TUNNEL OUVERT / TUNNEL FERMÉ

UN ZINE SUR LES RÉSEAUX PRIVÉS VIRTUELS

les icônes de ce zine sont dessinées à la main
la mise en page a été réalisée avec Scribus

la police de caractères pour le texte:
Liberation Mono
la police de caractères pour la couverture et le colophon:
sans-guilt-wafer d'OSP foundry

traduction en francais:
tierce, flatrongraad, e-Jim, harpo;-), Valhibou, Sigismond Perlimpimpon

pour des questions ou infos concernant ce zine:
email mara@multiplace.org
mastodon mara@systerserver.town

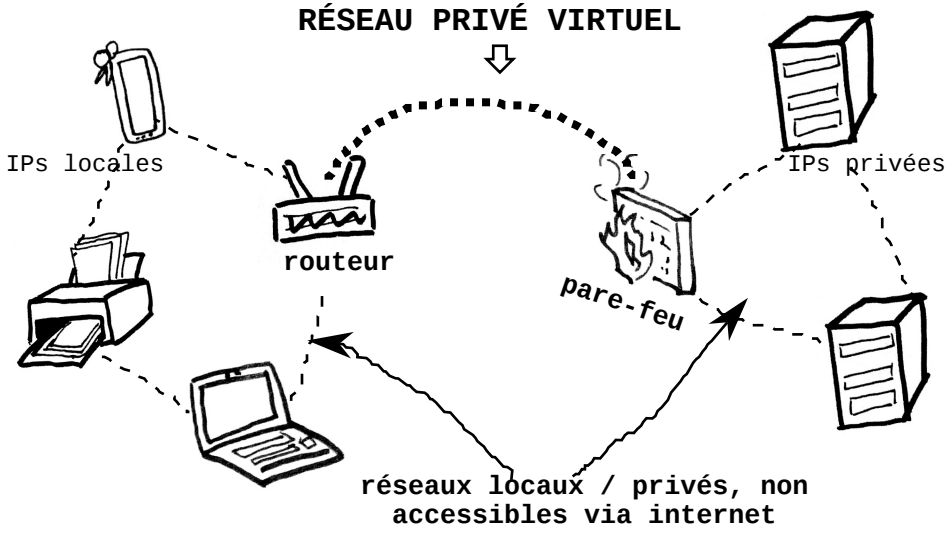
Une introduction aux tunnels,
comment ils fonctionnent,
pourquoi ils sont sûr et quels
outils utiliser pour configurer
IPsec et OpenVPN.

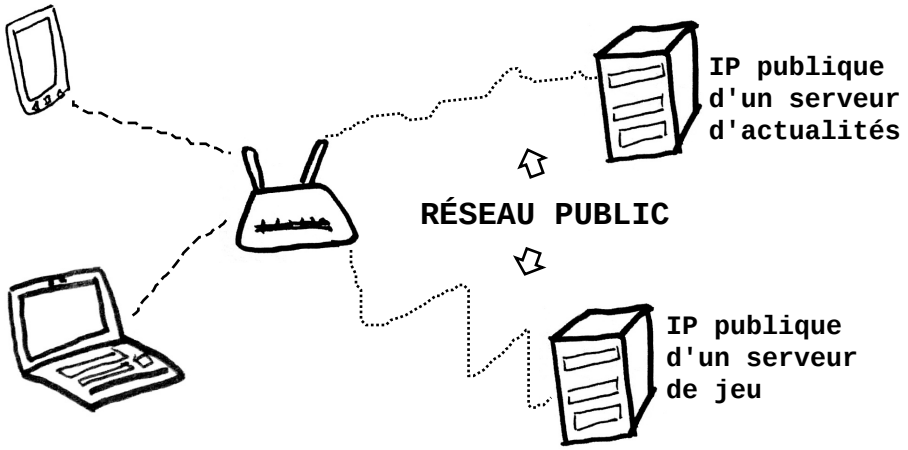
INDEX

Qu'est-ce qu'un VPN?

