Communications sécurisées – Protocoles sécurisants

Nicolas Hernandez

Cours de DUT informatique – 2ème année
IUT de Nantes – Département Informatique
2006 – 20**

Nantes, le February 1, 2021

Sommaire

Sécuriser une communication ? l.e comment assurer...

- Confidentialité des données contre des attaques de type packet sniffing (renifleur)
- Authentification d'une source (expéditeur d'un message ou bien personnel distant demandant un accès (site à site, nomade filaire, wifi, etc.) contre des attaques de type man-in-the-middle (MAC spoofing (usurpation), ARP Replay Attack...)
- Intégrité d'un message contre des attaques de type message alteration

Réseau Privée Virtuel

Définition

Virtual Private Network (VPN) : utilisation de protocoles sécurisants pour la création d'un canal de communication sécurisé à **usage privé**, au travers d'un **réseau public**[1] non sécurisé

- Cas d'usage : mis en oeuvre par une organisation 1) pour assurer la *sécurité* des échanges notamment pour l'**interconnexion de ses différents sites géographiques via Internet**
  2) ou bien pour **autoriser des utilisateurs nomades**
- Utilisation de protocoles sécurisants de **tunneling** (e.g. L2TP, IPsec, SSL/TLS)

[1] 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

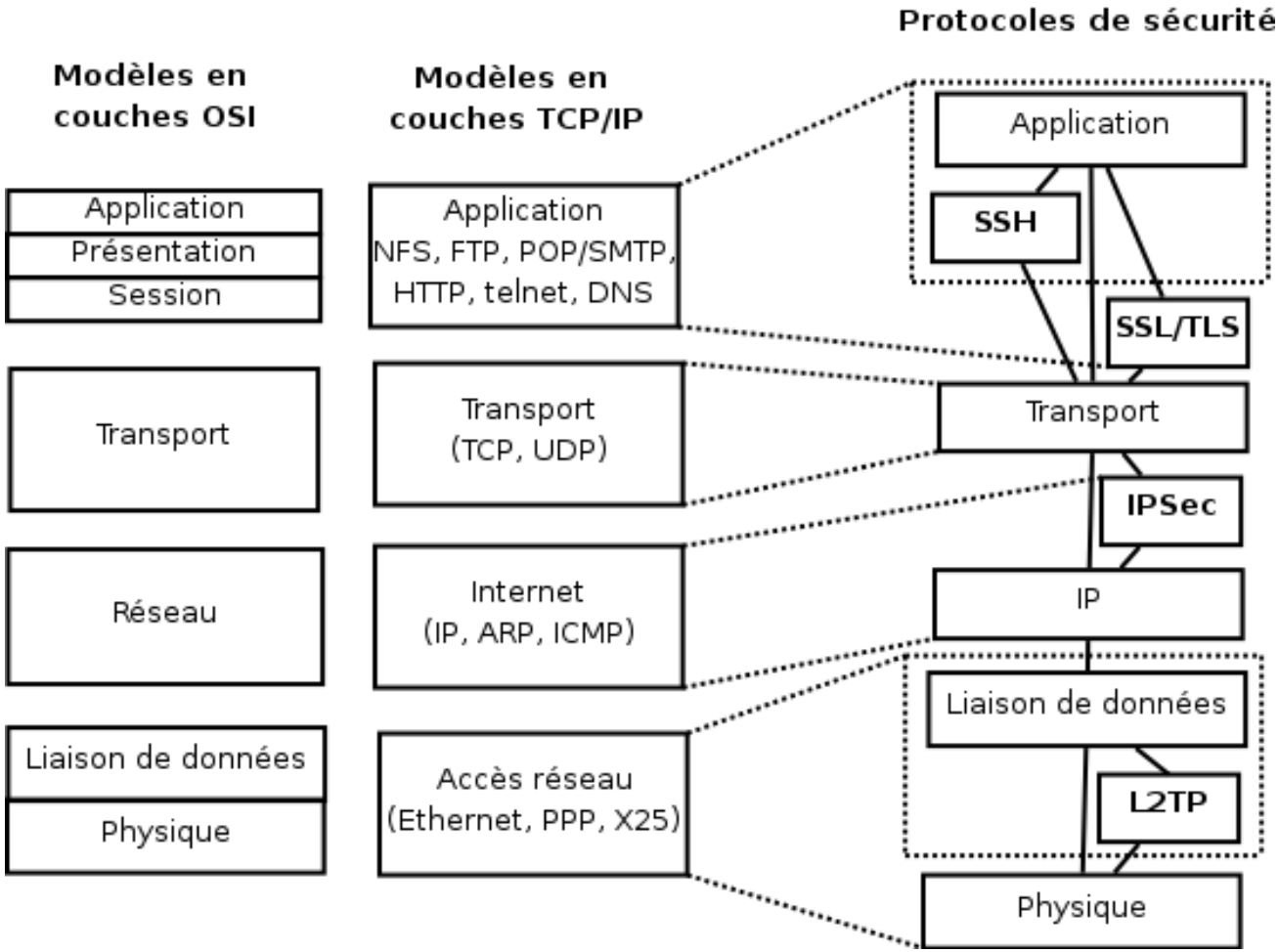
Tunnels

Définition

Tunneling Protocoles : protocole réseau qui encapsule (transporte) un autre protocole

- En pratique, encapsuler signifie rajouter un en-tête qui renseigne comment traiter les données transportées et à qui les adresser
- On peut mettre en place un tunnel indépendamment d'un VPN

Protocoles sécurisants en fonction des couches OSI



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

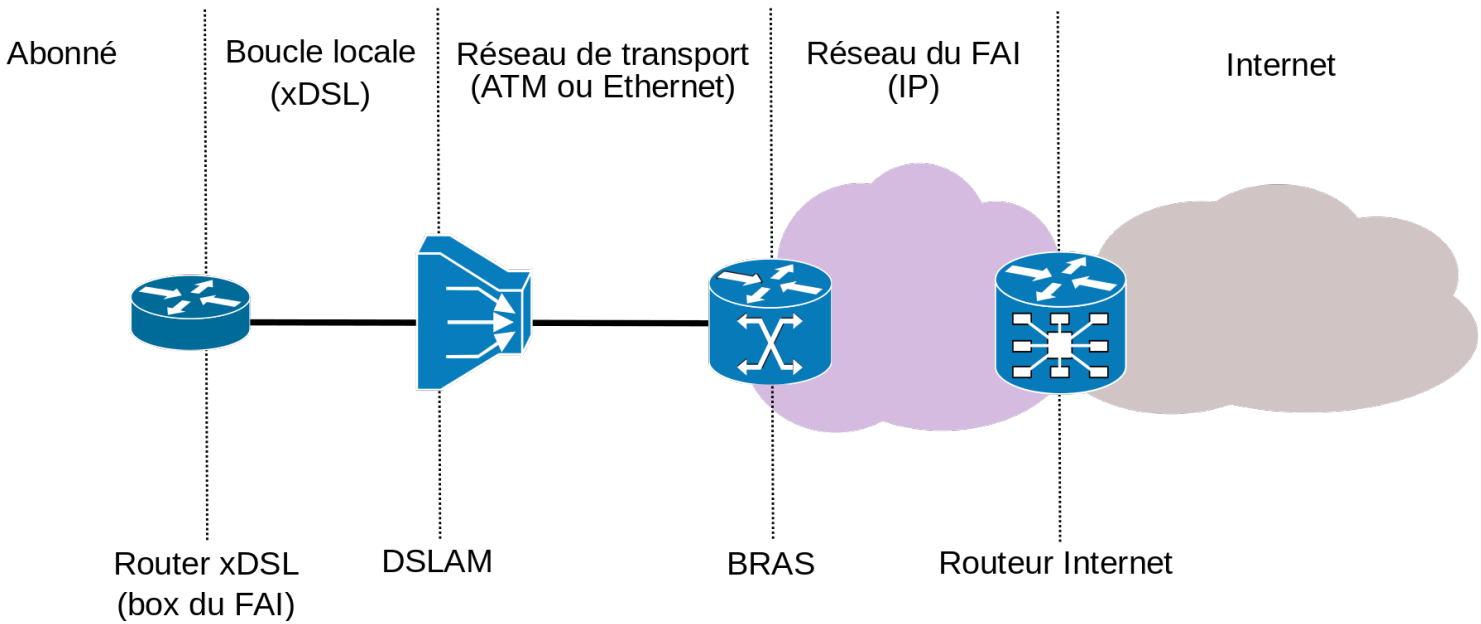
- Une entreprise choisira niveau 3 OSI car ne maîtrise pas les artères de connexion (niveau 2 OSI) entre plusieurs sites géographiques
- Un ISP[2] d'accès xDSL pourra choisir niveau 2 OSI pour l'accès à Internet...

