EXPOSE D'ADMINISTRATION ET SECURITES RESEAUX

IMPLEMENTATION D'UN VPN ET LES PROTOCOLES DE SECURITE DES SERVICES INTERNET : SSL, SSH, IPSEC

Rédigé et Présenté par : Rodrigue Martial **KENGNE**

Filière : Génie Logiciel, Niveau 3

Supervisé par :

M. Didier Frédéryck **MBANJOCK**

Année Académique

2021 / 2022

PLAN DE TRAVAIL

- INTRODUCTION
- CHAPITRE 1 : IMPLEMENTATION DU PROTOCOLE VPN
- CHAPITRE 2 : LES PROTOCOLES DE SECURITE DES SERVICES INTERNET : SSL, SSH, IPSEC
- CONCLUSION

INTRODUCTION

Dans le domaine de la sécurité dans les réseaux, il existe plusieurs solutions de sécurité telles que le protocole **ipsec (ip security),** le protocole **ssl/tls (socket secure layer/transport layer security)** et le protocole **ssh (secure shell).**

Un protocole c'est un ensemble de règles et procédures qui régissent les échanges entre les équipements d'un réseau.

CHAPITRE 1 : IMPLEMENTATION DU PROTOCOLE VPN

I. PRINCIPE GENERAL D'UN VPN

Un réseau VPN repose sur un protocole appelé « **protocole de tunneling** ». ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout À l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel.

II. CARACTERISTIQUES FONDAMENTALES D'UN VPN

Un système de VPN doit pouvoir mettre en œuvre les fonctionnalités suivantes :

- **Authentification d'utilisateur**. Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.
- **Gestion d'adresses**. Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pouvoir se connecter facilement au réseau et recevoir une adresse.
- **Cryptage des données**. Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.
- **Gestion de clés**. Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.
- **Prise en charge multi protocole**. La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

III. LES FONCTIONNALITES DES VPN

Il existe 3 types standard d'utilisation des VPN.

1. Le VPN d'Accès

Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN.

Il existe deux cas :

- **L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.**
- **L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.**

Les deux méthodes possèdent chacune leurs **avantages** et leurs **inconvénients** :

- **La première permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un fournisseur d'accès proposant un NAS compatible avec la solution VPN choisie par l'entreprise. De plus, la demande de connexion par le NAS n'est pas cryptée Ce qui peut poser des problèmes de sécurité.**
- **Sur la deuxième méthode ce problème disparaît puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée. Nous verrons que pour pallier Ce problème certaines entreprises mettent en place des VPN à base de SSL, technologie implémentée dans la majorité des navigateurs Internet du marché.**

Quelle que soit la méthode de connexion choisie, Ce type d'utilisation montre bien l'importance dans le VPN d'avoir une authentification forte des utilisateurs. Cette authentification peut se faire par une vérification « login /mot de passe », par un algorithme dit « Tokens sécurisés » (utilisation de mots de passe aléatoires) ou par certificats numériques.

