Communications sécurisées – Protocoles

- Sécuriser une communication

  I.e. confidentialité, authentification et intégrité

- Assurer le contrôle des accès distants et la confidentialité des communications

  (site à site, nomade filaire, wifi, etc.)

Introduction

Site de dépot des CM.pdf et éventuellement de la déclaration d'erratum ou autre information :
Soit http://infoweb.iut-nantes.univ-nantes.prive/~ hernandez-n/
Soit http:www.sciences.univ-nantes.fr/info/perso/permanents/hernandez/
Se tenir au courant...

Bref rappel du CM de cryptographie

- *Confidentialité des données* : *chiffrer* (algo. symétrique à clé secrète et asymétrique aux clés privé/publique) contre *packet sniffing* (renifleur)
- *Authentification de l'émetteur* : *signer* (algo. asymétrique avec clé privée) contre *identity spoofing / man-in-the-middle* (usurpation),
- *Intégrité d'un message* : *empreinte* (fonction de hachage) contre *message alteration*

Réseau Privée Virtuel

Définition

Virtual Private Network (VPN) : utilisation de protocoles sécurisés pour la création d'un canal de communication sécurisé à **usage privé**, au travers d'un **réseau public**[a] non sécurisé

[a] réseau téléphonique de bout en bout ; téléphonique pour l'accès puis réseau Internet jusqu'au réseau entreprise ; accès xDSL à Internet puis jusqu'à entreprise

- Souvent mis en oeuvre par une organisation pour assurer la *sécurité* des échanges notamment pour l'**interconnexion de ses différents sites géographiques via Internet** ou bien pour **autoriser des utilisateurs nomades**
- **Secure VPNs** : utilisation de protocoles réseaux sécurisés de **tunneling** (e.g. L2TP, IPsec, SSL/TLS)

Tunnels

Définition

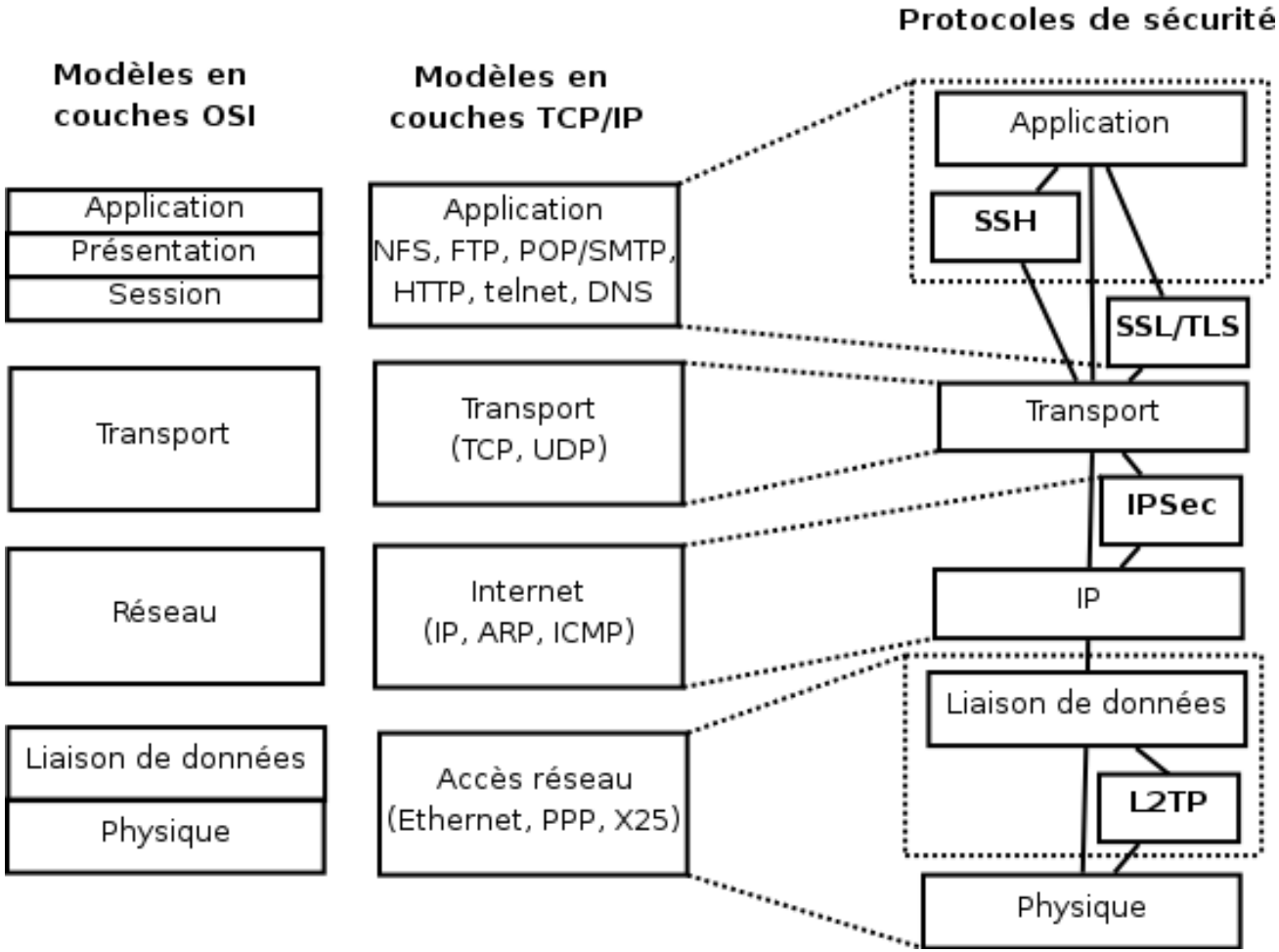
Tunneling Protocoles : protocole réseau qui encapsule un autre protocole

