REPUBLIQUE DU CAMEROUN
**********
Paix – Travail – Patrie
**********
MINISTRE DE L'ENSEIGNEMENT SUPRERIEUR

REPUBLIC OF CAMEROON
**********
Peace – Work - Fatherland
**********
MINISTRY OF HIGHER EDUCATION


# 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**

**FILIERE : Génie Logiciel**

**Niveau : BAC + 3**

**En cours**

**Supervisé par :**

**M. Didier Frédéryck MBANJOCK**

**ANNEE ACADEMIQUE : 2021 / 2022**

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

## SOMMAIRE

## DEFINITIONS DES SIGLES

**AH:** Authentication Header

**ESP:** Encapsulating Security Payload

**SSL/TLS:** (Socket Secure Layer/Transport Layer Security)

**IPSec:** (Internet Protocol Security)

**SSH:** (Secure Shell)

**VPN:** Virtual Private Network

**NAS :** (Network Access Server)

**SSL ( Secure Socket Layer)**

**HTTPS:** HyperText Transfer Protocol Secure

**FTP:** File Transfer Protocol

**CRL:** (Certificate Revocation List)

**SSH** : (Secure Schell)

**SFTP :** SSH File Transfer Protocol

**VNC:** Virtual Network Computing

**AES:** Advanced Encryption Standard

**3DES :** Data Encryption Standard

**HMAC:** Hash Based Message Authentication Code

**RFCs:** Research Fund for Coal and Steel

**ICMP:** Internet Control Message Protocol

**IGMP:** Internet Group Management Protocol

**RIP:** Routing Information Protocol

**SPD:** Session Protocol Description

**SAD:** Subacromial Decompression

**IETF:** Internet Engineering Task Force

**AIT :** Advanced Intelligent Tape

# 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). Actuellement, il ne s'agit plus uniquement de chercher à faire de nouveaux développements afin que le réseau soit plus fiable ou d'une manière générale soit plus sécurisé dans son fonctionnement global. Il faudrait adapter ces solutions aux besoins spécifiques des utilisateurs ainsi qu'à leurs environnements. Un protocole c'est un ensemble de règles et procédures qui régissent les échanges entre les équipements d'un réseau.

Les applications et les systèmes distribués font de plus en plus partie intégrante du paysage d'un grand nombre d'entreprises. Ces technologies ont pu se développer grâce aux performances toujours plus importantes des réseaux locaux. Mais le succès de ces applications a fait aussi apparaître un de leur écueil. En effet si les applications distribuées deviennent le principal outil du système d'information de l'entreprise, comment assurer leur accès sécurisé au sein de structures parfois réparties sur de grandes distances géographiques ? Concrètement comment une succursale d'une entreprise peut-elle accéder aux données situées sur un serveur de la maison mère distant de plusieurs milliers de kilomètres ? Les VPN ont commencé à être mis en place pour répondre à ce type de problématique. Mais d'autres problématiques sont apparues et les VPN ont aujourd'hui pris une place importante dans les réseaux informatique et l'informatique distribuées. Nous verrons ici quelles sont les principales caractéristiques des VPN à travers un

certain nombre d'utilisation type et nous nous intéresserons ensuite aux protocoles permettant leur mise en place.

# 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. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet.

Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans Ce cas, le protocole de tunneling encapsule les données en ajoutant un entête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

## 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.

Le VPN est un principe : il ne décrit pas l'implémentation effective de ces caractéristiques. C'est pourquoi il existe plusieurs produits différents sur le marché dont certains sont devenus standard, et même considérés comme des normes.

## III. LES FONCTIONNALITES DES VPN

Il existe 3 types standard d'utilisation des VPN.