Un réseau privé virtuel (“Virtual Private Network” en anglais, ou “VPN“) est une extension du réseau public. Par exemple, à la maison, nos appareils peuvent être connectés sur un réseau local, imaginez que votre appareil puisse se connecter au réseau local d'une autre maison :)... ou encore au réseau privé d'un groupe de serveurs situés derrière le pare-feu d'une organisation ou d'un bureau qui n'est pas accessible via le réseau public.

Le mot “virtuel” dans le nom indique qu'un VPN permet à des machines qui se trouvent dans des réseaux locaux différents de communiquer de manière directe, au travers d'un passage sécurisé, sans que les routeurs par lesquels le trafic de données passe n'interagissent avec les contenus échangés.



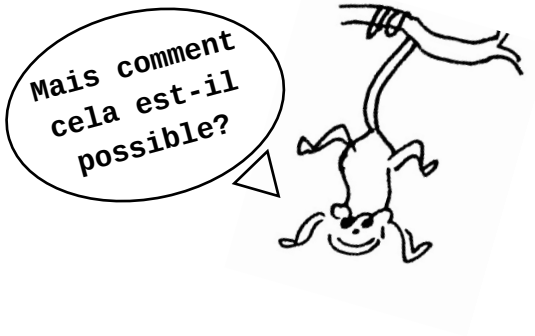


Tandis que le réseau public relie les appareils de votre maison ou de votre bureau aux serveurs qui ont des adresses IP publiques.

Types de VPN:

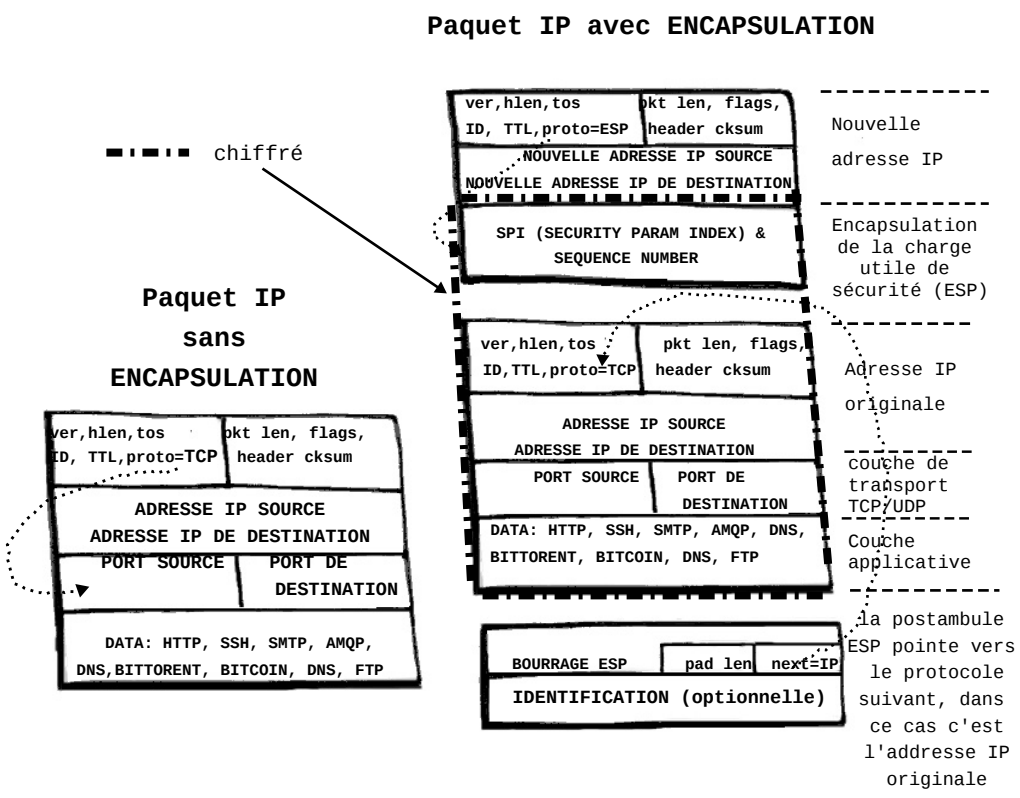
- d'hôte à hôte (accès à distance, par exemple d'un appareil à un serveur)
- de site à site / de passerelle à passerelle / de réseau à réseau