Deux sortes/orientations :

- **Datagramme** : L2TP, PPTP, IPSec
- **Streaming** : SSL/TLS, SSH

On peut mettre en place un tunnel indépendamment d'un VPN

Représentation en couches des protocoles de sécurité



Choix du niveau du tunneling et de la sécurité à mettre en oeuvre

Dépend de la maîtrise que l'on a (de l'infrastructure) du réseau

Examples

- Une entreprise choisira niveau 3 car ne maîtrise pas les artères de connexion (niveau 2) entre plusieurs sites géographiques
- Un ISP[a] d'accès xDSL pourra choisir niveau 2 pour l'accès à Internet...

[a] Internet Service Provider/Fournisseur d'Accès à Internet (FAI)

Sommaire

Layer 2 Tunneling Protocol (L2TP)

- Standardisé par l'IETF (*Internet Engineering Task Force*)
- Fusion des protocoles L2F (*Layer 2 Forwarding*) de Cisco et PPTP (*Point to Point Tunneling Protocol*) de Microsoft
- Sécurise la couche (OSI) **Liaison de données**

Définition

Transport des sessions PPP sur réseau IP

- **PPP** (*Point to Point Protocol*)
- Principalement **utilisé entre un client et un premier équipement de raccordement** au réseau (e.g. un utilisateur à son FAI lors d'une connexion par modem via une ligne téléphonique)

