Protezione delle reti

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Protezione delle reti

- Infrastrutture di rete (fisica e wifi)
- VPN

..

Proteggere l'accesso alla rete Ethernet

Proteggersi da collegamenti indesiderati alla rete:

- MAC locking: blocco delle porte mediante ACL sul MAC address
- ACL locking: blocco delle porte mediante regole più sofisticate (ad esempio non accetto due MAC address sulla stessa porta)
- 802.1X port authentication: configurazione che impedisce l'instaurarsi del collegamento fisico finché non è completata una fase di autenticazione
- NAC: network access control, configurazione in cui la fase di allacciamento alla rete è gestita ad alto livello e include, oltre all'autenticazione, anche altri controlli sul dispositivo (es. Presenza di antivirus, vulnerabilità), oppure il reindirizzamento su Captive portal.
- VLAN management: le porte sono assegnate a VLAN diverse e la Management VLAN è separata dalle altre e protetta da regole esplicite di accesso

802.1x:
Port Authentication

http://en.wikipedia.org/wiki/IEEE_802.1X

802.1x Port Authentication

Lo standard 802.1x è stato pensato per consentire il controllo dell'accesso alla rete a livello di porta.

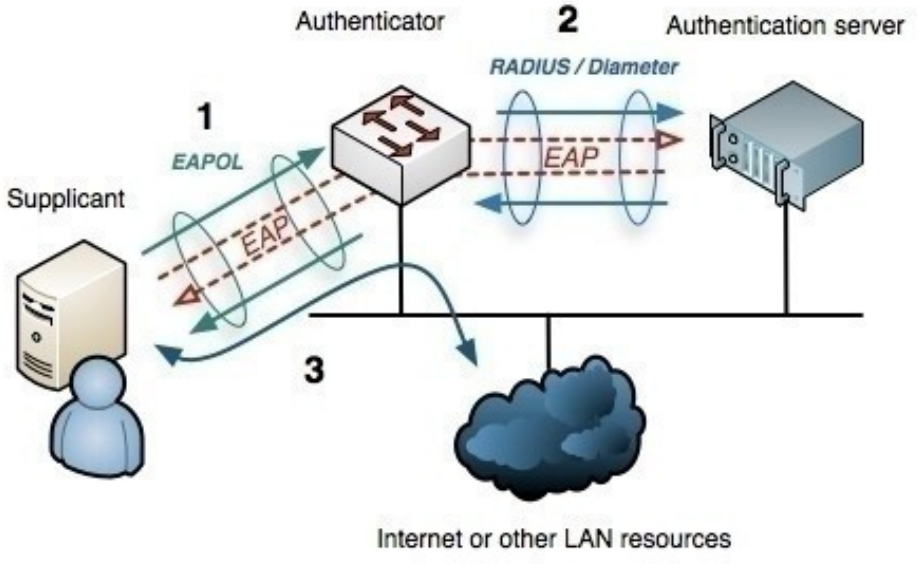
E' un'architettura di autenticazione a livello 2 (MAC)

La sicurezza port-based prevista da 802.1x permette ai dispositivi di rete di richiedere all'utente un'autenticazione prima che questo ottenga accesso alla rete.

