SISR 4-5

4.0

PACOME MASSOL

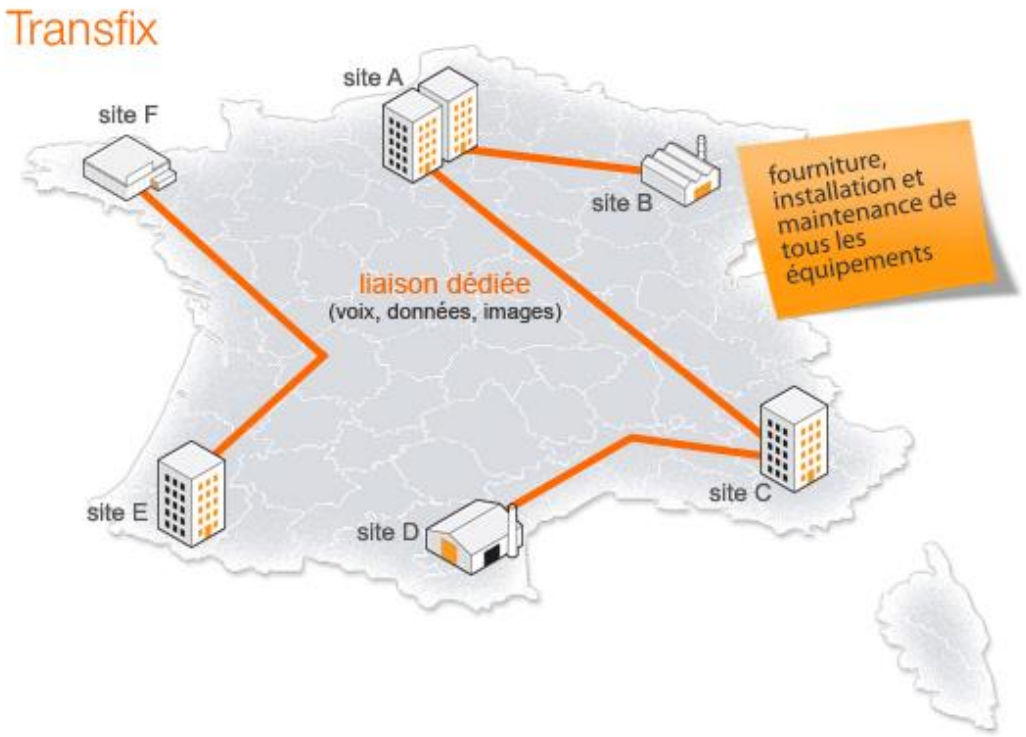
Table des matières

Cours : Accès distant

Objectifs

Présenter différentes technologies liées à l'accès distant
Interconnexion de sites

Historiquement, les liaisons entre sites d'une entreprise étaient louées auprès d'opérateurs :



Avantages	Inconvénients
Sécurisé	Dépendant de l'opérateur
Débit garantit	Point à point

De nos jours, Internet est largement utilisé. En fonction des besoins, différentes technologies sont mises en œuvre.

A. Supports

Les supports de communication en accès distant les plus répandus sont :

- filaire : cuivre (paire téléphonique) et fibre optique ;
- sans-fil : ondes radio.

