Etude du VPN

Introduction

Le terme « VPN » désigne la possibilité de connecter des réseaux privés LAN par l'intermédiaire d'un réseau WAN public, comme Internet. Lors de la mise en place de VLAN au sein d'un réseau local, le but est en général, de diviser un vaste réseau, le compartimenter et ainsi, pouvoir traiter les flux réseaux de manière distincte. Ce concept-là n'est valable que dans le LAN.

Imaginons maintenant, que l'on veuille pouvoir raccorder un utilisateur nomade ou tout un réseau géographiquement éloigné de notre réseau local on prévoirait éventuellement, des VLAN pour ceci. Par contre, le problème suivant va se poser : ce site distant où se situent les utilisateurs distants est relié actuellement, à un réseau LAN lambda, le seul moyen de connecter notre LAN et celui de notre utilisateur distant serait donc, d'utiliser internet ou en tous cas, un réseau WAN.

Le réseau de la société n'est vu, du point de vue de notre nomade, qu'à partir de son adresse IP publique. Donc, pour assurer une connexion, il faut que le nomade ou le poste de travail du site distant, s'adresse directement, à cette adresse IP publique pour pouvoir espérer dialoguer avec les machines côté LAN. Pour faire le lien entre IP publique et réseau LAN, il faut forcément passer par de la transition de port, du NAT, du PAT, qui s'avère souvent assez lourd, difficile à gérer, surtout si on dispose que d'une seule adresse IP publique.

Ainsi, pour chaque serveur ou machine à atteindre à partir du WAN, il faudra donc, faire une redirection de port explicite selon le service demandé. Cela reste faisable, mais plutôt complexe à mettre en place et surtout, à maintenir.

Au niveau de la sécurité, ce n'est pas forcément, une bonne approche, c'est pour cela que sont apparus les protocoles permettant de créer des réseaux privés virtuels, les VPN.

L'idée est qu'un nomade ou un site distant puisse s'adresser à la ressource d'un site central directement, par son adresse IP privée sans qu'on ait besoin de faire une quelconque redirection de port sans utiliser directement, l'IP WAN publique de l'accès WAN de notre site central, et le tout, complètement transparent pour les différents réseaux.

En gros, c'est faire du réseau privé sur du réseau public. On parle souvent d'ailleurs, de « Tunnel VPN » pour évoquer ce genre d'infrastructure. En effet, une fois le VPN monté, c'est comme si les deux réseaux distants ou le poste nomade du réseau central étaient directement connectés via un simple routeur.

Les VPN recouvrent énormément, de fonctionnalités pour une entreprise, le premier avantage est d'économiser de l'argent dans le sens où elle n'a pas besoin forcément, de souscrire à un abonnement à ligne dédié loué pour raccorder à un site distant. Il suffit d'un accès WAN quelconque pour mettre en place, le tunnel VPN. Cela ne dépend pas forcément, de l'opérateur.

Les VPN permettent aussi, le travail nomade car à partir de n'importe quel accès internet, l'employé d'une société peut accéder directement aux ressources de l'entreprise comme s'il était connecté sur le réseau local. Ce type de VPN est d'ailleurs, appelé « VPN Nomade ». Enfin, les protocoles VPN permettent surtout, de renforcer la sécurité, car ils comprennent quasiment tous, la possibilité d'utiliser une série d'algorithmes de cryptographie relativement avancés

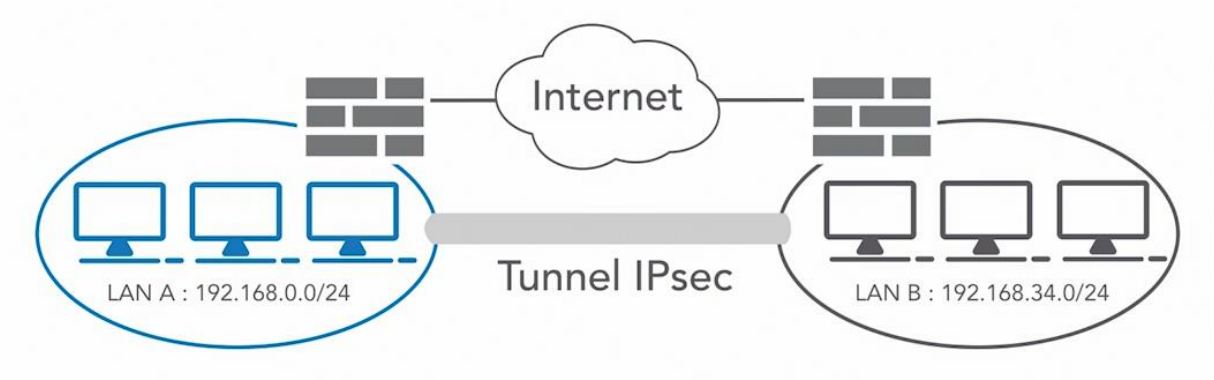
Les principaux sont IPsec et SSL. Dans certains cas d'ailleurs, on utilise même des tunnels VPN uniquement, dans le but de sécuriser des échanges entre deux serveurs.

