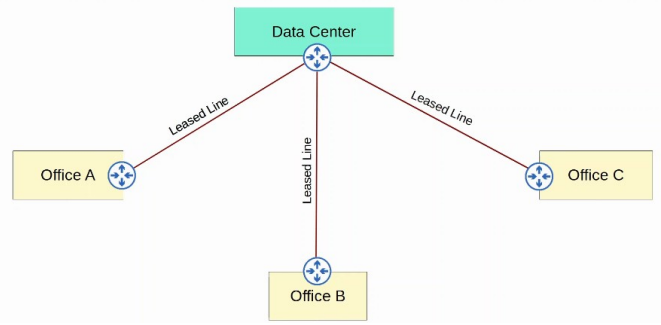
Cours 53 : Architectures WAN

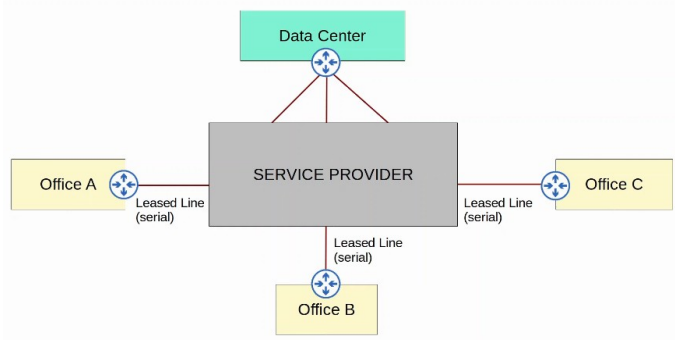
Dans ce cours nous ferons une introduction de WAN, puis un type de connexion utilisé par WAN appelé leased lines, ainsi qu'une autre technologie WAN appelé MPLS (Multi Protocole Label Switching) qui permet de fournir une sorte de VPN. Nous verrons également quelques options pour la connectivité internet, ainsi que les connexion Internet par VPN (Virtual Private Networks).

WAN est l'acronyme de Wide Area Network, un WAN est un réseau qui s'étend à travers une large zone géographique, par exemple entre des villes, des régions, etc...
Les WANs sont donc utilisés pour connecter géographiquement des LANs séparés.
Internet lui même peut être considéré comme un WAN, le terme WAN est de manière général utilisé pour se référer à des connexions à entreprise privée qui connecte ses sites et centre de données entre eux.
Il y a également les réseaux comme Internet, VPN (Virtual Private Networks) qui peuvent être utilisés pour créer des connexions privée par WAN.
Il y a eu différentes technologies WAN durant plusieurs années. En fonctiond de la localisation, certaines seront disponible d'autres ne le seront pas.
Les technologies qui sont considérés comme ancienne dans un pays peuvent continuer à être utilisé dans un autre pays.

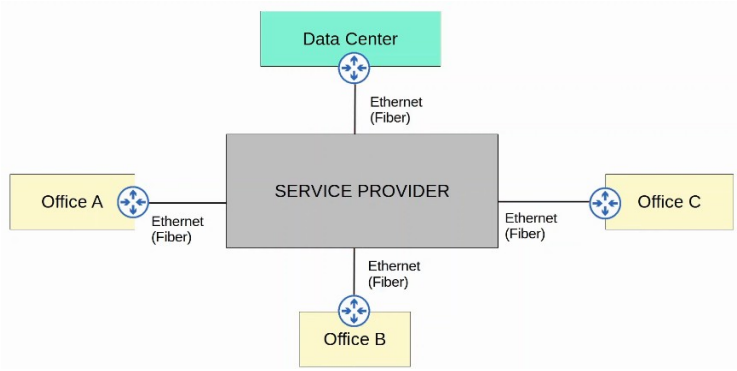
Par exemple sur le réseau suivant :



