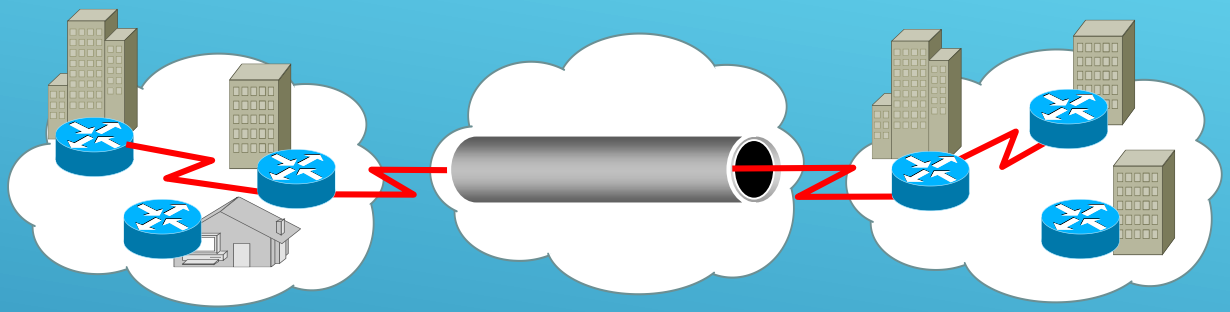
VPN | VIRTUAL PRIVATE NETWORK

PRÉSENTATION DES VPN

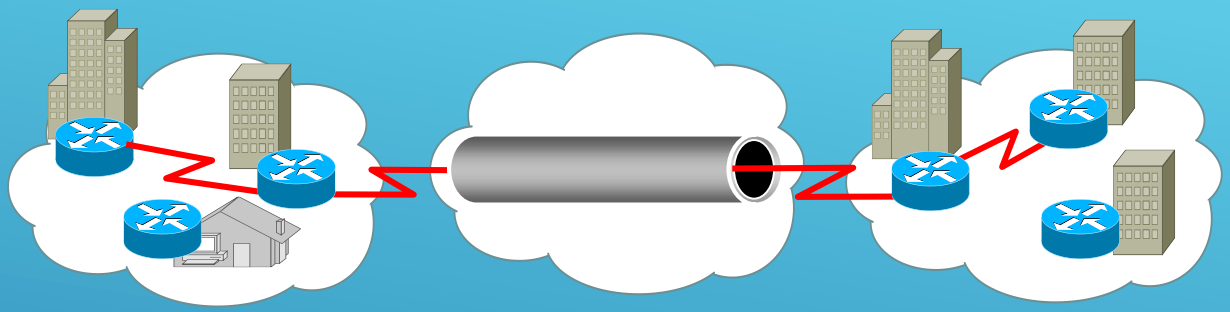


Un VPN transporte du trafic privé sur un réseau public en utilisant du cryptage et des tunnels pour obtenir:

- La confidentialité des données
- L'intégrité des données
- L'authentification des utilisateurs

- **Un réseau privé virtuel (VPN) est défini comme une connectivité réseau déployée sur une infrastructure partagée avec les mêmes politiques de sécurité que sur un réseau privé.**
- **Un VPN peut être entre deux systèmes d'extrémité ou entre deux ou plusieurs réseaux.**
- **Un VPN est construit en utilisant des tunnels et du cryptage. Un VPN peut être construit au niveau de n'importe quelle couche du modèle OSI.**
- **Un VPN est une infrastructure WAN alternative aux réseaux privés qui utilisent des lignes louées ou des réseaux d'entreprise utilisant Fame Relay ou ATM.**

PRÉSENTATION DES VPN



Un VPN transporte du trafic privé sur un réseau public en utilisant du cryptage et des tunnels pour obtenir:

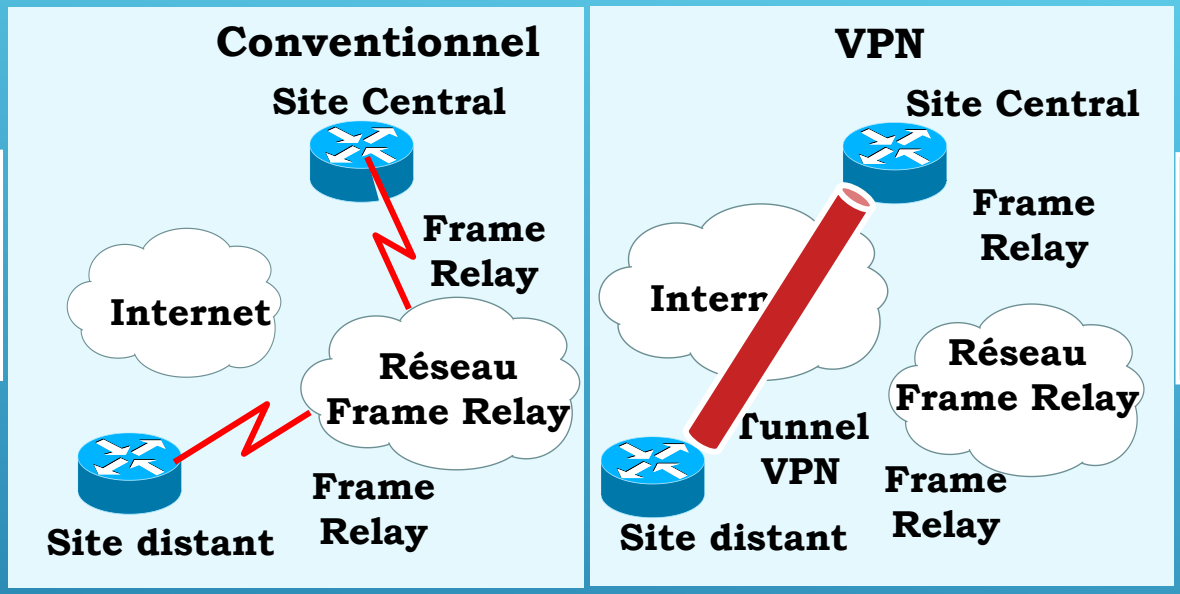
- La confidentialité des données
- L'intégrité des données
- L'authentification des utilisateurs

Les VPNs fournissent trois fonctions essentielles:

- **Confidentialité (cryptage)**
  - **L'émetteur peut crypter les paquets avant de les transmettre dans le réseau.**
  - **Par ce moyen, si la communication est interceptée les données ne pourront pas être lues.**
- **Intégrité des données**
  - **Le récepteur peut vérifier si les données n'ont pas été altérées lors de leur passage dans le réseau.**
- **Authentification**
  - **Le récepteur peut authentifier la source du paquet, garantissant et certifiant la source de l'information.**