Les types de tunnel VPN

Il existe plusieurs types de tunnels VPN, plusieurs protocoles utilisables mais, en général, on fait une première distinction entre les VPN gérés uniquement par l'entreprise, on les appelle les enterprise-managed VPN, et les VPN gérés par un opérateur qui sont donc appelés Provider-managed VPN. En France, on utilise le terme « VPN opérateur ».

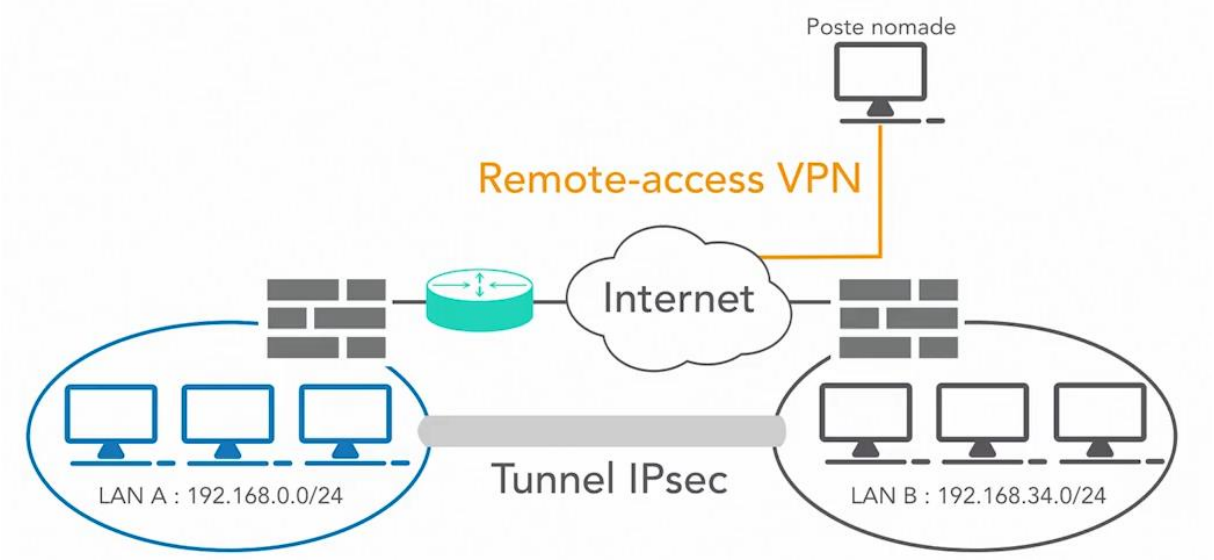
Enterprise-managed VPN

Le premier type est appelé VPN site-to-site. On utilise souvent également le terme de VPN IPsec mais par abus de langage. Ce type de tunnel est mis en place entre deux équipements, appelés passerelles VPN qui sont en général des routeurs ou des firewalls.



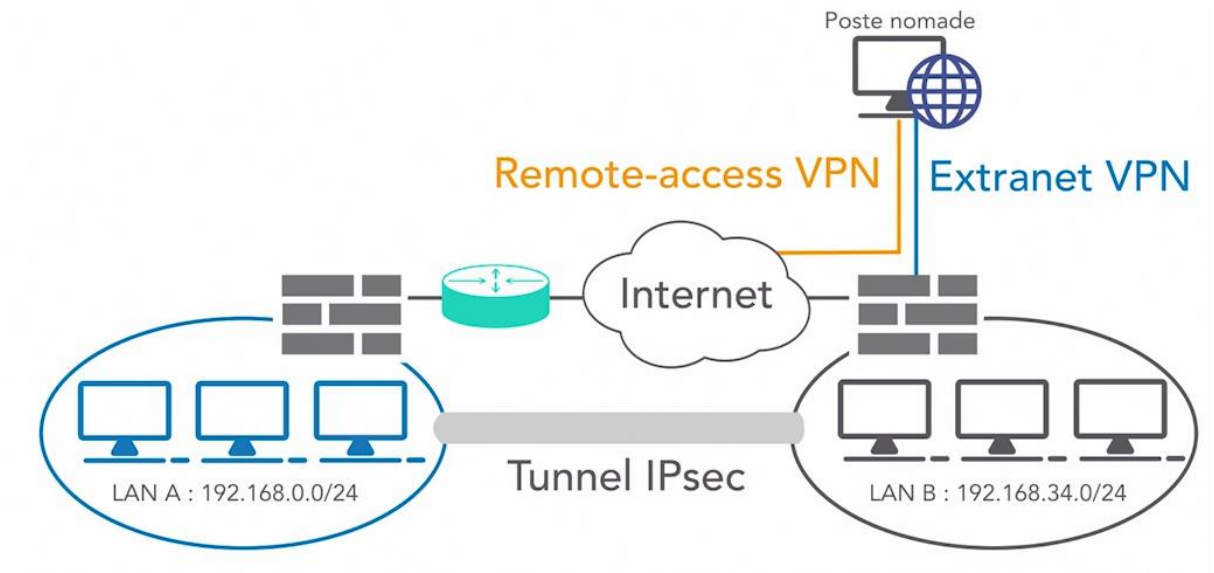
Ici, le LAN du site A peut communiquer directement avec n'importe quelle machine, n'importe quelle ressource adressée dans le LAN B, via l'adressage privé.

