaque paquet est unique et qu'il n'a pas été dupliqué. Les paquets IPsec sont protégés en comparant le numéro de séquence des paquets reçus avec une fenêtre glissante sur l'hôte de destination sur la passerelle de sécurité. Les paquets en retard et dupliqués sont abandonnés.

Services IPsec

- Deux protocoles sont utilisés pour assurer la sécurité:
  - un protocole d'authentification désigné par l'en-tête du protocole, Authentication Header (AH)
  - un protocole combiné de cryptage / authentification désigné par le format du paquet pour ce protocole, Encapsulating Security Payload (ESP).

protocoles IPsec

En-tête d'authentification

AH permet de procéder aux opérations suivantes :

- Authentification
- Intégrité

confidentialité n'est pas requise

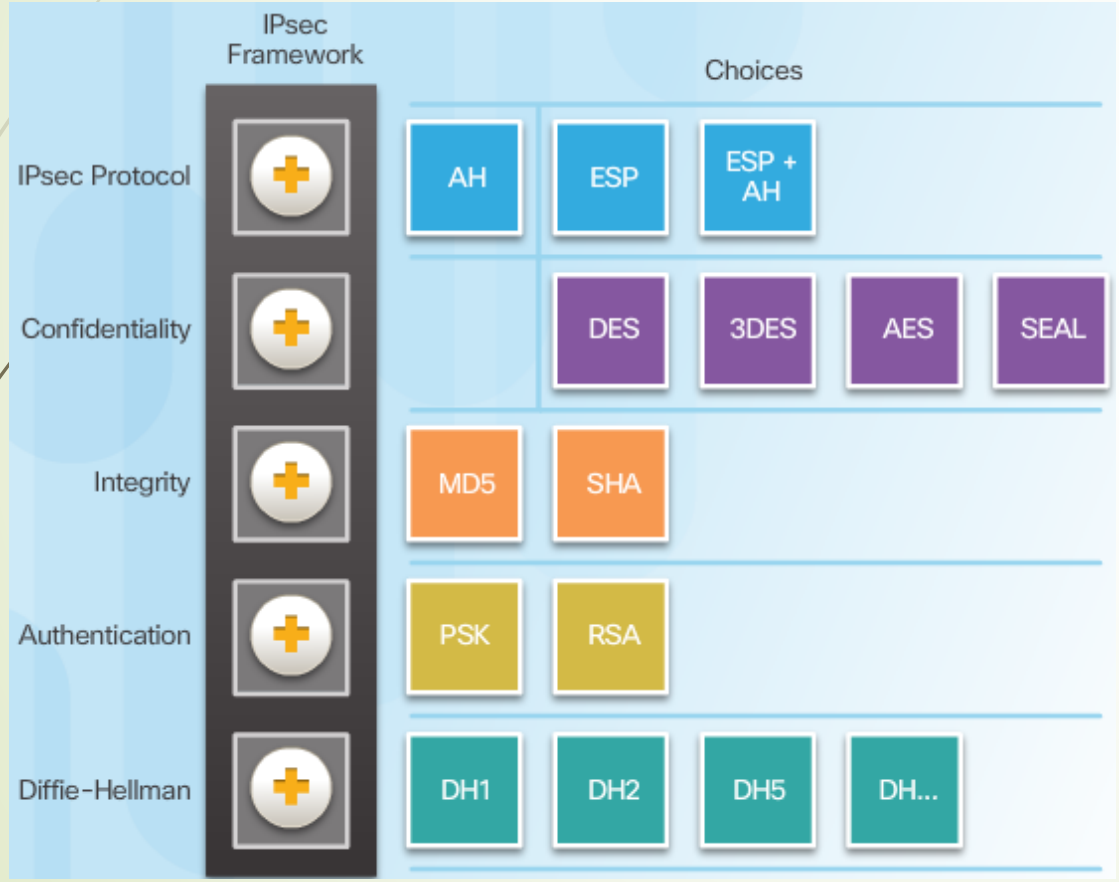
Encapsulation Security Payload

ESP permet de procéder aux opérations suivantes :

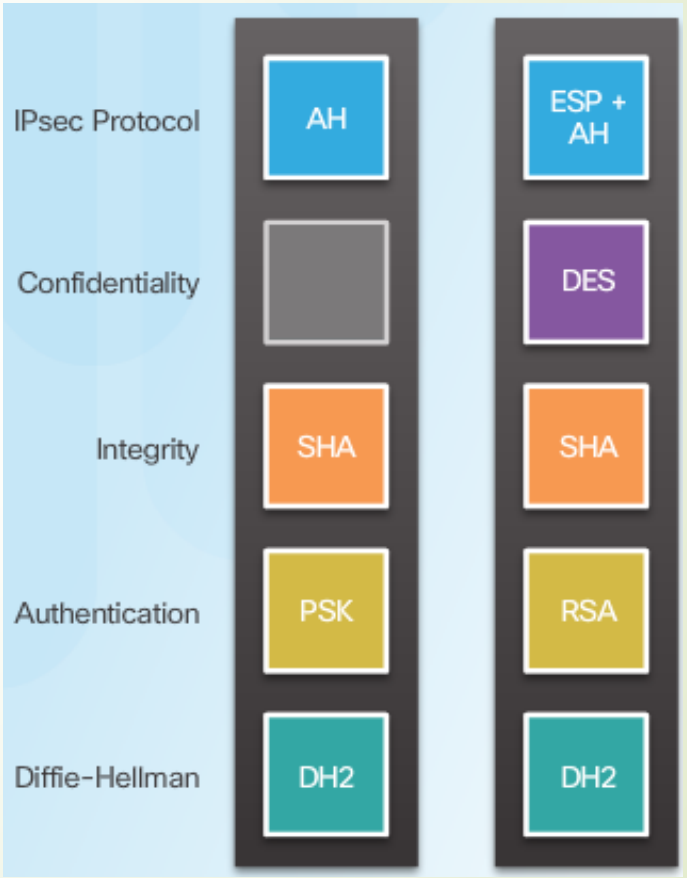
- Chiffrement
- Authentification
- Intégrité