AVANTAGES DES VPN

- Coût élevé
- Peu flexible
- Gestion WAN
- Topologies complexes

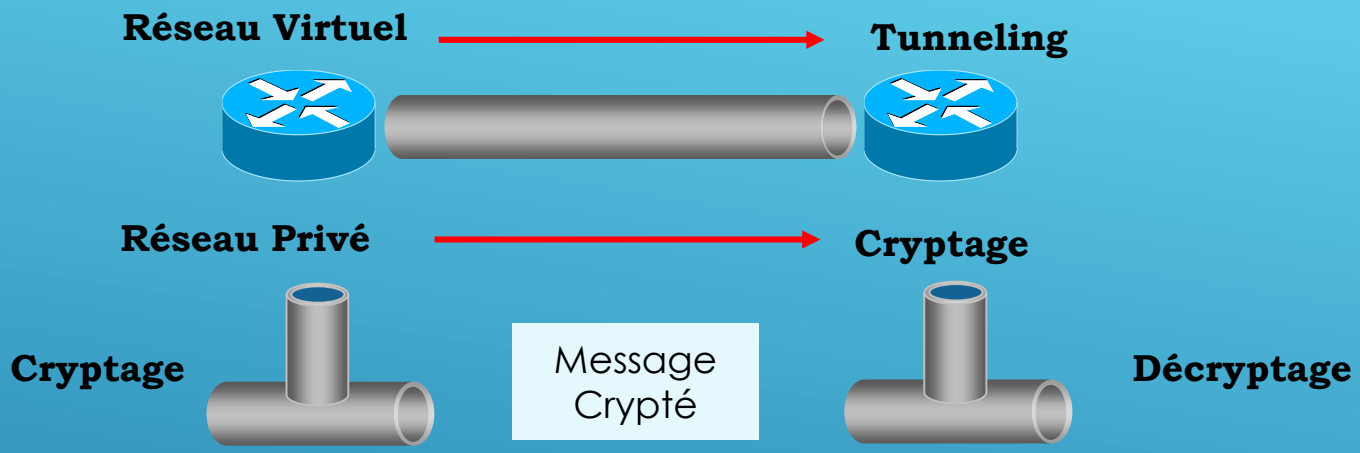


- Faible coût
- Plus flexible
- Gestion simplifiée
- Topologie tunnel

Les principaux avantages sont:

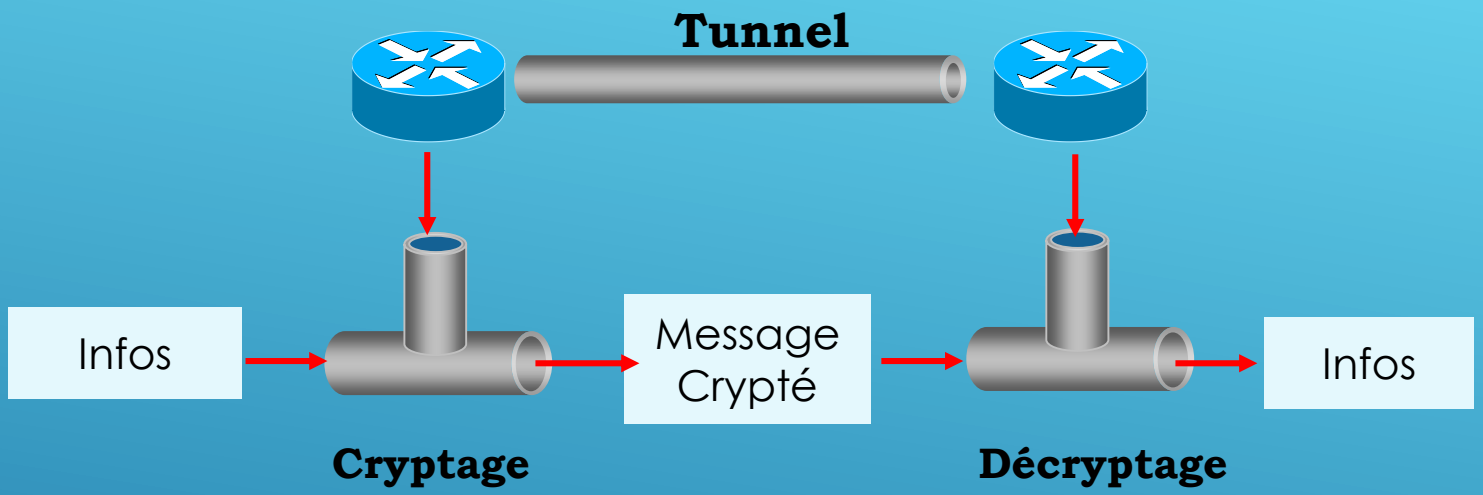
- Les VPNs amènent des coûts plus faibles que les réseaux privés.
  - Les coûts de la connectivité LAN-LAN sont réduits par rapport à une ligne louée. .
- Les VPNs offrent plus de flexibilité et d'évolutivité que des architectures WAN classiques
- Les VPNs simplifient les tâches de gestion grâce à l'exploitation de sa propre infrastructure de réseau.
- Les VPNs fournissent des topologies de réseaux avec tunnels qui réduisent les taches de gestion.

TUNNELING ET CRYPTAGE



- Un réseau virtuel est crée en utilisant la capacité de faire transporter un protocole par un autre (Tunnel) sur une connexion IP standard.
- GRE (Generic Routing Encapsulation) et L2TP (Layer 2 Tunneling Protocol) sont deux méthodes de "tunneling".
- La troisième méthode, IPSec.
- Un réseau privé assure la Confidentialité, l'Intégrité et l'Authentification.
- Le cryptage des données et le tunnel permettent aux données de traverser Internet avec la même sécurité que sur un réseau privé.

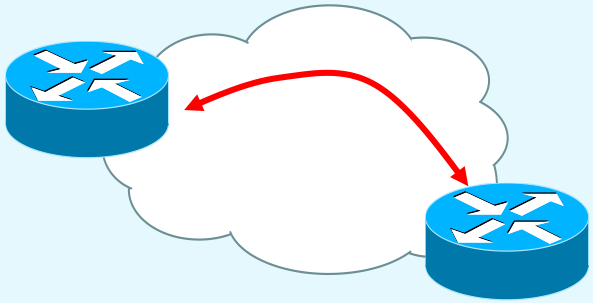
TUNNELING ET CRYPTAGE



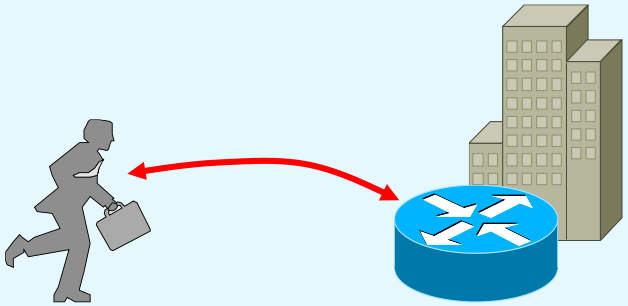
- Bien que Internet ait offert de nouvelles opportunités aux entreprises, il a aussi crée une grande dépendance des réseaux et un besoin de protection contre une grande variété de menaces sur la sécurité.
- La fonction principale d'un VPN est d'offrir cette protection avec du cryptage au travers d'un tunnel.
- Les tunnels fournissent des connexions logiques (Virtuelle) point à point au travers d'un réseau IP (ou autre) en mode non-connecté.
- Les Tunnels des solutions VPN emploient le cryptage pour protéger les données pour qu'elles ne soient pas lisibles par des entités non-autorisées et l'encapsulation multi-protocole si cela est nécessaire.
- Le cryptage assure que le message ne pourra pas être lu et compris uniquement par le receveur (confidentialité)
- Le cryptage transforme une information en un texte chiffré sans signification sous sa forme cryptée.
- Le décryptage restore le texte chiffré en information originale destinée au receveur.