Il existe ensuite des VPN que l'on appelle VPN nomades (Cisco désigne sous le nom de remote-access VPN). L'idée est de permettre l'accès aux ressources du LAN d'un site central,



Ici notre LAN A, à un utilisateur déporté. Ce dernier devra être équipé forcément d'un logiciel VPN client qui initiera le tunnel avec la passerelle située sur le site central. À partir de là, le poste nomade, et uniquement le poste, pas le réseau entier, accèdera aux ressources locales directement, de notre LAN A.

Enfin, une variante qui consiste à ne plus utiliser un client dédié sur le poste nomade, mais à permettre l'accès à des ressources locales bien spécifiques, toujours de manière sécurisée, par l'intermédiaire d'une interface web accessible sur la passerelle VPN du site central donc ici du LAN B. On parle d'Extranet VPN.



En France, on utilise souvent le terme VPN SSL, aussi par abus de langage car, en fait, ce sera souvent le protocole sous-jacent utilisé entre le navigateur du nomade et le serveur web du site central de la passerelle VPN. Dans cette configuration, l'avantage est qu'on peut contrôler finalement les machines nomades qui peuvent se connecter et les ressources précises auxquelles ces nomades peuvent accéder.

Provider-managed VPN

Les VPN opérateur sont des interconnexions de réseaux privés via le cœur réseau de l'opérateur. Le principe repose sur le fait de router directement, via les équipements réseaux de l'opérateur en question, les réseaux privés d'une société d'un bout à l'autre, et potentiellement, les nomades qui se connecteraient forcément, à une passerelle spécifique, mais directement connectée chez l'opérateur.

Pour résumer, à partir du moment où l'opérateur gère les accès WAN de deux sites distants, il peut les faire communiquer simplement, via l'adressage privé par du routage. Ces VPN opérateur sont souvent appelés VPN MPLS, du nom du protocole permettant de gérer facilement, les différentes interconnexions pour un client donné. MPLS veut dire Multiprotocol Label Switching.

À la base, le protocole a été mis au point pour accélérer les opérations de routage sur les cœurs de réseaux opérateur. En fait, au lieu de router classiquement des paquet IP, on est capable de ne plus aller lire l'entête IP du paquet, mais de directement commuter en niveau deux, donc, les trames, par

l'ajout d'un marqueur MPLS. Utiliser MPLS au lieu d'un routage traditionnel a permis une économie de ressources matérielles énorme lors de l'adoption du protocole, et a quand même révolutionné les réseaux des opérateurs.

Aujourd'hui on utilise surtout MPLS pour d'autres fonctionnalités, et notamment, sa gestion possible de plusieurs tables de routage virtuelles qu'on appelle les « VRF », et la mise en place de politiques de qualité de service avancée.

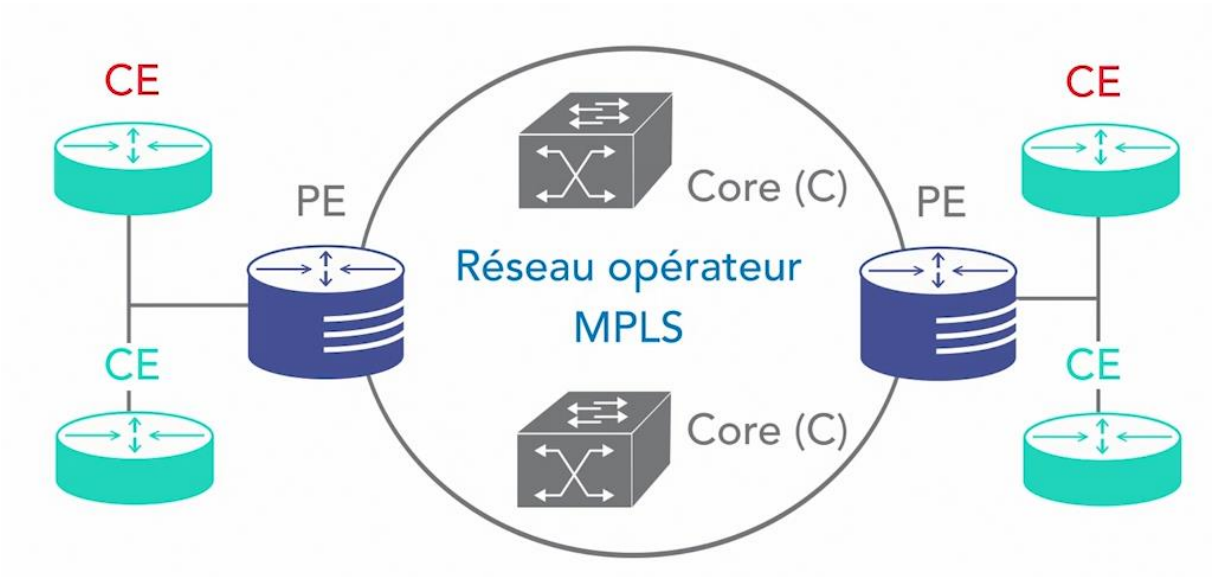
Pour simplifier, on aura une VRF globale pour chaque interconnexion d'une société donnée. On pourra alors traiter les réseaux privés de la société en question sans répercussion sur les autres réseaux privés des autres sociétés.