### 1. Le VPN d'accès

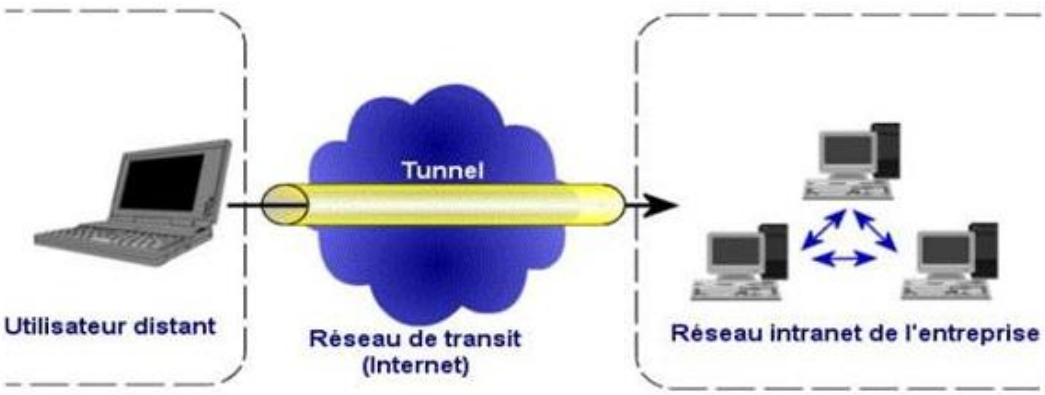


*Fig1. Représentation du VPN d'Accès*

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 :

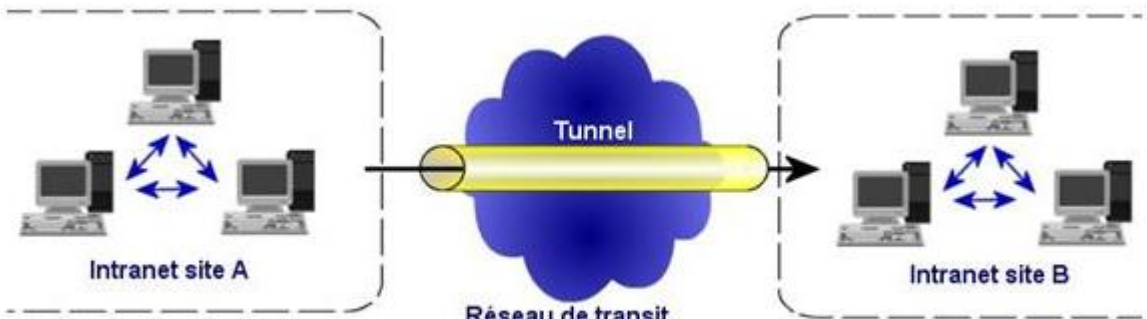
- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.
- L'utilisateur possède son propre logiciel client pour le VPN auquel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

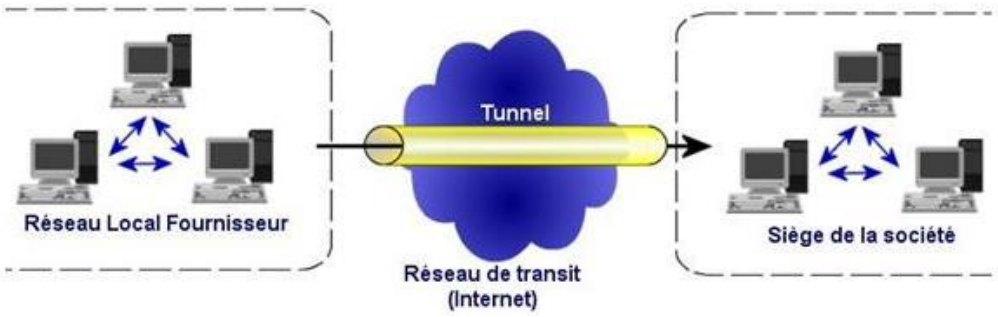
Quelle que soit la méthode de connexion choisie, Ce type d'utilisation montre bien l'importance dans le VPN d'avoir une authentification forte des utilisateurs. Cette authentification peut se faire par une vérification « login /mot de passe », par un algorithme dit « Tokens sécurisés » (utilisation de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

## 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. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières…). 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 plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutées aux paquets. 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. Le coût matériel des équipements de cryptage et décryptage ainsi que les limites légales interdisent l'utilisation d'un codage « infaillible ». 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.