IPsec Technologies

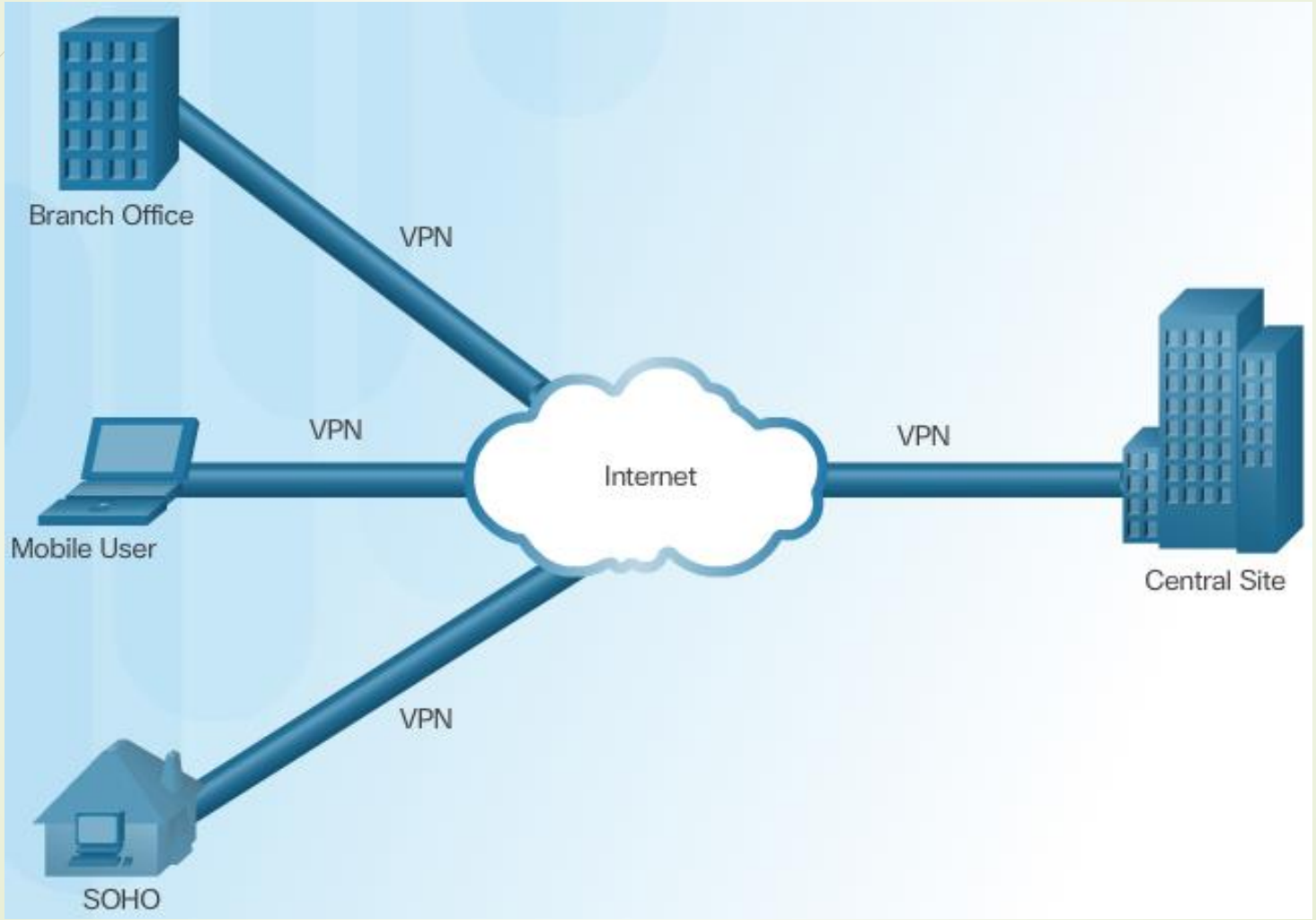
cadre IPsec



IPsec Exemples de mise en œuvre

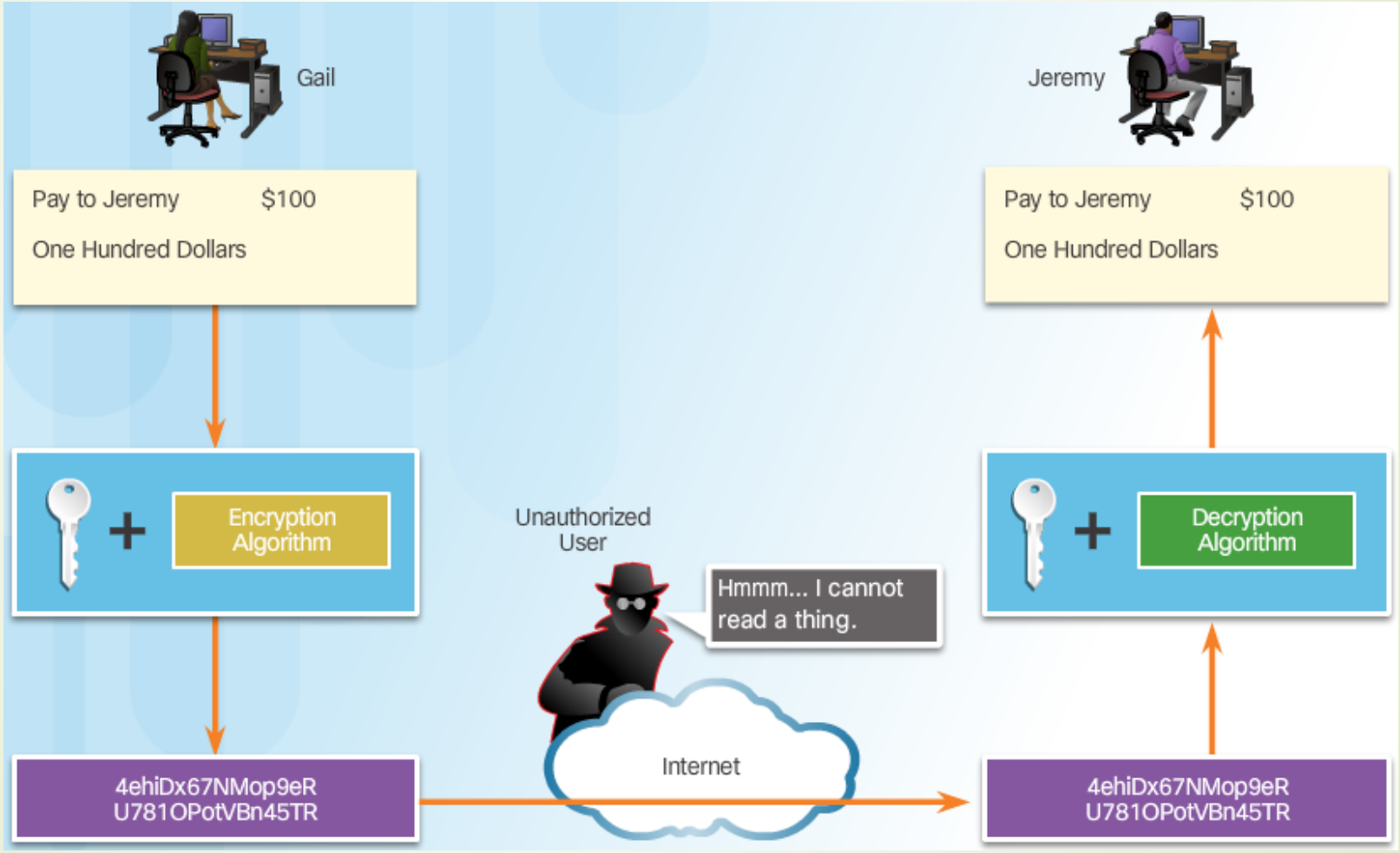


Couche 3 réseaux privés virtuels IPSec



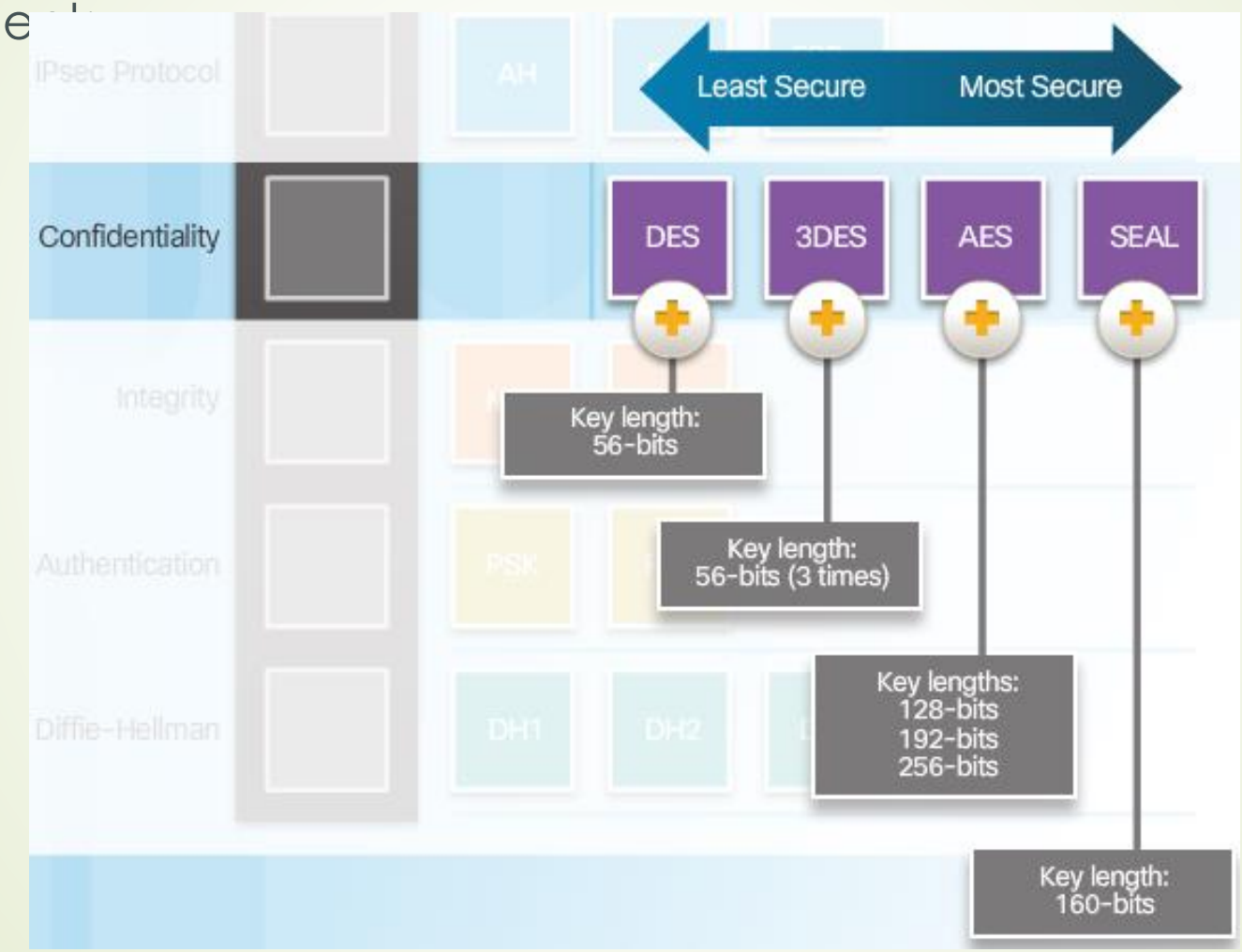
Confidentialité

Confidentialité avec chiffrement:



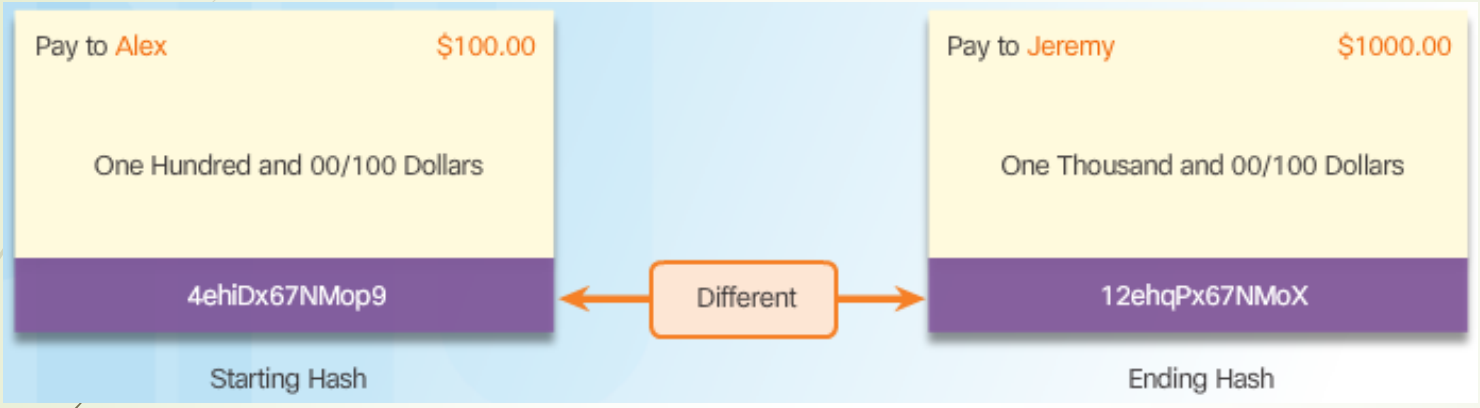
Confidentialité (Cont.)

