Questo manuale è parte del progetto
VPN-zine di psaroskalazines.gr

ha icone disegnate a mano

realizzazione del layout con Scribus

i font del testo sono liberation mono,
KP Programmer e CasaleTwo

il font della copertina e del colophon è
sans-guilt-wafer by OSP foundry

contatta chi ha scritto la zine su
mastodon systerserver.town/@mara

Traduzione in Italiano del progetto:
https://antennine.noblogs.org

TUNNEL SÙ / TUNNEL GIÙ

UNA FANZINE SULLE RETI DI TUNNEL VIRTUALI

We hope you enjoyed reading this technical zine!

Visit the story behind the VPN-zine project at:
https://zines.cucu.gr/prints/bundle-vpn-zine-en/

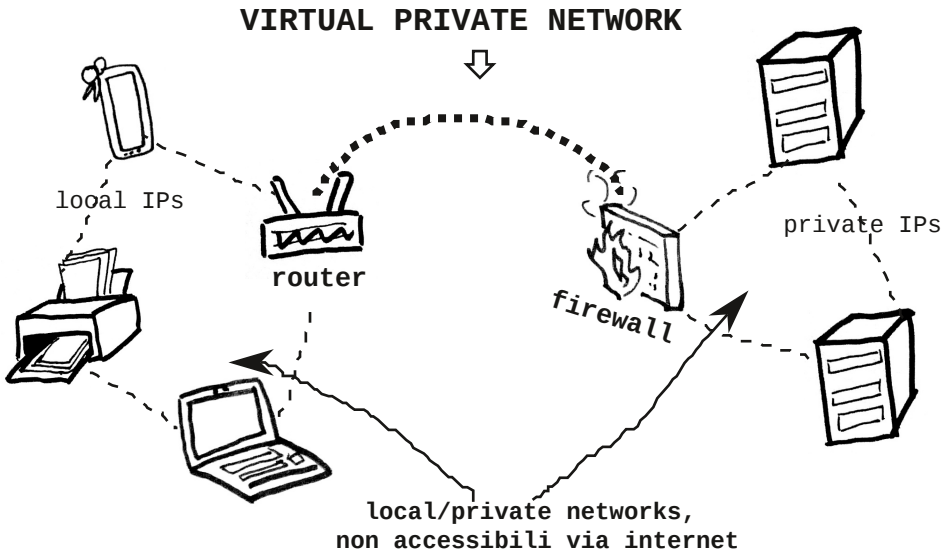
All VPN zines are available for download from psaroskalazines.gr, but if you like our project consider supporting us by purchasing a physical copy from zines.cucu.gr!

Una introduzione ai tunnel, come funzionano, perchè sono differenti dai proxy e più sicuri, e quali strumenti utilizzare per IPsec e openVPN.

Cos’è una VPN?

Virtual Private Network (VPN), una Rete Privata Virtuale è una estensione della rete pubblica, Per esempio, quando, a casa, i nostri apparecchi possono essere connessi alla rete locale. Immagina che il tuo dispositivo possa connetterti alla rete locale di un’altra casa :) o alla rete privata di un gruppo di server dietro ad un firewall di una organizzazione o di un ufficio, non accessibile dalla rete pubblica.

Quindi la parte del nome "Virtuale", poichè una VPN permette a computer che sono in differenti reti locali di comunicare, attraverso un passaggio sicuro che permette la consegna porta a porta senza interazione da parte dei router attraverso i quali passa il traffico.



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

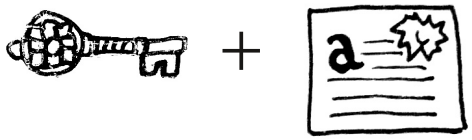
Some stories about the original OSI model before the TCP/IP took over in networking:
https://spectrum.ieee.org/tech-history/cyberspace/osi-the-internet-that-wasnt

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

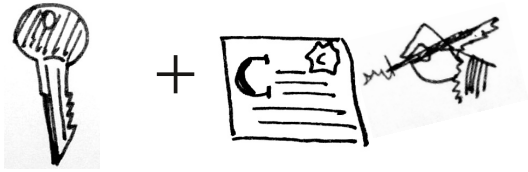
A performance guide on how encryption works
http://ooooo.be/cryptodance/

