Réseau virtuel privé

Les VPN

Les réseaux locaux d'entreprise sont des réseaux internes à une organisation, mais ces réseaux sont de plus en plus souvent reliés à Internet par l'intermédiaire d'équipements d'interconnexion. Il arrive ainsi souvent que des entreprises éprouvent le besoin de communiquer avec des filiales, des clients ou même du personnel géographiquement éloigné via internet.

Pour autant, les données transmises sur Internet sont beaucoup plus vulnérables car le chemin emprunté n'est pas défini à l'avance, ce qui signifie que les données empruntent une infrastructure réseau publique appartenant à différents opérateurs avec le risque que le réseau soit écouté ou détourné.

La première solution consiste à relier les réseaux distants à l'aide de liaisons spécialisées. Cependant, la plupart des entreprises n'ont pas les moyens d'utiliser ce type de ligne.

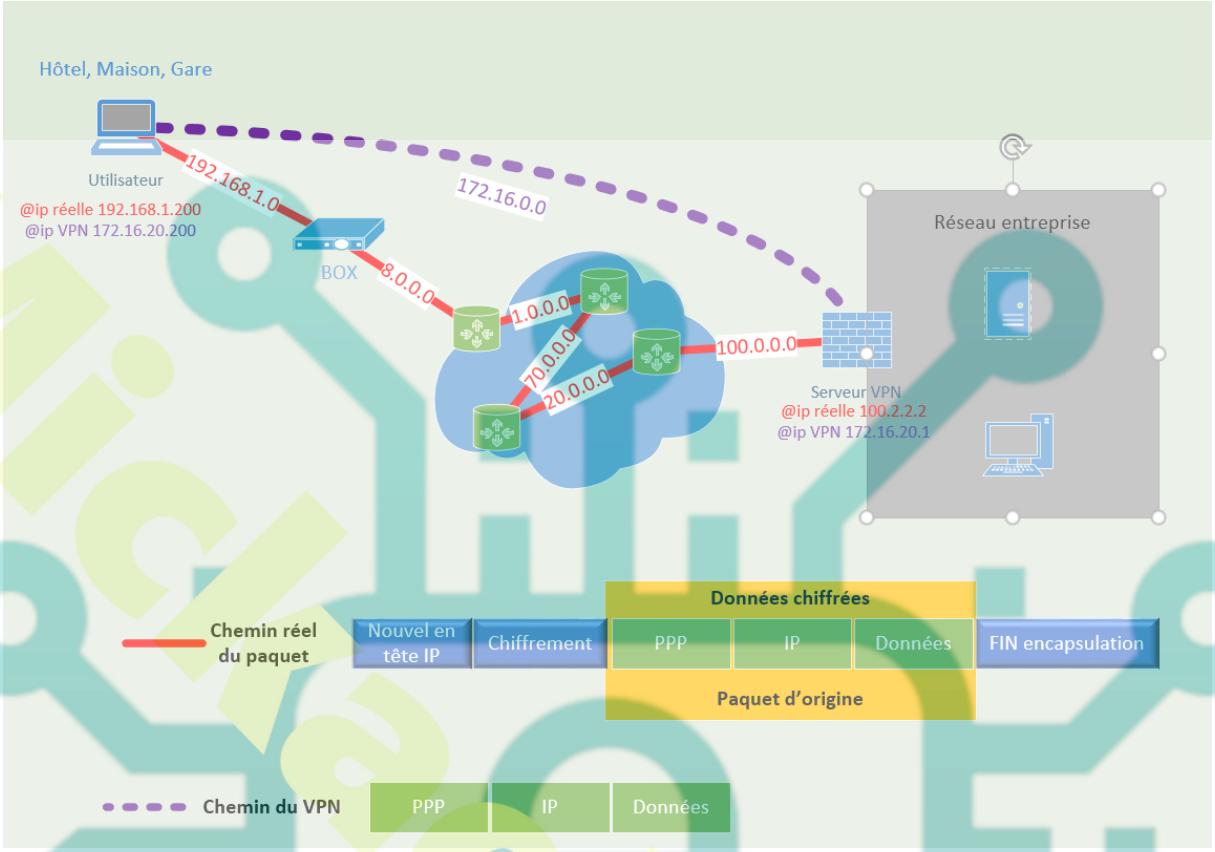
Un bon compromis consiste à utiliser Internet en utilisant un protocole d'encapsulation (tunneling) pour chiffrer les données. On parle alors de réseau privé virtuel pour ce type de connexion.