Les algorithmes de chiffrement

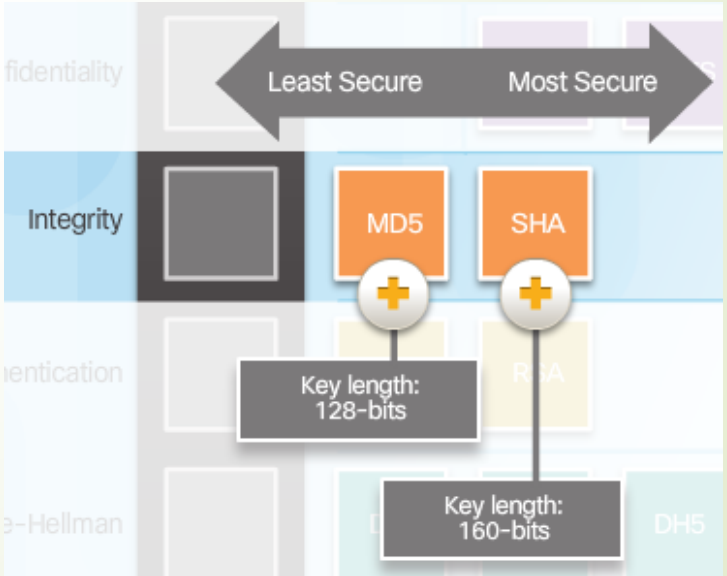


Intégrité

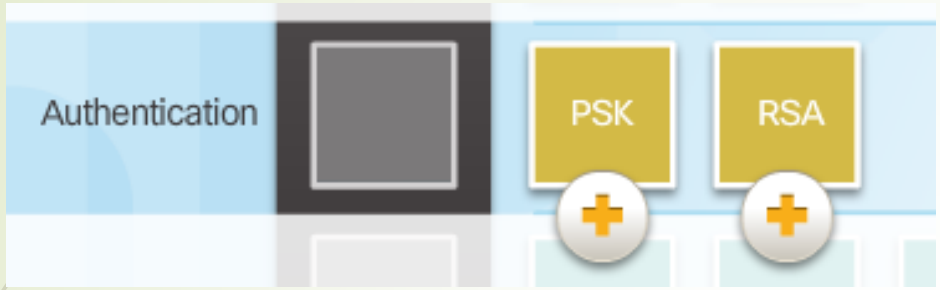
Les algorithmes de hachage



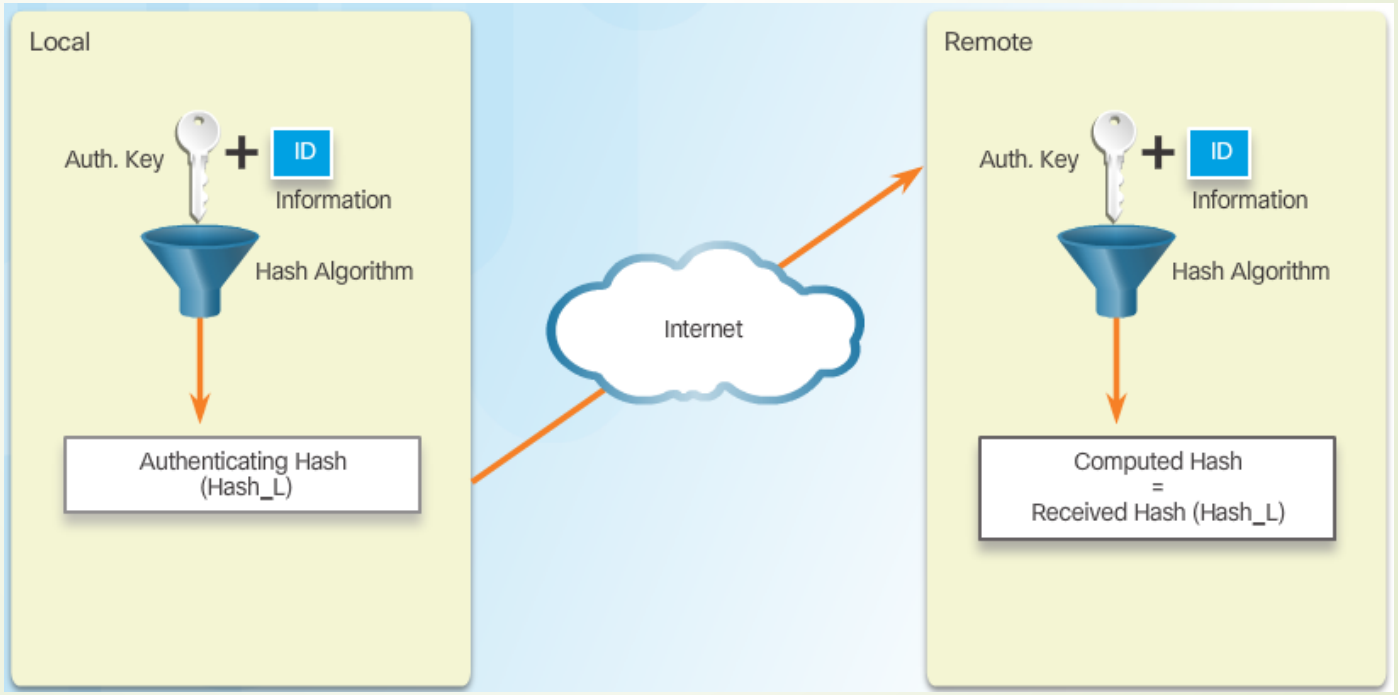
Sécurité des algorithmes de hachage



Authentification

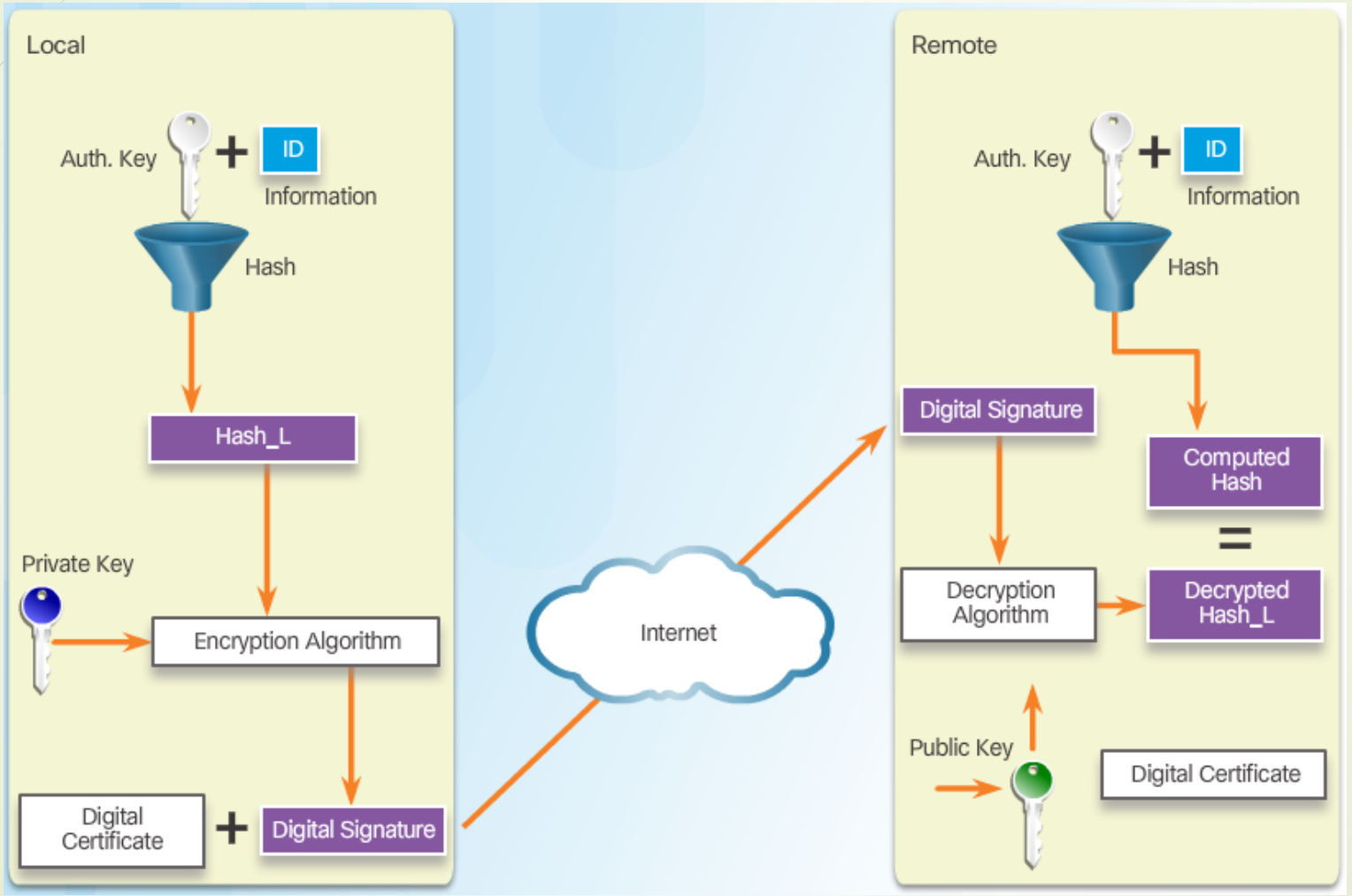


PSK



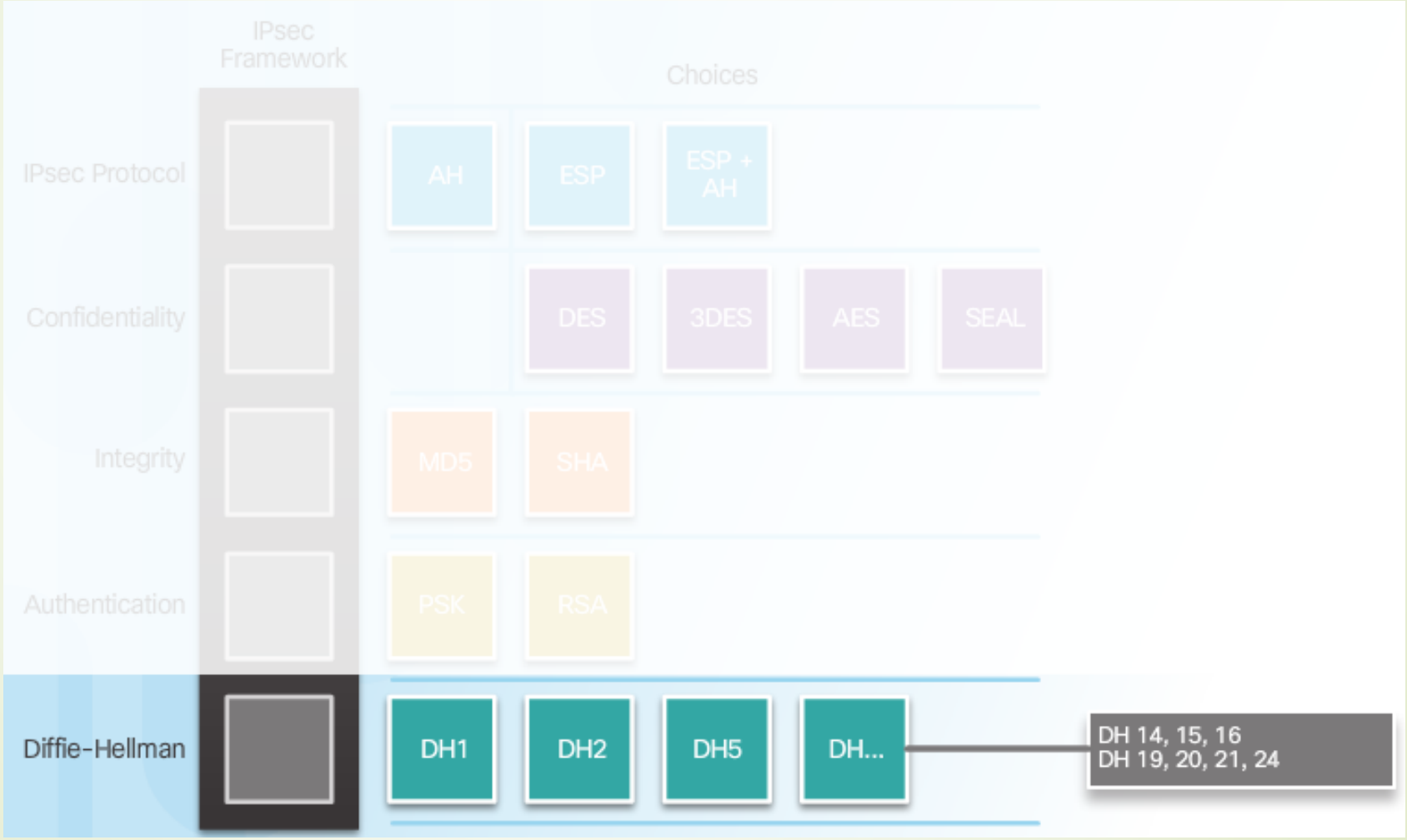
Authentification (Cont.)

RSA



Key Exchange sécurisé

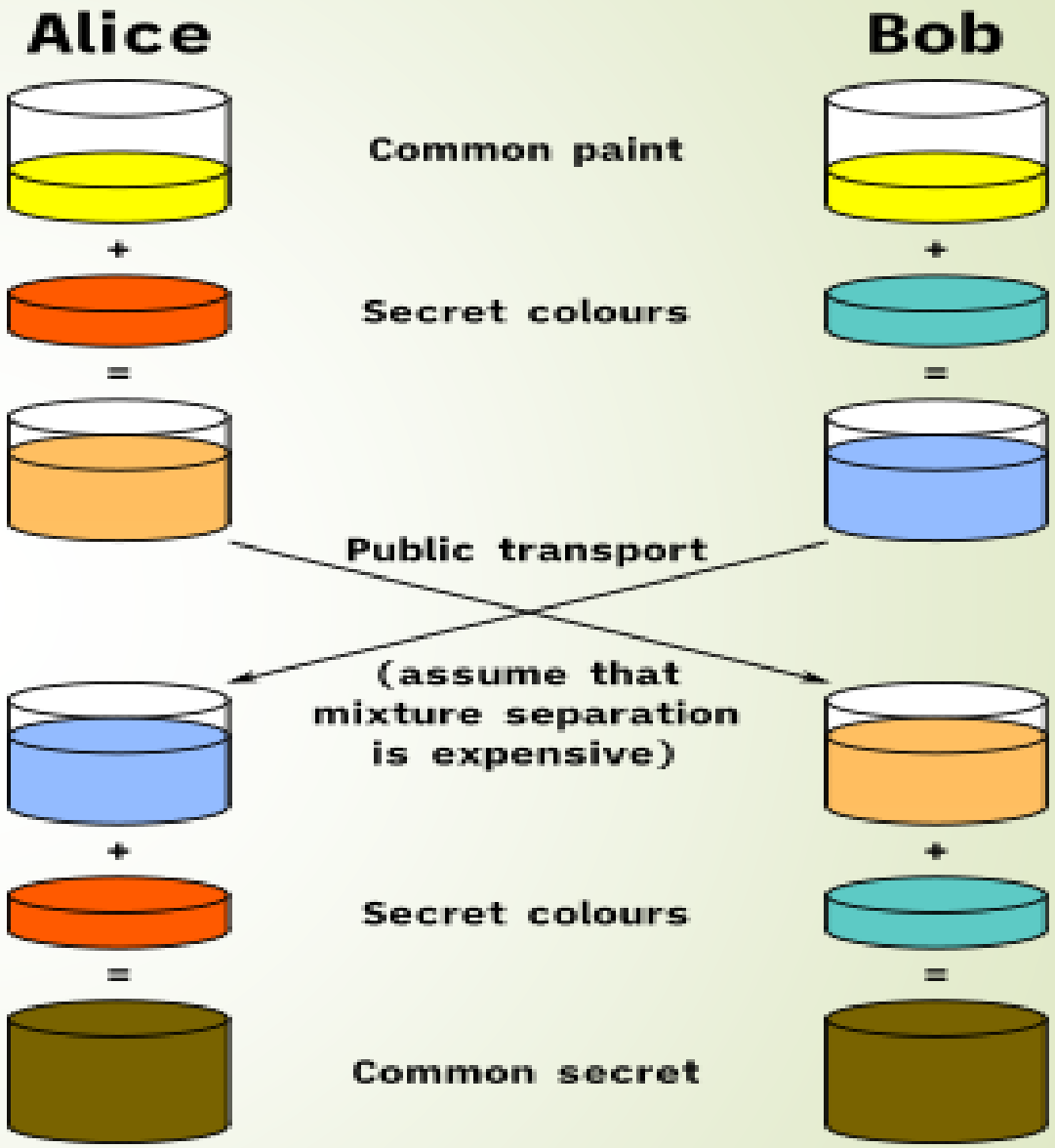
Diffie-Hellman Key Exchange



Diffie-Hellman Key Exchange

- Les groupes Diffie-Hellman déterminent la force de la clé utilisée dans le processus d'échange de clés. Les groupes portant un numéro supérieur sont plus sûrs, mais il faut plus de temps pour créer la clé.
- Fireware prend en charge ces groupes Diffie-Hellman :
- Groupe Diffie-Hellman 1 : groupe 768 bits
- Groupe Diffie-Hellman 2 : groupe 1 024 bits
- Groupe Diffie-Hellman 5 : groupe 1 536 bits
- Groupe Diffie-Hellman 14 : groupe 2 048 bits