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

Sommaire

Schéma d'un raccordement xDSL

Même principe pour les raccordements finaux avec des liaisons de très haut débit (fibre, câble...)



Scénario le plus simple (cas pour les grands opérateurs) : DSLAM et BRAS sont possédés par le FAI

Equipements de raccordement

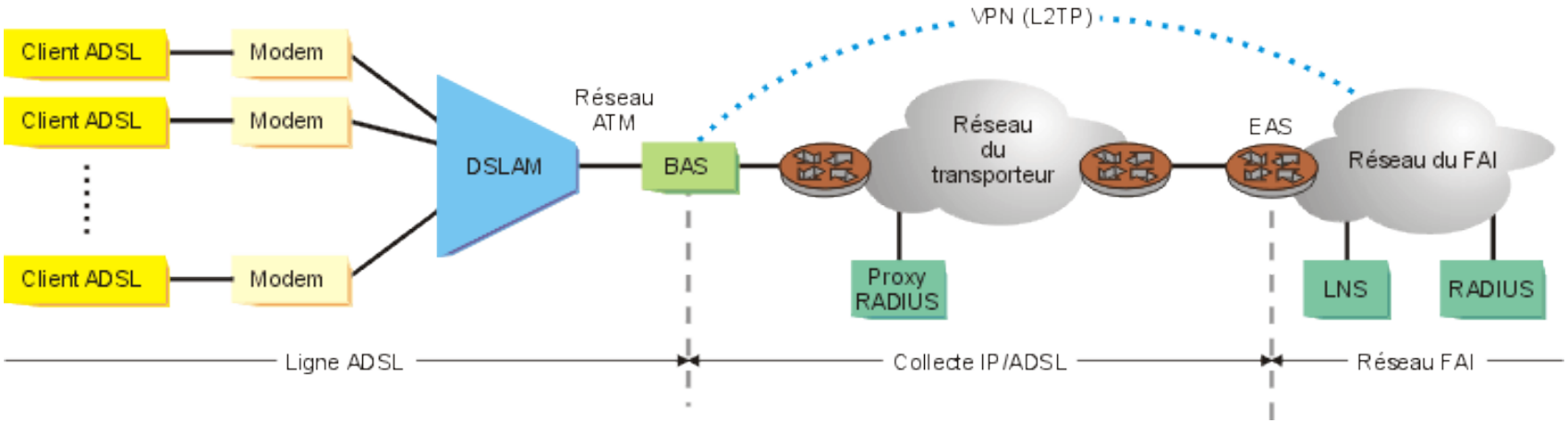
- Routeur chez abonné (box du FAI) conçu pour une technique d'acheminement de données numériques vers l'Internet (DSL, fibre...)
  Si raccordement est téléphonique on parle de Modem, convertit données numériques en signaux analogiques par *modulation* d'amplitude/fréquence
- *Digital Subscriber Line Access Multiplexer* (DSLAM)
  - "entonnoir" qui rassemble/converge flux des abonnés en un seul lien à fort débit (i.e. fibre optique) par multiplexage[3]
  - possédé par Orange ou par FAI (si dégroupage)
  - Selon la place, accueilli dans local des Noeuds de Raccordements d'Abonnés (NRA)
- *Broadband (Remote) Access Server* (B(R)AS), gère l'authentification du client auprès du FAI (via serveur/proxy RADIUS) et la transmission des paramètres IP
- Routeur du FAI pour s'interconnecter à d'autres réseaux

[3] technique pour faire passer plusieurs informations à travers un seul support de transmission e.g. temporelle, fréquentielle