SCÉNARIOS VPN

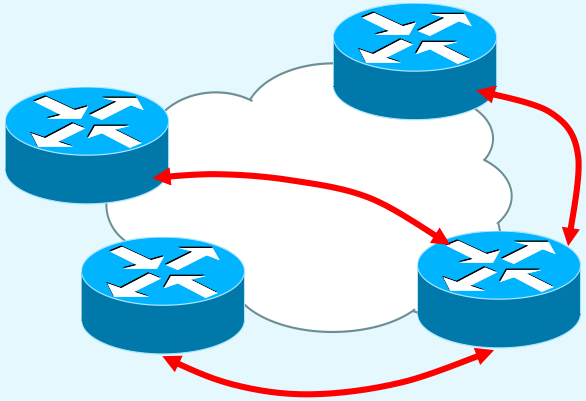
Routeur à Routeur



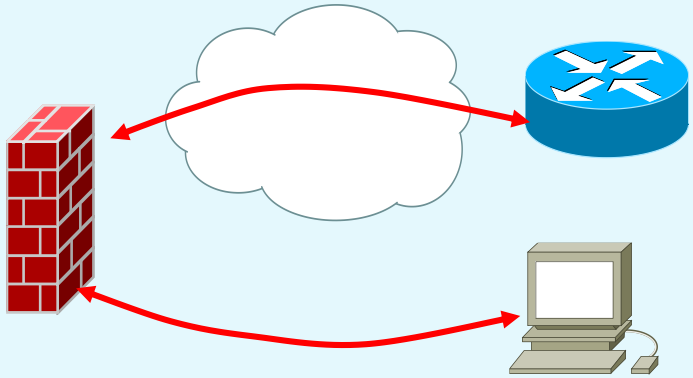
PC à Routeur/Concentrateur



Routeur à plusieurs routeurs

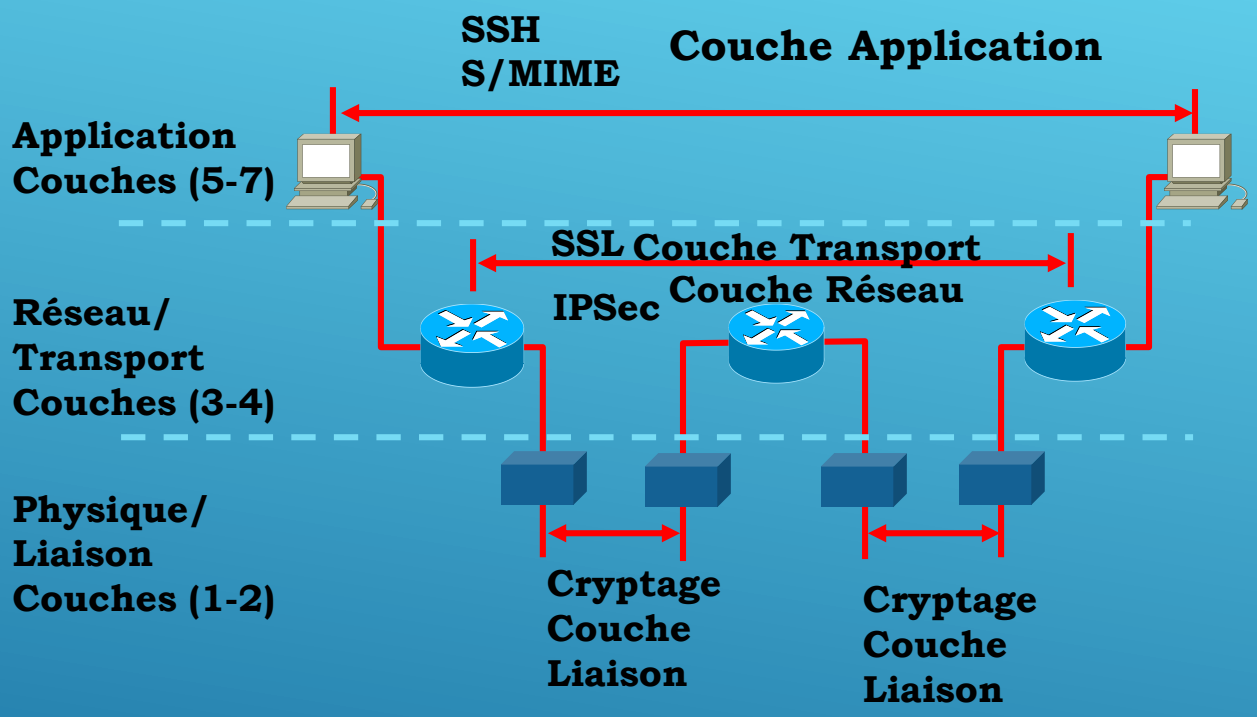


PC à Pare-Feu



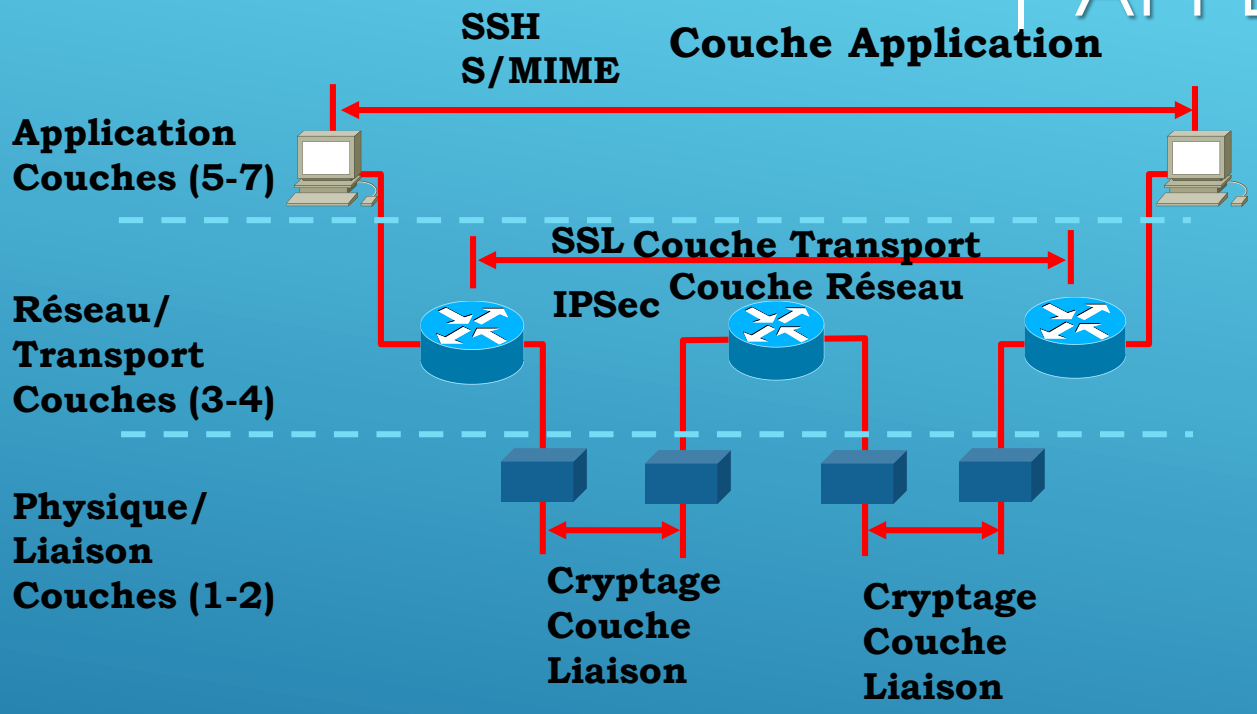
CHOIX DE TECHNOLOGIES VPN

CRYPTAGE DANS PLUSIEURS COUCHES



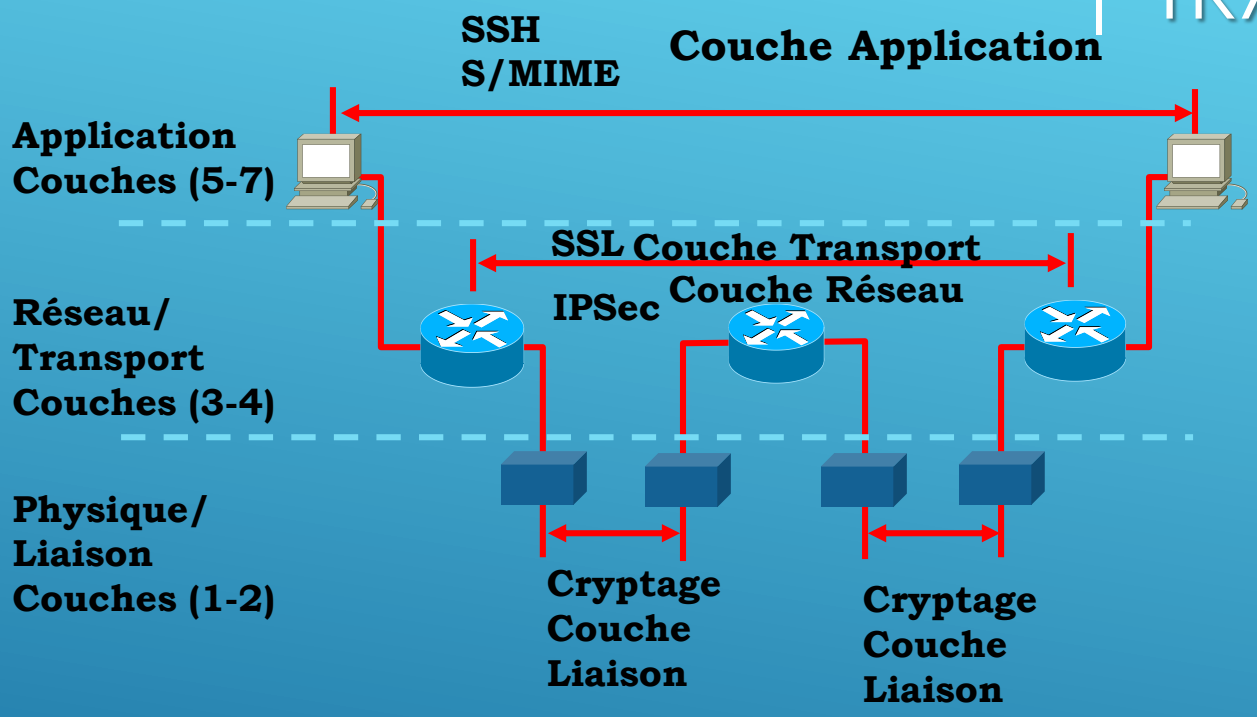
- Différentes méthodes pour la protection de VPN sont implémentées sur différentes couches.
- Fournir de la protection et des services de cryptographie au niveau de la couche application était très utilisé dans le passé et l'est toujours pour des cas très précis.