- Groupe Diffie-Hellman 15 : groupe 3 072 bits
- Groupe Diffie-Hellman 19 : groupe de courbe elliptique 256 bits
- Groupe Diffie-Hellman 20 : groupe de courbe elliptique 384 bits

Diffie-Hellman Key Exchange



Diffie-Hellman Key Exchange

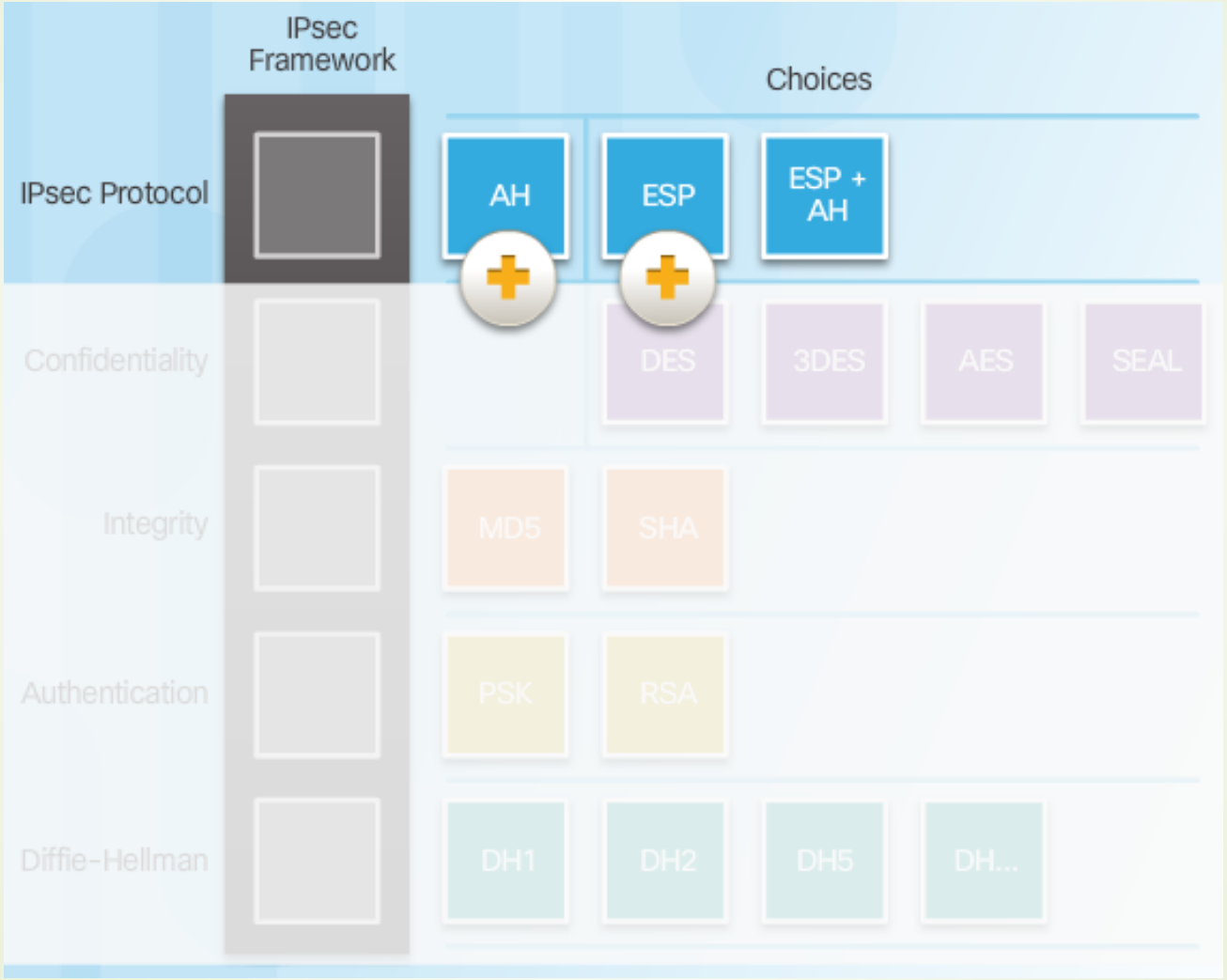
	Alice	Bob
Étape 1 :	Alice et Bob choisissent ensemble un grand nombre premier p et un entier $1 \leq a \leq p-1$. Cet échange n'a pas besoin d'être sécurisé.	
Étape 2 :	Alice choisit secrètement x_1.	Bob choisit secrètement x_2.
Étape 3 :	Alice calcule $y_1 = a^{x_1} \pmod{p}$	Bob calcule $y_2 = a^{x_2} \pmod{p}$.
Étape 4 :	Alice et Bob s'échangent les valeurs de y_1 et y_2. Cet échange n'a pas besoin d'être sécurisé.	
Étape 5 :	Alice calcule $y_2^{x_1} = (a^{x_2})^{x_1} = a^{x_1 x_2} \pmod{p}$ et appelle ce nombre K, la clé secrète à partager avec Bob.	Bob calcule $y_1^{x_2} = (a^{x_1})^{x_2} = a^{x_1 x_2} \pmod{p}$ et appelle ce nombre K, la clé secrète à partager avec Alice.