Layer 2 Tunneling Protocol (L2TP) 1/3

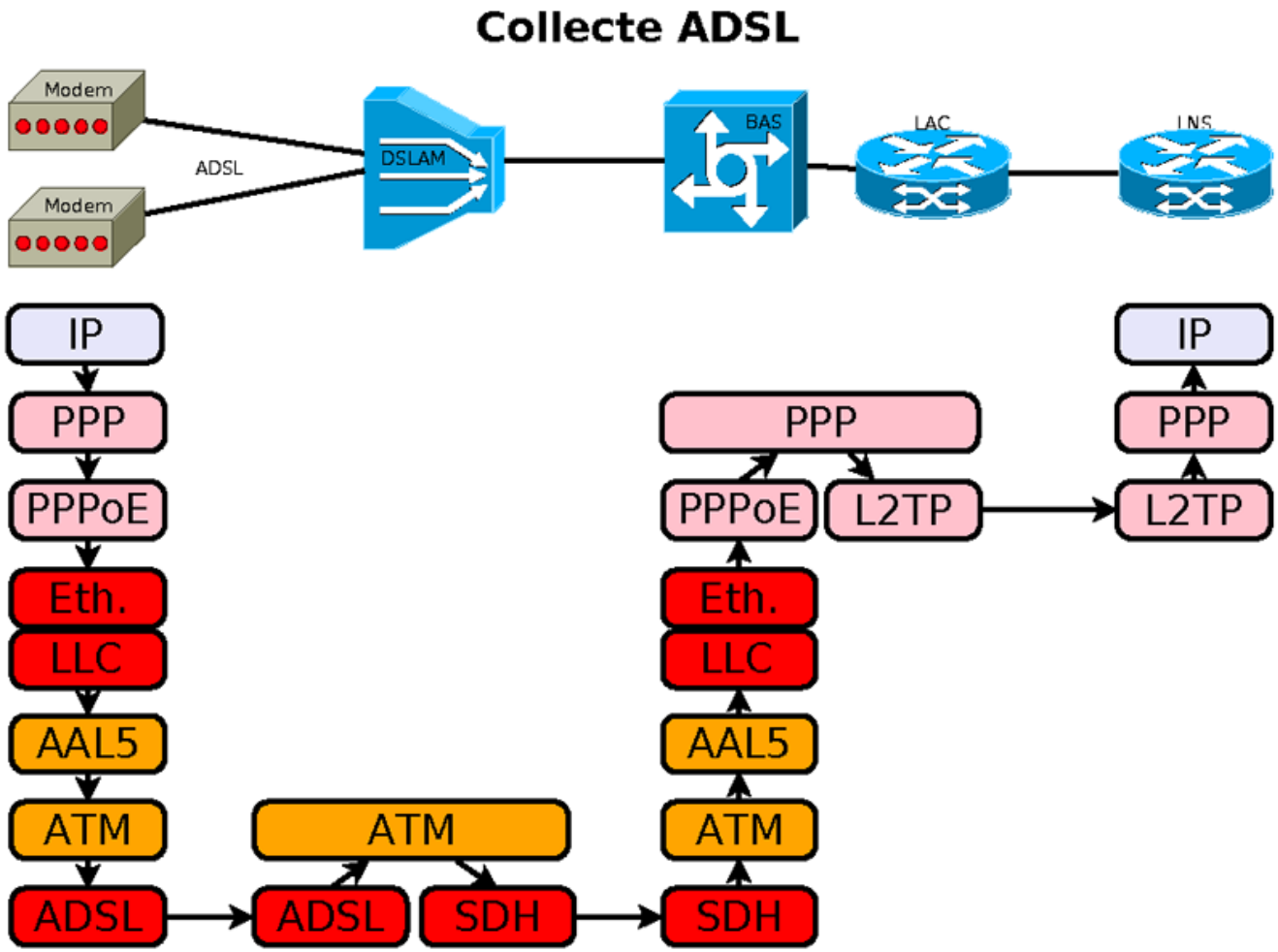
Si FAI ne possède pas de DSLAM et de BAS (i.e. n'a pas de liaison directe avec l'abonné), l'opérateur, propriétaire de l'infra, offre tunnélisation de niveau 2/Liaison OSI pour transporter les données de l'abonné au réseau du FAI

- Des trames PPP du modem au BAS...
- ...encapsulées dans des trames L2TP via deux serveurs :
  - le Concentrateur d'Accès L2TP (L2TP Access Concentrator (LAC)) situé au niveau du BAS
  - et le Serveur Réseau L2TP (*L2TP Network Server (LNS)*) situé dans le réseau du FAI derrière Équipement d'Accès au Service (EAS)



