TUNNEL UP / TUNNEL DOWN

this zine is made with hand drawn icons

layout designed with scribus

the font for text is liberation mono

the font for the cover and the colophon is sans-guilt-wafer by OSP foundry

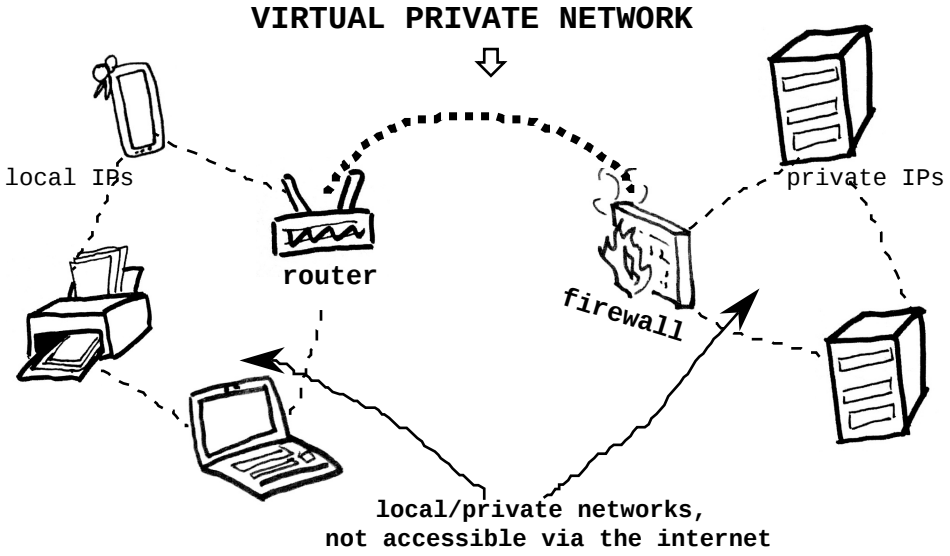
for zine inquires or other info contact:
author mara@multiplace.org

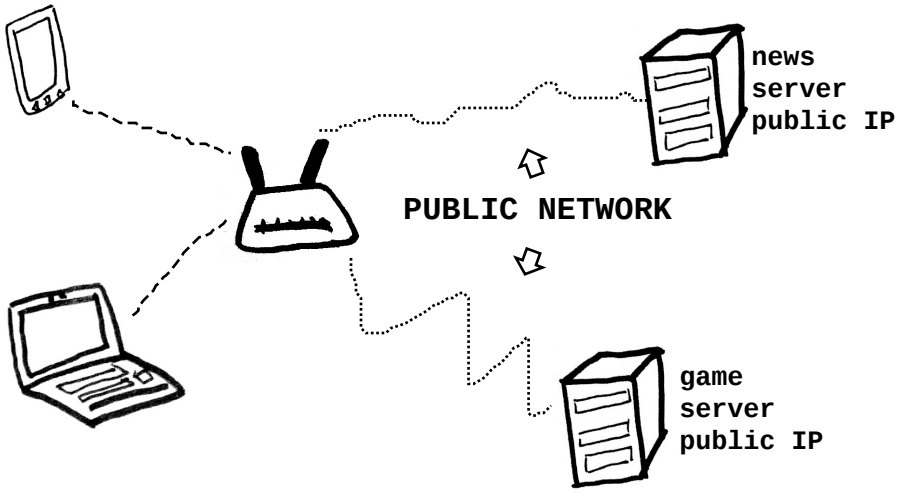
CC-BY-NC-SA 2019

what is a VPN?

Virtual Private Network (aka VPN) is an extension of the public network. For instance, when at home, our devices can be connected via the local network. Imagine that your device can connect to a local network of another home :) Or to a private network of a group of servers behind a firewall of an organization or office, not accessible from the public network.

Thus the "virtual" part of the name, since a VPN allows for machines which are in different local networks to communicate via a safe passage that enables door-to-door delivery with no interaction from the routers the traffic travels through.



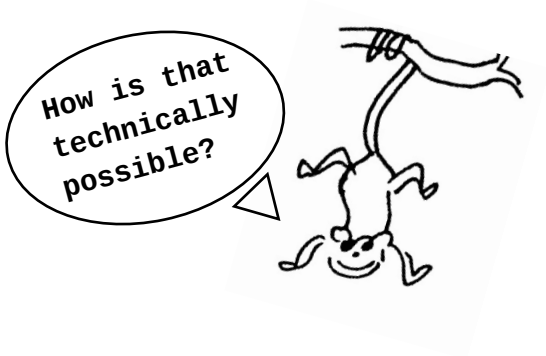


While the public network connects your home/office devices to a server with a public IP address.