CRYPTAGE DANS PLUSIEURS COUCHES | APPLICATION



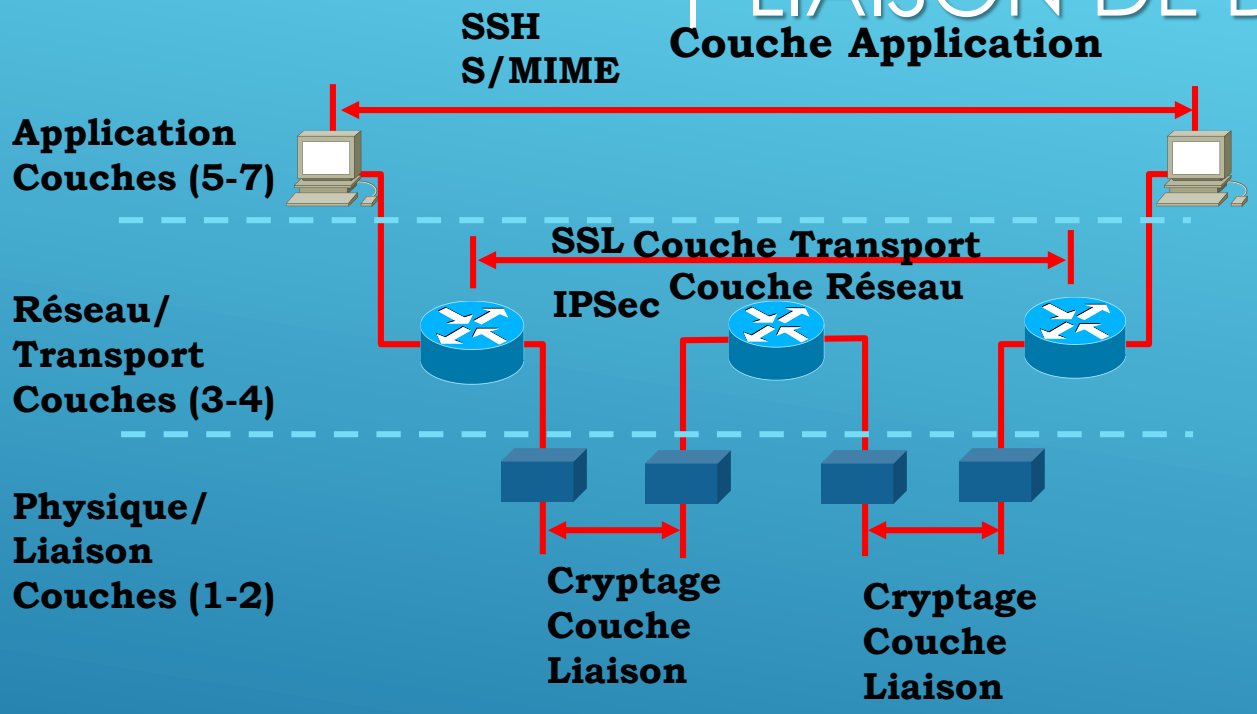
- L'IETF a un protocole basé sur des standards appelé S/MIME (Secure/Multipurpose Internet Mail Extensions) pour des applications VPNs générées par différents composants d'un système de communication.
- Agents de transfert de message, passerelles,...
- Cependant, la sécurité au niveau de la couche application est spécifique à l'application et les méthodes de protection doivent être implémentées à chaque nouvelle application.