Tous deux peuvent donner un accès à des ressources qui sont derrière un pare-feu, par exemple à des machines virtuelles ou à des stockages de médias. Seul le premier type de VPN permet d'accéder à des sites censurés.



Comment fonctionne un VPN?

Le VPN utilise le protocole de mise en tunnel (un protocole de communication) pour transférer des données sur internet comme s'il s'agissait d'un réseau privé.
Pour ce faire, la tunnellisation encapsule, «enveloppe», les paquets IP dans un nouvel en-tête IP. L'en-tête IP d'origine, encapsulé, contient l'adresse IP de destination (privée) alors que le nouvel en-tête, la capsule, visible par le réseau, a pour destination l'adresse IP publique du serveur VPN.

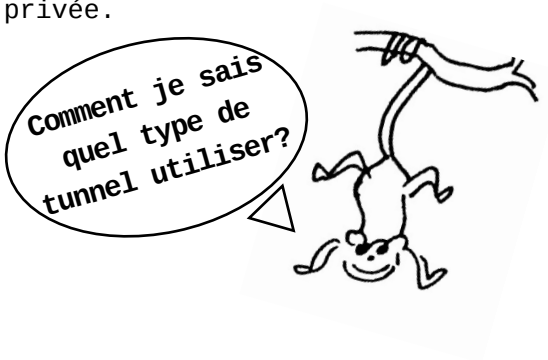


Les protocoles de tunnel courants

OpenVPN, IPsec: Internet Protocol Security, **IP dans IP:** p. ex. pour connecter deux réseaux IPv4 qui ne peuvent pas communiquer l'un avec l'autre, comme l'IP virtuelle d'un répartiteur de charge qui transmet des paquets à des serveurs ayant de vraies IP, **GRE**: Generic Routing Encapsulation, ou Encapsulation Générique de Routage, développé par Cisco, qui peut également encapsuler une adresse IPv6 dans une IPv4.

Nous allons nous concentrer sur IPsec et OpenVPN.
IPsec est préférable pour les tunnels de passerelle à passerelle, alors qu'OpenVPN est meilleur pour les tunnels d'accès à distance (connexion de client à serveur).

IPsec comparé à GRE
Les tunnels GRE sont parfois implémentés dans les routeurs Cisco, afin d'encapsuler une couche réseau dans une autre. Par exemple, il est possible de mettre en place un tunnel GRE qui va router des packets IPv4 dans un réseau qui utilise uniquement IPv6. GRE ne permet pas le chiffrement, et donc les tunnels GRE peuvent être complétés par IPsec pour améliorer la sécurité et la vie privée.



Quand avons-nous besoin d'un tunnel?

Choisir le type de tunnel dont on a besoin dépend de l'installation réseau et de ce qu'on cherche à faire:

1. Pour contourner un filtrage réseau imposé par un gouvernement, une université, une entreprise… autrement dit pour contourner la censure. Avec un tunnel, nos données sont cachées à l'intérieur de celui-ci jusqu'à ce qu'elles atteignent le serveur VPN, de là elles sont transmises à leur destination (p. ex. réseaux sociaux, vidéo, sites d'actualités…).