Crédit http://christian.caleca.free.fr/adsl/

Layer 2 Tunneling Protocol (L2TP) 2/3



Layer 2 Tunneling Protocol (L2TP) 3/3

- L2TP, protocole de tunneling (Virtual Private Network (VPN)) de niveau 2/Liaison OSI, fusion des protocoles L2F (Layer 2 Forwarding) de Cisco et PPTP (Point to Point Tunneling Protocol) de Microsoft
- En 1999, défini pour transporter des sessions PPP (RFC 2661),
- généralisé ensuite en 2005 (RFC 3931) pour transporter n'importe quel protocole de niveau 2 (e.g. Ethernet, ATM) entre deux noeuds IP (L2TPv3)
- Entre le LAC et le LNS, si le réseau est IP, les trames L2TP peuvent être encapsulés de l'IP/UDP
- L2TP offre intégrité et authentification d'origine. Si le réseau traversé par le tunnel n'est pas sûr, pour assurer la confidentialité, L2TP est utilisé avec IPsec

Avantages et Inconvénients

- **Avantages**
  - L2TP offre intégrité et authentification d'origine et avec IPsec on a la confidentialité
  - Usage de UDP (a contrario de TCP) rend L2TP plus rapide et facile à configurer avec certains pare-feux
- **Inconvénients**
  - En mode confidentiel, requiert le temps de 2 encapsulations (L2TP et IPsec)
  - Beaucoup de configuration pour utiliser avec IPsec (gestion de tiers de confiance PKI pour l'authentification des parties communicantes...)

Sommaire

Internet Protocol Security (IPSec)

Suite de protocoles ouverts pour la sécurisation des communications

via Internet Protocol (IP) i.e. couche 3 OSI

Motivation initiale : résoudre faiblesses de sécurité d'IPv4 (authentification et confidentialité) ; intégré à IPv6

Sécurisation de flots de données entre machines (host-to-host), entre passerelles (network-to-network), entre une passerelle et une machine (network-to-host)

Par sécurisation , on entend : peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection

Standard de l'IETF (créé en 1995 puis amélioré et étendu, e.g. `rfc4301` de 2005)

Deux modes de fonctionnement : Transport et Tunnel

Mode Transport

- usage : host-to-host
- un en-tête (*header*) IPSec s'intercale entre l'en-tête IP et les données sans modifier l'en-tête IP d'origine
- seulement la partie données est chiffrée et/ou authentifiée
- initialement des limites pour du PAT

Mode tunnel

- VPN (network-to-network), network-to-host, host-to-host (private chat)
- encapsule l'intégralité du paquet IP original dans un paquet IPSec auquel on ajoute un nouvel en-tête IP
- la totalité du paquet IP est chiffrée et/ou authentifiée

Des protocoles d'en-tête pour différents services de sécurité

Authentication Headers (AH) :

- assure authentification des datagrames IP
- intégrité des *données* et des *en-têtes IP*[4] ;
- protection aussi contre le rejoue

Encapsulating Security Payloads (ESP) :

- En plus d'une en-tête, ajoute une remorque (*trailer*) après données, garantie confidentialité et intégrité des *données et de la remorque*
- Authenticité possible de l'*en-tête IP*, des *données* et de la *remorque* en ajoutant une seconde *remorque*
- Protection aussi contre le rejoue