On le nomme réseau virtuel, car il s'agit d'un réseau point à point (routeur/routeur, client/routeur ou serveur/client) fictif car les données circulent par différents chemin sur internet.

Typologie des VPN

VPN d'accès distant (poste à passerelle)

L'utilisateur nomade se connecte, au serveur VPN de l'entreprise (routeur ou serveur), qui lui donne accès, une fois authentifié, à toutes (ou certaines) ressources de l'entreprise. Le gain en productivité et de réactivité est appréciable, l'utilisateur peut directement interagir avec les logiciels de l'entreprise comme s'il était dans un bureau de la maison mère.



VPN site à site (passerelle à passerelle)

Connexion de deux réseaux locaux via Internet. Les utilisateurs du réseau A peuvent accéder aux ressources du réseau B et vice versa, comme s'ils faisaient partie d'un seul et unique réseau.

VPN poste à poste

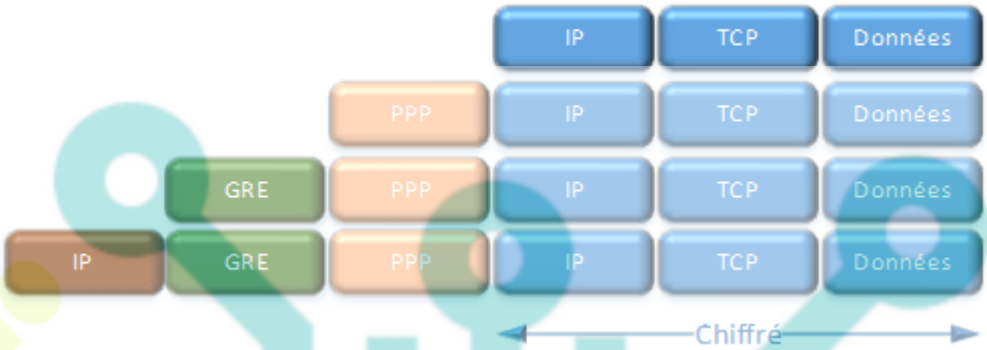
Liaison VPN entre un poste et un serveur VPN. Les utilisateurs accèdent uniquement à ce serveur ou bien alors à tout le réseau en fonction des paramétrages.

Les protocoles de tunnel

PPTP (Point to Point Tunnelling Protocol)

C'est un protocole de niveau 2 qui encapsule des trames PPP dans des datagrammes IP afin de les transférer sur un réseau IP.
PPTP permet le chiffrement des données PPP encapsulées mais aussi leur compression.
L'authentification utilise MSCHAP et le chiffrement RC4.