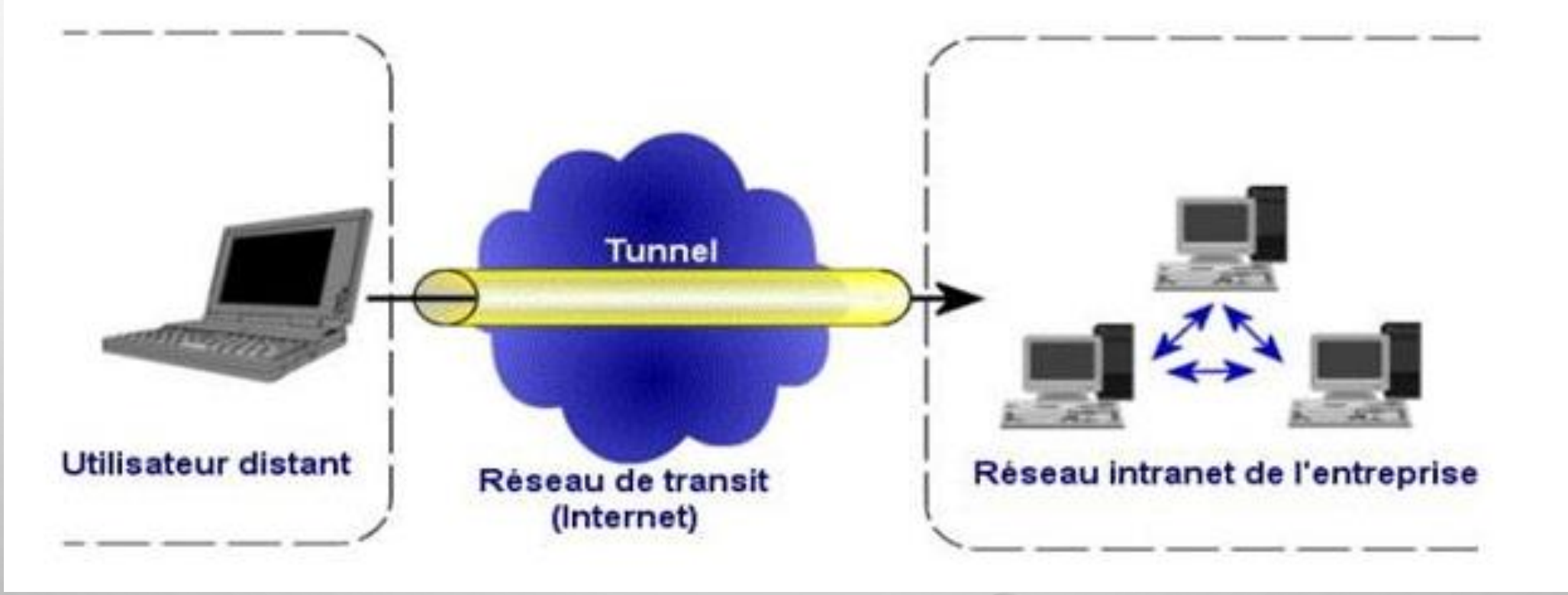

Fig1. Représentation du VPN d'Accès

2. L'intranet VPN

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans Ce type de réseau est de garantir la sécurité et l'intégrité des données. Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées.

Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation. La confidentialité des données est, elle aussi, basée sur des algorithmes de cryptographie.

La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite. Généralement pour la confidentialité, le codage en lui-même pourra être moyen à faible, mais sera combiné avec d'autres techniques comme l'encapsulation IP dans IP pour assurer une sécurité raisonnable.