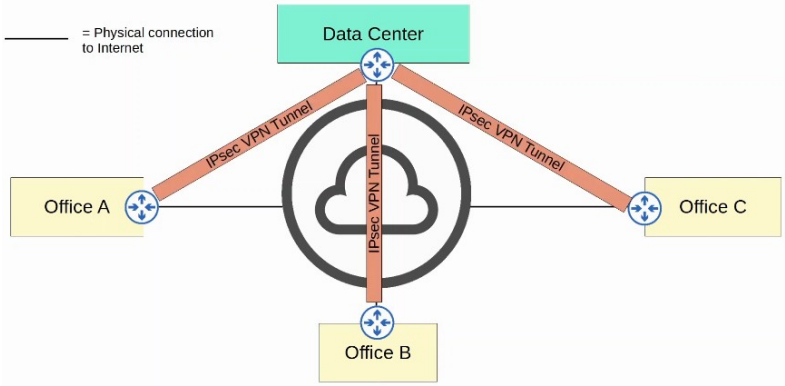
On peut voir que plusieurs sites sont connectés entre eux par l'intermédiaire du data center, la connexion est établi par des Leased Line qui sont des connexion spéciale pour connecter deux sites. Ce n'est pas une connexion partagé mais une connexion privée afin de connecter plusieurs sites entre eux. Ce type de topologie est d'ailleurs appelé topologie en étoile pour un réseau LAN, mais en terme de WAN on utilise les termes : Hub et Spoke, le Data center est appelé le Hub tans dis que les office sont appelés les Spoke. C'est une topologie Hub and Spoke.
Une représentation plus précise de Least Line est le suivant, dans lequel le Data center ainsi que les offices sont connectés aux au fournisseur Internet par le moyen de câble Serial.



Il est aussi possible de remplacer les connexion Serial par des câbles fibre.



Internet peut aussi être utilisé pour des connexion WAN entre différents sites, mais Internet n'est pas un réseau privé mais un réseau publique partagé donc envoyer des données à travers internet de façon non protégé n'est pas une bonne idée, pour mettre en place une connexion entre ces sites de manière sécurisé l'entreprise peut mettre en place des VPN comme sur le réseau suivant :



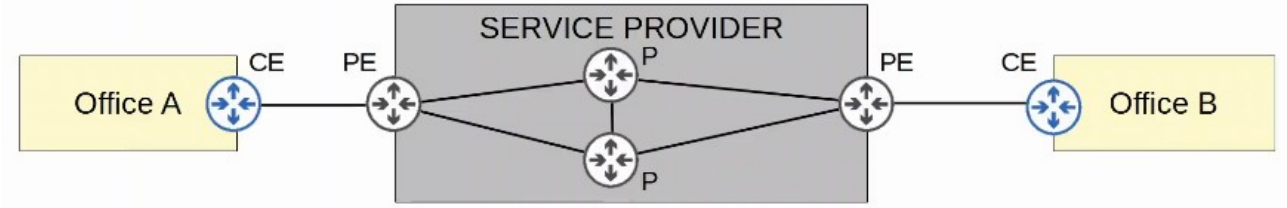
Un Leased Line est un lien physique dédié qui permet de connecter deux sites. Les Leased Line utilisent des connexions Serial (PPP ou HDLC encapsulation). Il y a une grande variété de standard qui fournissent différentes vitesses et différents standard sont disponibles dans différents pays.

System	North American	Japanese	European (CEPT)
Level zero (channel data rate)	64 kbit/s (DS0)	64 kbit/s	64 kbit/s
First level	1.544 Mbit/s (DS1) (24 user channels) (T1)	1.544 Mbit/s (24 user channels)	2.048 Mbit/s (32 user channels) (E1)
(Intermediate level, T-carrier hierarchy only)	3.152 Mbit/s (DS1C) (48 Ch.)	–	–
Second level	6.312 Mbit/s (DS2) (96 Ch.) (T2)	6.312 Mbit/s (96 Ch.), or 7.786 Mbit/s (120 Ch.)	8.448 Mbit/s (128 Ch.) (E2)
Third level	44.736 Mbit/s (DS3) (672 Ch.) (T3)	32.064 Mbit/s (480 Ch.)	34.368 Mbit/s (512 Ch.) (E3)
Fourth level	274.176 Mbit/s (DS4) (4032 Ch.)	97.728 Mbit/s (1440 Ch.)	139.264 Mbit/s (2048 Ch.) (E4)
Fifth level	400.352 Mbit/s (DS5) (5760 Ch.)	565.148 Mbit/s (8192 Ch.)	565.148 Mbit/s (8192 Ch.) (E5)