Objectif

Dépasser le point de raccordement au réseau IP

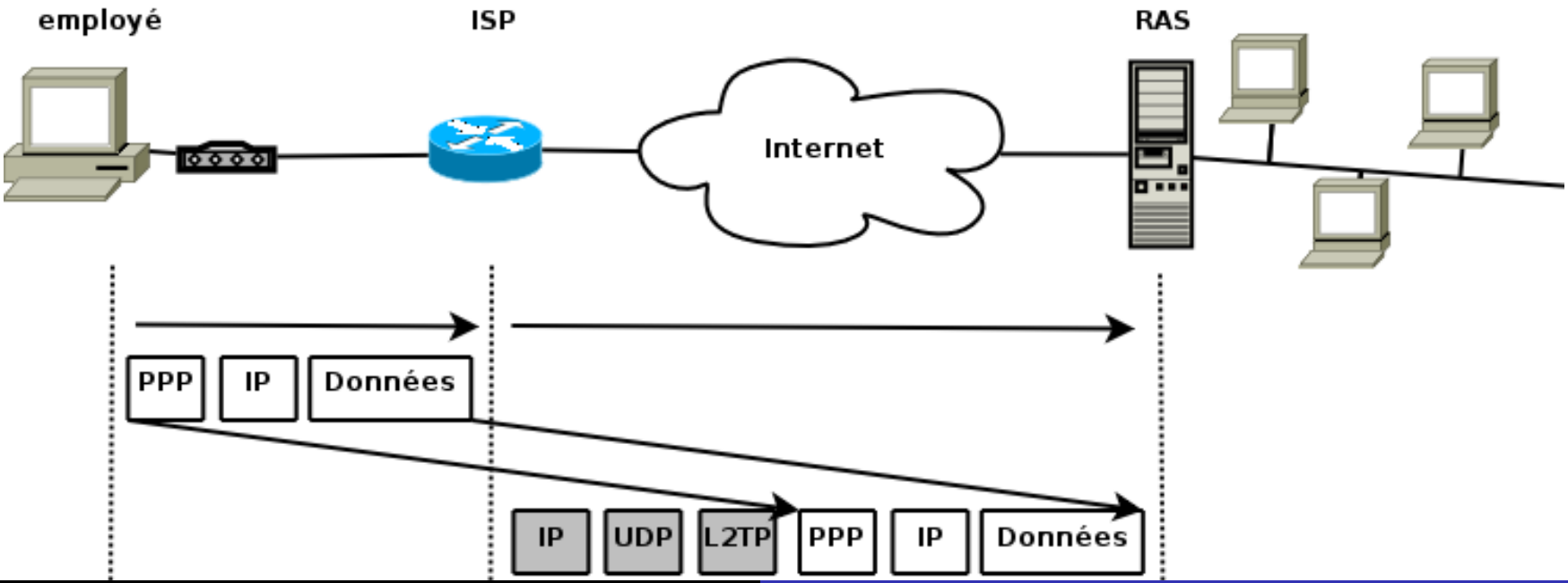
E.g. ISP qui permet à des employés de se connecter d'accéder au réseau de leur entreprise par n'importe quel point de présence de l'ISP

Mise en oeuvre de L2TP

Principe

Encapsulation *des paquets PPP* **dans des paquets UDP** *avec insertion d'une* **en-tête L2TP** *devant l'en-tête PPP*

Exemple de tunnel L2TP, créé par l'ISP jusqu'au RAS (*Remote Access Server*) de l'entreprise ; la jonction entre l'employé et l'ISP est ici gérée en PPP



Internet Protocol Security (IPSec)

- Standardisé par l'IETF
- Sécurise la couche (OSI) **Réseau**
- **Pour résoudre faiblesses de sécurité d'IPv4** (authentification et confidentialité)
- **Intégrée à IPv6**
- Requiert mises à jour de la pile pour en disposer dans *IPv4*
- Selon les besoins, assure la confidentialité, l'authentification et l'intégrité des données

Modes Transport et Tunnel

- Permettent de créer des *Réseaux Privées Virtuels*

Définition

Mode Transport : un en-tête IPSec s'intercale entre l'en-tête IP et les données sans modifier l'en-tête IP d'origine

Définition

Mode tunnel : encapsule l'intégrité du paquet IP original dans un paquet IPSec auquel on ajoute un nouvel en-tête IP

Protocoles AH et ESP

Contenu des IPSec Header dépend du protocole de sécurité utilisé[1]

Définition

AH (Authentification Header) assure authenticité et intégrité des *données* + des *en-têtes IP*[a]

[a] Hormis champs modifiables lors d'un routage i.e. Type de service, TTL, Flags, Offset, Checksum ; les non-modifiables : Version, IHL, Longueur, Id, Protocole

Définition

ESP (Encapsulating Security Payload) ajoute un *trailer* après données, garantie confidentialité et intégrité *données* + *trailer*
En option : authenticité *header* + *données* + *trailer* en ajoutant un second *trailer*

[1] Dans des cas particuliers, peuvent être utilisés conjointement.