Peuvent se combiner

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

Protocoles AH et ESP et algorithmes cryptographiques

HMAC-SHA1 intégrité et authentification

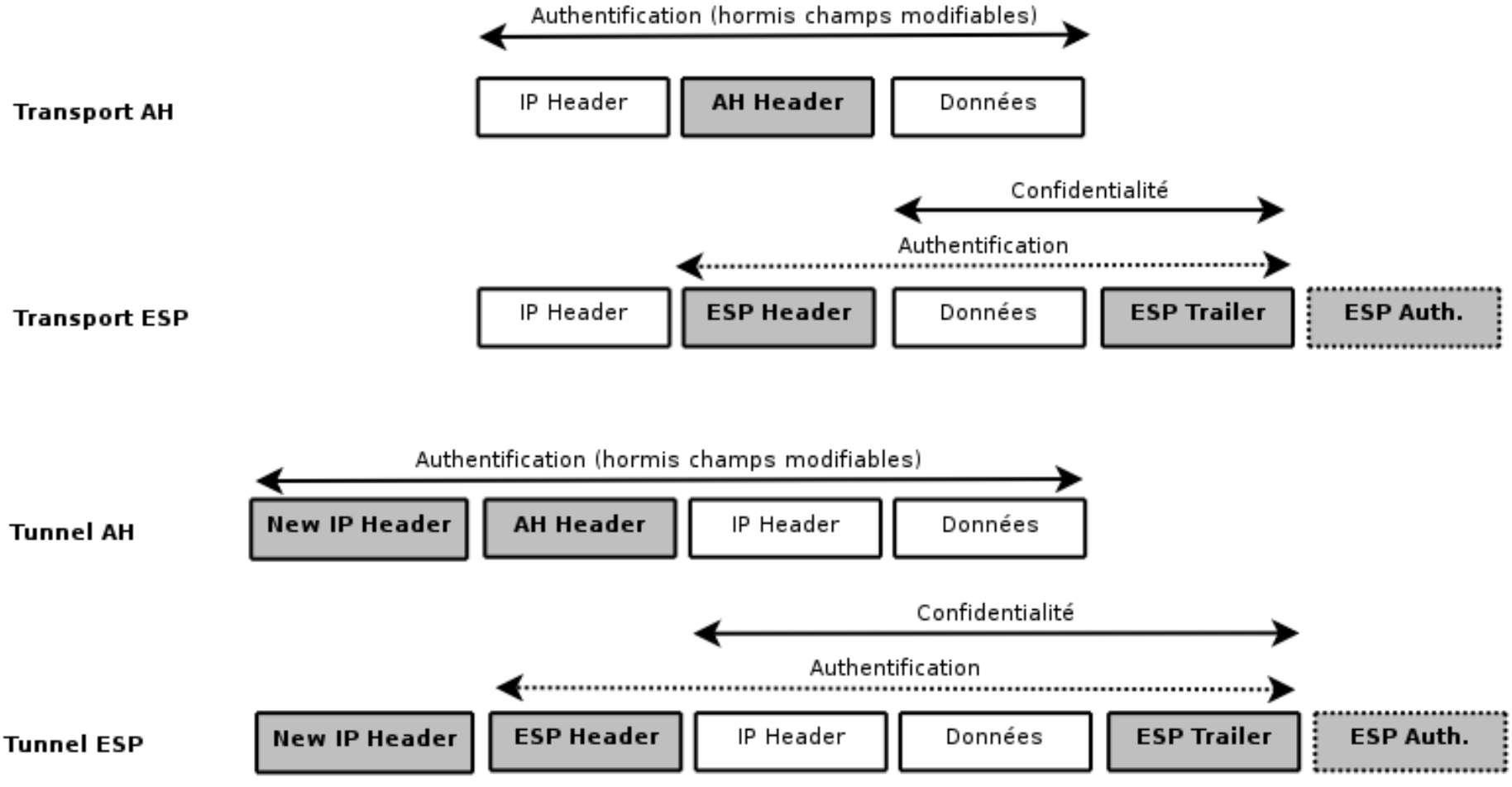
TripleDES-CBC confidentialité (clé secrète)

AES-CBC confidentialité (clé secrète)

AES-GCM confidentialité (clé secrète) et authentification

RFC 7321

IPSec : modes et protocoles



Comment les intéressés négocient la sécurité de leur communication ?

A Security Association (SA)

correspond à l'ensemble de paramètres partagés entre les entités du réseau souhaitant communiquer : choix des opérations de sécurité (AH/ESP), mode de transport (tunnel/transport), algorithmes, clés de chiffrements...
I.e. Choix de configuration pour un sens de la connexion

Pour établir des Security Association

Internet Security Association and Key Management Protocol (ISAKMP) :
permet 1) d'établir/négogier/modifier/effacer/gérer des *security associations* 2) gérer des clés

ISAKMP requiert d'autres protocoles pour échanger des clés

(souvent Transport UDP et port 500)

Internet Key Exchange (IKE) est une des implémentations largement utilisées avec ISAKMP pour l'échange de clés

v1 en 1998, v2 en 2010, RFC la plus récente : `RFC7321` (2014)

Etablissement d'**A**ssociations de **S**écurité (**SA**)

IKE (Internet Key Exchange)

(v2) protocole permettant à deux entités de négocier les algorithmes et les clés à utiliser pour s'assurer une communication sécurisée