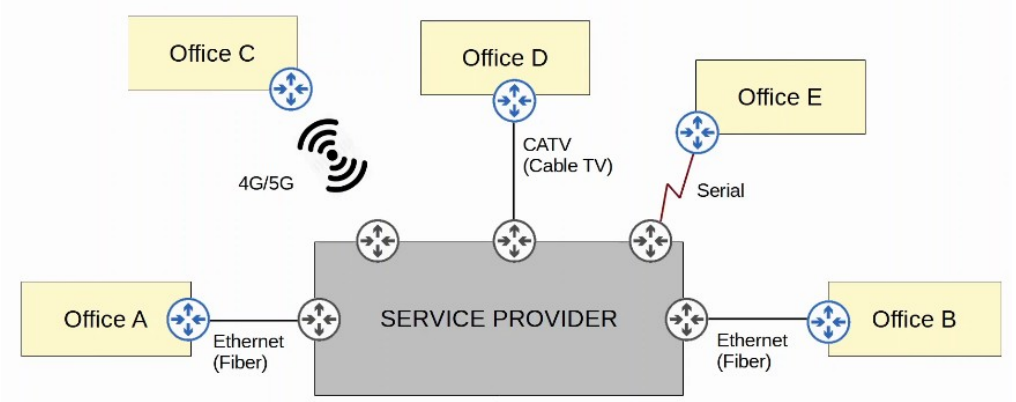
Par exemple aux Etats-Unis le standard commence par T1 - T2 – T3.
En Europe le standard commence par E1 - E2 – E3.
A cause des coût chère, du temps d'installation élevé et de de la vitesse lente des Leased Lines, Les technologies Ethernet WAN deviennent plus populaire.

MPLS est l’acronyme de « Multi Protocole Label Switching », de manière similaire à Internet le fournisseur Internet MPLS partagent des Infrastructures car plusieurs entreprises clientes s’y connectent et partagent la même infrastructure pour faire des connexions WAN.
Le label switching dans le nom de MPLS permet aux VPNs d’être crées à travers l’infrastructure MPLS pour l’utilisation de labels, ces label sont fait pour séparer le trafique de différents clients afin d’être certain qu’il ne mélange pas le trafique avec d’autres clients.
Certains termes important sont :
CE Router : Customer Edge Router
PE Routeur : Provider Edge Router
P Router : Provider Core Router

Le diagramme suivant permet de mieux comprendre :