Protocoles AH et ESP et algorithmes cryptographiques

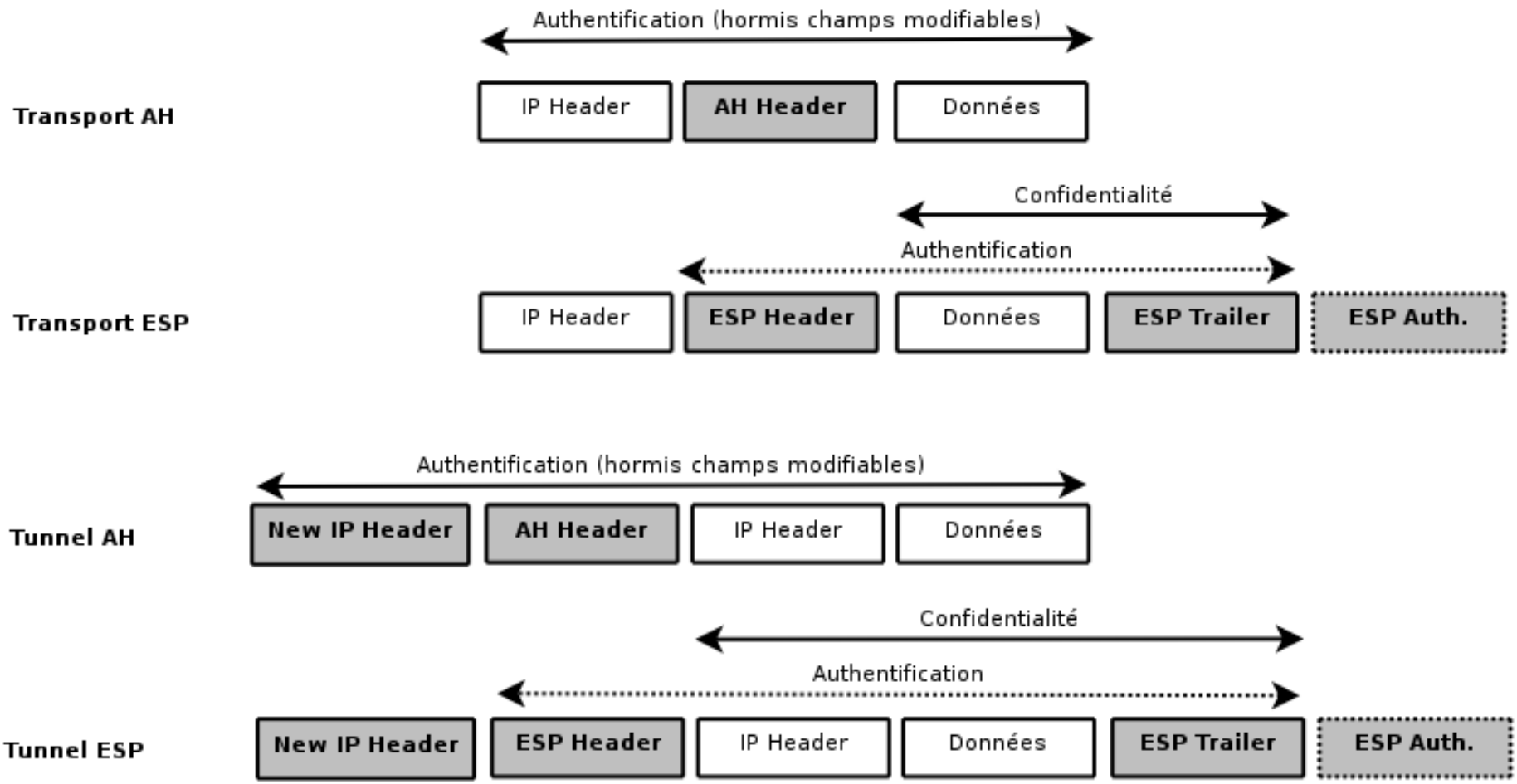
AH (Authentification Header)

- *Intégrité* : fondée sur HMAC qui peut utiliser les algo. de hachage MD5 et SHA-x
- *Authentification* : indirectement par la fonction de hachage, car celle-ci présuppose le partage d'une clé secrète que seules les communiquants sont censés connaître...

ESP (Encapsulating Security Payload)

- *Confidentialité* : le chiffrement repose uniquement sur algo. à clé secrète : DES, RC5, IDEA, Blowfish et AES
- *Intégrité et Authentification* : Similaire à AH.

IPSec : modes et protocoles



Etablissement d'Associations de Sécurité

Définition

IKE (Internet Key Exchange) : protocole permettant à deux entités de s'accorder sur les algorithmes et les clés à utiliser pour s'assurer une communication sécurisée

- Développé pour IPSec mais ouvert à d'autres protocoles

Principe

Fonctionne en 2 phases :

- **Etablissement d'une Association de Sécurité IKE (IKE SA)** *: définit l'ensemble des paramètres permettant de protéger la seconde phase. Ces paramètres sont : algorithmes de chiffrement, fonctions de hachage, méthode d'authentification, etc.*
- **Etablissement d'Associations de Sécurité AH et/ou EPS (IPSec SA)** *Négociation aboutissant au moins à deux SA (une pour chaque sens de communication)*

Avantages et Inconvénients

Bien qu'IPSec soit un protocole jeune, de nombreuses mises en oeuvre existent.