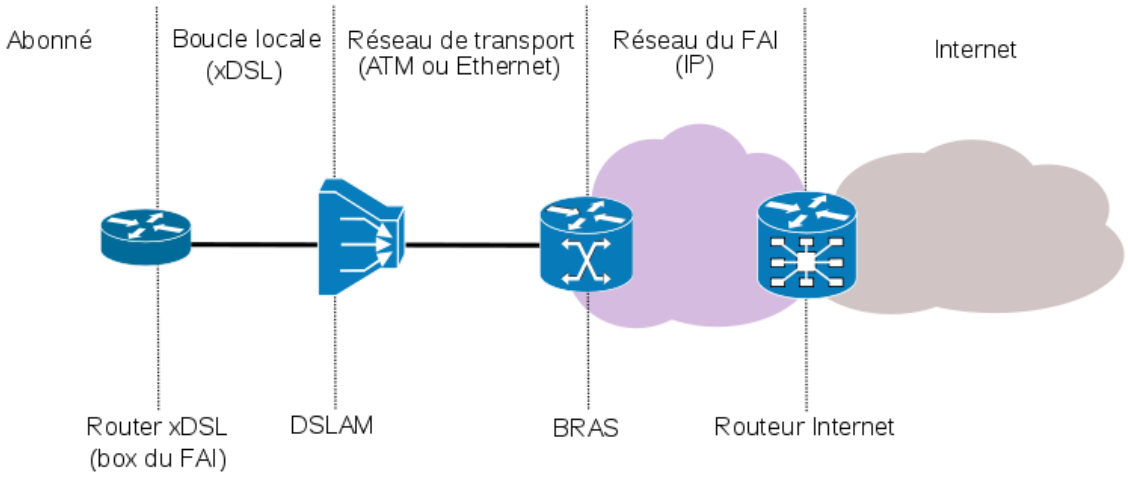
B. Niveau OSI1

1. Sur réseau téléphonique (cuivre)

Le réseau téléphonique est utilisé par les technologies xDSL :

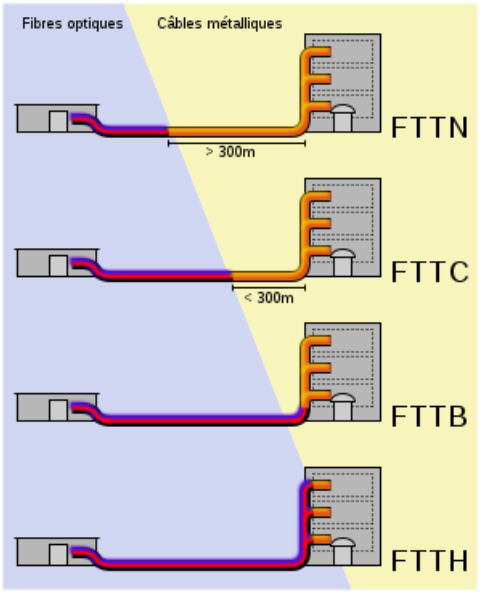
- ADSL : débit asymétrique, faible en upload, peu de garanties
- SDSL : débit symétrique par tranche de 2Mbps cumulables, garanties
- VDSL : améliore l'ADSL au niveau débit et distances

Le schéma général d'une connexion xDSL est le suivant :



2. Fibre optique

La fibre optique permet de couvrir de grandes distances et un bon débit :



La fibre peut arriver plus ou moins des locaux. Voir : *https://fr.wikipedia.org/wiki/FTTx*[1]

3. Sans-Fil

Ces technologies permettent de couvrir des zones non desservies par l'ADSL ou la fibre :

- WiMAX
- 3G, 4G
- Satellite

Elles peuvent également servir de liaison de secours lorsque la connexion filaire est indisponible.

[1] https://fr.wikipedia.org/wiki/FTTx

Exemple

Exemple d'un routeur avec bascule automatique entre ADSL et 4G :

C. Niveau OSI2

Au-dessus des supports de communication présentés ci-dessus, différents protocoles sont utilisés. Parmi les plus répandus :

1. PPP

Point-to-Point Protocol (PPP, protocole point à point) est un protocole de transmission pour l'internet qui permet d'établir une connexion entre deux hôtes sur une liaison point à point :