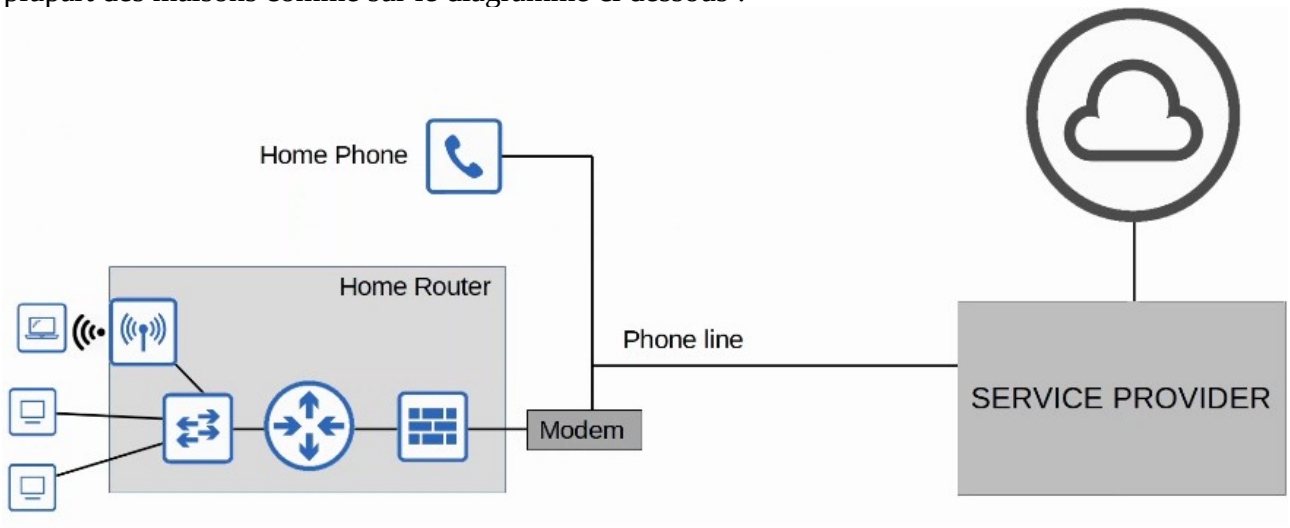


Le routeur CE est à la limite du routeur client et sont connectés au routeur PE (Provider Edge Router) chez le service fournisseur il y a les routeur Core Provider qui fournissent le réseau interne à l’infrastructure mais qui ne sont pas connectés directement au routeur du client.
Lorsque le routeur PE reçoit une trame du routeur CE il ajoute un label à la trame.
Ces labels sont utilisés pour faire partager des décisions du service fournisseur du réseau et non pas la destination IP.
Le routeur CE n’utilise pas MPLS, MPLS est utilisé uniquement pas les routeurs PE et P.
Lorsque l’on utilise la couche 3 MPLS VPN, les pairs de routeurs CE et PE utilisant OSPF par exemple pour partager des informations de routage.
Par exemple dans le diagramme ci dessus le CE d’Office A s’appareille avec le PE et le CE d’Office B s’appareille avec le PE. Le CE d’Office A apprend à propos de Office B ses routes par l’appairage OSPF, et le CE d’Office B apprend aussi des routes d’Office A.
Lorsque l’on utilise une couche 2 de MPLS VPN, les routeurs CE et PE ne forment pas un appairage. Le fournisseur de service réseau est totalement transparent avec les routeurs CE.
Dans les fais c’est comme les deux routeurs CE directement connectés, leurs interfaces WAN sera dans le même sous réseau. Si un protocole de routage est utilisé les deux routeurs CE vont s’appairer directement entre eux, le fournisseur de service fais alors comme office de Switch pour faire passer le réseau des deux routeurs CE.
Différentes technologies peuvent être utilisés pour connecter un fournisseur Internet de réseau MPLS pour un service WAN, Office A et Office B utilisent un câble Ethernet Fibre, Office C utilise La 4G/5G, Office D utilise des câble TV, Office E utilise un câble Serial.



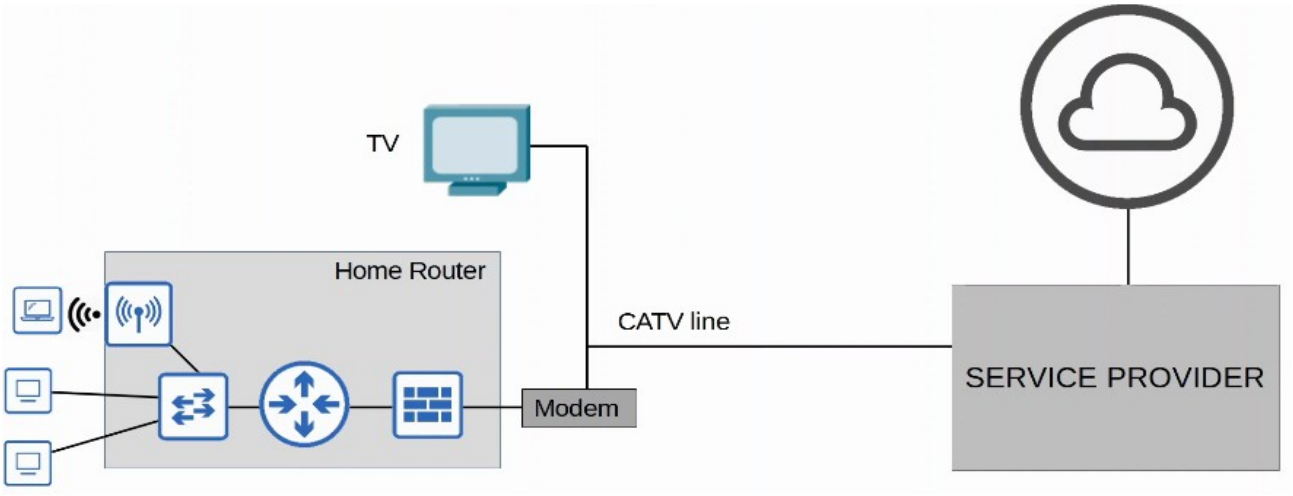
Il existe un tas de manière pour une entreprise de se connecter à Internet. Par exemple une technologie WAN privée comme les Leased Lines et MPLS VPN peuvent être utilisé pour connecter à des fournisseurs de service d'infrastructure Internet.
En plus des technologies comme CATV et DSL communément utilisés par les clients (accès Internet maison) peuvent être utilisés par les entreprises.
De nos jours les entreprises et clients d'accès Internet, les connexions fibres optiques Ethernet augmentent en popularité avec la haute vitesse de connexion qu'ils fournissent sur des longues distances. Voyons à présent deux technologies d'accès Internet mentionnés auparavant :
CATV et DSL.