- **Avantages**
  - Différents objectifs de sécurité possibles (confidentialité, authentification, intégrité)
  - Flexibles dans son paramètrage
  - Sécurité transparente pour les applications
  - Sécurisation de tout protocole situé au dessus d'IP
  - NAT (Network Address Translation) et PAT (Port Address Translation) possibles avec le protocole ESP
- **Inconvénients**
  - NAT et PAT impossibles avec le protocole AH
  - Interaction non normalisée entre le protocole d'échanges de clés et les infrastructures à clé publique (PKI)
  - Entorses propriétaires nuisibles à l'interopérabilité

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

- Conçu et développé par Netscape
- **En cours de standardisation** par l'IETF sous le nom de TLS
- **Entre la couche applicative et la couche TCP**
- TCP(Id. protocole : 6) – HTTP(Port : 80)
  TCP(Id. protocole : 6) – SSL/TLS – HTTPS(Port : 443)
- Actuellement à la version 3

Définitions

Connexion : moyen de transport associé à des *services sécurisés*
Session : association entre un client et un serveur ; plusieurs connexions sont possibles pour une même session

Services de sécurité

- **Authentification** : s'appuie sur *certificats électroniques X.509* (certificats des autorités de certification intégrés au navigateur) ; *obligatoire pour le serveur*, optionnelle pout le client ; utilisation de RSA (de même pour signer) ;
- **Confidentialité** : s'appuie sur algo. à clés symétriques négociées lors de la phase d'établissement de la session ; exemple d'algo. : IDEA, DES, 3DES...
- **Intégrité** : fondée sur fonction de hachage HMAC qui requiert une clé secrète partagée et une fonction de hachage primaire (MD5 ou SHA-x)
- **Non-rejeu** : couvert par l'utilisation de numéro de séquence

Protocoles utilisés pour son fonctionnement

- **Handshake** : établissement d'une connexion SSL avec authentification et négociation des paramètres cryptographiques
- **Record** : chiffrement et calcul d'empreinte
- **Alert** : échange de messages prédéfinis sur l'état d'une connexion SSL (e.g. fermeture d'une connexion, expiration d'un certificat)
- **CCS (Change Cipher Security)** : modification des paramètres d'une connexion SSL en cours

SSL/TLS et VPN

OpenVPN Project

- Licence GPL
- http://openvpn.net
- VPN qui implémente les couches 2 et 3 du modèle OSI et utilise le protocole SSL/TLS pour la sécurité
- Son avantage pratique : est accessible de tout point d'accès **wireless** qui autorise SSL alors que la plupart des autres VPN ne marche pas pour ce type d'accès

Avantages et Inconvénients

Protocole jeune, mais de nombreuses mises en oeuvre existent (commerce électronique, banque à distance)

- **Avantages**
  - Intégration dans tous les navigateurs du marché (Mozilla, Ms Internet Explorer, Opera...)
  - Etablissement rapide d'une session
  - Transparence : pas de contraintes pour l'utilisateur
  - Standardisation en cours
- **Inconvénients**
  - Authentification non obligatoire de l'utilisateur
  - Méthodes de sécurité peu sophistiquées pour des transactions demandant haut niveau de confidentialité
  - Modèle client-serveur insuffisant pour des services de paiement d'un site marchand incluant un tiers (une banque)

Secure SHell (SSH)

- la commande *ssh* est une **version sécurisée de** *rsh* (Remote Shell) et *rlogin*
- **Entre la couche applicative et la couche TCP**

Définition

Permet d'obtenir un interprète de commande (shell) distant sécurisé avec un système cible donné