En fait, on a des tunnels MPLS niveau 2 et des tunnels niveau 3. L'idée d'un VPN MPLS niveau 2 est de permettre d'étendre un réseau, précisément au domaine de Broadcast via le WAN. Donc, deux sites peuvent être géographiquement éloignés, mais on utilisera le même plan d'adressage pour les deux sites, c'est vraiment une extension d'un réseau local via le WAN. Alors, pour cela, il existe deux technologies, l'Ethernet over MPLS, qui est aussi appelé « Virtual Private Wire Service », ce sont en fait, des tunnels point à point qui peuvent être établis sur des liaisons ATM ou Ethernet IP.

On rencontre également les VPLS, pour Virtual Private LAN Switching, où plusieurs instances de service, plusieurs réseaux déportés partagent le même domaine de Broadcast, virtuellement. Les machines, en fait, sont identifiées comme appartenant à un site différent en fonction de leur adresse MAC.

Les VPN MPLS de niveau 3 permettent de fournir un routage de niveau 3, donc, entre différence sites distants, à condition que chaque accès WAN soit géré par le même opérateur.

Fonctionnellement, on est sur le même principe que les tunnels site-to-site à base d'IPsec. Au sein de l'interconnexion, les routes sont échangées en principe dynamiquement, via un protocole de routage dynamique. Le routeur client, donc, celui qui est dans les locaux de l'entreprise, est appelé le « CE » pour Customer Edge. Il est connecté un routeur PE, Provider Edge. Sur un PE arrivent plusieurs connexions de différents clients, plusieurs CE, donc, puis les paquets sont véritablement gérés ensuite par les routeurs dits les routeurs Core ou Backbone, appelés P ou C, qui gèrent les échanges entre les différents PE, et donc, au final, entre les différents CE.



Quand on parle d'échange, majoritairement, c'est du routage. Dans ce type d'infrastructure et grâce à, justement, notre fameux protocole MPLS, chaque interconnexion de client sera gérée de manière indépendante par une instance virtuelle de routage, la VRF, qui est une table de routage virtuelle dédiée à un client donné qui sera propagée à l'ensemble des routeurs, et notamment, propagée au PE grâce à MPLS.

C'est dans ce type de VPN, le FAI qui fournit le routage et qui met en place l'intégralité du VPN. Pour une infrastructure multi-site c'est parfaitement adapté, sachant qu'en plus, à partir du moment où un unique opérateur gère l'interconnexion, on peut faire de la qualité de service poussée et d'obtenir, surtout, des garanties sur l'acheminement des paquets et des débits.

Bien sûr ce type de VPN a un certain coût. Il est intéressant dans l'optique de mise en place de qualité de service, qui ne serait pas possible avec des tunnels entreprise site-to-site tel IPsec où on n'a pas besoin d'opérateur. À noter également que de base, les tunnels opérateur ne proposent pas de sécurité. Les communications inter-site dans l'infrastructure ne sont pas chiffrées (de base …)

Commercialement, les fournisseurs d'accès proposent ce type de service en mettant justement, l'accès sur la bande passante garantie, la QoS, la qualité de service, pour, par exemple, pouvoir prioriser des communications ToIP par rapport à de la data. Effectivement, à partir du moment où l'opérateur gère le routage des sites de bout en bout, il est techniquement en mesure d'offrir ses services, et notamment, grâce à ce fameux protocole MPLS.

Si un opérateur vous propose ce même type de service, mais sur une interconnexion où il ne gère pas tous les sites distants, toute l'interconnexion au niveau des accès WAN, en fait, par exemple, pour un site à l'étranger où il n'est pas présent physiquement, où il a aucun Pop, point de présence, ce type de service reste alors techniquement, quasi impossible à assurer à moins à ce que le FAI ait passé des accords avec un FAI étranger, mais ça reste relativement rare, et en général, non réalisé, et parfois, non réalisable techniquement.