## 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.

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

## I. LE PROTOCOLE SSL

### 1. Généralités

Récemment arrivé dans le monde des VPN, les **VPN à base du protocole SSL ( Secure Socket Layer)** présente une alternative séduisante face aux technologies contraignantes que sont les VPN présentés jusque ici. Les VPN SSL présentent en effet le gros avantage de ne pas nécessiter du coté client plus qu'un navigateur Internet classique. 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 est un protocole de couche 4 (niveau transport) utilisé par une application pour établir un canal de communication sécurisé avec une autre application.

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 serveurs de messageries web, telles que Outlook Web Access, Exchange et Office Communications Server.
- Les connexions entre un client de messagerie, tel que Microsoft Outlook et un serveur mail, tel que Microsoft Exchange.
- Le transfert de fichiers via des services HTTPS et FTP, dans les cas de mise à jour de sites Internet par exemple ou de transferts de gros fichiers.
- Les connexions aux panneaux de contrôle et applications tels que Parallels, cPanel, et bien d'autres encore.
- Les applications de flux de travail et de virtualisation comme les plateformes Citrix Delivery ou les plateformes informatiques sur le cloud.
- Les connexions aux panneaux de contrôle d'activités d'hébergement tels que Parallels, cPanel, et bien d'autres encore.

## 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. Le client vérifie aussi la date de validité du certificat et peut également consulter une CRL (Certificate Revocation List). Si toutes les vérifications sont passées, le client génère une clé symétrique et l'envoie au serveur. Le serveur peut alors envoyer un test au client, que le client doit signer avec sa clé privée

correspondant à son propre certificat. Ceci est fait de façon à Ce que le serveur puisse authentifier le 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.

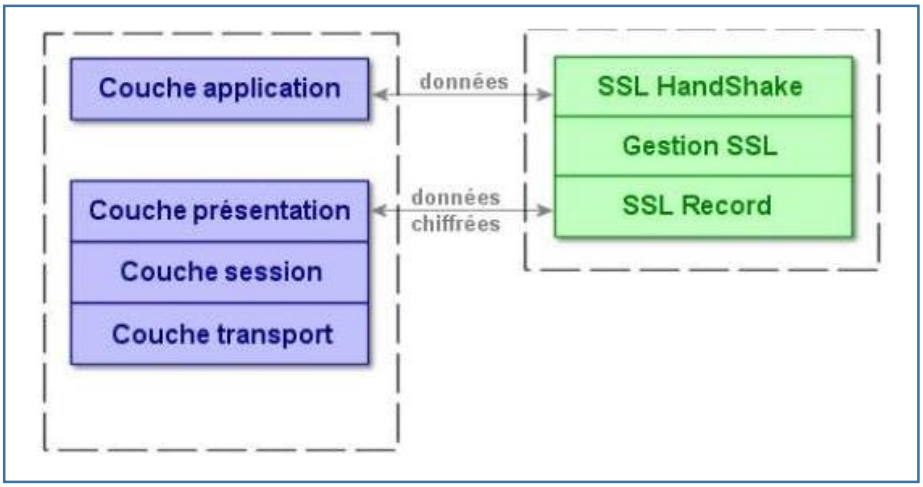



*Fig. Les fonctionnalités du protocole SSL*

## II. LE PROTOCOLE SSH

### 1. Généralités

Le protocole SSH (Secure Schell) constitue une approche puissante, pratique et sécurisé pour protéger les communications sur un réseau d'ordinateurs, notamment les

opérations sensibles, la transmission de fichiers, les fonctionnalités importantes telles que le tunneling et la redirection de port.

L**e 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 (Man-in-The-Middle).