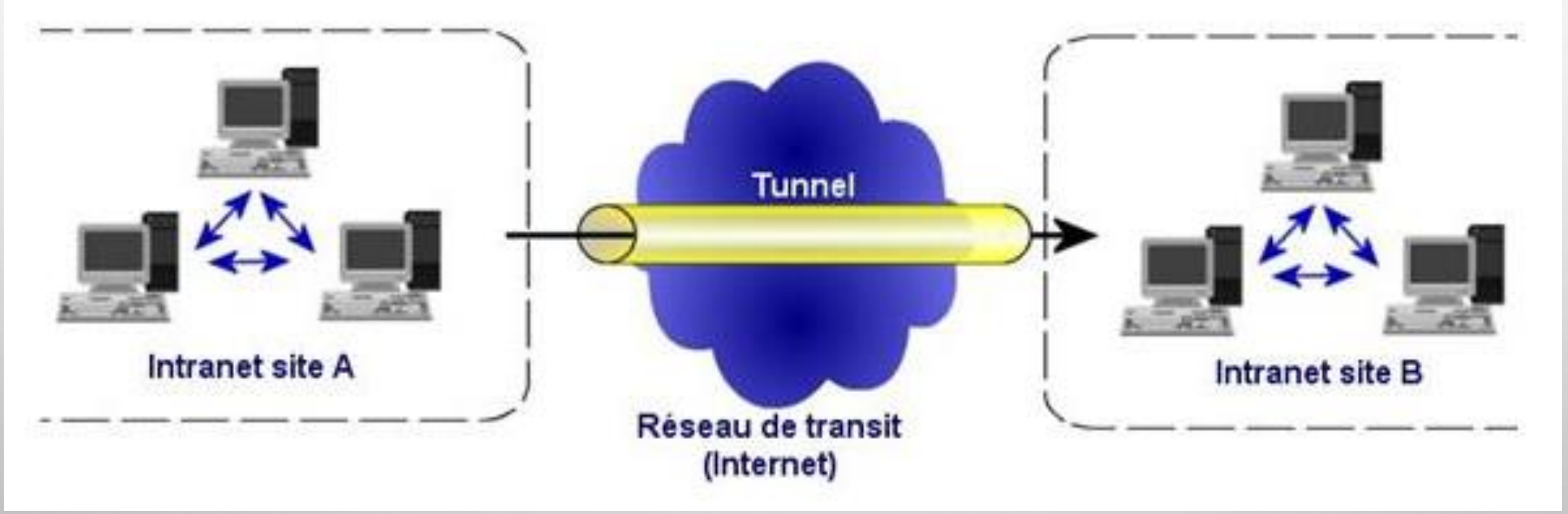

Fig2. Représentation de l'Intranet VPN

3. L'Extranet VPN

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans Ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

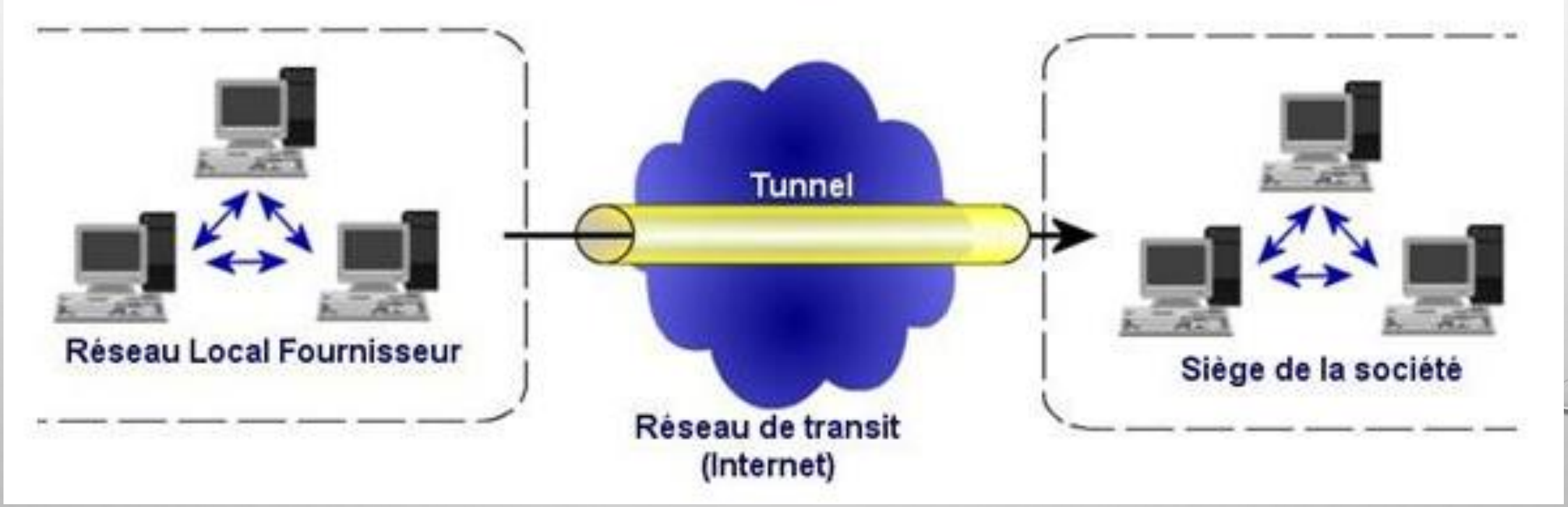

Fig3. Représentation de l'Extranet VPN

CHAPITRE 2 : LES PROTOCOLES DE SECURITE DES SERVICES INTERNET : SSL, SSH, IPSEC

I. LE PROTOCOLE SSL

1. Généralités

Le protocole **SSL** est un protocole de couche 4 (niveau transport) utilisé par une application pour établir un canal de communication sécurisé avec une autre application.

En effet le protocole SSL utilisé pour la sécurisation des échanges commerciaux sur Internet est implémenté en standard dans les navigateurs modernes. Le protocole SSL a deux grandes fonctionnalités : **l'authentification du serveur et du client à l'établissement de la connexion et le chiffrement des données durant la connexion.**

2. Caractéristique du protocole SSL

- **Chiffrement** : protège les transmissions de données (par ex : navigateur à serveur, serveur à serveur, application à serveur, etc.).
- **Authentification** : garantit que le serveur auquel vous êtes connecté est le bon serveur.
- **Intégrité des données** : garantit que les données qui sont demandées ou soumises sont bien celles qui sont fournies.