Les protocoles utilisés pour les VPN

Présentation

Premier protocole, le protocole L2F, pour Layer 2 Forwarding, est un vieux protocole qui a été mis au point par Cisco dans le but de mettre place, justement, une connexion de niveau 2 simplement à partir d'un client nomade. On parle de connexion VPN Dial-up. De son côté, Microsoft a mis au point le même type de tunnel appelé PPTP, Point-to-Point Tunneling Protocol. Les deux constructeurs ont ensuite collaboré pour la mise en place et l'aboutissement d'un protocole appelé L2TP (Layer 2 Tunneling Protocol), encore utilisé aujourd'hui, qui peut être utilisé pour du client VPN nomade, mais aussi pour relier deux sites distants en les plaçant dans le même domaine de broadcast, donc du tunnel de niveau 2.

Un petit peu plus tard sont apparus les tunnels de niveau 3, avec tout d'abord le protocole GRE, pour Generic Routing Encapsulation. L'idée est de mettre en place ce type de tunnel entre deux routeurs, donc du site-to-site pour simuler une connexion point à point totalement virtuelle, mais en utilisant le protocole IP. Il ne s'agit pas de PPPoE ou PPP qui sont utilisés pour faire l'inverse, c'est-à-dire encapsuler IP et non pour être encapsulés.

Enfin, et c'est le protocole le plus courant ou plutôt le plus connu, IPsec, qui est en fait une suite de protocoles, et qui garantit notamment une très bonne sécurité, qui reste cependant complexe à

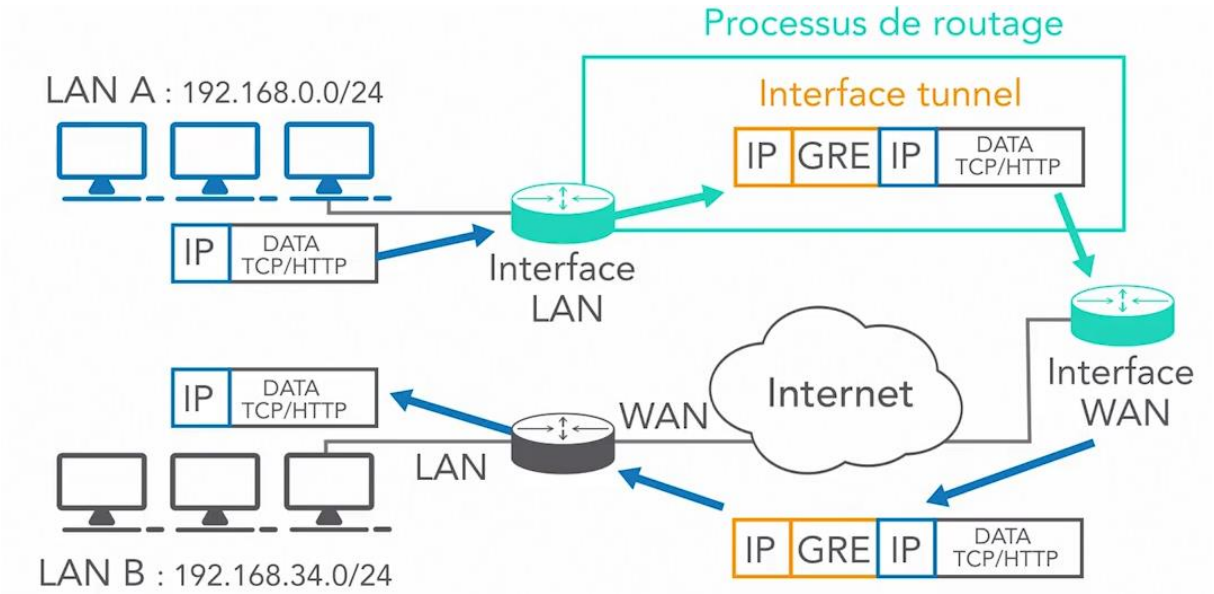
maîtriser et à configurer du fait de ses nombreuses possibilités, ses subtilités et un nombre assez important d'options de configuration. Il n'est pas rare d'utiliser GRE avec une couche supplémentaire IPsec sur le même tunnel pour sécuriser la connexion car GRE ne propose nativement aucune possibilité de chiffrement et d'authentification.

Enfin il existe d'autres protocoles destinés à la base, notamment, pour de la configuration en mode nomade, mais qui peuvent aussi s'utiliser en site-to-site pour la plupart, il s'agit des VPN SSL, et des VPN type OpenVPN, qui est une solution open source qui fonctionne plutôt bien. On peut citer également plus récemment l'apparition d'une solution qui s'appelle SoftEther, libre elle aussi et gratuite, qui permet de construire des tunnels niveau 2 et ou niveau 3 assez facilement en utilisant plusieurs protocoles pour effectuer l'encapsulation. De base, il utilise SSL, mais on peut aussi encapsuler nos données dans du DNS ou dans de l'ICMP.