2. Pour se connecter à un intranet (c.-à-d. à un réseau privé ou local) qui se trouve physiquement à distance de notre appareil. P. ex. une connexion ssh permet d'accéder à un serveur distant qui a une IP publique, un tunnel permettra la même connexion à un serveur privé ou à une machine située dans la maison de quelqu'un ;)

Un proxy peut masquer votre adresse IP, est plus facile à installer et est moins cher à fournir, cependant il ne peut pas chiffrer les données qu'il fait transiter. Les tunnels VPN permettent d'accéder à des ressources protégées par un pare-feu, alors qu'un proxy ne fait que transférer le trafic vers un autre serveur.

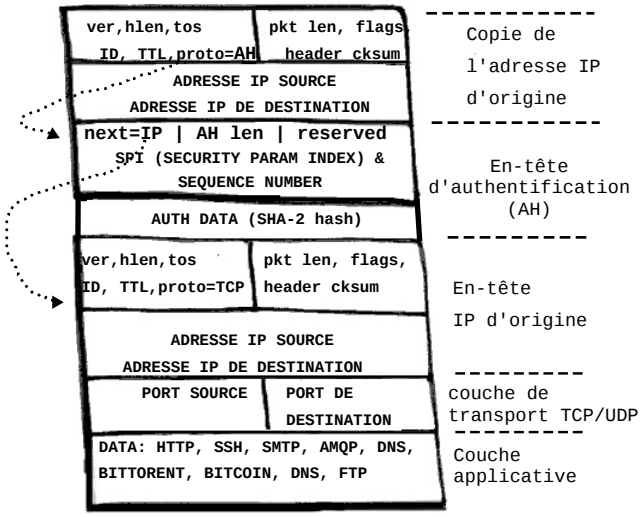
Donc un proxy peut couvrir le cas 1, c'est-à-dire l'anonymisation face à un filtrage IP, mais en l'absence de chiffrement, il ne couvre pas le cas 2, soit la création d'un réseau privé et l'accès à des ressources protégées par un pare-feu.

Donc un VPN est plus sûr qu'un proxy car

il crée un tunnel qui peut se faire avec ou sans chiffrement. Il nécessite toujours une **authentification** et peut vérifier l'intégrité des données tout en s'assurant que personne ne les a altérées lors de la communication. Il peut également être **chiffré**.

Les en-têtes d'authentification (AH, authentication header) prouvent qu'un utilisateur ou un réseau a bien une autorisation d'accès en fournissant un nom d'utilisateur et/ou un mot de passe. L'authentification IPsec s'effectue généralement à l'aide d'un secret pré-partagé ou d'une configuration plus complexe avec des clés privées et des certificats. OpenVPN utilise des clés privées et des certificats.

Paquet IP avec en-tête d'authentification (AH)

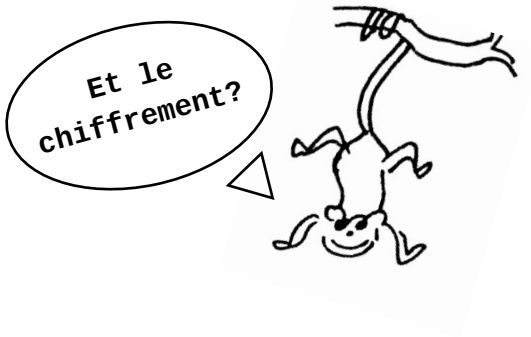


Un mécanisme de hachage
permet de vérifier l'intégrité des données en s'assurant qu'elles n'ont pas été modifiées ou interceptées en route. Il existe deux algorithmes utilisés par les VPN pour vérifier l'intégrité des données : le SHA et la famille des MD. Les algorithmes de hachage hmac-md5 et **hmac-sha2*** ou **hmac-sha3**** sont des types de codes d'authentification de message (MAC, Message Authentication Code) impliquant une fonction de hachage cryptographique et une clé secrète. HMAC ne chiffre pas le paquet IP. À la place, le hachage MAC (le code d'authentification du message) doit être envoyé en parallèle avec le paquet. À l'arrivée, le hachage du paquet IP est calculé à nouveau grâce à la clé secrète, si le hachage calculé et celui reçu correspondent, alors la vérification est correcte. Dans le cas contraire, le paquet est rejeté.