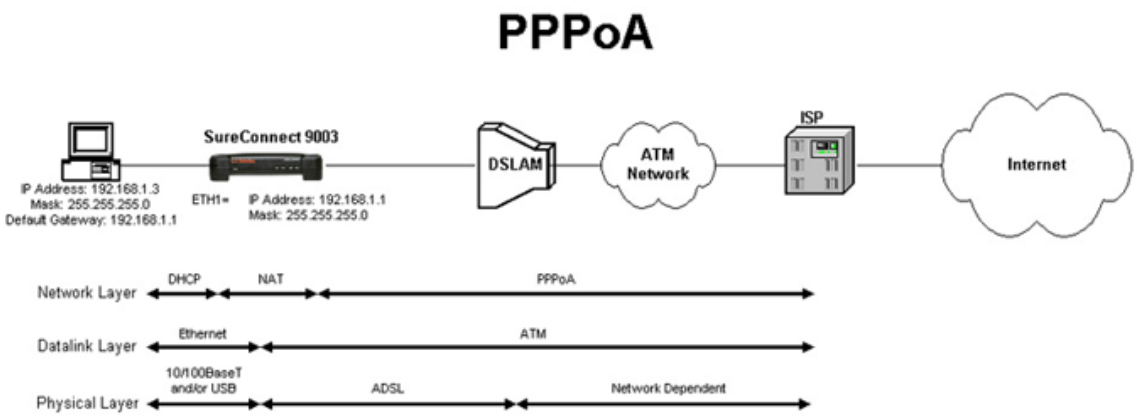
- prend en charge des mécanismes d'authentification, comme PAP ou CHAP ;
- permet l'agrégation de lien (on parle de PPP Multilink) ;
- permet la compression des données.

Il est soit directement basé sur HDLC (connexion RTC), soit encapsulé (par exemple PPPoX, utilisé par les connexions ADSL et câble). Suivant l'opérateur, PPPoX se décline en :

- PPPoA (encapsulé dans ATM) ;
- PPPoE (encapsulé dans Ethernet)

Exemple : PPPoA

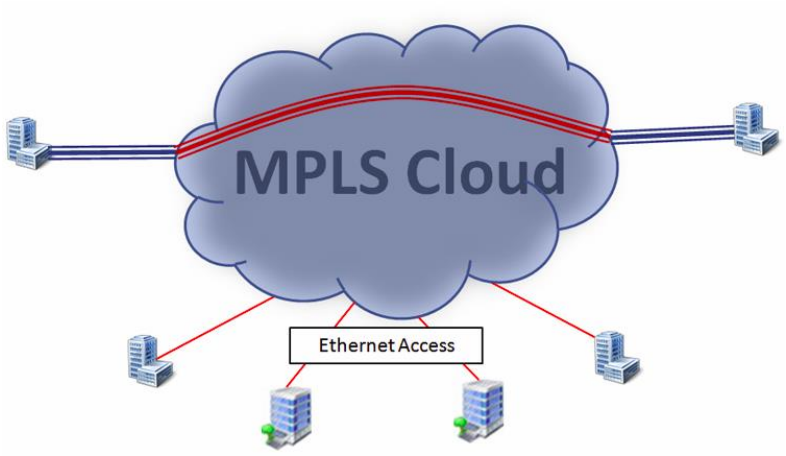
Le schéma suivant (source : USR) montre bien l'usage des différents protocoles (PPPoA dans l'exemple) :



2. Ethernet

Ethernet étant universellement répandu dans les entreprises, il peut être pratique d'utiliser ce protocole de bout en bout. On parle de **convergence** ou de **LAN étendu**.

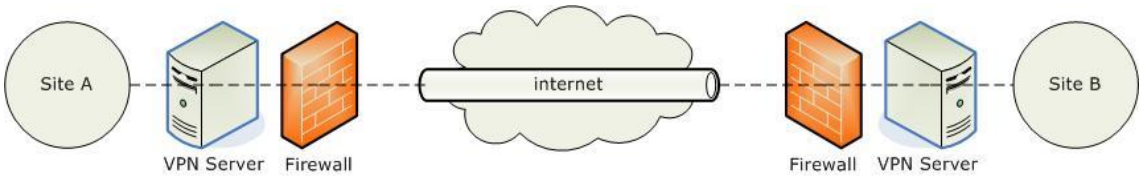
Ce type de réseau est basé sur VPLS (*Virtual Private LAN Service*) qui est un service Ethernet multipoint-à-multipoint et fonctionne au-dessus d'un réseau IP (comme Internet par exemple) muni d'un mécanisme de tunnel (en général MPLS pour *MultiProtocol Label Switching*)



Avantage = tunnel (communications chiffrées) et multipoint.