OpenVPN

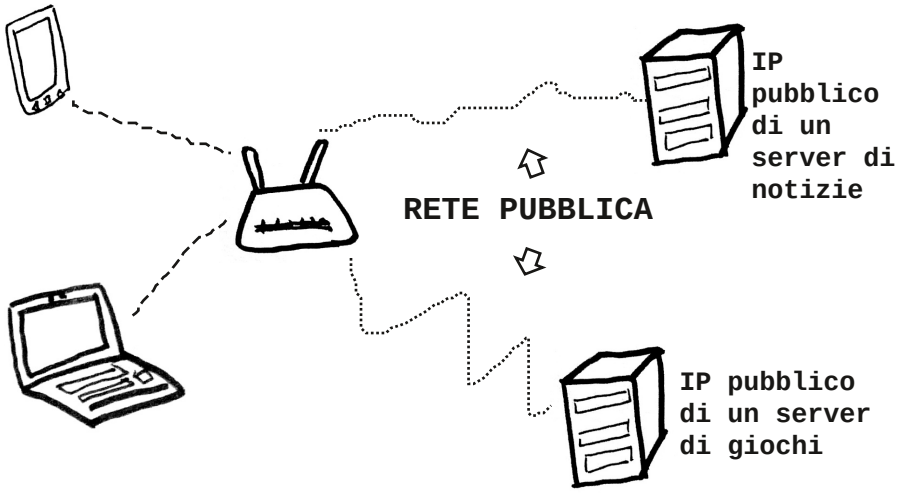
OpenVPN usa openssl per generare chiavi private e certificati per:
- la Certificate Authority che firma tutti gli altri certificati



- il server
- per gli utenti, che possono avere certificati individuali o condividere lo stesso (più facile ma meno sicuro se su molti utenti).



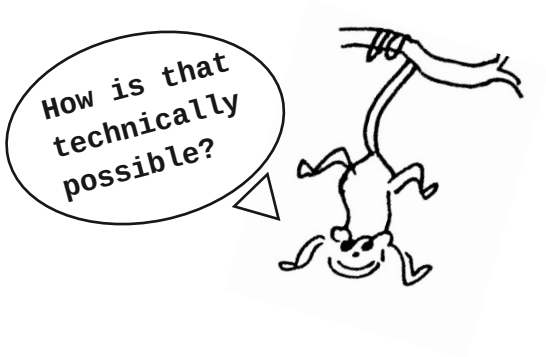
Il numero delle persone connesse in maniera concorrenziale può essere stabilito nelle **server.conf**, che è il file con tutte le optioni di cui abbiamo bisogno per impostare il nostro tunnel e viene installato con il software openVPN. *Critico: impostare un valore molto alto per il parametro Diffie-Helman*. Un’altra libreria che è installata con openVPN è easy-rsa che aiuta con la generazione delle chiavi e dei certificati. Una volta che questi sono stati emessi, il file di configurazione del client deve avere le stesse impostazioni come server.conf ed essere inviato al client insieme al suo certificato e alla chiave.



Mentre la rete pubblica connette il tuo device di casa o ufficio ad un server con un IP pubblico.

Tipi di VPN:
- host-to-host (accesso remoto, es. dal PC al server)
- site-to-site / gateway-to-gateway / network-to-network

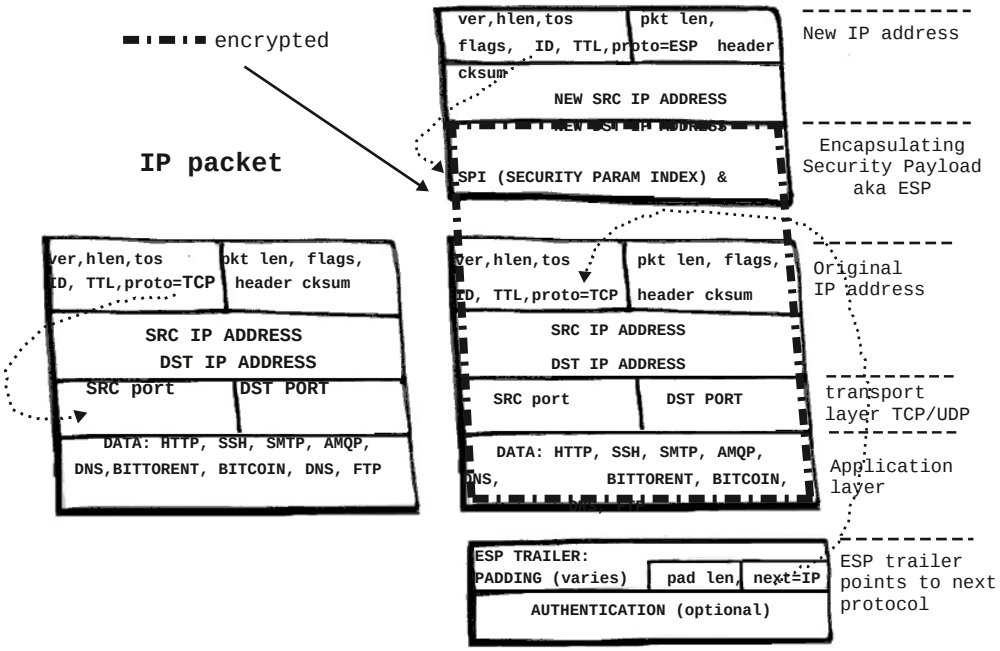
entrambi i tipi possono fornire accesso a risorse dietro un firewall quali macchine virtuali, file audio/video, mentre la prima può fornire un accesso via internet a siti censurati.