CRYPTAGE DANS PLUSIEURS COUCHES | TRANSPORT



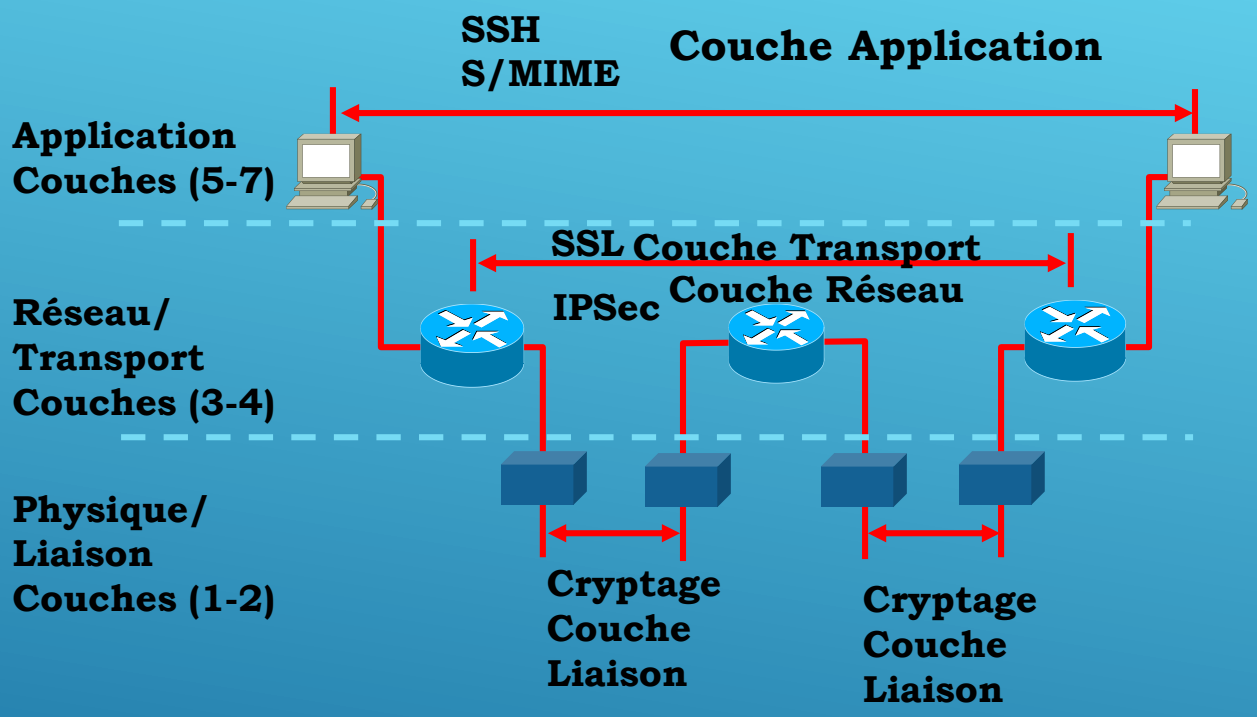
- Des standards au niveau de la couche transport ont eu beaucoup de succès
- Le protocole tel SSL/TLS (Secure Socket Layer/Transport Layer Security) fournit de la protection, de l'authentification de l'intégrité aux applications basées sur TCP.
- SSL/TLS est communément utilisé par les sites de e-commerce mais manque de flexibilité, n'est pas facile à implémenter et dépend de l'application.

CRYPTAGE DANS PLUSIEURS COUCHES | LIAISON DE DONNÉES



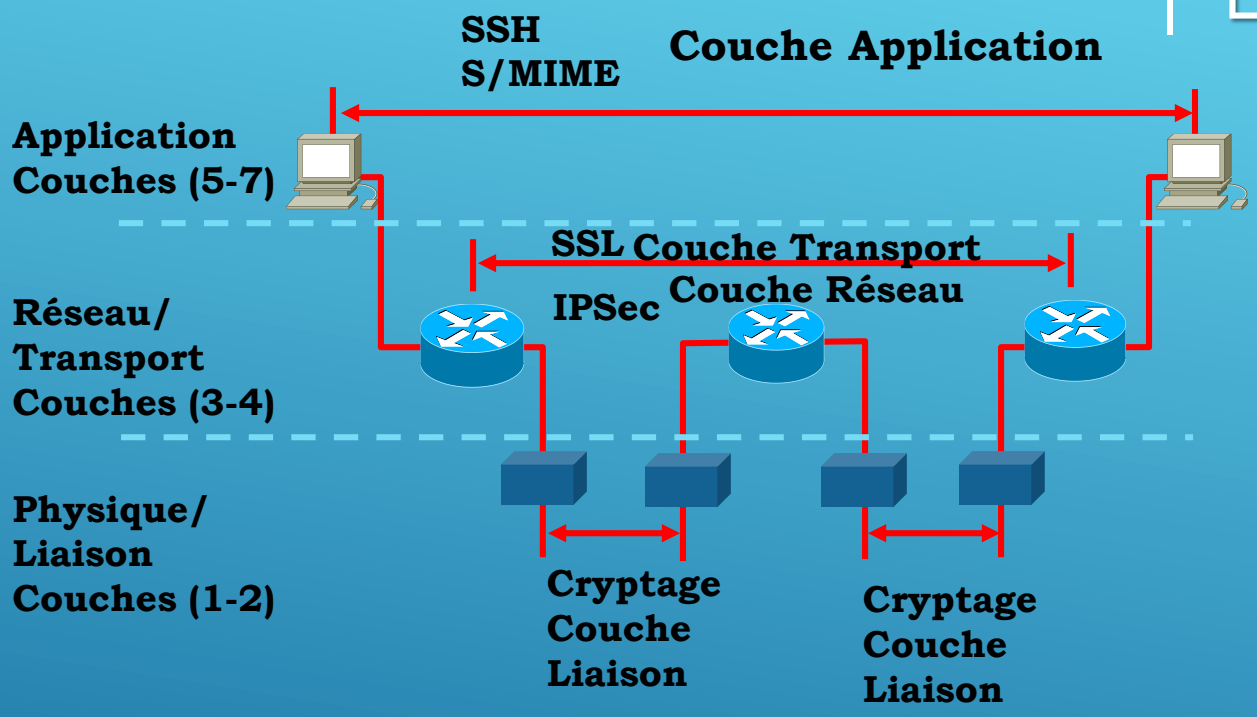
- La protection aux niveau des couches basses du modèle à été aussi utilisée dans les systèmes de communication, spécialement par la couche liaison.
- Cette protection au niveau de la couche liaison fournissait une protection indépendante du protocole sur les liaisons non-sécurisées.
- La protection au niveau de la couche liaison coûte cher car elle doit être réalisée pour chaque liaison.
- Elle n'exclut pas l'intrusion au moyen de stations intermédiaires ou de routeurs et de plus est très souvent propriétaire.