*** créé par la NSA**

**** créé par NIST, une agence du département du Commerce des États-Unis**

P.S. C'est sans surprise qu'il est raisonnablement probable que les agences secrètes étasuniennes explorent les lacunes de ces algorithmes.



Chiffrement

Deux variantes principales:
Le chiffrement asymétrique - Deux clés sont utilisées, une clé publique et une clé privée. Les données sont chiffrées à l'aide de la clé publique et déchiffrées avec la clé privée. On parle aussi de cryptographie à clef publique. C'est cette méthode que les clients de messagerie électronique utilisent avec pgp.
Le chiffrement symétrique - Une clé unique est utilisée pour chiffrer et déchiffrer les données.

L'échange de clé publique RSA est un algorithme de cryptographie asymétrique. Il peut être utilisé pour des signatures numériques, pour des échanges de clés et pour du chiffrement.
L'échange de clés Diffie-Hellman* (DH) est couramment utilisé pour assurer une confidentialité persistante (“forward secrecy” en anglais). Il peut en effet générer suffisamment rapidement de nouvelles paires de clés, ce qui permet de les renouveller à chaque session et de pouvoir les rejeter à la fin de celle-ci. Le processus est le suivant: d'abord les deux pairs s'accordent sur des paramètres communs et génèrent chacun une clé grâce à leurs clés privées; ensuite, ils s'échangent cette clé symétrique via le réseau et chacun mélange la nouvelle clé qu'il a reçue avec sa propre clé privée; le résultat est une clé finale identique des deux côtés; ils peuvent alors utiliser cette clé secrète (sans plus devoir l'envoyer) pour chiffrer leur communication**.

*Les clés DH de faible longueur peuvent être craquées comme cela a été prouvé après les révélations de Snowden.

**fr.wikipedia.org/wiki/Écchange_de_clés_Diffie-Hellman

Les outils pour construire un tunnel

IPsec et OpenVPN sont les configurations les plus populaires et peuvent être mises en place avec des logiciels libres. Mais il faut d'abord décider du type de connexion que l'on veut établir. Si on veut connecter des machines derrière un pare-feu (gateway-to-gateway) et que l'on est dans une situation où il n'y a pas de censure ou de filtrage, alors IPsec peut convenir et permet de garder un tunnel ouvert en permanence. En cas de censure, par contre, les ports standards d'IPsec (50, 51, 500 et 4500) seront certainement bloqués par les autorités.

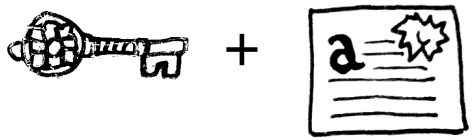
OpenVPN est pratique pour créer un accès à distance entre client et serveur (host-to-host) dans les cas où il faut accéder à des sites dont l'accès est restreint, non accessibles par l'Internet public, ou lorsque l'on souhaite faire transiter tout ou une partie du trafic par un tunnel. En effet, OpenVPN peut être configuré avec n'importe quel port ouvert (pour autant que le port ne soit pas utilisé par d'autres protocoles comme SMTP, VoIP, TLS…). Le tunnel ne sera alors pas détecté par le fournisseur d'accès ou les autorités**. Il permet de connecter de nombreux utilisateurs à un VPN, et il est également facile à installer sur les téléphones portables.

*Il existe une variante communautaire et une variante plus commerciale d'OpenVPN. Cette dernière propose une interface web qui permet une configuration plus facile, mais le nombre d'accès utilisateurs doit être acheté. La version gratuite permet un nombre illimité d'utilisateurs.

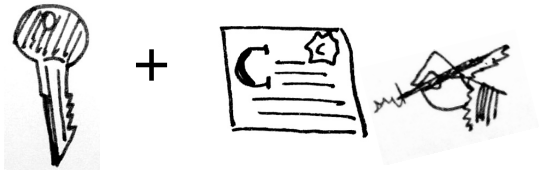
**Les FAI/autorités bloquent certains ports pour filtrer les contenus.