Encapsulation PPTP d'une trame PPP

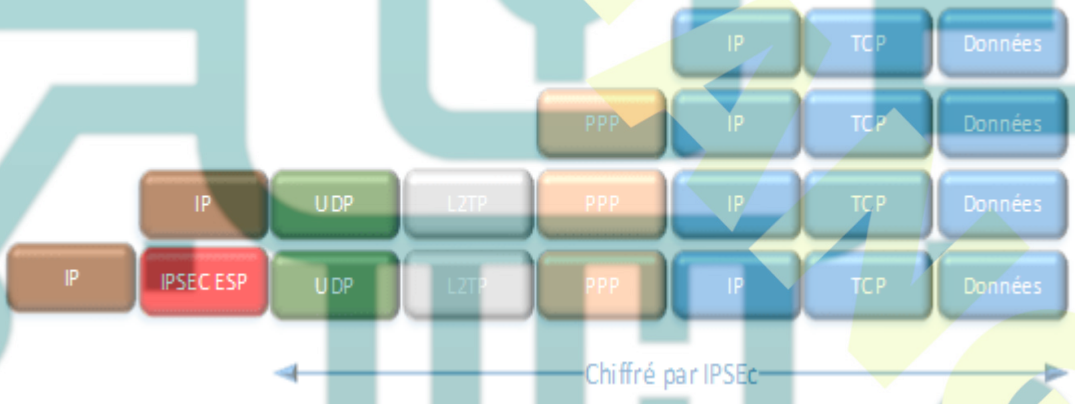


L2TP (Layer Two Tunnelling Protocol)

L2TP est un protocole réseau qui encapsule des trames PPP pour les envoyer sur des réseaux IP, X25, relais de trames ou ATM. Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunnelling sur Internet. Dans ce cas, L2TP transporte des trames PPP dans des paquets IP. Il se sert d'UDP pour envoyer les trames PPP dans du L2TP.

La sécurité du transfert s'appuie sur IPSEC.

L'illustration suivante représente l'encapsulation L2TP et IPSec d'une trame PPP.



IPSEC

IPSec est un protocole défini par l'IETF permettant de sécuriser les échanges au niveau de la couche réseau. Il garantit la confidentialité, l'intégrité et l'authentification des échanges.

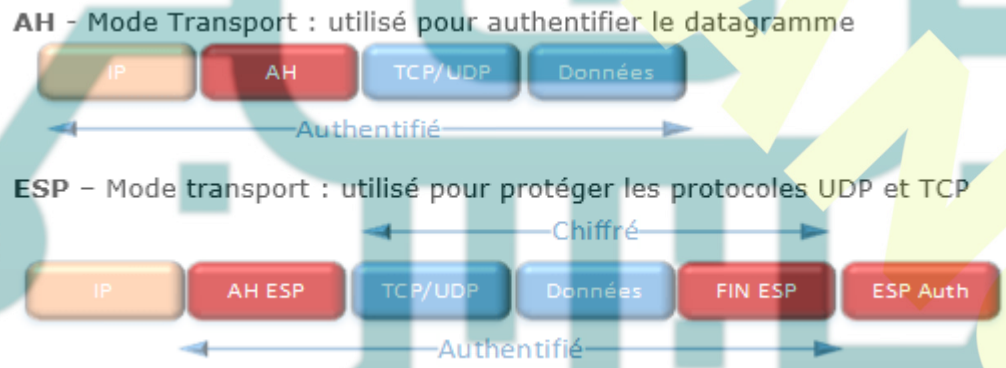
IPsec utilise 3 protocoles principaux :

IKE (Internet Key Exchange) authentifie les différentes parties et leur fourni du matériel pour générer des clés (symétrique ou asymétrique) Ce protocole s'appuie sur les méthodes DES, 3DES, AES, RSA, MD5, SHA
AH (Authentication Header), est employé pour assurer l'authentification des machines aux deux extrémités du tunnel. Il permet aussi de vérifier l'unicité des données grâce à l'attribution d'un n° de séquence. Il assure l'intégrité de celles-ci à l'aide d'un code de vérification de données (Intégrity Check Value)
ESP (Encapsulating Security Payload), répond, quant à lui, au besoin de chiffrer les données. Il peut toutefois aussi gérer l'authentification et la vérification de l'intégrité mais de manière moins poussée qu'AH.
Option **PFS** garantit que les clés de chiffrement pour les négociations IPsec SA sont créées séparément pour chaque négociation.