Il faut savoir également que certains constructeurs ont développé forcément leurs propres protocoles, mais la plupart du temps, dans le cas d'un VPN nomade, notamment, c'est SSL ou IPsec qui sont utilisés, car ce sont des protocoles ouverts. Le logiciel client, la partie cliente spécifiquement développée par le constructeur est, elle, payante, même s'il existe des clients VPN nomades compatibles SSL IPsec qui sont totalement gratuits et donc, compatibles.

Le protocole de tunneling GRE

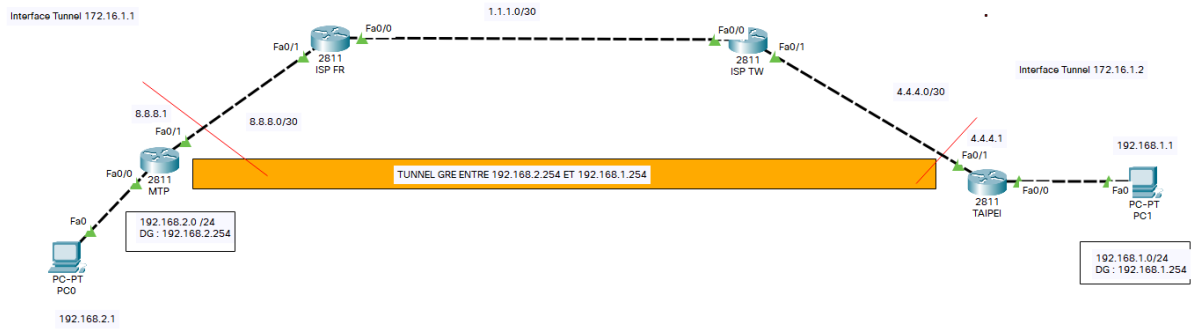
GRE a été l'un des premiers protocoles utilisés pour la fonction de VPN. Il a l'avantage d'être très simple à mettre en place, à configurer. GRE permet en soi, d'encapsuler n'importe quel paquet de la couche réseau. Il a été développé par Cisco avec le principe selon lequel il n'est pas nécessaire de maintenir une session permanente justement, entre les deux extrémités du tunnel. Ces deux extrémités n'ont pas besoin d'être connectées au WAN via le même opérateur. L'inconvénient, c'est qu'il n'est pas du tout conçu pour être sécurisé. Donc, tous les flux encapsulés dans GRE, sont en fait encapsulés en clair. GRE est maintenant surtout utilisé pour transporter des flux multicast concernant de la vidéo ou des protocoles de routage dynamique, au travers d'un réseau WAN, donc dans le monde opérateur. Il n'est plus utilisé ou très rarement quand on n'a pas le choix, dans une optique de raccordement d'une société à une autre, ni même dans les architectures VPN nomades.



Une machine du LAN A s'adresse à une machine du LAN B, les paquets vont être encapsulés avec GRE via le WAN. Le contenu du paquet arrivant sur l'interface du routeur WAN de notre LAN A contient des données, par exemple, une requête web, donc utilisation d'HTTP et de TCP, puis le poste de travail accole un entête IP avec l'IP privée du serveur web de destination, qui est dans le LAN B. On symbolise ici, le processus de routage du routeur du LAN A : le routeur analyse l'adresse IP de destination, voit que c'est un réseau privé, en examinant sa table de routage, il verra une route spécifique pour atteindre le réseau B via une interface tunnel GRE préalablement configurée.

À ce moment-là, le paquet est routé vers l'interface tunnel du routeur, les interfaces virtuelles. C'est-à-dire que concrètement, le routeur va rajouter un entête GRE au paquet, ainsi qu'un entête IP, mais contenant maintenant, les IP de chaque extrémité du tunnel. C'est-à-dire, les IP WAN publiques des deux extrémités. On encapsule donc le paquet IP original. La destination du paquet encapsulé étant l'IP publique du routeur de l'autre extrémité, le paquet est donc naturellement envoyé sur le réseau via l'interface WAN du routeur. Il va transiter via internet, puis arrivera à la destination qui va faire le travail à l'inverse, il va désencapsuler le paquet en enlevant l'entête GRE et l'entête IP avec les IP publiques, puis fera suivre le reste du paquet à la machine concernée du LAN B.