OpenVPN

openVPN utilise OpenSSL pour générer les clés privées et les certificats pour:
- l'Autorité de Certification qui signe les autres certificats

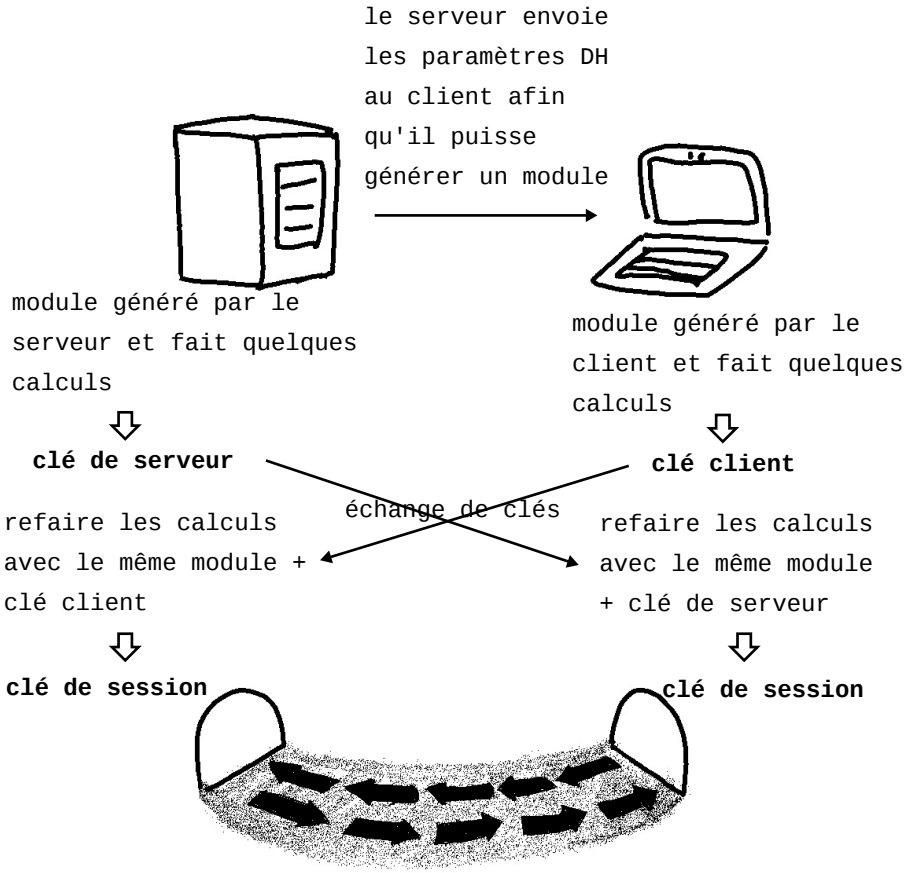


- le serveur,
- les utilisateurs qui peuvent avoir des certificats individuels ou partager le même (plus facile mais moins sûr s'il y a beaucoup d'utilisateurs).



Le nombre d'utilisateurs connectés en même temps peut être fixé dans le fichier "server.conf" qui contient toutes les options que l'on peut définir pour le tunnel. Il est créé à l'installation du logiciel OpenVPN. **Attention : il faut prévoir un nombre élevé pour le paramètre diffie-helman**. La librairie easy-rsa est également installée en même temps qu' OpenVPN. Elle facilite la génération des clés et des certificats. Une fois qu'ils ont été générés, le fichier de configuration client est censé avoir les mêmes paramètres que le fichier server.conf et est envoyé au client en même temps que son certificat et sa clef.