Fonctionne en 2 phases

1. **Etablissement d'une Association de Sécurité IKE (IKE SA)** : définit le paramétrage de la SA et gère l'échange d'un secret ; génère un secret partagé soit à partir d'un secret déjà partagé, soit par Diffie–Hellman, soit généré par l'un et échangé via certificat (clé asym). De ce secret est généré 3 clefs : 1) l'authentification 2) chiffrement des communications IKE et 3) pour phase 2
2. **Etablissement d'Associations de Sécurité AH et/ou ESP (IPSec SA)** Négociation aboutissant au moins à deux SA (une pour chaque sens de communication) ; utilise la clé générée en phase 1 pour générer des clefs de session

Développé pour IPSec mais ouvert à d'autres protocoles

Avantages et Inconvénients

- **Avantages**
  - Permettent de créer des *Réseaux Privées Virtuels*
  - Différents objectifs de sécurité possibles (confidentialité, authentification, intégrité)
  - Flexibles dans son paramétrage
  - Installé sur routeur/pare-feu, sécurisation de tout protocole situé au dessus d'IP : transparent pour les applications
  - NAT (Network Address Translation) et PAT (Port Address Translation) possibles avec le protocole ESP
- **Inconvénients**
  - NAT et PAT avec contraintes avec le protocole AH
  - Performance de communication impactée par les opérations de sécurisation
  - Difficulté de configuration de la traversée des NAT et pare-feu
  - Clients IPsec souvent incompatibles, nuit à l'interopérabilité

Sommaire

Transport Layer Security (TLS)

- Entre la couche Transport TCP et la couche Application
- Conçu et développé par Netscape et connu sous le nom de Secure Socket Layer (SSL)
- Standardisé par l'IETF sous le nom de TLS
- TCP(Id. protocole : 6) – HTTP(Port : 80)
  TCP(Id. protocole : 6) – SSL/TLS – HTTPS(Port : 443)
- SSL v3 = TLS v1 en 1999, v1.3 en 2018 (RFC 8446)

Services de sécurité

- Négociation et échange de clés Diffie–Hellman (DHE) et sa version *elliptic-curve Diffie–Hellman* (ECDHE)
- Authentification : s'appuie sur certificats électroniques X.509 (certificats des autorités de certification intégrés au navigateur) ; obligatoire pour le serveur, optionnelle pour 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 ; Advanced Encryption Standard (AES)
- Intégrité : S'appuie sur l'*authenticated encryption with associated data (AEAD)*, forme de chiffrement qui assure simultanément la confidentialité et l'authenticité
- Non-rejeu : couvert par l'utilisation de numéro de séquence

Protocoles utilisés pour son fonctionnement

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

TLS et VPN

OpenVPN Project

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

Avantages et Inconvénients

Protocole de facto pour le commerce électronique, banque à distance

- **Avantages**
  - Intégration dans tous les navigateurs du marché (Chrome, Firefox, MS Internet Explorer TLS v1.3 depuis août 2020...)
  - Etablissement rapide d'une session
  - Transparence : pas de contraintes pour l'utilisateur
  - TLS V1.3 profite de 20 ans d'expérience... handshake désormais rendu confidentiel, réduction des primitives cryptographiques (large nombre à l'origine de failles)
- **Inconvénients**
  - Authentification non obligatoire de l'utilisateur
  - Modèle client-serveur insuffisant pour des services de paiement d'un site marchand incluant un tiers (une banque)

Sommaire

Secure SHell (SSH)

Définition

Permet d'obtenir, après authentification, un interprèteur de commande (shell) au bout d'un canal confidentiel sur un système cible donné (en théorie distant mais soi-même possible)

- la commande *ssh* est une version sécurisée de *rsh* (Remote Shell) et *rlogin* (Remote Login)
- une application au niveau Application OSI

Méthodes d'authentification et de chiffrement

- Le mode d' authentification le plus classique est celui qui fait appel aux paires de clés asymétriques.
  - Pour ce faire, installer sa clé publique sur les systèmes où l'on souhaite se connecter.
  - Localement on pourra protéger la clé privée par un mot de passe.
- Le chiffrement du canal de communication repose sur l'usage d'une clé symétrique (une pour chaque sens)

  telle que 3DES, IDEA (plus performant), Blowfish (très rapide) et AES

Accès à un shell distant de manière sécurisée avec ssh

- Un serveur *ssh* doit tourner sur la machine distante.
  Le port d'écoute par défaut est 22
- Le client doit avoir un compte sur la machine où tourne le serveur
- `ssh -l login hostname`
  ou bien
  `ssh login@hostname`
  avec *login* le username du compte sur le serveur et *hostname* l'adresse IP du serveur
- A la demande de connexion, le mot de passe du compte *login* sur le serveur distant est demandé