Pratique : Création d'un tunnel GRE entre 2 sites distants



Vérification du ping des 2 routeurs publiques

Vérification qu'il est impossible de ping PC0 et PC1

Mise en place du tunnel sur MTP :

MTP#conf t
MTP(config)#interface tunnel 1
MTP(config-if)#ip address 172.16.1.1 255.255.255.0
MTP(config-if)#tunnel source fastEthernet 0/1
MTP(config-if)#tunnel destination 4.4.4.1
MTP#show interfaces

Mise en place du tunnel sur TAIPEI :

TAIPEI#conf t
TAIPEI(config)#interface tunnel 1
TAIPEI(config-if)#ip address 172.16.1.2 255.255.255.0
TAIPEI(config-if)#tunnel source fastEthernet 0/1
TAIPEI(config-if)#tunnel destination 8.8.8.1
TAIPEI#show interfaces

Le tunnel est monté mais il est impossible de communiquer entre les PC, il manque des routes :

MTP(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.2
TAIPEI(config)#ip route 192.168.2.0 255.255.255.0 172.16.1.1

Le ping entre les 2 PC fonctionne, on peut vérifier le tunnel par un tracert

Le protocole IPSec

IPsec, au premier abord, peut sembler plutôt complexe. IPsec n'est en soi, pas un protocole, mais une bibliothèque, un framework de plusieurs protocoles et d'algorithmes de chiffrement qui vont vous permettre de chiffrer, d'authentifier des communications IP niveau 3 de bout en bout. À noter également qu'IPsec encapsule uniquement du trafic IP, là où le GRE qu'on a vu précédemment est, lui, beaucoup plus tolérant.

Au niveau de la sécurité, il existe deux protocoles. Le premier, appelé « AH » pour Authentification Header, permettait en fait, d'assurer uniquement l'authenticité de chaque extrémité. AH n'apporte aucune fonction de chiffrement des données à l'intérieur des paquets. Donc, très vite, il a été abandonné au profit d'ESP (Encapsulating Security Payload). C'est une avancée majeure car avec ESP, les paquets sont maintenant chiffrés avec des algorithmes comme 3DES ou AES. Avec ESP, on est capable de renforcer l'authentification des deux extrémités, donc, des deux passerelles VPN, afin de pouvoir vérifier l'intégrité du message s'il n'a pas été modifié pendant sa transmission et d'éviter ce que l'on appelle « le rejeu », c'est-à-dire le fait de pouvoir rejouer la communication par une entité qui n'appartient pas au tunnel.

IPsec peut utiliser des algorithmes de hachage, notamment par rapport à cette intégrité, tels que MD5. Au niveau authentification et chiffrement des données, on peut également se baser, au choix, sur des algorithmes qui sont symétriques, ou, et c'est le plus sécurisé, des algorithmes asymétriques avec certificats, clés publiques, clés privées.

Concrètement, les données sont encapsulées dans des paquets AH ou ESP, selon le cas, qui sont donc des protocoles niveau 3, mais ces paquets sont seulement échangés une fois que le tunnel a été mis en place. Et pour mettre en place ce tunnel, on utilise une famille de protocoles appelée « IKE-ISAKMP » (Internet Key Exchange – Internet Security Association and Key Management Protocol agissant sur le port 500 en UDP) qui définit un ensemble d'algorithmes qui vont permettre de mettre en place la communication sécurisée à chaque extrémité du tunnel.

Il faut donc, que les deux extrémités utilisent dans tous les cas, les mêmes protocoles et les mêmes algorithmes. En général, un tunnel va s'établir en deux phases. La première phase établit une connexion sécurisée entre les deux extrémités clairement identifiées, et sur cette connexion sécurisée, qu'on appelle « Phase 1 ISAKMP », les deux extrémités vont ensuite pouvoir négocier la Phase 2 que l'on appelle « l'IPsec SA ».

Dans ces phases, on négocie surtout les algorithmes de chiffrement et d'authentification que l'on va utiliser. On parle d'ailleurs, de SA pour Security Association,

Pour chaque phase, on choisit les algorithmes également de hachage pour assurer l'intégrité et l'anti rejeu.

En résumé, lors de la Phase 1, les deux extrémités mettent en place une communication sécurisée pour s'échanger de manière sécurisée, des clés de chiffrements qui serviront vraiment à chiffrer les données dans la Phase 2.

La plus difficile quand on configure un tunnel VPN IPsec, est de ne pas confondre algorithme et protocole. Au niveau des échanges réseaux, on ne verra passer que des paquets IKE et des paquets de données, mais encapsulées dans AH ou ESP, et c'est tout.

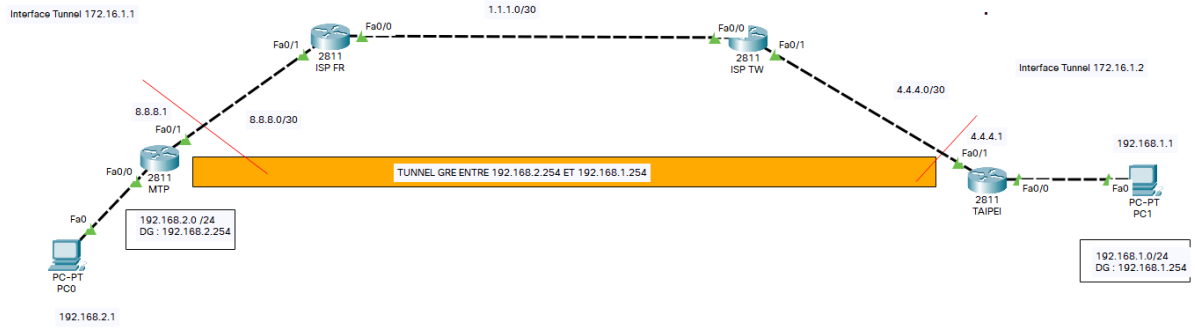
Il existe une multitude de combinaisons d'algorithmes que l'on va pouvoir choisir et configurer pour chacune de ces phases.