CRYPTAGE DANS PLUSIEURS COUCHES | RÉSEAU



- IPSec est un bon choix pour sécuriser les VPNs d'entreprise
- IPSec est un cadre de standards ouverts qui fournissent la confidentialité, l'intégrité et l'authentification des données entre deux extrémités.
- IPSec fournit ces services de sécurité en utilisant IKE (Internet Key Exchange) pour gérer la négociation de protocoles et d'algorithmes basée sur une politique locale et de générer les clés d'authentification et de cryptage devant être utilisées par IPSec.

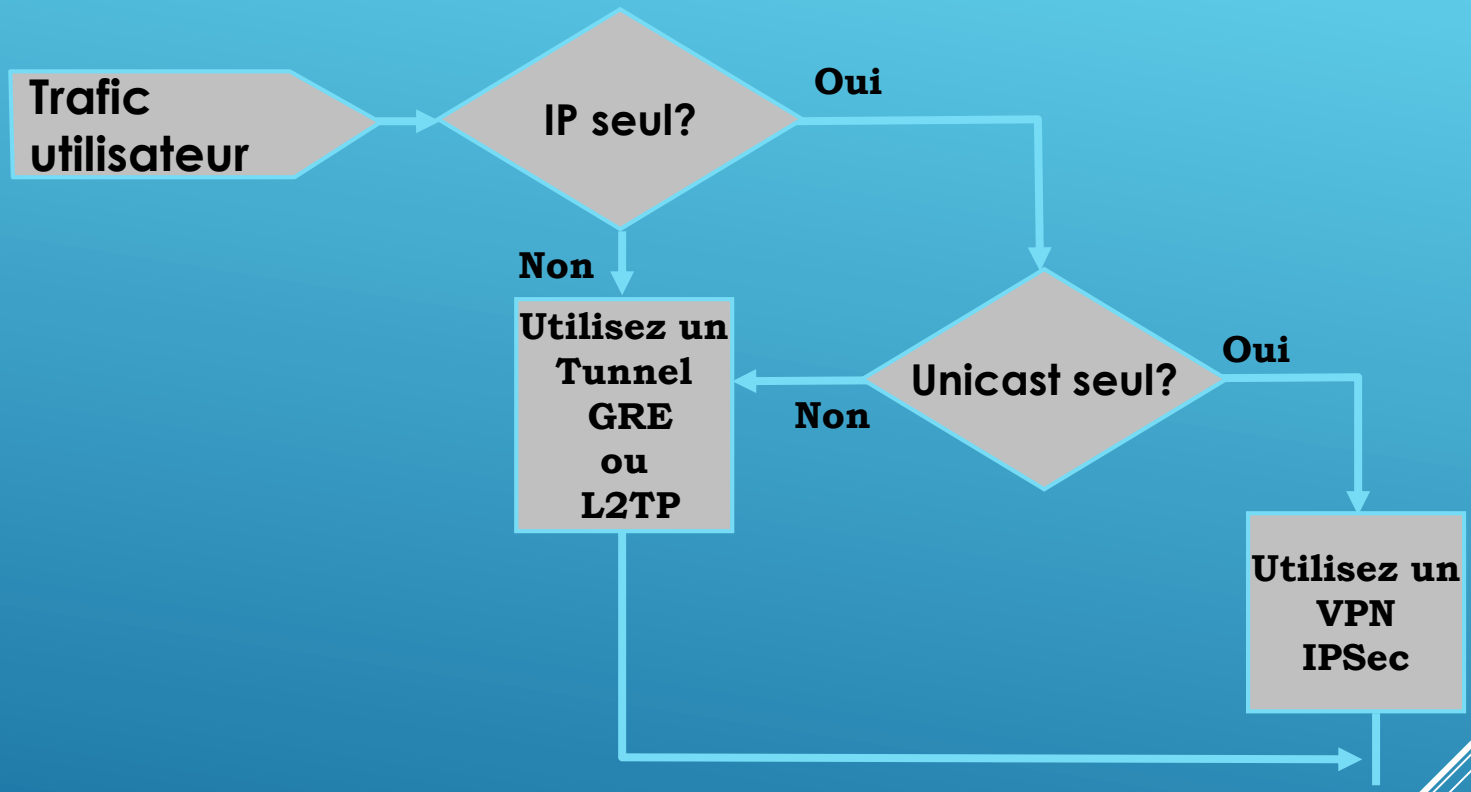
CRYPTAGE DANS PLUSIEURS COUCHES | EXEMPLES



- Un ensemble de technologies de couche réseau sont disponibles pour permettre le tunneling de protocoles au travers de réseaux pour réaliser des VPNs.
- Les trois protocoles de tunneling les plus utilisés sont:

Protocoles VPN	Description	Standard
L2TP	Layer 2 tunneling Protocol	RFC 2661
GRE	Generic Routing Encapsulation	RFC 1701 et 2784
IPSec	Internet Protocol Security	RFC 2401

CHOIX DE LA MEILLEURE TECHNOLOGIE



- Sélectionnez la meilleure technologie VPN pour fournir une connectivité réseau selon les besoins du trafic.
- Le diagramme ci-dessus montre le processus de choix d'un tunneling de couche réseau basé sur les différents scénarios de VPN.