Come funziona una VPN?

Le VPN usano il protocollo di tunnelling (un protocollo di comunicazione) per trasferire dati attraverso internet come se fosse una rete privata. Per farlo l'intunnellamento incapsula, sostanzialmente avvolge il pacchetto IP con un nuovo IP header (intestazione). L'intestazione IP originale così celata, contiene l'indirizzo IP di destinazione (privato), mentre il nuovo livello superiore di pacchetto IP ha come destinazione l'indirizzo IP pubblico del server VPN.

pacchetto IP con INCAPSULAMENTO



IPsec

Una opzione in free software per costruire tunnel IPsec è **strongswan** con varie scelte di autenticazione e cifratura.

Ci sono 2 modalità in IPsec: Modalità Transporto, dove solo il carico del pacchetto IP è cifrato o autenticato. L'instradamento rimane intatto dal momento che l'intestazione IP Header non è modificata né cifrata. **Nota:** quando viene utilizzato un AH (Authentication Header), gli indirizzi IP non possono passare attraverso una traduzione degli indirizzi di rete (NAT), perchè questo invalida sempre il valore di hash perchè l'indirizzo IP prima e dopo il NAT viene cambiato.

Modalità Tunnel, quando l'intero pacchetto IP packet è cifrato ed autenticato. Viene incapsulato in un nuovo pacchetto IP con una nuova intestazione. La modalità tunnel è **IL VERO TUNNEL** utilizzato per creare reti private virtuali e soprattutto per comunicazioni network-to-network (es. tra router a punti di collegamenti), ma può anche fare comunicazioni host-to-network (es. un utente ad un accesso remoto) e comunicazioni host-to-host (es. chat private).

Che strumenti ci sono per costruire tunnel?

IPsec e OpenVPN sono le configurazioni più diffuse e sono disponibili opzioni in software libero. Per prima cosa dobbiamo decidere il tipo di connessione che vogliamo stabilire. Se vogliamo connettere computer dietro ad un firewall (gateway-to-gateway), e non ci preoccupiamo della censura, perchè se lo facciamo le porte standard di Ipsec, la 50, 51, 500 e 4500 sono facilmente bloccate dall'autorità. Ma se la censura non è un problema e vogliamo tenere un tunnel stabilmente attivo, allora IPsec è una buona scelta.

Per un accesso remoto client-server (host-to-host) dove abbiamo bisogno di accedere a siti privati, non accessibili pubblicamente in Internet, oppure vogliamo inoltrare tutto o parte del nostro traffico tramite tunnell, allora openVPN* è maneggevole poichè può essere configurato con qualsiasi porta aperta (che non sia già utilizzata da un altro protocollo, es. SMTP, VoIP, TLS) mentre il tunnel rimane invisibile ai provider e alle autorità**. Si possono connettere molti utenti alla VPN, ed è anche facilmente installabile su smartphone.

* ha una versione community ed una commerciale. La seconda si presenta con una interfaccia web ed una configurazione semplificata, ma il numero degli accessi degli utenti deve essere acquistato. La versione libera permette tanti utenti quanti si desidera.