3. VPN

Dans un VPN (*Virtual Private Network*), on retrouve la notion de tunnel :



Les principaux protocoles de VPN au niveau OSI 2 sont les suivants :

- PPTP (*Point-to-Point Tunneling Protocol*) développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- L2TP (*Layer Two Tunneling Protocol*) est l'aboutissement des travaux de l'IETF (RFC 2661) pour faire converger les fonctionnalités de PPTP et L2F. Il s'appuie sur PPP.

Remarque

Suivant le protocole utilisé, un VPN peut aussi agir au niveau OSI 3.

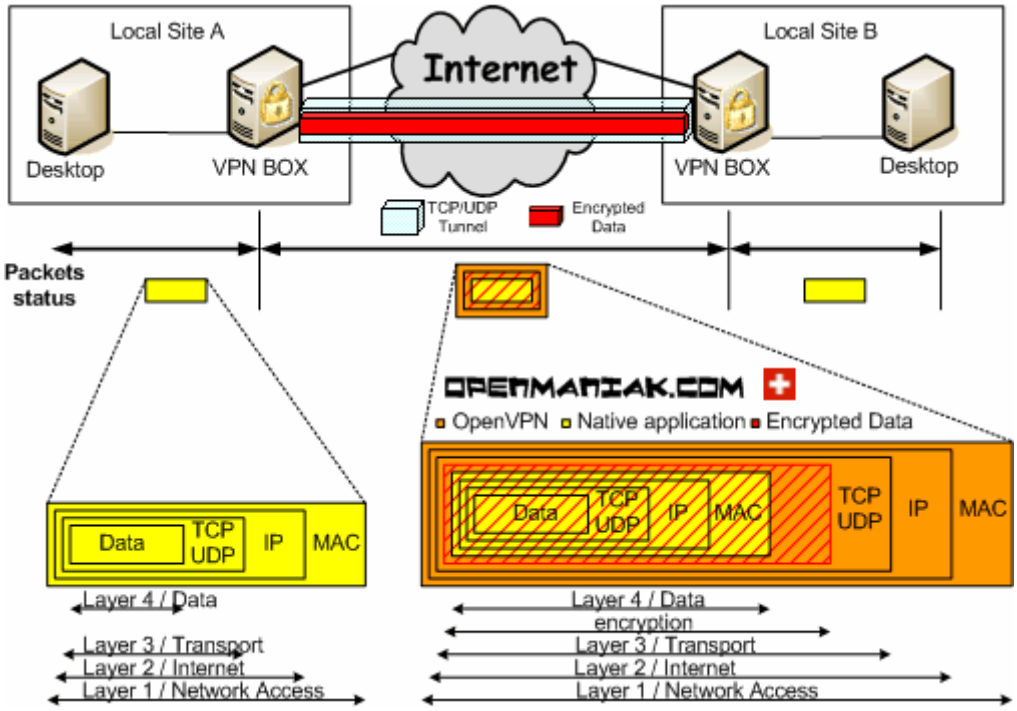
D. Niveau OSI3+

Les VPN de niveau 3 utilisent les protocoles suivants :

- IPSec, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP
- SSL/TLS (idem https) : par exemple, mis en oeuvre par *OpenVPN*[2] (inclus dans pfSense)

Lorsque les paquets (en clair) sortent du réseau local pour passer dans le VPN, ils sont chiffrés puis **encapsulés** dans un paquet TCP ou UDP à destination de l'autre côté du tunnel.