Le SSL peut être utilisé dans les cas suivants pour sécuriser :

- **Les transactions bancaires en ligne ou autres paiements en ligne.**
- **Les trafics intranet, tels que les réseaux internes, le partage de fichiers, les extranets et les connexions aux bases de données.**
- **Les connexions entre un client de messagerie, tel que Microsoft Outlook et un serveur mail, tel que Microsoft Exchange.**

3. Fonctionnalités du protocole SSL

Le protocole SSL Handshake débute une communication SSL. Suite à la requête du client, le serveur envoie son certificat ainsi que la liste des algorithmes qu'il souhaite utiliser. Le client commence par vérifier la validité du certificat du serveur. Cela se fait à l'aide de la clé publique de l'autorité de certification contenue dans le navigateur du client.

De nombreux paramètres sont échangés durant cette phase : **type de clé, valeur de la clé, algorithme de chiffrage.**

La phase suivante consiste en l'échange de données cryptées (protocole SSL Records). Les clés générées avec le protocole Handshake sont utilisées pour garantir l'intégrité et la confidentialité des données échangées.

Les différentes phases du protocole sont:

- Segmentation des paquets en paquets de taille fixe.
- Compression (mais peu implémenté dans la réalité).
- Ajout du résultat de la fonction de hachage composé de la clé de cryptage, du numéro de message, de la longueur du message, de données …
- Chiffrement des paquets et du résultat du hachage à l'aide de la clé symétrique générée lors du Handshake.
- Ajout d'un entête SSL au paquet.

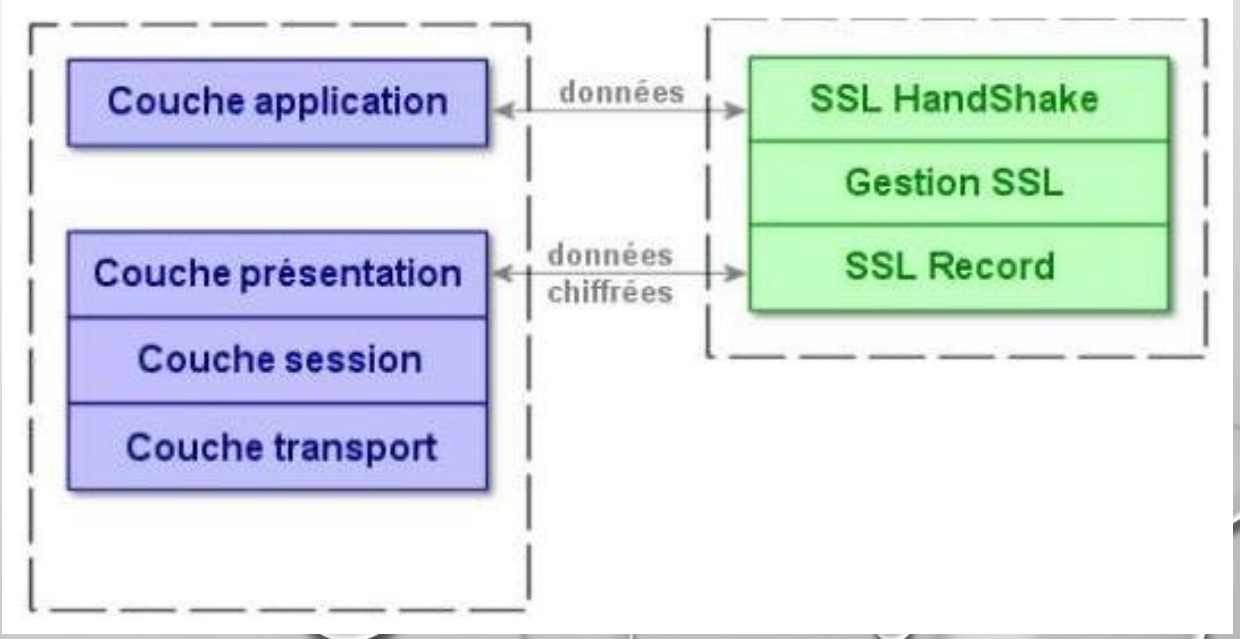

Fig3. Fonctionnement du protocole SSL

II. LE PROTOCOLE SSH

1. Généralités

Le **protocole SSH (Secure Shell)** est utilisé pour établir un accès sécurisé permettant d'effectuer des opérations sensibles sur des machines distantes et d'effectuer des transferts de fichiers à travers un réseau public tout en garantissant l'**authentification**, la **confidentialité** et l'**intégrité** des données.