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**
- Une authentification est obligatoire par mot de passe ou échange de clé sécurisée
- Génération d'une clé de session pour chiffrer toute la communication.
- Gestion des serveurs auxquels il n'est pas possible d'accéder localement
- Transfert de fichiers sécurisé
- Création sécurisée de sauvegardes
- Connexion entre deux ordinateurs utilisant le chiffrement de bout en bout
- Télémaintenance d'autres ordinateurs

Le développement de SSH a également influencé d'autres protocoles. Par exemple, le protocole FTP non sécurisé, avec lequel il est possible de télécharger des fichiers sur un serveur et de les télécharger à nouveau à partir de là, a été développé dans le protocole SFTP (SSH File Transfer Protocol).

Un avantage de SSH est que le protocole fonctionne **sur tous les systèmes d'exploitation courants.** Comme il s'agissait à l'origine d'une application Unix, il est également implémenté par défaut sur toutes les distributions Linux et sur MacOs. Mais SSH peut aussi être utilisé sous Windows si vous installez un programme approprié.

## 3. Fonctionnement 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.

En fait le protocole SSH permet d'aller plus loin comme transférer des fichiers ou être utilisé pour la communication avec d'autres applications. Par exemple, on peut utiliser la prise en main VNC pour passer à transfert SSH.

Pourquoi ? Car la communication entre client et le serveur SSH est chiffrée. Ainsi un attaquant ne peut pas sniffer les communications afin de voler des données.

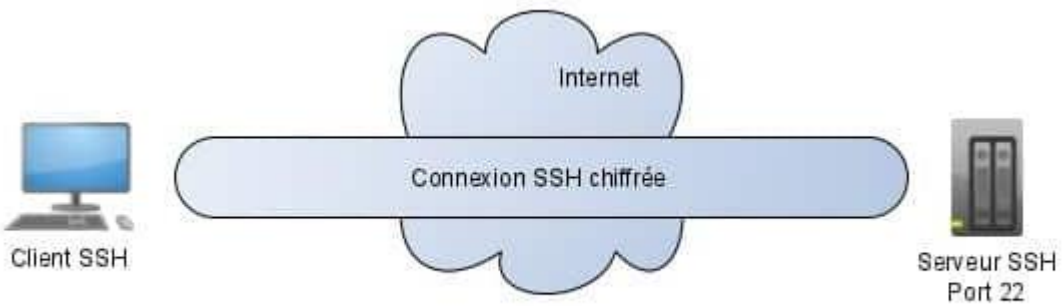


*Fig. Etablissement de la connexion SSH*

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.

## a. L'authentification

SSH supporte deux méthodes d'authentification

- Par mot de passe
- Par une paire de clés. On parle de **clés SSH**.

Les clés SSH peuvent avoir jusqu'à 4096 bits de longueur, ce qui les rend longues, complexes et difficiles à pirater par force brute. Ces clés font généralement au moins 1024 bits, ce qui est l'équivalent de sécurité d'un mot de passe d'au moins 12 caractères.

**Sécuriser un serveur SSH**

Les paires de clés SSH peuvent être utilisées pour authentifier un client auprès d'un serveur.
Le client crée une paire de clés, puis télécharge la clé publique sur tout serveur distant auquel il souhaite accéder. Celui-ci est placé dans un fichier appelé **authorized_keys** dans le répertoire **~/ .ssh** du répertoire de base du compte utilisateur sur le serveur distant.

Une fois le chiffrement symétrique établi pour sécuriser les communications entre le serveur et le client, le client doit s'authentifier pour pouvoir accéder. Le serveur peut utiliser la clé publique de ce fichier pour crypter un message de défi adressé au client. Si le client peut prouver qu'il a pu déchiffrer ce message, il a démontré qu'il possède la clé privée associée. Le serveur peut alors configurer l'environnement pour le client.