Les modes d'IPSEC

Le mode Transport

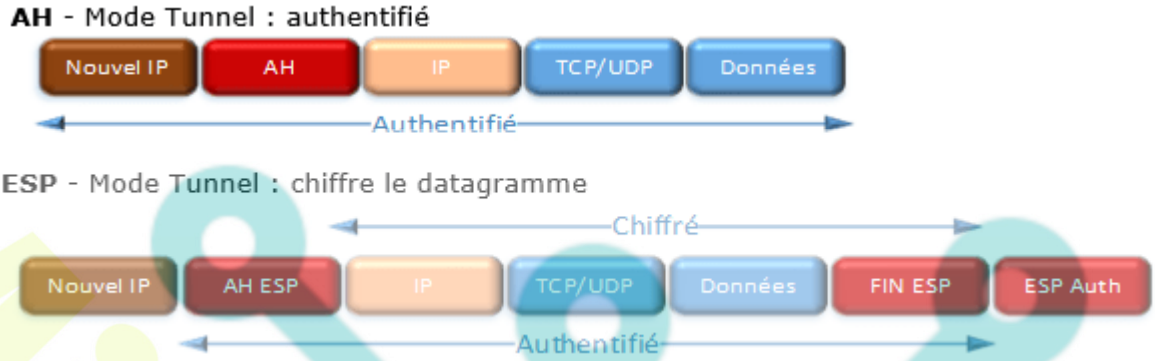
Il récupère les données provenant de la couche 4 (TCP), les authentifie et les chiffre puis enfin les envoie à la couche 3 (IP) Ce mécanisme ne modifie pas l'en tête IP existant mais intercale le header AH/ESP entre le header IP et les données.



IIPSEC mode de transport

Le mode Tunnel

Il est généralement utilisé quand on veut relier un site à un autre (de passerelle à passerelle) Il ne modifie pas l'en tête d'origine mais rajoute le header AH/ESP et encapsule le tout avec un nouvelle en tête IP à destination de la passerelle.



IPSEC mode tunnel

> Des modifications peuvent être nécessaires pour permettre à IPSEC de travailler avec des services comme NAT, car il ne supporte pas les modifications de ses en-têtes.

Exemple de configuration de serveur VPN routeur à routeur en IPsec

SSL

SSL (Secure Sockets Layers) est un procédé de sécurisation des transactions effectuées via Internet. Le standard SSL a été mis au point par Netscape, en collaboration avec Mastercard, Bank of America, MCI et Silicon Graphics.
Il repose sur un procédé de cryptographie par clé publique afin de garantir la sécurité de la transmission de données sur internet.

Le système SSL est indépendant du protocole utilisé, ce qui signifie qu'il peut aussi bien sécuriser des transactions faites sur le Web par le protocole HTTP que les connexions via

le protocole FTP, POP ou IMAP. En effet, SSL agit telle une couche supplémentaire permettant d'assurer la sécurité des données situées entre la couche application et la couche transport.

TLS – Transport Layer Security

Au milieu de l'année 2001, le brevet de SSL appartenant jusqu'alors à Netscape a été racheté par l'IETF (Internet Engineering Task Force) et a été rebaptisé pour l'occasion TLS (Transport Layer Security)

Le client et le serveur négocient d'abord les paramètres de sécurité de TLS (en fait, les algorithmes cryptographiques et de compression). Ensuite, ils s'échangent leurs certificats, ce qui leur permet de calculer un secret commun chacun de leur côté. Ils utilisent ce secret commun pour en extraire les clés cryptographiques de la session TLS.

Protocole	Port Standard	Protocole sécurisé	Port Sécurisé
HTTP	80	HTTPS	443
LDAP	389	SLDAP	636
FTP Data	20	SFTP	989
FTP Control	21	SFTP	990
TELNET	23	SSH	22
IMAP	143	SIMAP	993
POP	110	SPOP	995
SMTP	25	SMT-TLS	465

VPN SSL/TLS

Les VPN de ce type, permettent l'accès aux réseaux de l'entreprise par l'intermédiaire d'un client lourd. Ils diffèrent des VPN SSL utilisant un navigateur, en proposant l'accès aux réseaux et non plus qu'aux seules applications supportant SSL/TLS.

SSTP

C'est un protocole Microsoft qui permet l'encapsulation de paquets PPP (protocole point à point) sur HTTP. Il facilite l'établissement d'une connexion VPN via un pare-feu ou via un périphérique de traduction d'adresses réseau.