DSL est l'acronyme de Digital Subscriber Line, il fournit une connectivité Internet aux clients à travers les lignes téléphoniques et peuvent partager la même ligne de téléphone qui est installé dans la plupart des maisons comme sur le diagramme ci dessous :

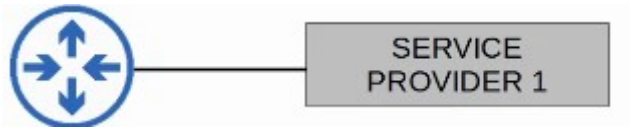


Le modem DSL (Modular demodulator) est requis pour convertir les données en un format approprié pour être envoyé à travers des ligne téléphonique.
Le modem peut être un appareil séparé ou bien être intégré au « routeur de maison ».

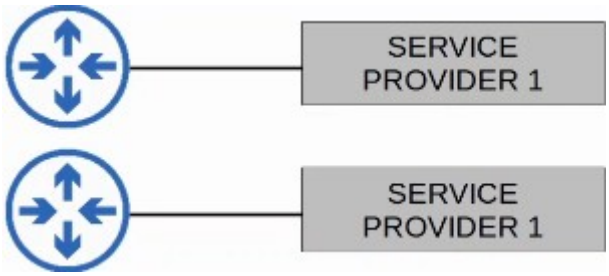
Les câbles Internet est un concept similaire à DSL et fournissent un accès Internet par le même CATV (Câble de Télévision) la ligne utilisé pour le service TV.
Tout comme DSL un câble modem est requis pour convertir des données en un format adapté pour être envoyé à travers le câble CATV. Tout comme DSL, cela peut être un appareil séparé ou intégré à un « routeur de maison »



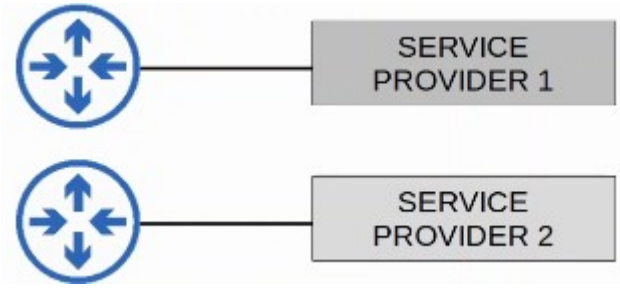
Pour les réseaux de maison la perte de connexion Internet n’est pas grave, mais pour une entreprise une perte de connexion peut poser problème, c’est pour cela qu’il est préférable d’avoir une solution redondante. Voici les termes à connaître :
Si une seule connexion à l’ISP est fait cela est appelé : « Single Homed », c’est comme une connexion standard de maison, pour une entreprise ça n’est pas idéal.



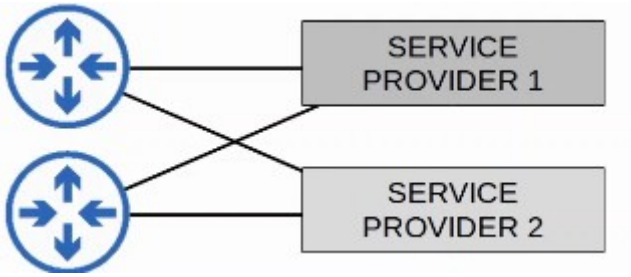
S’il y a deux connexions vers l’ISP cela est appelé « Dual Homed », cela fournit une redondance mais n’est pas le plus efficace.