Exemple

- Inutile de préciser que les valeurs en jeu dans cet exemple sont bien trop faibles pour une utilisation réelle.
- Alice et Bob choisissent en commun $p = 53$ et $a = 9$.
- Alice choisit $x1 = 8$.
- Bob choisit quant à lui $x2 = 12$.

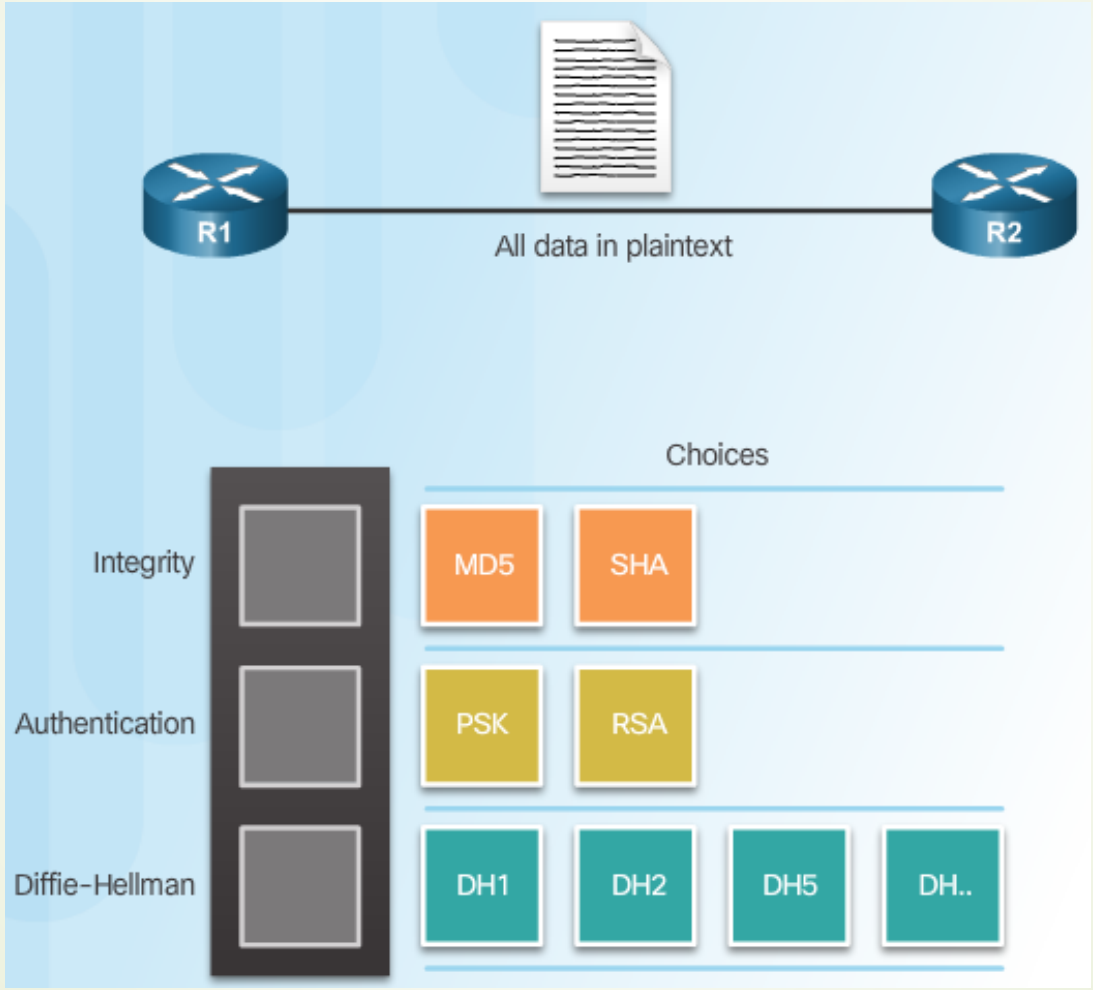
Protocole IPsec Vue d'ensemble

IP sec Protocol d'encapsulation

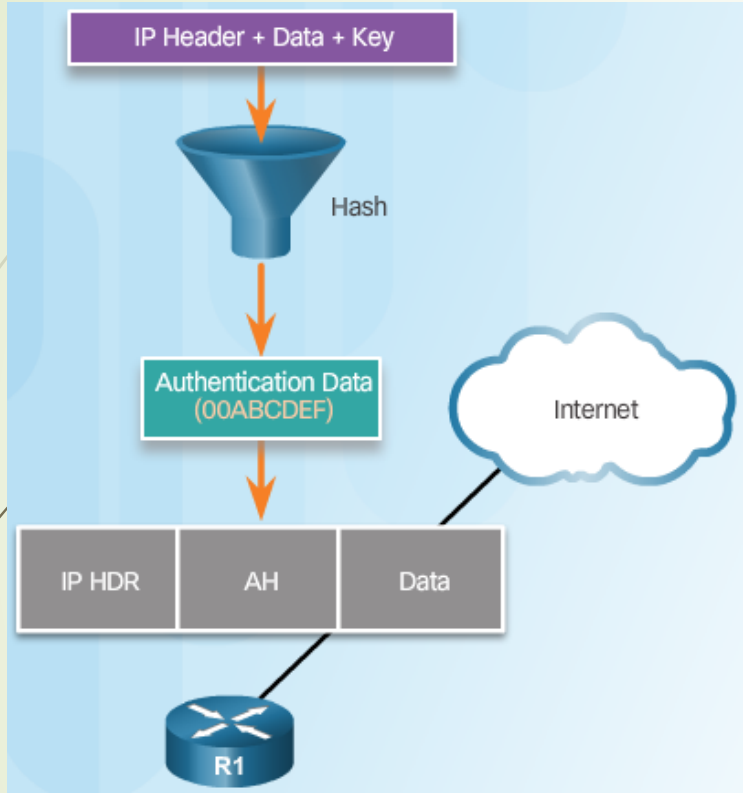


En-tête d'authentification

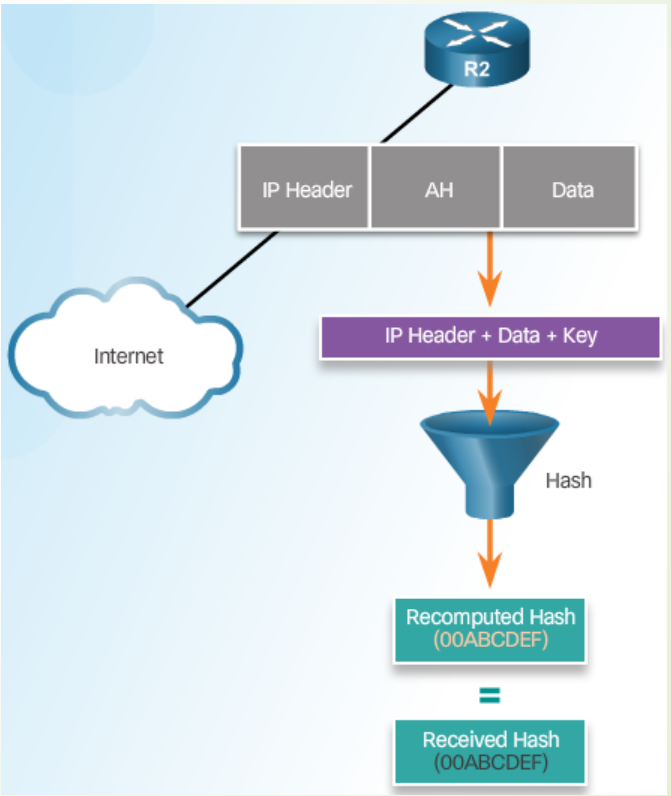
Protocoles AH



En-tête d'authentification (Cont.)