Le principal objectif de SSH était de résoudre le problème de transmission en clair de toutes les informations sur le réseau (LAN ou Internet) ouvrant la porte à toutes les attaques de type homme du milieu.

Depuis l'apparition de SSH, son rôle a évolué pour ne pas se limiter à une simple fonctionnalité de connectivité à distance pour le shell. La version 2 de ce protocole, normalisée en janvier 2006, propose la sécurisation de n'importe quel protocole applicatif et ceci grâce à ses mécanismes de « port forwarding » et de « tunneling ».

- **Le réacheminement de port (port forwarding ou port mapping en anglais) consiste à rediriger des paquets réseaux reçus sur un port donné d'un ordinateur ou un équipement réseau vers un autre ordinateur ou équipement réseau sur un port donné**

- **Le tunneling, plus communément appelé transfert de port, est le processus de transmission de données qui est destiné à un usage privé uniquement.**

2. Caractéristiques du protocole SSH

Les caractéristiques d'une connexion sécurisée SSH sont :

- **Le port réseau par défaut du serveur SSH est le port 22**
- **Authentification par mot de passe obligatoire ou échange de clé sécurisée**
- **Génération d'une clé de session pour chiffrer toute la communication.**
- **Création sécurisée de sauvegardes**
- **Transfert de fichiers sécurisé**
- **Télémaintenance d'autres ordinateurs**

3. Fonctionnalités du protocole SSH

SSH est donc un **protocole de communication** qui vise à rendre la communication sûre. Généralement, un administrateur l'utilise pour prendre la main sur une machine distante.

L'établissement de la connexion SSH se fait avec le processus suivant :

- **Un client SSH se connecte à serveur SSH installé sur une machine distante. Par exemple un serveur sur internet ou une autre machine du LAN. Il peut aussi s'agir d'un équipement réseau comme un routeur.**
- **On s'authentifie soit avec une clé sécurisée, soit par mot de passe**
- **L'administrateur ouvre alors un Shell et peut passer des commandes sur la machine distante.**

Le protocole fonctionne dans le modèle **client-serveur**. Ce qui signifie que la connexion est établie par le client SSH se connectant au serveur SSH. Le client SSH pilote le processus de configuration de la connexion et utilise la cryptographie à clé publique pour vérifier l'identité du serveur SSH. Après la phase de configuration, le protocole SSH utilise un algorithme de chiffrement pour garantir la confidentialité et l'intégrité des données échangées entre le client et le serveur.

Trois phases se succèdent:

- **L'authentification du client SSH auprès du serveur.**
- **Une pré-phase de chiffrement symétrique où les deux parties se mettent d'accord sur l'algorithme à utiliser pour chiffrer la session SSH.**
- **La session SSH est établit.**