En général, dans la Phase 1, on ne va définir que les adresses IP publiques des deux extrémités, des deux routeurs, et dans la Phase 2, par contre on désignera les réseaux LAN qui vont pouvoir parler ensemble.

Dans le cas de plusieurs réseaux à router entre deux sites distants, on pourra créer une seule Phase 1 et plusieurs Phase 2.

Enfin, CISCO a mis au point une fonction appelée DMVPN Dynamic Multipoint Virtual Private Network, adapté aux configurations VPN pour les interconnexions avec de nombreux sites distants à relier. L'idée, c'est d'avoir une passerelle centrale appelée « hub » sur laquelle se connectent les sites distants, appelée « spoke ». L'architecture est dite « hub and spoke ». Il suffit de créer un seul profil IPsec VPN sur le hub central au lieu de configurer habituellement, un profil VPN par site distant. Et de plus, les spokes qui sont reliés au hub vont à leur tour mettre en place des connexions point à point VPN, directement entre eux.

Pratique : Création d'un tunnel IPSec entre 2 sites distants



Nous allons débuter par la phase 1. Il est hyper important que les configurations soient identiques des 2 cotés !!!

Nous allons créer une politique de chiffrement isakmp avec l'identifiant 10 dans laquelle nous utiliserons l'algorithme de chiffrement AES et dont l'authentification se fera de manière symétrique avec une clé pré-partagée (Azerty02) dont la force de chiffrement Diffie Hellman sera de 1024 bits (groupe 2)

MTP#conf t
MTP(config)#crypto isakmp policy 10
MTP(config-isakmp)#encryption aes
MTP(config-isakmp)#authentication pre-share
MTP(config-isakmp)#group 2
MTP(config-isakmp)#exit

Création de la clé destinée à l'adresse du routeur distant 4.4.4.1

MTP(config)#crypto isakmp key Azerty02 address 4.4.4.1

La crypto policy et la crypto key sont des ensembles indépendants qui vont fixer l'ensemble d'algorithmes pour sécuriser la mise en place de la connexion.

Nous allons maintenant devoir créer une ACL étendue qui va devoir matcher le traffic dans le tunnel :

MTP(config)#access-list 110 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

Il est donc indispensable d'effectuer strictement la même configuration sur le routeur de TAIPEI

TAIPEI#conf t
TAIPEI(config)#crypto isakmp policy 10
TAIPEI(config-isakmp)#encryption aes
TAIPEI(config-isakmp)#authentication pre-share
TAIPEI(config-isakmp)#group 2
TAIPEI(config-isakmp)#exit

TAIPEI(config)#crypto isakmp key Azerty02 address 8.8.8.1

TAIPEI(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

Dans un premier temps, nous allons préciser un jeu d'algorithmes utilisables (transform-set) que nous nommerons VPN-SET et qui utilisera esp-3des (pour le chiffrement) et esp-sha-hmac (pour le hachage) :

MTP(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac

La phase 1 est terminée, le lien entre la phase 1 et la phase 2 va se faire au sein de ce qu'on appelle une "crypto map" que nous nommerons VPN-MAP avec une priorité fixée à 20 (dans le cas où on aurait plusieurs crypto map) de type ipsec-isakmp, utilisant le jeu d'algorithme VPN-SET matchant avec l'ACL 110 créée précédemment.

MTP(config)#crypto map VPN-MAP 20 ipsec-isakmp
MTP(config-crypto-map)#description VPN vers TAIPEI
MTP(config-crypto-map)#set peer 4.4.4.1
MTP(config-crypto-map)#set transform-set VPN-SET
MTP(config-crypto-map)#match address 110

Nous allons enfin appliquer cette cryto map à notre interface coté WAN :

MTP(config)#interface fa0/1
MTP(config-if)#crypto map VPN-MAP

Il nous reste la même chose à appliquer à TAIPEI :

TAIPEI(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac

TAIPEI(config)#crypto map VPN-MAP 20 ipsec-isakmp

TAIPEI(config-crypto-map)#description VPN vers MTP
TAIPEI(config-crypto-map)#set peer 8.8.8.1
TAIPEI(config-crypto-map)#set transform-set VPN-SET
TAIPEI(config-crypto-map)#match address 110

TAIPEI(config)#interface fa0/1
TAIPEI(config-if)#crypto map VPN-MAP