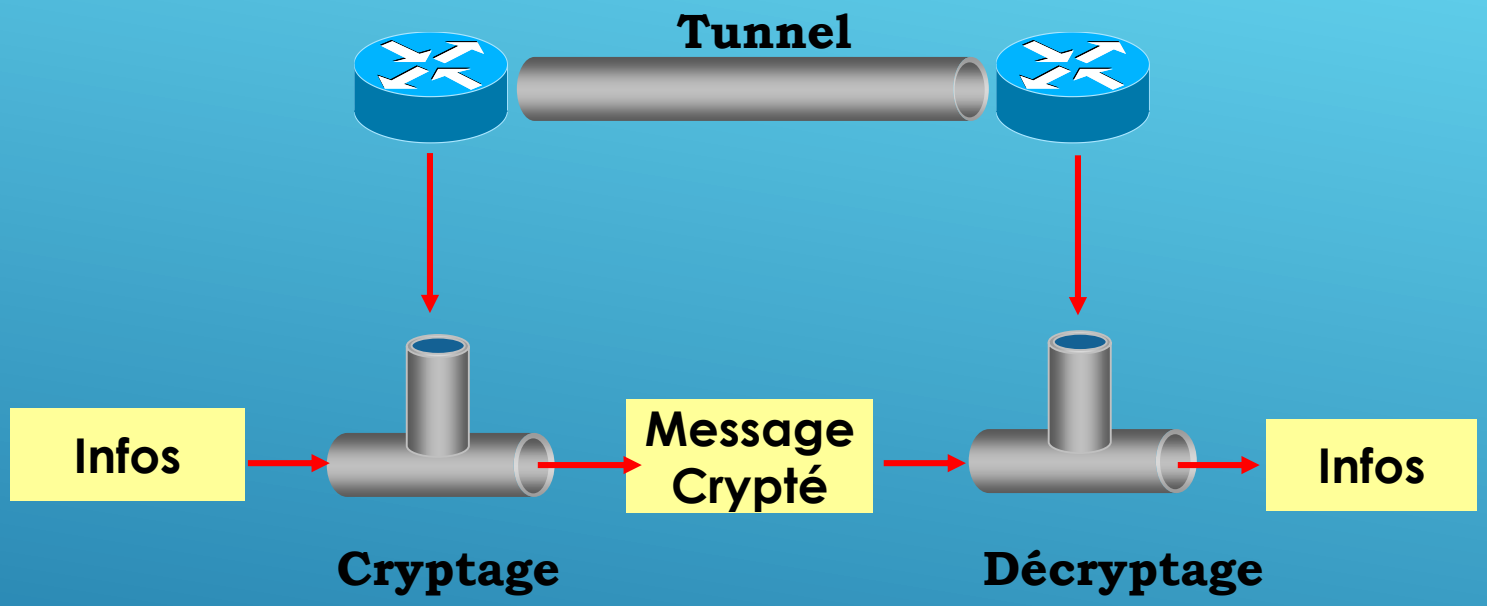
CHOIX DE LA MEILLEURE TECHNOLOGIE

- IPSec est le meilleur choix pour sécuriser des VPNs d'entreprise.
  - Malheureusement IPSec supporte uniquement le trafic IP unicast.
  - Si les paquets IP unicast doivent être encapsulés dans un tunnel, l'encapsulation IPSec est suffisante et moins compliquée à configurer et à vérifier.
- Pour du tunneling multiprotocole ou IP multicast, utilisez GRE ou L2TP.
  - Pour des réseaux qui utilisent Microsoft, L2TP peut être le meilleur choix.
  - A cause de son lien avec PPP, L2TP peut être souhaitable pour des VPNs accès distant avec support multiprotocole.
- GRE est le meilleur choix pour des VPNs site à site avec support multiprotocole.
  - GRE est également utilisé pour des tunnels de paquets multicast tels les protocoles de routage.
  - GRE encapsule tout trafic, quelque soit la source ou la destination.
- Ni L2TP, ni GRE supportent le cryptage des données ou l'intégrité des paquets.
- Utilisez IPSec en combinaison avec L2TP et/ou GRE pour obtenir le cryptage et l'intégrité IPSec.

VPN - TERMES CLÉS

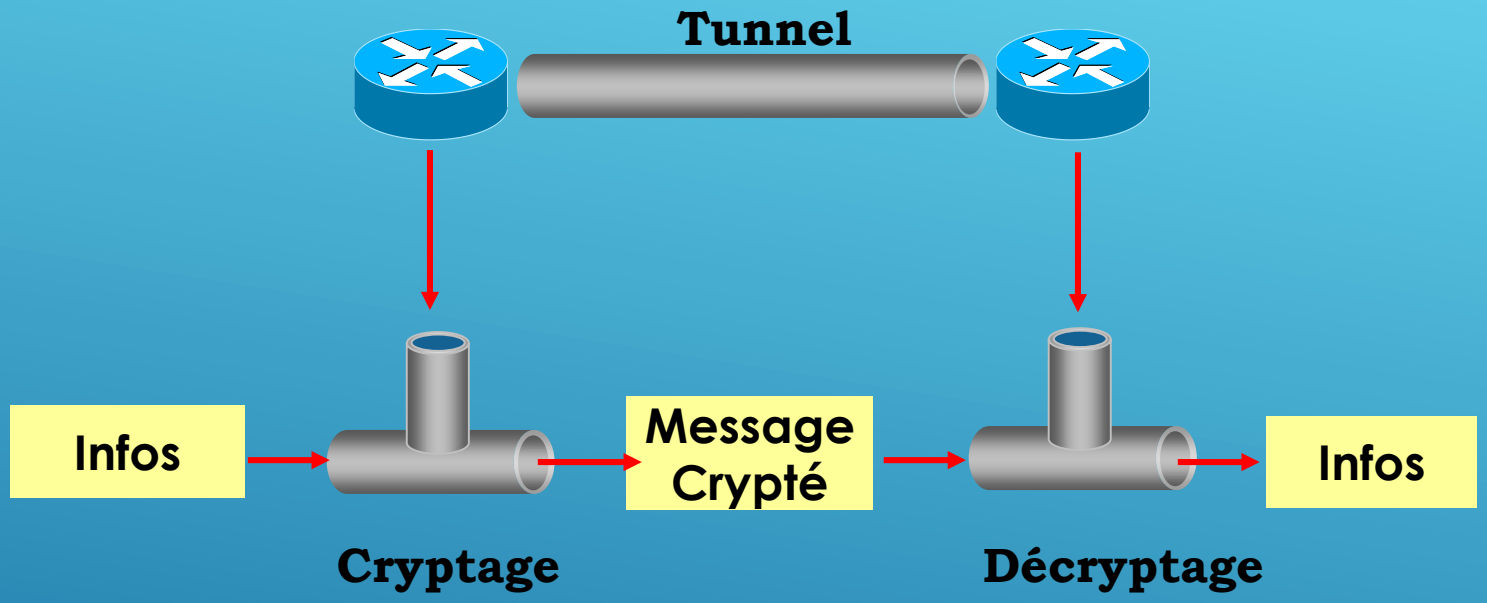
- **Tunnel**
- **Crypto-système**
- **Cryptage/Décryptage**
- **Hachage**
- **Gestion de clé**
- **Authentification**
- **Autorisation**
- **Certificat**

VPN - TERMES CLÉS | TUNNEL



- **Tunnel** : Connexion virtuelle point à point utilisée dans un réseau pour transporter le trafic d'un protocole encapsulé dans un autre protocole. Par exemple du texte crypté transporté dans un paquet IP.