** I fornitori di Internet e le autorità bloccano certe porte per censura.

Protocolli comuni per tunnel

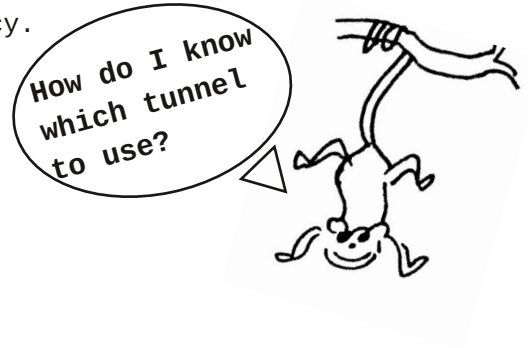
- IP in IP (es. connette 2 reti IPv4 che non sarebbero in grado di parlarsi l'un l'altra, come un IP virtuale in un bilanciatore del carico che inoltra pacchetti verso un server con un IP pubblico)
- **IPsec** (Internet Protocol Security)
- **OpenVPN**
- GRE (Generic Routing Encapsulation di Cisco, può anche incapsulare indirizzi IPv6 dentro un indirizzo IPv4)

Qui approfondiremo IPsec e openVPN

IPsec è preferibile per tunnel gateway-to-gateway, mentre openVPN è migliore per tunnel da accesso remoto (client to server)

IPsec vs GRE

I tunnel GRE possono essere implementati nei router Cisco per l'incapsulamento di un protocollo del livello di rete sopra un altro. Per esempio, possiamo implementare un tunnel GRE per indirizzare pacchetti IPv4 attraverso una rete che usa solamente IPv6. GRE fornisce cifratura, per questo i tunnel GRE possono essere integrati da IPSec per ragioni di sicurezza e privacy.



Quando abbiamo bisogno di un tunnel?

Decidere che tipo di tunnel usare, dipende dal setup della nostra rete e da quello che vogliamo ottenere:

1. Aggirare un filtro all’instradamento del traffico imposto da un governo, una università, un ufficio, anche detto “censura”. Con un tunnel i nostri dati sono nascosti dentro al tunnel fino a quando non raggiungiamo il server VPN, da dove sono inoltrati verso la destinazione finale (es. social media, video, siti di notizie)
2. Connettersi ad una intranet (aka rete privata o locale) la quale è fisicamente situata lontano dal nostro dispositivo, ad esempio ssh può offrire un accesso remoto ad un server con un indirizzo IP pubblico. Un tunnel può fornire un accesso ssh a un server privato. O ad un computer che sta a casa di qualcuno ;)

Che cosa usano IPSec e openVPN?

IKE (Internet Key Exchange) è un protocollo per impostare associazione sicure (SA – security associations) per IPSec. Attraverso queste SA viene creato un segreto di sessione condiviso, dal quale sono derivare le chiavi per la cifratura dei dati tunnellati. IKE è anche usato per autenticare I due peer IPSec con le opzioni di segreto pre-condiviso o chiavi pubbliche/private.

Il modulo ESP (incapsulamento) in IPsec utilizza algoritmi di crittografia che operano sui dati in unità di dimensione “blocco”. Per questo motivo, il trailer ESP ha un padding, “imbottitura”, per adattare la dimensione dei dati crittografati alla dimensione del blocco richiesta dall'algoritmo (si veda lo schema a pag. 3 "Pacchetto IP con incapsulamento").

La chiave di cifratura in IPsec può essere creata con gli algoritmi DES/3DES/AES.
DH è usato per cifrare quella chiave e inviarla (descrizione molto sintetica)
In openVPN l’algoritmo DH è usato per lo scambio di chiave (Key Exchange). I parametri di DH sono inviati al client permettendogli di generare un segreto condiviso. Quindi viene generato un nuovo segreto da questo ed utilizzato come chiave di sessione per cifrare la comunicazione.

Cifratura

In due salse principali:

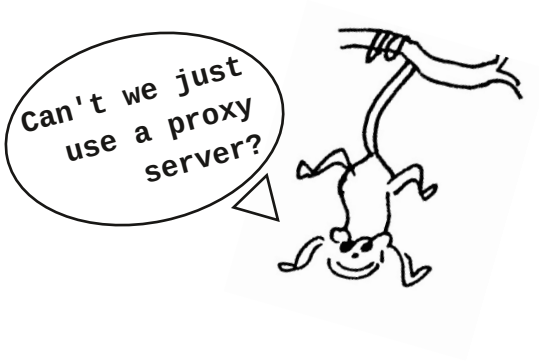
Cifratura Asimmetrica - Vengono usate due chiavi, una chiave pubblica ed una chiave privata. I dati sono cifrati usando la chiave pubblica. I client email utilizzano questo metodo con pgp.
Cifratura simmetrica – Una sola chiave è usata per cifrare i dati e decifrarli.

Lo scambio di chiave pubblica RSA è un algoritmo di cifratura asimmetrica. Può essere usato per le firme digitali, scambi di chiave e per cifrare.