## b. Chiffrer la communication

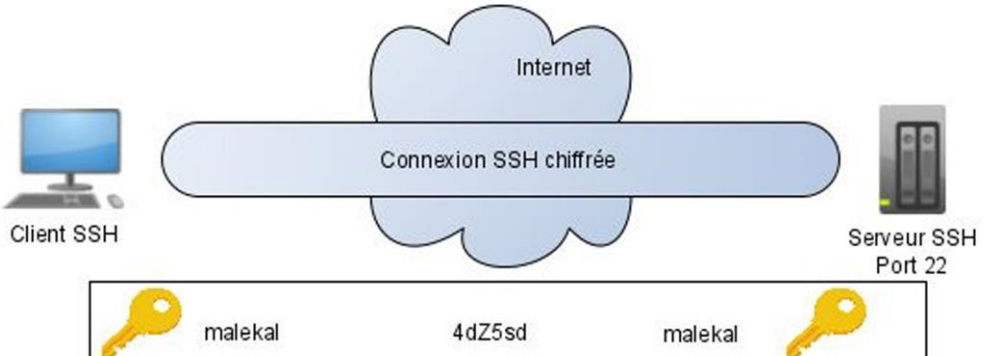
Afin de sécuriser la transmission des informations, SSH emploie un certain nombre de différents types de techniques de manipulation de données à divers points de la transaction.

- Le client et le serveur s'accordent sur l'algorithme de chiffrement symétrique à utiliser et génèrent la clé ou les clés de chiffrement qui seront utilisées pour la session SSH. Leur échange se fait à travers **l'algorithme Diffie-Hellman**. SSH permet **un chiffrement symétrique ou asymétrique**.
- Puis garantit l'intégrité des données transmises en utilisant des algorithmes de hachage standard

## SYMETRIQUE

Le chiffrement symétrique est une méthode où les messages entre le client SSH et le serveur SSH sont chiffrés et déchiffrés à l'aide d'une clé secrète. Le chiffrement symétrique est souvent appelé **clé partagée (shared key)** ou **secret partagé (shared secret)**. On utilise alors qu'une seule clé, ou parfois une paire de clés où une clé peut facilement être calculée à l'aide de l'autre clé.

La clé secrète est créée via un processus appelé **algorithme d'échange de clés**. Cet échange a pour résultat que le serveur et le client arrivent tous deux à la même clé indépendamment en partageant certaines données publiques et en les manipulant avec certaines données secrètes.



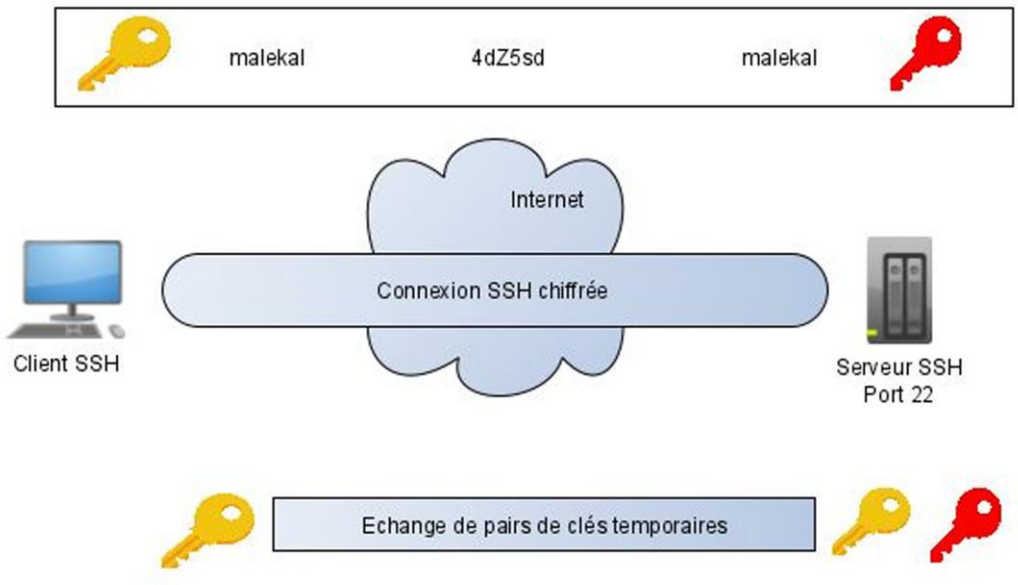
SSH supporte une variété de systèmes de chiffrement symétriques différents, y compris **AES**, **Blowfish, 3DES**, **CAST128** et **Arcfour.**