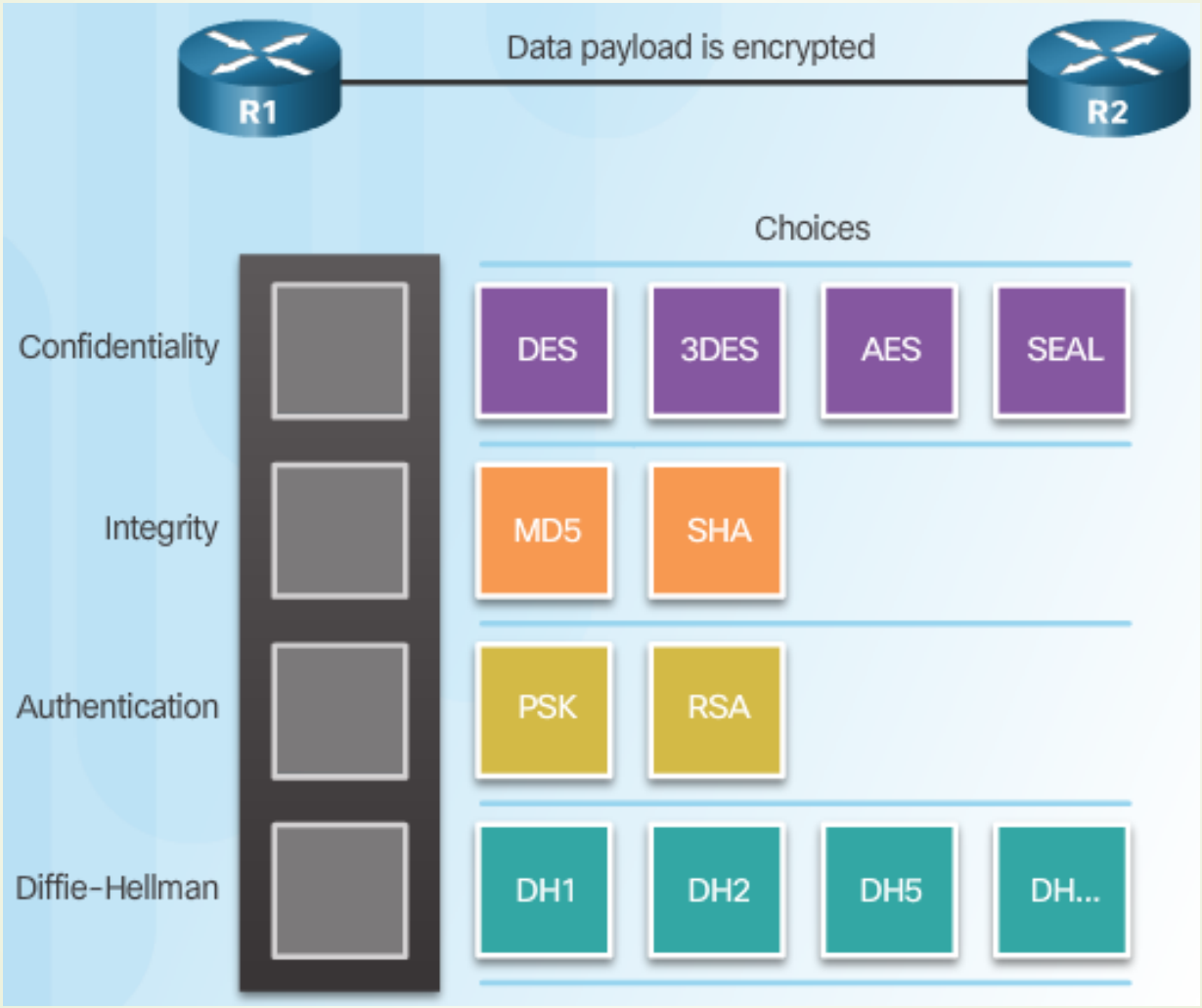


Routeur R1 crée Hash et Transmet to R2

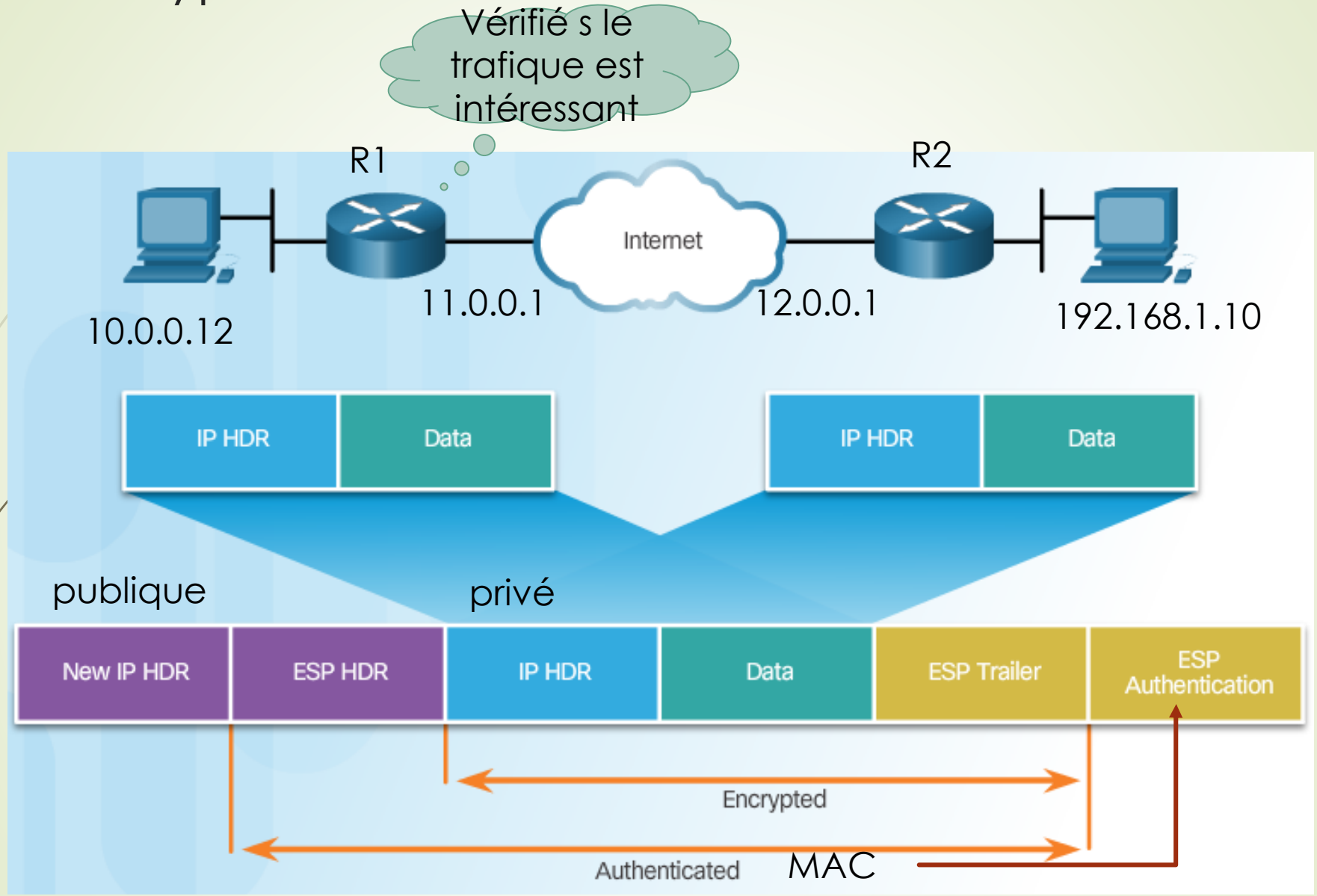


Routeur R2 Compares Hash recalculée au Hash reçu

ESP

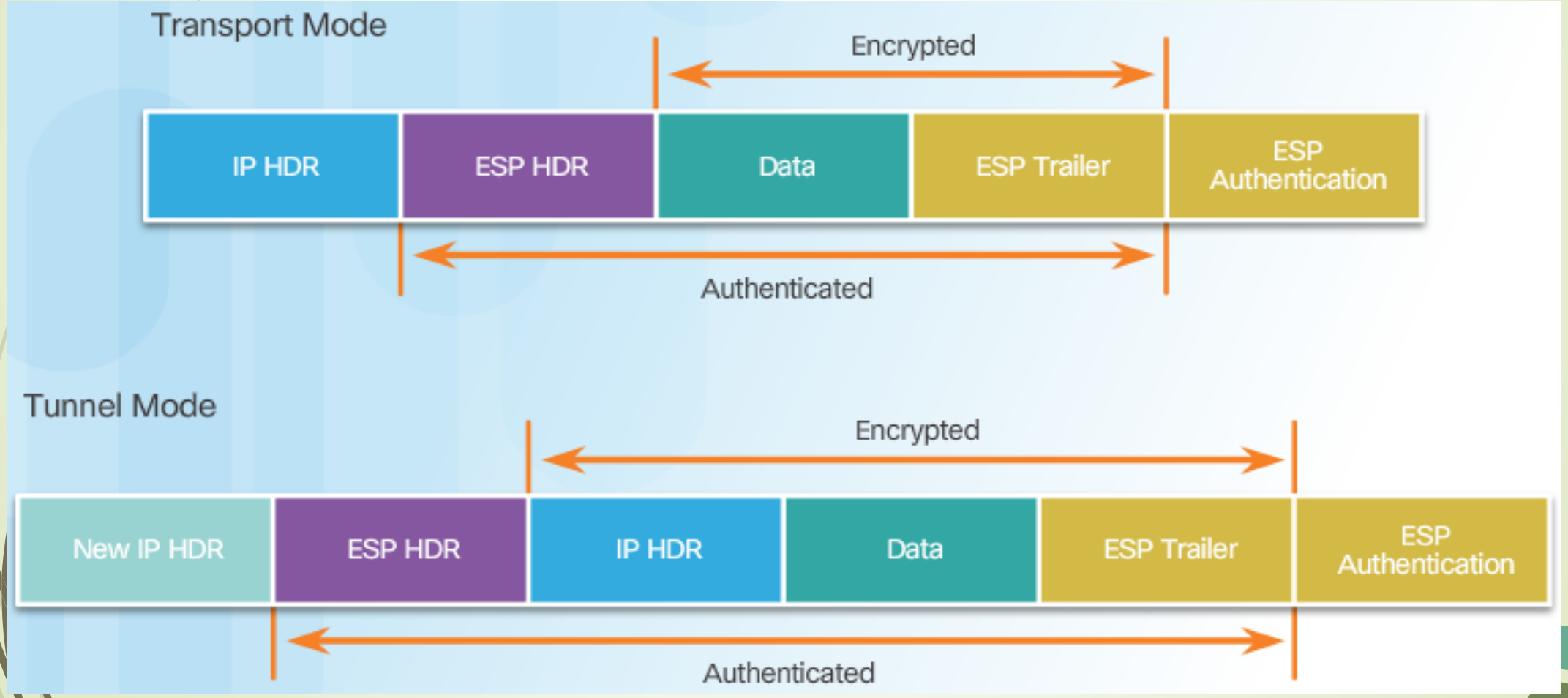

R1
Data payload is encrypted
R2
Choices
Confidentiality
DES
3DES
AES
SEAL
Integrity
MD5
SHA
Authentication
PSK
RSA
Diffie-Hellman
DH1
DH2
DH5
DH...