Types of VPNs:

- host-to-host (remote access, ex. device to server)
- site-to-site / gateway-to-gateway / network-to-network

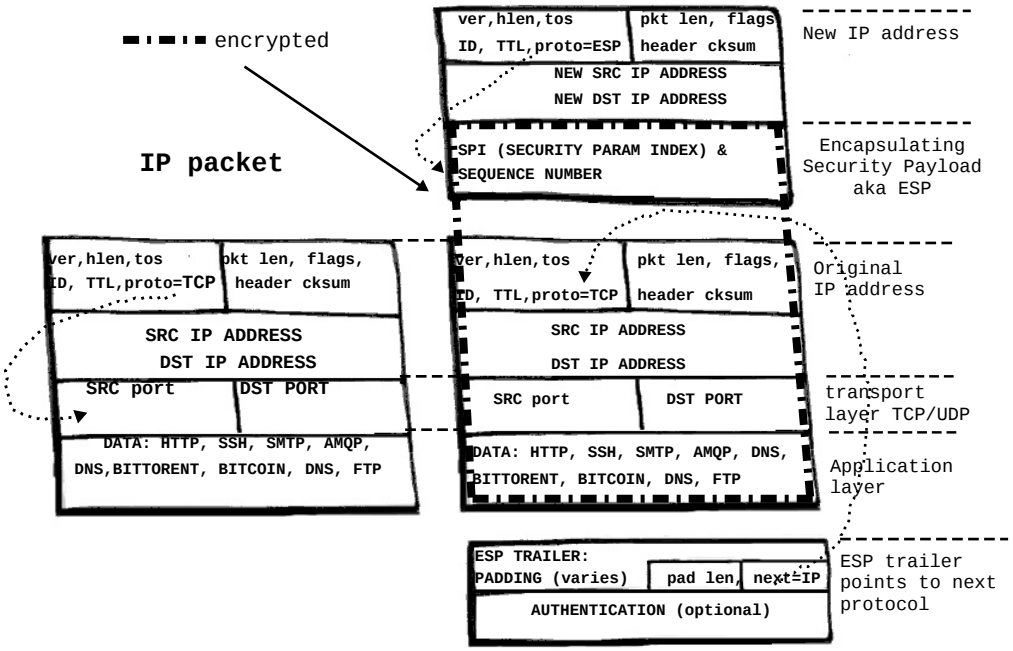
both types can provide access to resources behind a firewall such as virtual machines, media storages, while the first can provide Internet access to censored sites.



How does a VPN work?

VPN uses the tunneling protocol (a communication protocol) to transfer data across the Internet as if it was a private network.
To do so, tunneling encapsulates, basically wraps, IP packet within a new IP header.
The wrapped original IP header contains the destination (private) IP address while the new IP packet layer has as destination the public IP of the VPN server.

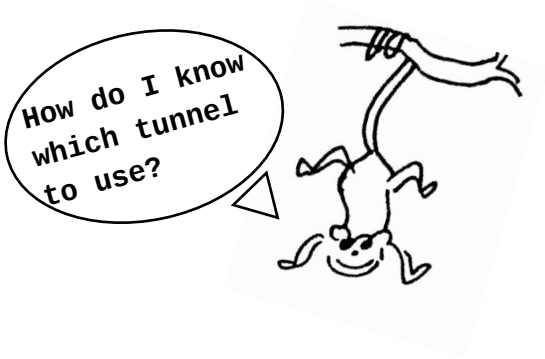
IP packet with ENCAPSULATION



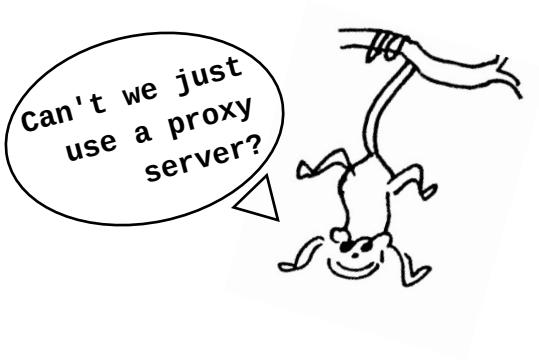
Common tunnel protocols

- IP in IP (ex. connects 2 IPv4 networks that wouldn't be able to talk to each other, such as a virtual IP in a load balancer forwarding packets to servers with real IPs)
- **IPsec** (Internet Protocol Security)
- **OpenVPN**
- GRE (Generic Routing Encapsulation by Cisco, can also encapsulate an IPv6 address within an IPv4)

Here we'll focus on IPsec and openVPN
IPsec is preferable for gateway-to-gateway tunnels, where openVPN is better for remote access tunnels (client to server)
IPsec vs GRE
GRE tunnels can be implemented in cisco routers for encapsulation of a network layer protocol over another. For example, we could implement a GRE tunnel to route IPv4 packets across a network that only uses IPv6. GRE doesn't provide encryption, therefore GRE tunnels can be supplemented by IPSec for security and privacy purposes.



when do we need a tunnel?