## ASYMETRIQUE

La seconde méthode communication SSH consiste à utiliser des pairs de clairs.
Pour rappel :

- La clé publique sert à chiffrer les données
- Seule la clé privée permet de déchiffrer les données

Le chiffrement asymétrique n'est pas utilisé pour chiffrer toute la session SSH. Il n'est utilisé que pendant l'algorithme d'échange de clés de chiffrement symétrique. Avant d'initier une connexion sécurisée, les deux parties génèrent **des paires de clés publiques-privées temporaires** et partagent leurs clés privées respectives pour produire la clé secrète partagée.



### c. Hachage des messages

Une fois la session SSH établie, il y a donc communication entre client et le serveur.

SSH s'appuie ensuite sur **HMAC** pour garantir que les messages échangées sont intacts et non modifié.
Pour faire simple, à chaque message, le hash de ce dernier est aussi envoyé.

Pour cela, un algorithme HMAC est choisi parmi ceux proposés par le client SSH. Le premier de cette liste que le serveur prend en charge sera utilisé. Chaque message envoyé après la négociation du chiffrement doit contenir un MAC afin que l'autre partie puisse vérifier l'intégrité du paquet. Le MAC est calculé à partir du secret partagé symétrique, du numéro de séquence du paquet du message et du contenu réel du message.

Le MAC lui-même est envoyé en dehors de la zone cryptée symétriquement en tant que partie finale du paquet. Les chercheurs recommandent généralement cette méthode pour crypter les données d'abord, puis pour calculer le **MAC (Media Access Control).**

## 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. Ces mécanismes sont couramment désignés par le terme IPSec pour IP Security Protocols.

Le protocole IPsec est l'une des méthodes permettant de créer des **VPN** (réseaux privés virtuels), c'est-à-dire de relier entre eux des systèmes informatiques de manière sûre en s'appuyant sur un réseau existant, lui-même considéré comme non sécurisé. Le terme sûr a ici une signification assez vague, mais peut en particulier couvrir les notions d'intégrité et de confidentialité. L'intérêt majeur de cette solution par rapport à d'autres techniques (par exemple

les tunnels SSH) est qu'il s'agit d'une méthode standard (facultative en **IPv4**, mais obligatoire en **IPv6**), mise au point dans ce but précis, décrite par différentes **RFCs**, et donc interopérable. Quelques avantages supplémentaires sont l'économie de bande passante, d'une part parce que la compression des entêtes des données transmises est prévue par ce standard, et d'autre part parce que celui-ci ne fait pas appel à de trop lourdes techniques d'encapsulation, comme par exemple les tunnels PPP sur lien **SSH**. Il permet également de protéger des protocoles de bas niveau comme **ICMP et IGMP, RIP**.

IPSec présente en outre l'intérêt d'être une solution évolutive, puisque les algorithmes de chiffrement et d'authentification à proprement parler sont spécifiés séparément du protocole lui-même. Celle-ci a cependant l'inconvénient inhérent de sa flexibilité et sa grande complexité rend son implémentation délicate

## 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 IPSEC

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.

Il s'agit d'une structure de données servant à stocker l'ensemble des paramètres associés à une communication donnée. Une SA est unidirectionnelle, en conséquence, protéger les deux sens d'une communication classique requiert deux associations, une dans chaque sens. Le rôle d'une SA est de consigner, pour chaque adresse IP avec laquelle l'implémentation IPsec peut communiquer certaines informations suivantes.

- **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 services IPSec sont basés sur des mécanismes cryptographiques. Pour cela, IPsec fait appel à deux protocoles de sécurité qui viennent s'ajouter au protocole IP classique : il s'agit des protocoles **AH** et **ESP**. IPsec offre ainsi deux possibilités d'encapsulation distinctes.