[2]https://openvpn.net/



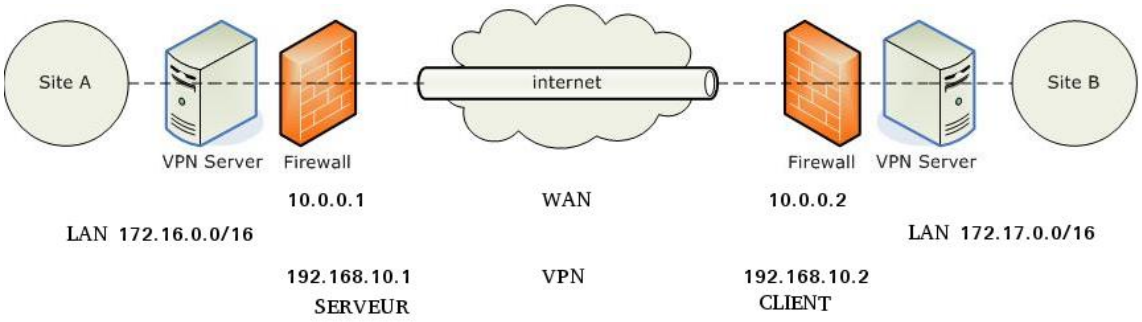
A la réception, le logiciel de VPN qui dispose de la clé, extrait les données chiffrées, déchiffre et envoie le paquet en clair sur le réseau local.

TP : VPN

Objectifs
Installer et configurer un VPN en mode "point-à-point"

A. Mise en oeuvre

Exemple de VPN en mode "point-à-point" avec OpenVPN :



Remarque

Fonctionne en mode client-serveur : un OpenVPN est serveur, l'autre client

Lorsque le VPN est actif, 1 interface virtuelle est créée et dispose de son propre adressage

En labo physique

Topologie à mettre en place des deux côtés :

1 PC physique représente le "LAN" connecté à

1 boîtier pfSense pour le pare-feu et le VPN

En pur Virtualbox

Deux VM pfSense reliées par un réseau Virtualbox interne spécifique.

B. Configuration du OpenVPN serveur

Question

Configurer le premier pfSense en mode serveur OpenVPN.

C. Configuration du OpenVPN client

Question

Configurer le deuxième pfSense en mode client OpenVPN.

D. Tests / Validations

Question 1

Vérifier l'état de la connexion sur le client OpenVPN. Est-ce que cela fonctionne ?

Question 2

Si on suppose que client et serveur VPN sont bien configurés, où peut-on trouver dans pfSense des informations pour nous aider ?

Question 3

Que faire pour y remédier ?

Question 4

Est-ce que la connexion est établie maintenant ?

Question 5

Sur le client, allez dans "Diagnostics / ping". Essayez d'envoyer des pings sur l'interface de l'autre pfSense côté LAN 172.16.0.x. Est-ce que cela fonctionne ?