Si une connexion est présente pour chaque ISP cela est appelé « Multihomed ».
Cela améliore la redondance car dans ce cas de figure, si un ISP (fournisseur Internet) rencontre un problème, le deuxième ISP prend le relais.



Lorsque deux connexions pour deux ISP sont présente cela est appelé « Dual Multihomed ». Cela permet la meilleure redondance.



Les services privés WAN comme Leased Lines et MPLS fournissent de la sécurité car chaque trafique client est séparé en utilisé une connexion physique dédié. (Leased Line) ou par un tag MPLS.
Lorsque l'on utilise Internet avec WAN pour connecter des sites entre eux, il n'y a pas de sécurité préconçu par défaut. Pour fournir une communication sécurisé à travers Internet, les VPNs (Virtual Private Networks) sont utilisés.
Nous verrons deux types de connexions VPN :
- VPN Site to Site utilisant IPsec
- Remote access VPN utilisant TLS

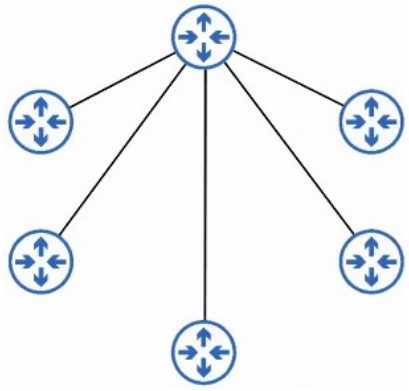
Un VPN site to Site est un VPN entre deux appareils et est utilisé pour connecter deux sites entre eux à travers Internet.
Sur un VPN « un tunnel » est crée entre les deux appareils en encapsulant le paquet IP original avec l'entête VPN et la nouvelle entête IP.
Lorsque l'on utilise IPsec, le paquet original est crypté avant d'être encapsulé avec la nouvelle entête.

Le paquet suivant est envoyé à travers le réseau :

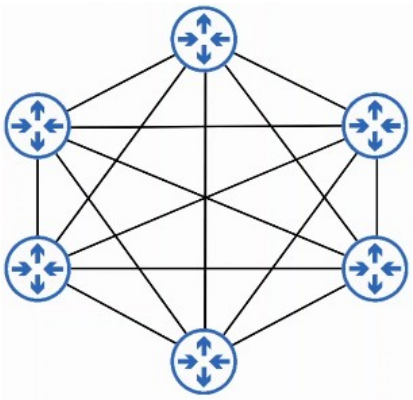
L'appareil envoyeur combine le paquet original et la session de clé (cryptage de clé) et les lance à travers une formule de cryptage. L'appareil envoyeur encapsule le paquet crypté avec une entête VPN et la nouvelle entête IP. L'appareil envoyeur envoie le nouveau paquet à l'appareil placé de l'autre côté du tunnel. Celui ci décrypte les données pour recevoir le paquet original et repartage le paquet original vers sa destination.
Dans une VPN Site to Site, un tunnel est formé seulement entre les deux extrémités du tunnel (Par exemple, les deux routeurs connectés à Internet)
Tous les autres appareils de chaque site n'ont pas besoin de créer un VPN pour eux même. Ils peuvent envoyer des données non cryptés à leur routeur de site qui va crypter et repartager dans le tunnel comme décrit auparavant.
Il y a certaines limitations au standard IPsec :
IPsec ne supporte pas le trafique Broadcast et Multicast mais seulement le Unicast. Cela signifie que le protocole de routage comme OSPF ne peuvent pas être utilisé à travers les tunnels puisqu'ils se basent sur un trafique multicast. Cela peut être résolu avec « GRE over IPsec »
Un autre problème majeur est que la configuration d'un tunnel totalement maillé entre plusieurs sites est une tâche laborieuse et demande beaucoup de temps.
Cela peut être résolu avec la solution Cisco DMVPN.