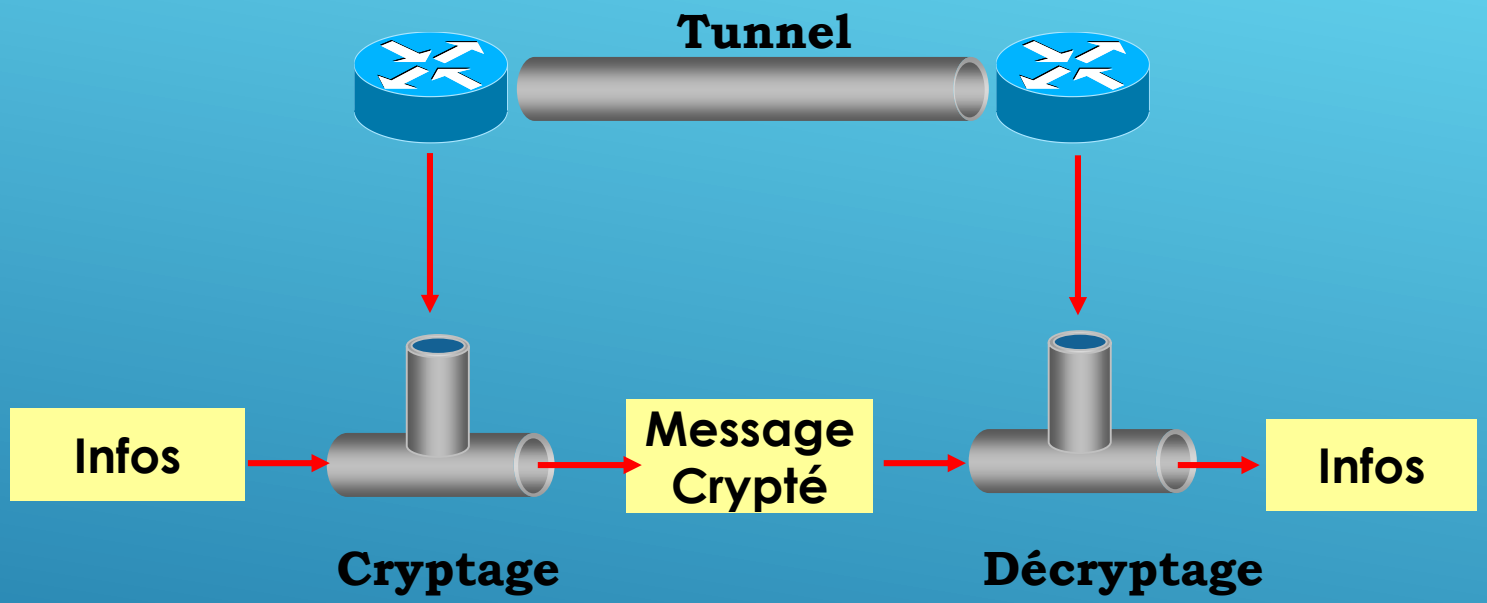
VPN - TERMES CLÉS | CRYPTAGE/DÉCRYPTAGE



Cryptage/Décryptage :

- Le cryptage est un processus qui transforme une information en un texte chiffré qui pourra pas être lu ou utilisé par des utilisateurs non-autorisés.
- Le décryptage restore le texte chiffré en information originale qui pourra être lue et utilisée par le receveur

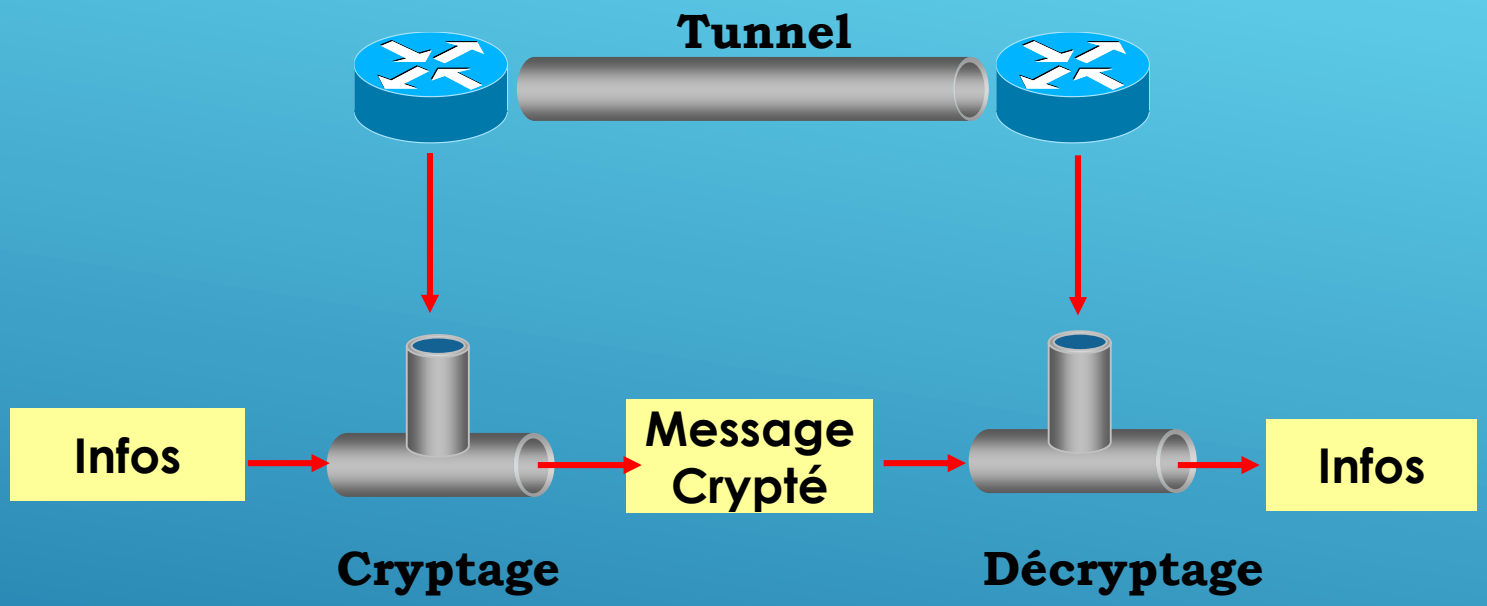
VPN - TERMES CLÉS | CRYPTOSYSTÈME



Cryptosystème :

- Système qui réalise le cryptage/décryptage, l'authentification de l'utilisateur, le hachage et le processus d'échange de clés.
- Un cryptosystème peut utiliser une des ces différentes méthodes selon la politique choisie en fonction des différents trafics de l'utilisateur.

VPN - TERMES CLÉS | HACHAGE



- **Hachage** : Technologie d'intégrité des données qui utilise un algorithme pour convertir un message de longueur variable et une clé secrète en une seule chaîne de caractères de longueur fixe. L'ensemble message/clé et hash traversent le réseau de la source vers la destination. A la destination, le hash recalculé est comparé avec le hash reçu. Si les deux valeurs sont identiques, le message n'a pas été corrompu.

VPN - TERMES CLÉS

- **Authentification : Processus d'identification d'un utilisateur ou d'un processus tentant d'accéder à une ressource.**
  - **L'authentification assure que l'individu ou le processus est bien celui qu'il prétend être**
  - **L'authentification n'attribut pas de droits d'accès**
- **Autorisation : Processus qui donne accès à des ressources à des individus ou à des processus authentifiés.**
- **Gestion de clés - Une clé est généralement une séquence binaire aléatoire utilisée pour exécuter les opérations dans un cryptosystème.**
  - **La gestion de clés est la supervision et le contrôle du processus par lequel les clés sont générées, stockées, protégées, transférées, chargées, utilisées et détruites.**

SYSTÈME DE CRYPTAGE