ESP Crypte et authentifie



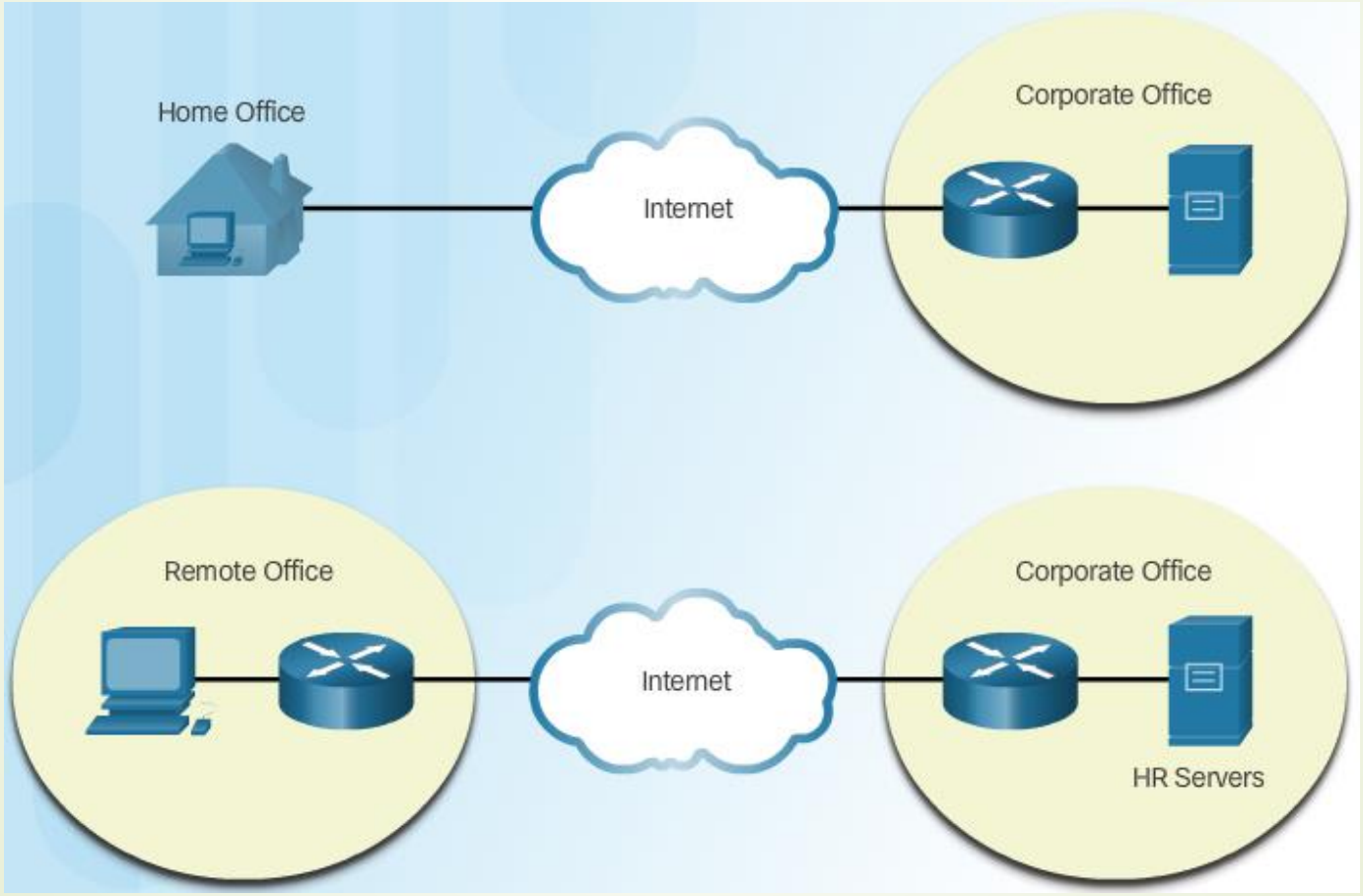
Modes de transport et tunnel

Appliquer ESP et AH en deux modes



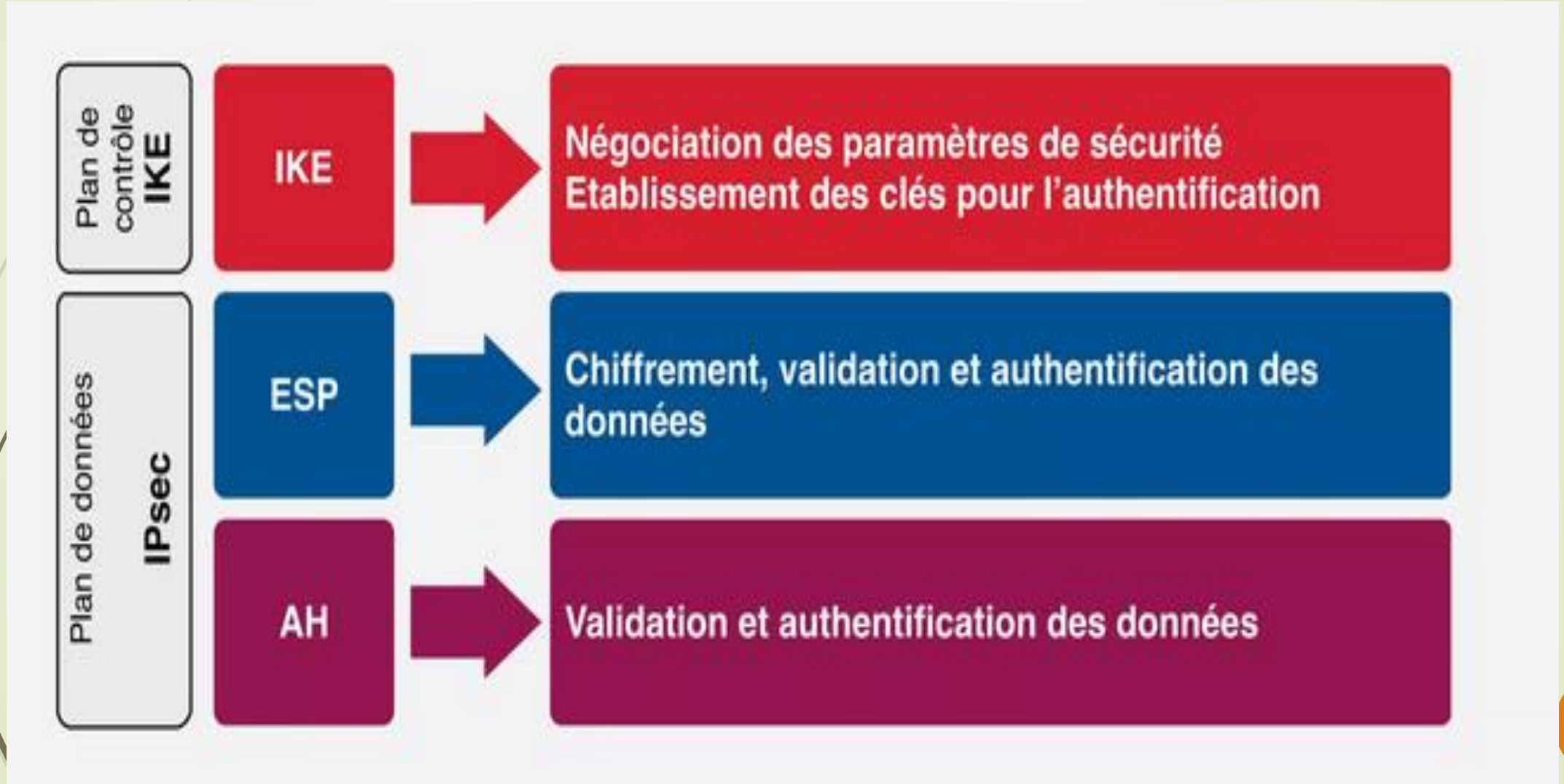
Modes Transport et Tunnel (Cont.)