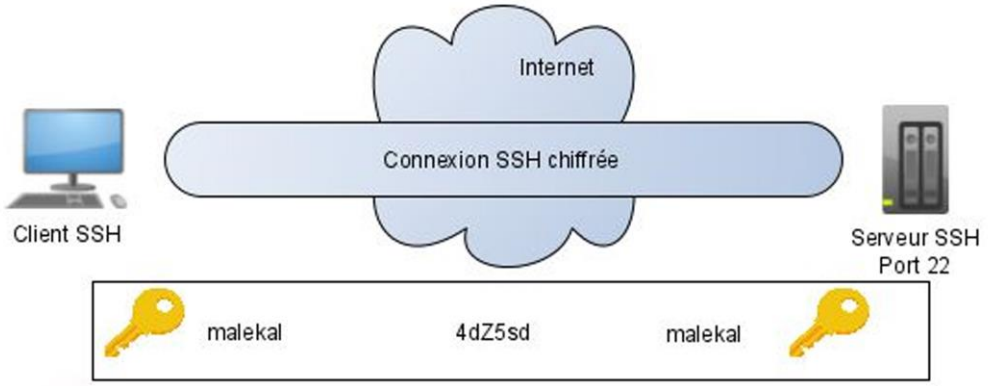

Fig4. Fonctionnement du protocole SSH

III. LE PROTOCOLE IPSEC

1. Généralités

IPsec vise à sécuriser les échanges au niveau de la couche réseau. Le réseau IPv4 étant largement déployé et la migration complète vers IPv6 nécessitant encore beaucoup de temps, il est vite apparu intéressant de définir des mécanismes de sécurité qui soient communs à la fois à IPv4 et IPv6

2. Caractéristiques du protocole IPSEC

- **Des mécanismes de confidentialité et de protection contre l'analyse du trafic.**
- **Des mécanismes d'authentification des données (et de leur origine).**
- **Des mécanismes garantissant l'intégrité des données (en mode non connecté).**
- **Des mécanismes de protection contre le rejet.**
- **Des mécanismes de contrôle d'accès.**

3. Fonctionnement du protocole IPSECT

Les implémentations IPSec s'appuient ainsi sur les composants suivants :

- **SA** : l'association de sécurité IPsec est une connexion qui fournit des services de sécurité au trafic qu'elle transporte.

- **SPD** : les protections offertes par IPSec sont basées sur des choix définis dans une base de données de politique de sécurité. Cette base de données est établie et maintenue par un administrateur. Elle permet de décider, pour chaque paquet, s'il se verra apporter des services de sécurité, s'il sera autorisé à passer outre ou sera rejeté.

- **SAD** : de manière à pouvoir gérer les associations de sécurité actives, on utilise une base de données des associations de sécurité. Elle contient tous les paramètres relatifs à chacune de SA et sera consultée pour savoir comment traiter chaque paquet reçu ou à émettre.

Les deux modes de fonctionnement IPSec sont :

a. Le Mode Transport

Le mode transport prend un flux de niveau transport (couche de niveau 4 du modèle OSI) et réalise les mécanismes de signature et de chiffrement puis transmet les données à la couche IP. Dans ce mode, l'insertion de la couche IPsec est transparente entre TCP et IP. TCP envoie ses données vers IPsec comme il les enverrait vers IPv4.

L'inconvénient de ce mode réside dans le fait **que l'en-tête extérieure est produite par la couche IP c'est-à-dire sans masquage d'adresse. L'intérêt de ce mode réside dans une relative facilité de mise en œuvre.**

b. Le Mode Tunnel

- Dans le mode tunnel, les données envoyées par l'application traversent la pile de protocole jusqu'à la couche IP incluse, puis sont envoyées vers le module IPsec. L'encapsulation IPsec en mode tunnel permet le masquage d'adresses. Le mode tunnel est généralement utilisé entre deux passerelles de sécurité (routeur, firewall, ...) alors que le mode transport se situe entre deux hôtes.