Toutefois, l'évolution de ce protocole fait qu'**ESP** assure désormais l'ensemble des fonctionnalités des deux mécanismes. Au-delà de **AH** et **ESP**, l'**IETF** a jugé judicieux d'offrir un service supplémentaire appelé chiffrement en mode **Fast Forward** qui conserve la même taille de datagrammes et ainsi des performances optimales.

Cependant, il protège en confidentialité uniquement. L'en-tête IP et la longueur du datagramme restent inchangés (sauf éventuellement le champ d'options IP qui peut être chiffré). Les SA contiennent tous les paramètres nécessaires à IPsec, notamment les clés utilisées.

La gestion des clés pour IPsec n'est liée aux autres mécanismes de sécurité de IPsec que par le biais des **SA**. Une **SA** peut être configurée manuellement dans le cas d'une situation simple, mais la règle générale consiste à utiliser un protocole spécifique qui permet la négociation dynamique de SA et notamment l'échange des clés de session.

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**. De plus, le fait de terminer les traitements par la couche IP ne permet pas de garantir la non-utilisation des options IP potentiellement dangereuses. **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.

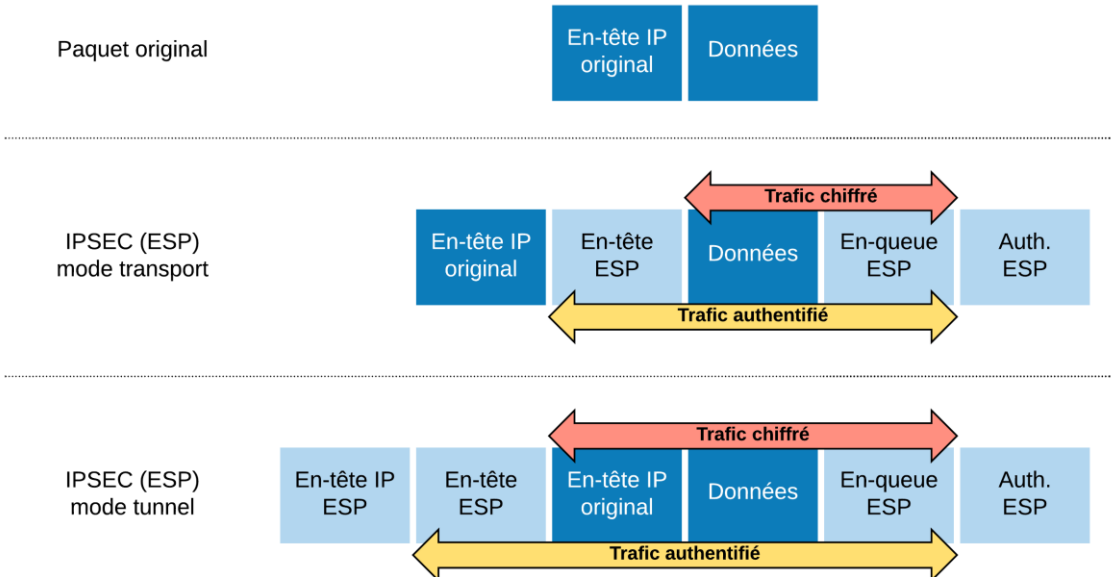



*Fig. Fonctionnement du protocole IPSec*

## 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.

Ce bloc de données est appelé « valeur de vérification d'intégrité » (ICV). La protection contre le rejet se fait grâce à un numéro de séquence. Il est à noter que l'utilisation du protocole AH interdit l'utilisation des mécanismes de translation d'adresses.

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.

## BIBLIOGRAPHIE ET REFERENCE

https://www.globalsign.com/fr/centre-information-ssl/definition-ssl

https://vpnactu.fr/les-caracteristiques-dun-bon-vpn/

https://www.appsystem.fr/192385/quelles-caracteristiques-retenir-lors-du-choix-dun-vpn/

https://wikimemoires.net/2012/08/virtual-private-network-principe-et-fonctionnalites-des-vpn/

SSH : comment ça marche - malekal.com

https://www.memoireonline.com/10/12/6146/Etude-des-protocoles-de-securite-dans-le-reseau-internet.html