ESP Tunnel Mode



Le protocole IKE

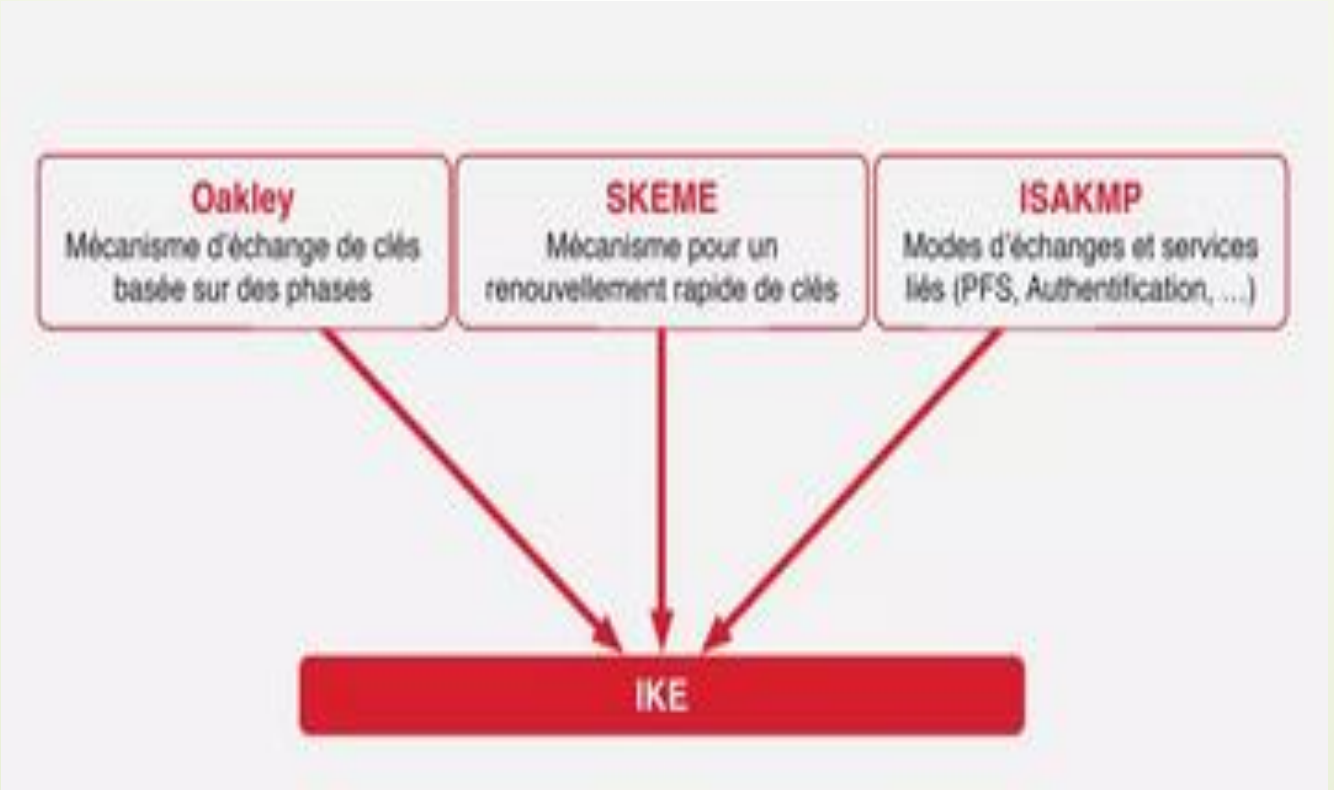
Le protocole *IKE* (*Internet Key Exchange*) est chargé de négocier la connexion. Avant qu'une transmission IPSec puisse être possible, IKE est utilisé pour authentifier les deux extrémités d'un tunnel sécurisé en échangeant des clés partagées.



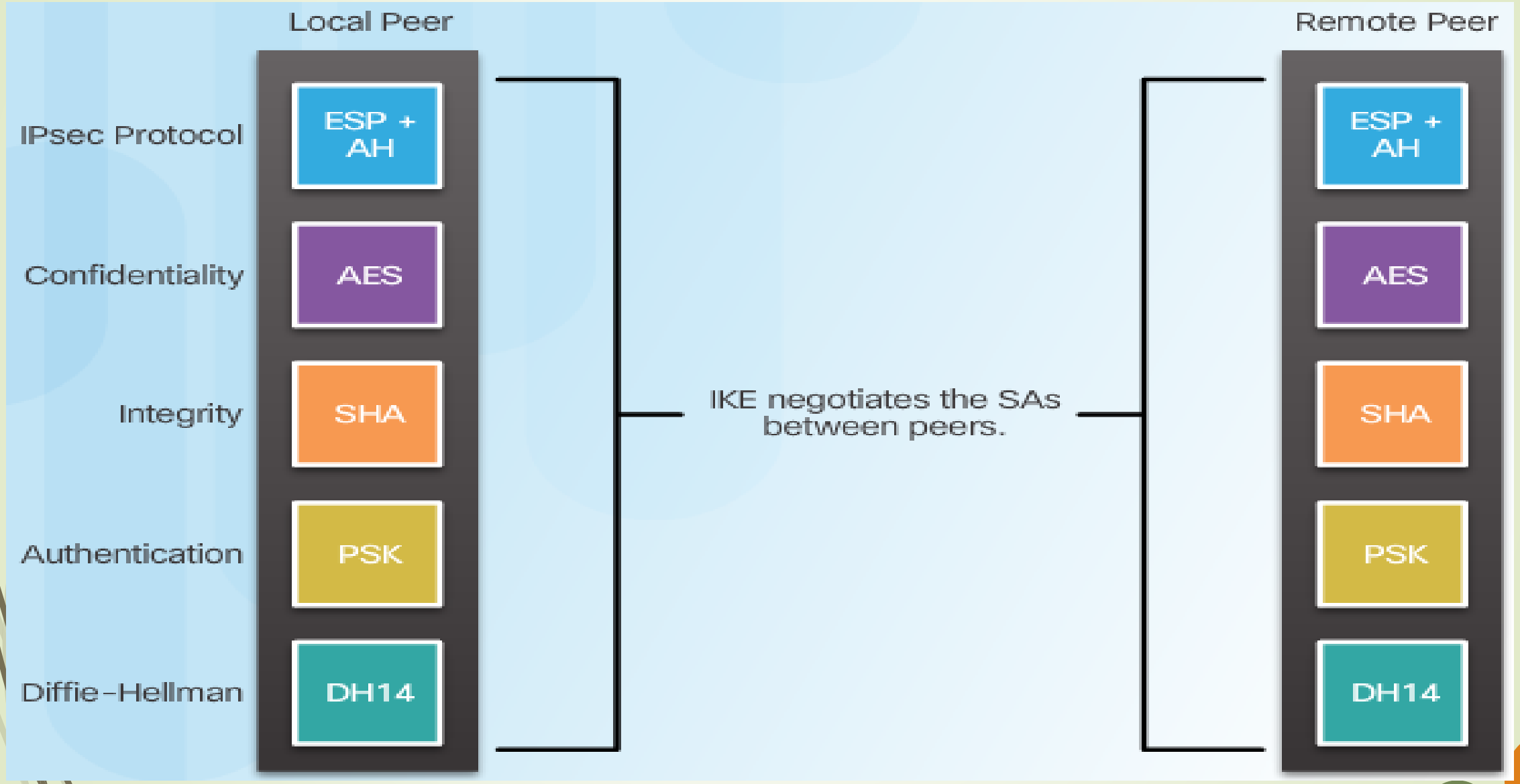
Le protocole IKE

ISAKMP , SKEME, Oakley
IKE est encapsulé dans un datagramme UDP port 500
Donc si j ai un FW je doit ouvrir ce port

Dans cisco, IKE utilise ISAKMP

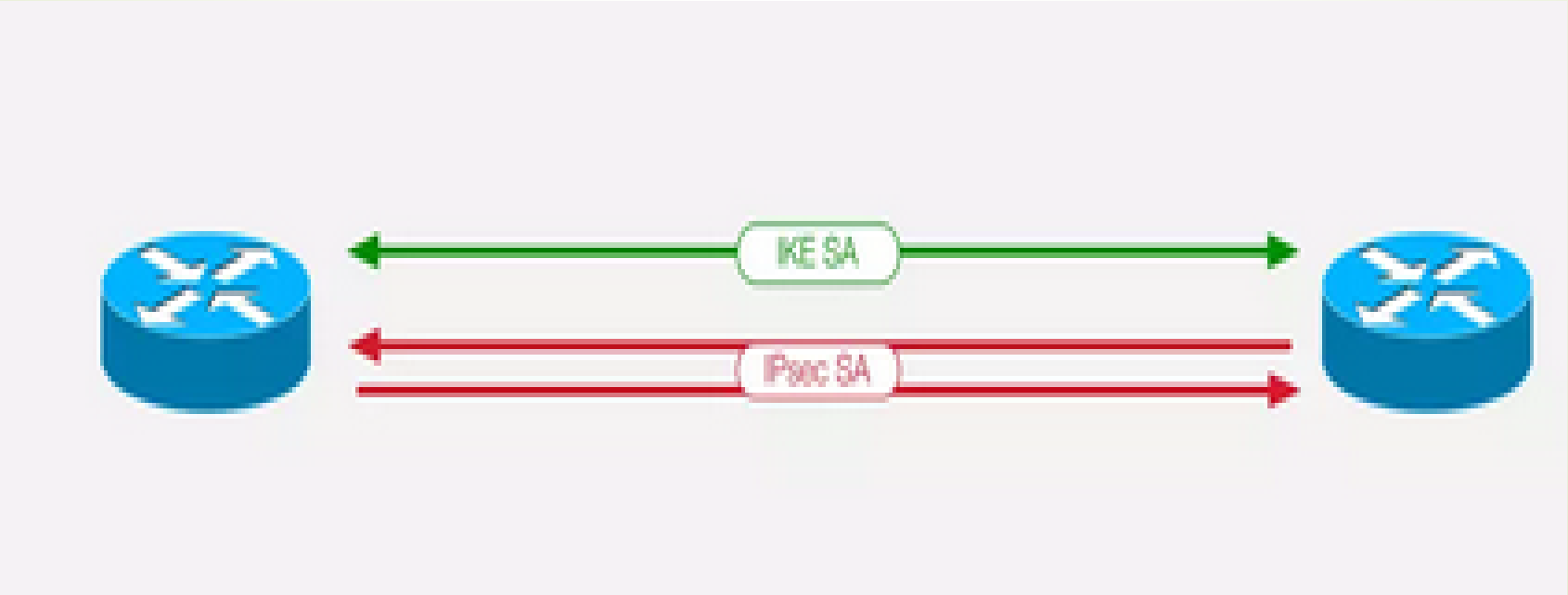


Le protocole IKE



IKE/Ipsec et Security association

- Protocol en deux phases
- phases 1 : établissement entre deux paires d'un tunnel bidirectionnelle « canal de gestion » qui envoi les messages de contrôle
- phases 2 : établissement entre deux paires de deux tunnel unidirectionnelle « canal de donné »



Comparaison entre IP sec et SSL

	SSL	IPsec
Applications	Applications Web, partage de fichiers, e-mail	Toutes les applications basées sur le protocole IP
Chiffrement	**Modéré à fort** Longueurs de clé comprises entre 40 et 256 bits	**Fort** Longueurs de clé comprises entre 56 et 256 bits
Authentification	**Modéré** Authentification unidirectionnelle ou bidirectionnelle	**Fort** Authentification bidirectionnelle utilisant des secrets partagés ou des certificats numériques
Complexité de connexion	**Faible** Nécessite uniquement un navigateur Web.	**Moyen** Peut être difficile à mettre en œuvre pour des utilisateurs non techniciens.
Options de connexion	Possibilité de connexion de n'importe quel périphérique	Seuls des périphériques spécifiques présentant des configurations particulières peuvent se connecter.