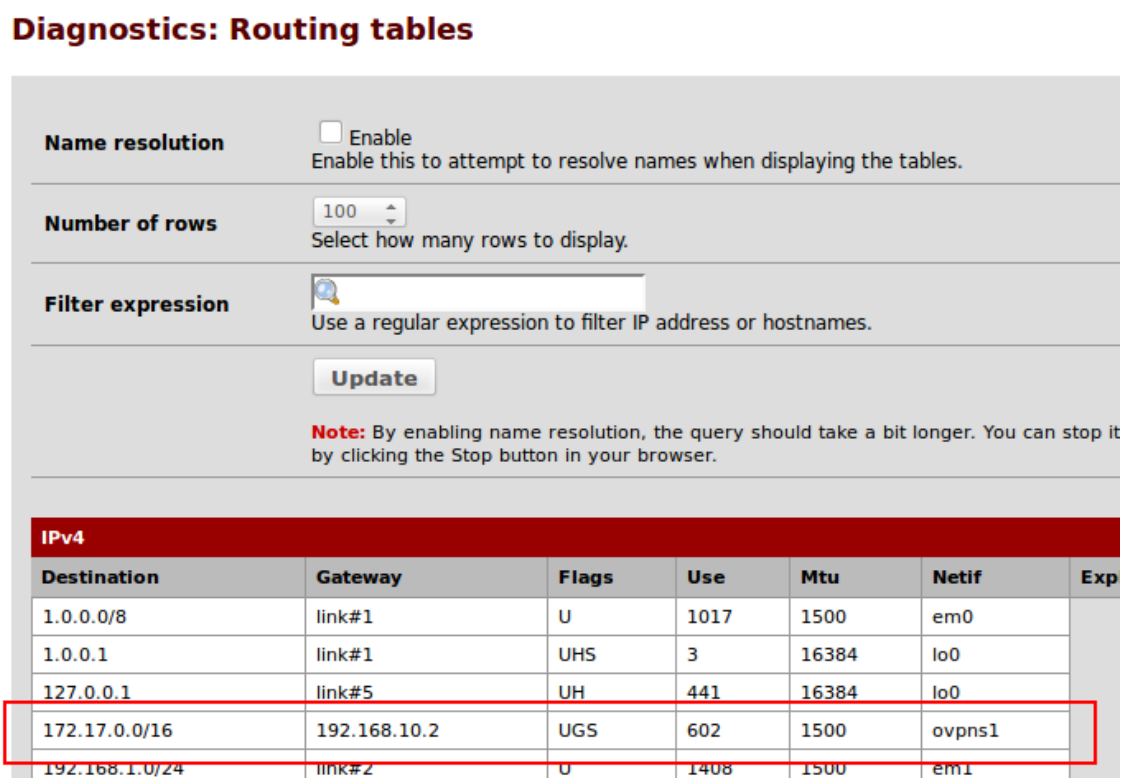
Question 6

Encore le pare-feu qui bloque. Sur le client et le serveur, créez une règle de pare-feu affectée à l'interface réseau OpenVPN autorisant tout type de trafic.

E. Vérifications / validations

Les pings doivent passer dans les deux sens.

On vérifie la table de routage. Par exemple, sur le serveur :



On a bien une route qui explique que depuis le serveur VPN pour joindre le réseau 172.17.0.0/16, on doit passer par l'interface openvpns1, donc dans le tunnel.

Lancez un ping infini depuis une machine derrière le serveur VPN vers une machine derrière le client VPN. Allez dans "Diagnostics / Packet capture". Si vous capturez sur l'interface WAN, vous voyez ce type de trafic (le ping chiffré) :

```
1 10:17:28.701342 IP 1.0.0.2.11572 > 1.0.0.1.1194: UDP, length 132
2 10:17:28.701985 IP 1.0.0.1.1194 > 1.0.0.2.11572: UDP, length 132
3 10:17:29.702530 IP 1.0.0.2.11572 > 1.0.0.1.1194: UDP, length 132
4 10:17:29.703076 IP 1.0.0.1.1194 > 1.0.0.2.11572: UDP, length 132
```

Par contre, si vous capturez sur l'interface OpenVPN, vous voyez ce type de trafic (le ping en clair) :

```
1 10:17:47.729685 IP 172.17.0.101 > 172.16.0.1: ICMP echo request, id 2546, seq 35,
  length 64
2 10:17:47.730822 IP 172.16.0.1 > 172.17.0.101: ICMP echo reply, id 2546, seq 35,
  length 64
3 10:17:48.732046 IP 172.17.0.101 > 172.16.0.1: ICMP echo request, id 2546, seq 36,
  length 64
4 10:17:48.733106 IP 172.16.0.1 > 172.17.0.101: ICMP echo reply, id 2546, seq 36,
  length 64
5 10:17:49.734328 IP 172.17.0.101 > 172.16.0.1: ICMP echo request, id 2546, seq 37,
  length 64
```

Les paquets ICMP sont chiffrés puis encapsulés dans des paquets UDP. Ceci est le **tunnel**.