Voyons rapidement chacune des solutions précédemment évoqués :
- GRE over IPsec, GRE est l'acronyme de Generic Routing Encapsulation, permet de créer des tunnels comme Ipsec, quand bien même cela n'encrypte pas le paquet original donc cela n'est pas sécurisé.
Il a tout de même l'avantage d'avoir la possibilité d'encapsuler un grande variété de protocole de couche 3 comme messages Broadcast et multicast.
Pour avoir la fléxibilité de GRE avec la sécurité de IPsec, « GRE over IPsec » peut donc être utilisé.
Le paquet original sera encapsulé par une entête GRE et une nouvelle entête IP, puis le paquet GRE est crypté et encapsulé, l'entête IPsec VPN avec la nouvelle entête IP est ensuite ajouté.

- DMVPN est l'acronyme de Dynamic Multipoint VPN, cette solution a été développé par Cisco et permet aux routeur de dynamiquement créer un maillage total d'un tunnel IPsec sans avoir à configurer manuellement chaque tunnel.
Voici comment le configurer en deux étapes :
1. configuration du tunnel IPsec à un site hub, ci dessous le routeur au dessus est le hub est les autres routeurs sont les spoke qui sont connectés avec un tunnel IP vers le hub.

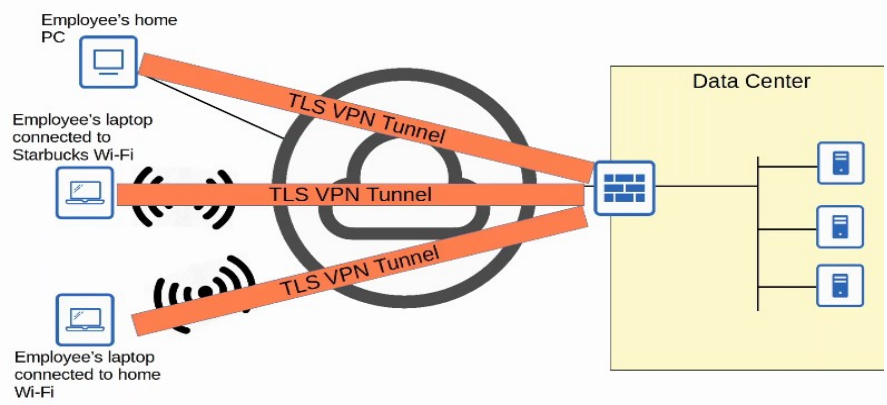


2. Le routeur hub donne à chaque routeur l'information à propos de comment former un tunnel IPsec avec les autres routeurs.



Les VPN site to Site sont utilisés pour faire une connexion site to site entre deux sites à travers Internet, les remote access VPN sont utilisé pour autoriser les appareil finaux (PC, téléphone) d'accéder aux ressources interne de manière sécurisé à travers Internet.
Remote Access VPN utilise TLS (Transport Layer Security), TLS est aussi ce que fournit comme sécurité pour HTTPS (HTTP sécurisé), TLS est comme SSL (Secure Sockets Layer) et a été développé par Netscape, mais a été renommé en TLS lorsqu'il a été standardisé par IETF.
Les logiciels clients VPN (comme Cisco Anyconnect) est installé sur l'appareil final (par exemple une entreprise fournit des ordinateurs portables à ses employés qui utilisent pour travailler depuis chez eux)
Ces appareil finaux forment un tunnel sécurisé à l'une des compagnies du routeur/mur de feu qui fonctionne comme serveur TLS.

Cela permet à l’utilisateur final de sécuriser l’accès des ressources du réseau interne de l’entreprise sans être directement connecté au réseau de l’entreprise.
Voici un diagramme pour mieux visualiser :



Les différences entre Site to Site VPN et Remote Access VPN sont les suivantes :
Les VPN Site to Site utilisent IPsec tandis ce que les Remote Access VPN utilisent TLS.
Les VPN Site to Site fournissent des services à plusieurs appareils au sites auxquelles ils sont connectés tandis ce que les Remote Access VPN fournissent des service à l’appareil final sur lequel est installé le logiciel client VPN.
Les VPN site to Site sont utilisé pour connecter de manière permanente deux sites à travers internet tandis ce que les Remote Access VPN sont utilisé pour fournir un accès sur demande pour les appareils finaux qui veulent accéder de manière sécurisé aux ressources d’une entreprise au leiu de se connecter à un réseau qui n’est pas sécurisé.