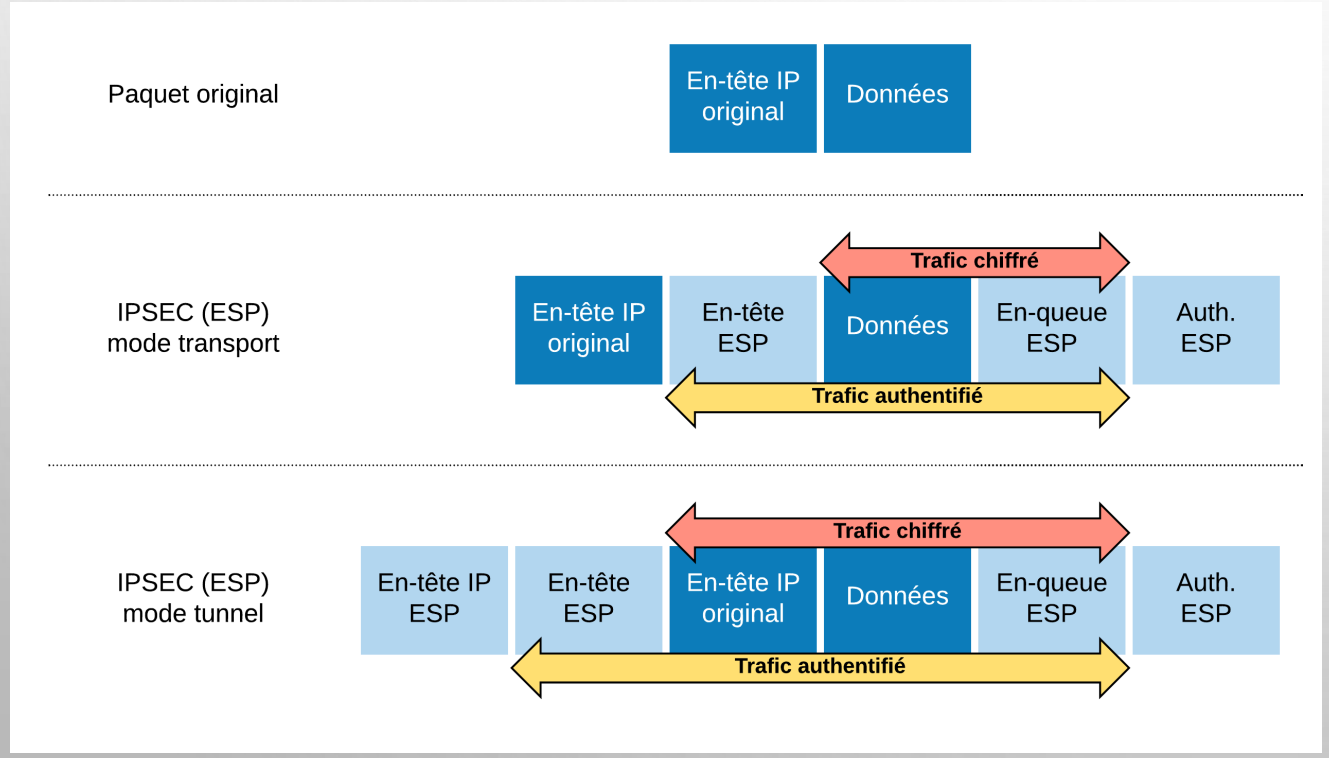

Fig4. Fonctionnement du protocole IPsec

4. Les Protocoles d'Authentification IPSec

a. Le protocole AH

Le protocole AH (Authentification Header) est conçu pour assurer l'intégrité en mode non connecté et l'authentification de l'origine des datagrammes IP sans chiffrement des données (pas de confidentialité). Son principe est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme

En effet, le contenu de la trame n'étant pas chiffré, le protocole AH ajoute une signature numérique au paquet IP sortant : un mécanisme de translation d'adresses réécrivant l'adresse source, fausse systématiquement le calcul de vérification de la signature numérique effectuée à l'autre bout du tunnel VPN

b. Le protocole ESP (Encapsulating Security Payload)

- Le protocole ESP peut assurer, au choix, un ou plusieurs des services suivants :

❖ **Confidentialité des données et protection partielle contre l'analyse du trafic si l'on utilise le mode tunnel ;**

❖ **Intégrité des données en mode non connecté et authentification de l'origine des données, protection partielle contre le rejet.**

❖ **Contrairement au protocole AIT (Advanced Intelligent Tape), où l'on se contentait d'ajouter une en-tête supplémentaire au paquet IP, le protocole ESP fonctionne suivant le principe d'encapsulation : les données originales sont chiffrées puis encapsulées.**

CONCLUSION

IPSec est un système très complet qui peut répondre à beaucoup de besoins en matière de sécurité et s'adapter à de nombreuses situations. Sa conception en fait un système très sûr et sa nature de norme garantit l'interopérabilité entre les équipements de différents fournisseurs. Ces avantages, couplés à la prédominance grandissante du protocole IP, vont certainement faire d'IPSec un acteur important de la sécurité des réseaux informatiques. Il lui manque encore, pour être utilisé à grande échelle, un peu de maturité et surtout un système de gestion centralisée et dynamique des politiques de sécurité. Les avancées actuelles dans ce domaine laissent à penser qu'il ne s'agit que d'une question de temps avant qu'un tel système ne voie le jour. L'apparition d'infrastructures à clefs publiques fonctionnelles et reconnues est également indispensable pour une utilisation pratique et répandue d'IPSec.

THANKS!!!