Un tunnel avec openVPN



le tunnel commence!
chiffrement symétrique avec la même clé de session

Avec OpenVPN, DH est utilisé pour l'échange de clés. Les paramètres DH sont envoyés au client, ce qui lui permet de générer un secret partagé. Un nouveau secret est alors généré à partir de celui-ci et est utilisé comme clé de session pour chiffrer les données de communication.

IPsec

Strongswan est une option logicielle libre qui permet de configurer IPsec avec plusieurs choix d'authentification et de chiffrement.

Il y a 2 modes dans IPsec:
Le mode transport, où seules les données utiles du paquet IP sont chiffrées ou authentifiées. Le routage n'est pas altéré, puisque l'en-tête IP n'est ni modifié ni chiffré. Remarque: lorsqu'un en-tête d'authentification (AH) est utilisé, les adresses IP ne peuvent pas passer par un NAT (un routeur qui fait de la translation d'adresse réseau), car, comme l'adresse IP n'est plus la même avant et après le NAT, la valeur du hachage ne sera jamais valide.

Le mode tunnel, où l'entièreté du paquet IP est chiffré et authentifié. Il est ensuite encapsulé dans un nouveau paquet IP avec un nouvel en-tête IP. Le mode tunnel est LE VRAI TUNNEL. Il est surtout utilisé pour créer des réseaux privés virtuels, principalement pour des communications de réseau à réseau (p. ex. entre des routeurs pour relier des sites entre eux), mais il permet aussi d'établir des communications d'hôte à réseau (p. ex. pour un accès à distance) et des communications d'hôte à hôte (p. ex. pour un chat privé).

Un tunnel avec IPSec

IKE (Internet Key Exchange) est un protocole utilisé pour mettre en place des informations de sécurité partagées (SA, “security assocation” en anglais) dans IPSec. À l'aide de ces SA, un secret partagé est créé pour chaque session et permet de générer les clefs qui serviront au chiffrement des données envoyées dans le tunnel. IKE sert également à authentifier les deux pairs IPSec à l'aide d'un secret partagé à l'avance ou par un jeu de clefs privées/publiques.

Le module ESP (encapsulation) d'IPsec utilise des algorithmes de chiffrement qui traitent les données par blocs d'une taille prédéfinie. C'est pour cette raison que la postambule ESP (les derniers bits) dispose d'une zone de bourrage qui permet d'ajuster la taille des données chiffrées afin de remplir le bloc à la taille requise par l'algorithme (voir schéma en page 3: «Paquet IP avec encapsulation»). La clef de chiffrement dans IPsec peut être créée avec les algorithmes DES/3DES/AES. DH est utilisé pour chiffrer cette clef et l'envoyer (en très bref).

Liens pratiques

Configurer un VPN site à site avec IPsec (en anglais):
https://blog.ruanbekker.com/blog/2018/02/11/setup-a-site-to-site-ipsec-vpn-with-strongswan-and-preshared-key-authentication/

Options de configuration pour IPsec avec logiciel Strongswan (https://www.linguee.fr/francais-anglais/search?source=auto&query=strongswan)
(en anglais):
https://wiki.strongswan.org/projects/strongswan/wiki/ConnSection

Un guide utile sur l'authentification et l'encapsulation, avec des exemples tant pour le mode transport que le mode tunnel d'IPsec (en anglais):
http://www.unixwiz.net/techtips/iguide-ipsec.html

Configurer un tunnel d'accès distant avec OpenVPN
(en anglais):
https://community.openvpn.net/openvpn/wiki/HOWTO

Un peu d'histoire concernant le modèle OSI originel, avant la suprématie du protocole TCP/IP dans les réseaux
(en anglais):
https://spectrum.ieee.org/tech-history/cyberspace/osi-the-internet-that-wasnt

L'article de Wikipedia sur les tunnels et des protocoles:
https://fr.wikipedia.org/wiki/Tunnel_(reseau_informatique)

Une performance événementielle sur le fonctionnement du chiffrement (en anglais)
http://ooooo.be/cryptodance/