Lo scambio di chiavi Diffie-Hellman* è una scelta frequente per la “segretezza in avanti” (forward secrecy) generando nuove coppie di chiavi abbastanza velocemente per ogni sessione e scartandole alla fine della stessa. Il processo funziona con due peer che si accordano su parametri comuni e generano una chiave con le loro chiavi private. Quindi si scambiano questa chiave simmetrica via cavo. Ciascuno dei due mescola la nuova chiave ricevuta dall'altro con la propria chiave privata più volte. Il risultato è una chiave finale identica a quella dell'altro. Possono usare questa chiave identica (senza inviarla via cavo) per crittografare le loro comunicazioni successive.

* DH con una lunghezza ridotta può essere rotto, come è stato dimostrato post Snowden

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

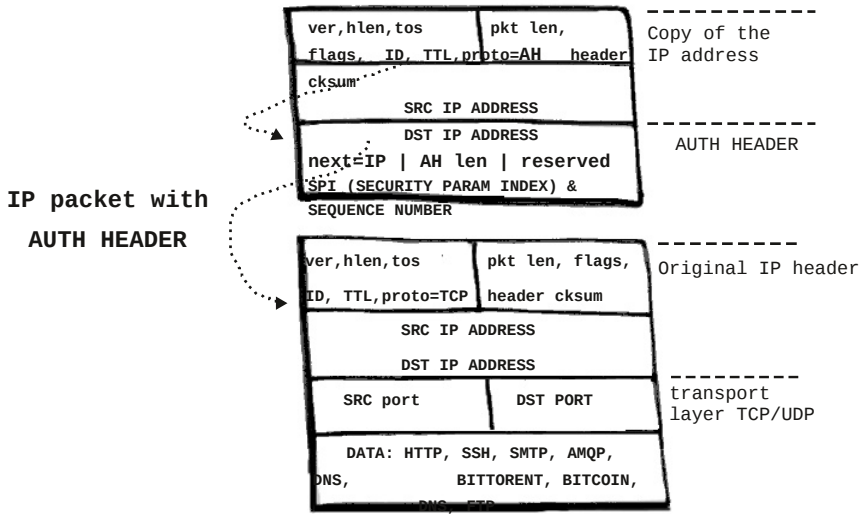


Mentre un proxy piò nascondere il tuo indirizzo IP, ed è più facile da installare o I fornitori lo offrono ad un costo minore, questo non nasconde il tuo traffico. I tunnel VPN permettono accesso a risorse dietro ad un firewall, mentre un proxy inoltra semplicemente il traffico ad un altro server. Quindi un proxy può coprire il caso 1, – anonimato contro filtraggio IP (censura), anche senza cifratura, esso non copre il caso 2 – instaurare reti private ed accedere a risorse dietro a dei firewalls.

Quindi una VPN è più sicura di un proxy,perchè

è un tunnel che può essere creato con o senza cifratura. Ma richiede sempre una autenticazione e può verificare l’integrità dei dati, garantendo che nessuno abbia manomesso i nostri dati in transito. E può anche essere **cifrato**.

Authentication Header - AH
Dimostra che ad un utente o ad una rete sia consentito l'accesso, fornendo un nome utente e/o una password. L'autenticazione IPsec avviene di solito con un segreto pre-condiviso o con una configurazione più complessa con chiavi private e certificati. OpenVPN utilizza chiavi private



Integrità
L'integrità garantisce che i dati non siano stati alterati/intercettati durante il transito. Viene utilizzato un meccanismo di hash per garantire ciò. Due famiglie di algoritmi utilizzati da server VPN per verificare l’integrità dei dati, sono SHA e MD. Gli algoritmi di hash hmac-md5 e hmac-sha2* o hmac-sha3** sono tipologie di codice di autenticazione dei messaggi (MAC - message authentication code) che coinvolgono una funzione hash crittografica e una chiave crittografica segreta. HMAC non cifra il pachetto IP. Invece, l’hash del MAC deve essere inviato insieme al pacchetto. Le parti con la chiave segreta calcolano l'hash del pacchetto IP quando arriva al punto di ricezione del tunnel e, se è autentico, l'hash ricevuto e quello calcolato dovrebbero corrispondere. Se no, il pacchetto viene scartato.

* progettato dall'NSA

**progettato da NIST, una agenzia del Dipartimento del Commercio degli Stati Uniti. Non meraviglia perché sia abbastanza plausibile credere che le agenzie segrete statunitensi esplorino le vulnerabilità di questi