Deciding on what type of tunnel to use, depends on our network setup and what we try to achieve:

1. Circumvent a network traffic filter imposed by a government, a university, work office, otherwise called “censorship”. With a tunnel, our data hides inside the tunnel until it reaches the VPN server, from where it gets forwarded to the final server destination (e.x social media, video, news sites)

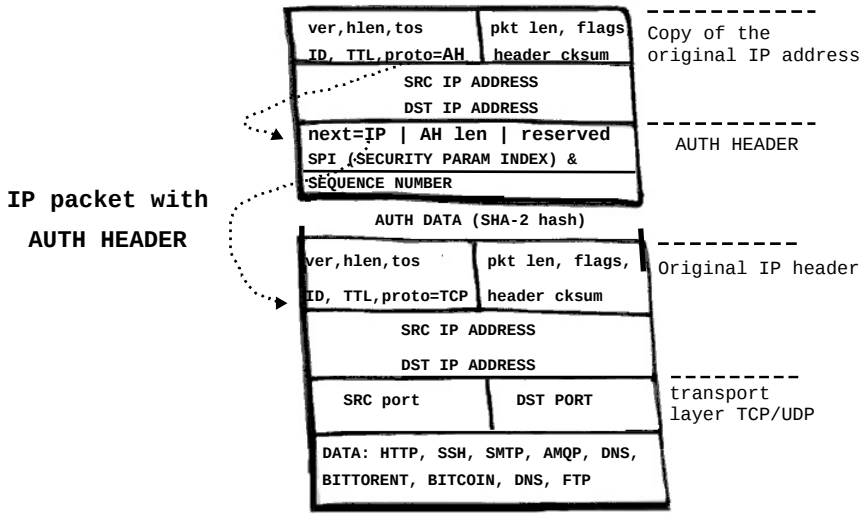
2. Connect to an intranet (aka private or local network) which is physically located away from our device.
Ex. ssh can offer remote server access to a server with a public IP. A tunnel can grant ssh access to a private server. Or to a machine located at someone’s home ;)

While a proxy can hide your IP, and is easier to install or providers offer at a lesser cost, it doesn’t encrypt your traffic. VPN tunnels allow access to resources behind a firewall, while a proxy only forwards traffic to another server. So a proxy can cover case 1, – anonymity against IP filtering, although without encryption, it doesn’t cover case 2 – establishing private networks and accessing resources behind firewalls.

So VPN is more secure than a proxy, because

is a tunnel that can happen with or without encryption. But it always requires **authentication** and can verify **integrity** of data making sure that no one has tampered with our data in transit. And can be **encrypted** too.

Authentication Header - AH
Proves a user or a network is allowed access, by providing a username and/or password.
IPsec authentication happens usually with pre-shared secret, or more comlex setup with private keys and certificates. OpenVPN uses private keys and certificates.



Integrity
ensures data has not been altered/intercepted when in transit. A hash mechanism is used to ensure that. Two algorithms a VPN server uses for verifying integrity of data are the SHA and the MD family. The hash algorithms hmac-md5 and hmac-sha2* or hmac-sha3** are types of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key. HMAC does not encrypt the IP packet. Instead, the MAC hash must be sent alongside the packet. Parties with the secret key will compute the hash of the IP packet when arrives to the receiving point of the tunnel, and if it is authentic, the received and computed hashes should match. If not, the packet is discarded.

* designed by NSA

**designed by NIST, an agency of the US department of commerce

PS. No wonder why is fairly plausible for US secret agencies to explore vulnerabilities of these algorithms

encryption

Two main flavors:
Asymmetric encryption - Two keys are used, a public key and a private key. Data is
encrypted using the public key and decrypted with the private key. Also known as public key encryption. Email clients use this method with pgp.

Symmetric encryption - A single key is used to encrypt data and decrypt data.

RSA public key exchange is an asymmetric encryption algorithm. It can be used with digital signatures, key exchanges and for encryption.

Diffie-Hellman* key-exchange
is a frequent choice for forward secrecy by generating new key pairs fast enough for each session and discard them at the end of it.
The process works by two peers agreeing on common parameters and generating a key with their private keys. Then they exchange this symmetric key over the wire. Each of the two mixes the new key they received from the other with their own private key again. The result is a final key that is identical to the other's final key. They can use this identical key (without sending it over the wire) to encrypt their onwards communication.

* DH with low length can be cracked as it was proved post Snowden

** https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange#Secrecy_chart

what IPSec and openVPN use?