`netstat -taupe | grep ESTABLISHED`
permettra de voir les connexions établies notamment celles avec *ssh*

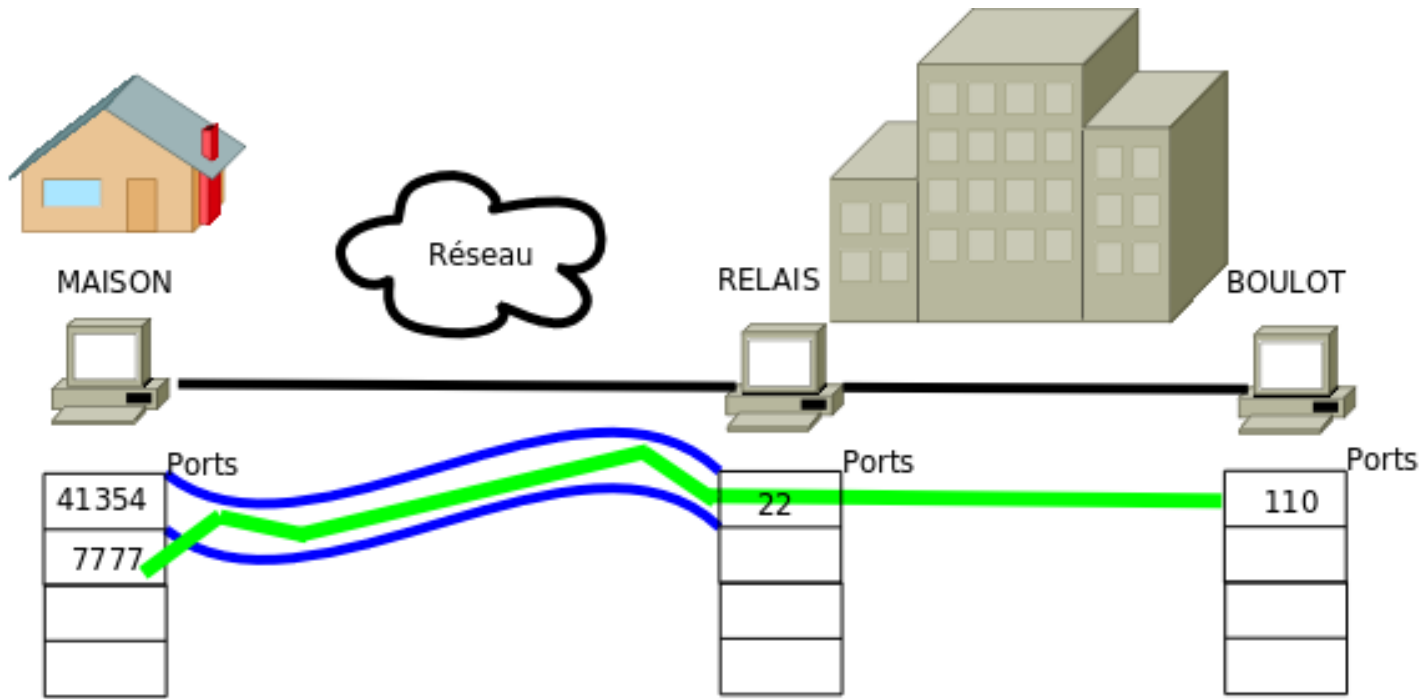
Méthode de tunneling avec ssh

- 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

Méthode de tunneling avec ssh

Exemple d'accès du domicile, machine MAISON, à un serveur *pop* (port 110) sur la machine BOULOT se trouvant derrière la machine *RELAIS* au sein de l'entreprise :

```
ssh hernandez@RELAIS -L 7777:BOULOT:110
```



L'accès au serveur mail de BOULOT à partir de MAISON est ainsi sécurisé, un client mailer sur MAISON peut se connecter sur le port local 7777 et les communications seront redirigés avec un rebond vers BOULOT

Avantages et Inconvénients

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
  - Chiffrement 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)

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