Méthodes d'authentification et de chiffrement

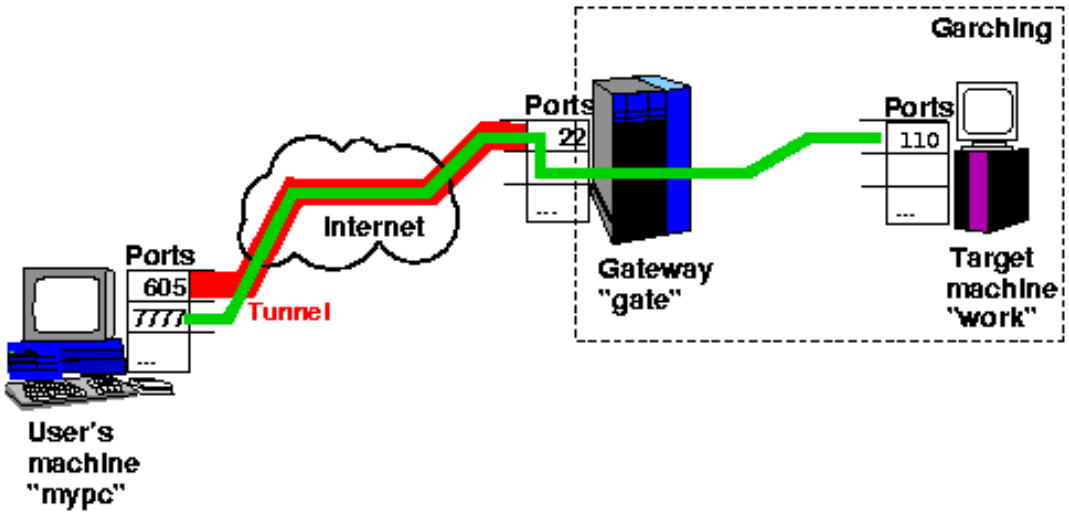
Authentification

- **Types de clés utilisées**
  - **Clé hôte** paire de clés asymétriques permettant l'authentification du serveur (*type de clé le plus courant*)
  - **Clé utilisateur** : paire de clés asymétriques permettant l'authentification de l'utilisateur
  - **Clé de session** : clé symétrique chiffrant le canal de communication (une pour chaque sens)
- **Mode d'authentification**
  - **Login** : lors de la connexion, transmission chiffrée du login/password de l'utilisateur au serveur qui vérifie l'identité clamée
  - **Jeu de clés publique/privé** :
  - **Rhosts** : le serveur stoque dans les fichiers */etc/rhosts* et *˜ /.rhosts* les sites clients certifiés à se connecter. Faille du système
  - **Certifications** X.509

Chiffrement : 3DES, IDEA (plus performant), Blowfish (très rapide) et AES (nouveau standard pour communications gouvernementales non secrètes)

Méthode de tunneling avec ssh

- Peut sécuriser d'autres protocoles avec sa fonctionnalité *port forwarding*
  Le flux de l'application considérée est encapsulé à l'intérieur du tunnel créé par la connexion (session) *ssh*
- Non adapté pour VPN (connexion à un seul serveur) mais tunnels ok



Exemple de pop sécurisé : à l'aide de la commande
ssh -l userpipo -L 7777:work:110 gate
Je me connecte au serveur *pop* (port 110) de la machine *work* se trouvant derrière la machine *gate*

Avantages et Inconvénients

Protocole jeune, mais de nombreuses mises en oeuvre existent (administration de système, transfert sécurisé de données)

- **Avantages**
  - Remplace les fameuses commandes Remote : *rsh* et *rlogin* par *ssh*, *rcp* par *scp*, *ftp* par *sftp*
  - Authentification par clés asymétriques des serveurs et utilisateurs
  - Chiffrage et compression de la connexion
  - Redirection possible (*forward*) de tout flux TCP dans tunnel sécurisé
  - Renforcement de la sécurité des accès et de l'administration des serveurs sensibles
- **Inconvénients**
  - Incompatibilités entre différentes versions de *ssh*
  - Accès par SSH à une machine interne donne aussi accès par tunnel SSH à toutes les autres machines internes et tous les protocoles (possibilité de bloquage des relais par un pare-feu)
  - Avenir incertain face à IPSec, qui peut chiffrer et authentifier des protocoles IP/TCP/UDP et partie intégrante d'IPv6

Quizz de synthèse

- Qu'est ce qu'un Virtual Private Network ? Donner deux situations montrant son utilité.
- Quels sont les critères qui me pousseront à choisir tel ou tel protocole sécurisé et pas un autre ?
- Donner au moins 3 avantages du protocoles IPSec