IKE (Internet Key Exchange) is a protocol for setting up security associations (SA) for IPSec. Through these SA a shared session secret is created from which keys are derived for encryption of tunneled data. IKE is also used to authenticate the two IPSec peers with the options of a preshared secret or public/private keys.

The ESP (encapsulation) module in IPsec uses encryption algorithms that operate on data in units of a block size. That's why the ESP trailer has a padding to adjust the size of the encrypted data to the required by the algorithm block size (see schema in p.3 "IP packet with encapsulation").

Encryption key in IPsec can be created with the algorithms DES/3DES/AES.
DH is used to encrypt that key and send it over (very brief description)

In openVPN the DH is used for Key Exchange. The DH parameters are sent to client allowing it to generate a shared secret. Then a new secret will be generated from that and used as a session key to encrypt communication data.

What tools are out there for building a tunnel?

IPsec and OpenVPN are the popular setups and free software options are available. First we need to decide on what type of connection we want to establish. If we want to connect machines behind a firewall (gateway-to-gateway), and we are not concerned with censorship, because if we do then IPsec's standard ports 50, 51, 500 and 4500 are easily blocked by authorities. But if filtering isn't the problem, and we want to keep the tunnel constantly alive, then IPsec is suitable.

For a client-server remote access (host-to-host) where we need to access restricted sites not accessible by public Internet, or we want to forward all or some of our traffic via a tunnel, then openVPN* is handy since it can be configured with any open port (which is not taken by other protocols, e.x SMTP, VoIP, TLS) while the tunnel staying undetected by the provider/authority**. It can connect many users to the VPN, and it is also easily installed on mobile phones.

* openVPN has a community and a commercial flavor. The second comes with a web interface with easier configuration but the number of users' access has to be purchased. The free version allows as many users as desired.
** Internet providers/authorities block certain ports for filtering.

IPsec

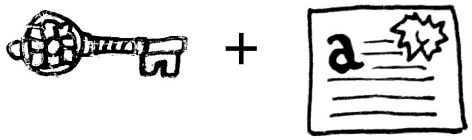
A free software option for building IPsec is **strongswan** with various authentication and encryption choices.

There's 2 modes in IPsec:
Transport mode, where only the payload of the IP packet is usually encrypted or authenticated. The routing is intact, since the IP header is neither modified nor encrypted; **Note:** when the AH is used, the IP addresses cannot pass through a network address translation (NAT), as this always invalidates the hash value since the IP address before and after NAT has changed.

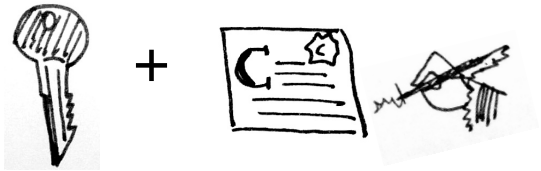
Tunnel mode, where the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is **THE REAL TUNNEL** used to create virtual private networks mostly for network-to-network communications (e.g. between routers to link sites), but can also do host-to-network communications (e.g. remote user access) and host-to-host communications (e.g. private chat)

OpenVPN

openVPN uses **openssl** to generate private keys and certificates for:
- the Certificate Authority that signs all other certificates



- the server
- for the users, who can have individual certificates or share the same (easier but less secure if many users).



The number of users connected concurrently can be set in the **server.conf**, which is the file with all the options we need to set for our tunnel and it's installed with the openVPN software. *Critical: set a high number for diffie-helman parameter*. Another library that's installed with openVPN is the easy-rsa which helps to generate keys the keys and the certificates. Once those have been issued, the client's config file has to have same settings as the server.conf and sent to the client together with their certificate and the key.

Cheat Sheet

Configure a site-to-site VPN with IPsec:
https://blog.ruanbekker.com/blog/2018/02/11/setup-a-site-to-site-ipsec-vpn-with-strongswan-and-preshared-key-authentication/

Options for IPsec with stongswan configuration:
https://wiki.strongswan.org/projects/strongswan/wiki/ConnSection

A usuful guide to Authentication and Encapsulation with illustrations in both transport and tunnel mode for IPsec:
http://www.unixwiz.net/techtips/iguide-ipsec.html

Configure a remote access tunnel with openVPN
https://community.openvpn.net/openvpn/wiki/HOWTO

Some stories about the original OSI model before the TCP/IP took over in networking:
https://spectrum.ieee.org/tech-history/cyberspace/osi-the-internet-that-wasnt

Wikipedia's article on tunneling protocol with a list of tunnels:
https://en.wikipedia.org/wiki/Tunneling_protocol

A performance guide on how encryption works
http://ooooo.be/cryptodance/