Il encapsule les trames PPP dans un datagramme IP et utilise le port 443, ensuite le chiffrement est réalisé par SSL/TLS.

SSTP utilise l'AES pour le chiffrement, ce qui en fait une option sûre.

Open VPN

OpenVPN est à la fois un protocole VPN et un logiciel qui utilise les techniques VPN pour sécuriser les connexions point à point et site à site. C'est l'un des protocoles VPN open source les plus populaires parmi les utilisateurs VPN.

OpenVPN ne supporte pas L2TP, IPSec et PPTP, il utilise son propre protocole personnalisé basé sur TLS et SSL.

OpenVPN utilise un cryptage OpenSSL 256 bits, mais il peut également utiliser les algorithmes AES, Camellia, 3DES, CAST-128 ou Blowfish.

OpenVPN fonctionne dans l'espace utilisateur au lieu de l'espace noyau.

SSH

Le protocole SSH (Secure Shell) permet à des utilisateurs d'ouvrir une session interactive sur une machine distante à travers une communication chiffrée.

SSH n'est généralement pas considéré comme un protocole VPN « pur». Toutefois, celui-ci permet de faire du tunneling et propose certaines fonctionnalités de VPN.

VPN d'anonymat

TOR

Tor, pour « The Onion Router », est un outil de pointe pour protéger la vie privée et l'anonymat sur Internet.

Tor est un réseau composé de milliers de **nœuds** bénévoles, également appelés **relais**. Pour chaque demande de connexion à un site Web, le chemin est généré de manière aléatoire. Aucun des relais ne conserve d'enregistrement de ces connexions, il n'existe donc aucun moyen pour un relais de connaître le trafic qu'il a transmis.

Le réseau Tor se compose de près de 7 000 relais et de 3 000 passerelles.

Lorsque l'on se connecte au réseau Tor en utilisant le navigateur Tor, toutes les données envoyées et reçues passent par ce réseau, via une sélection aléatoire de nœuds. Tor chiffre toutes ces données plusieurs fois avant qu'elles ne quittent le PC, y compris l'adresse IP

du nœud suivant. Une couche de chiffrement est supprimée à chaque fois que les données atteignent un autre nœud jusqu'à ce qu'il atteigne le nœud de sortie final. L'ensemble de ce processus est appelé **routage en oignon**. Cela signifie que personne, pas même ceux qui exécutent les nœuds, ne peut consulter les données ni leur destination.

NB. Tor utilise un système de clés asymétriques basées sur un échange Diffie Elman pour l'échange des clés symétriques.

Limites de Tor

Surfer à l'aide du navigateur Tor est totalement anonyme, mais **d'autres activités ne le sont pas** (Javascript, DNS…) Pour connecter d'autres applications et services au réseau Tor, les choses se compliquent.

Nord VPN

Ce service offre une connexion chiffrée, ce qui rend presque impossible de voir les données que tout appareil connecté à Internet envoie et reçoit.

En plus du chiffrement des données, NordVPN offre également la possibilité d'accéder à des sites Web et à des services qui pourraient ne pas être normalement disponibles dans une région en raison des restrictions gouvernementales sur le contenu ou des restrictions géographiques imposées sur le contenu par le diffuseur.

NordVPN dispose d'une connexion "Double VPN" où les données de l'utilisateur sont envoyées via 2 serveurs VPN avant d'atteindre sa destination. Il utilise également le principe du double NAT pour améliorer l'anonymat des adresses IP.

NordVPN dispose en option d'une connexion Onion Over VPN. Un client se connecte à un serveur NordVPN, qui achemine ensuite tout le trafic via un réseau Tor. Le trafic est d'abord crypté dans la couche NordVPN puis envoyé vers le réseau Tor.

NordVPN s'appuie sur le protocole « fait maison », nommé NordLynx. Cette nouvelle technologie basée sur le protocole de chiffrement open-source WireGuard.

https://www.youtube.com/watch?v=bnV-_BN9OkE

VPN SSL/TLS