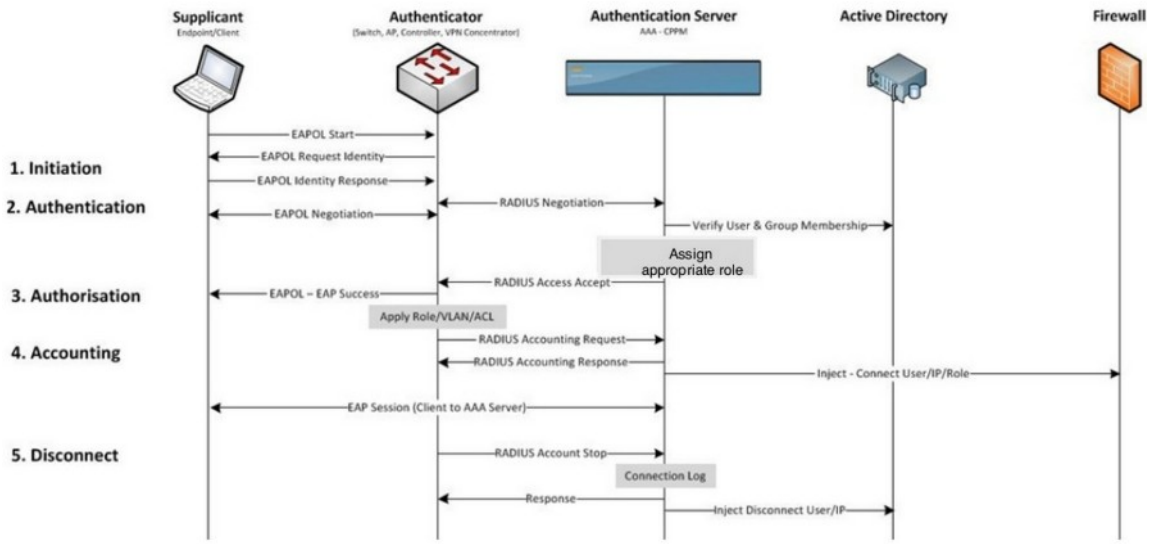
Vi sono implementazioni di 802.1x sia nelle reti wired che wireless.

Presente praticamente sempre nel wireless sta prendendo piede anche nel mondo wired.

802.1x: Port Authentication



1) Il supplicant si connette alla rete e viene messo dal dispositivo su una VLAN separata dove c'è solo l'authenticator. Fra i due avviene la richiesta di autenticazione EAP.
2) L'authenticator tramite Radius chiede conferma dell'autenticazione al server centrale (es. Active Directory)
3) Se autenticazione OK il supplicant viene ammesso nella rete aziendale.



EAP (Extensible Authentication Protocol) è un framework che permette di usare diversi metodi di autenticazione. Non definisce un protocollo vero e proprio, ma solo i messaggi che devono essere scambiati fra i partecipanti.
Per diventare un protocollo di rete c'è bisogno di incapsulare l'EAP in qualche modo

- EAP-MD5 (username/password, leggero ma debole, ok solo in LAN)
- EAP-TLS (certificati digitali, da gestire)
- EAP-TTLS (solo il client autentica il server con un certificato, il Server autentica il Client con username+password)
- ...

EAPOL=EAP over lan

Proteggere l'accesso alla rete Wireless

http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

- WEP (insicuro da evitare)
- WPA - WPA2 = WiFi Protected Access

Dal 2006 WPA2 (802.11i) obbligatorio su tutti i dispositivi.

- WPA-Personal: WPA-PSK (Pre-shared key) mode, is designed for home networks and doesn't require an authentication server. Each wireless network device authenticates with the access point using the same 256-bit key generated from a password or passphrase.
- WPA-Enterprise: WPA-802.1X mode is designed for enterprise networks and requires a RADIUS authentication server.

Proteggere l'accesso alla rete Wireless

WPA3

Inizio 2018 nasce WPA3.
Sarà un lungo percorso implementativo e di coesistenza (inizio nel 2019)
Chiave a 128 (personal) e 192 (enterprise).
Gestione password dinamica per rendere inutili gli attacchi offline (registro flusso dati e provo a decrittare offline con calma).
Gestione migliorata device senza monitor (QR code).

Authentication Server

AAA = Authentication, Authorization, Accounting (A=Auditing)

RADIUS

TACACS+

Le funzionalità di un server AAA sono Authentication, Authorization, Accounting (implementata esternamente la quarta A=Auditing)

Accounting=Radius record espliciti (billing)

Auditing=analisi di tutto quanto succede

http://en.wikipedia.org/wiki/RADIUS RADIUS (Remote Authentication Dial-In User Service) basato su UDP. Due passaggi (inseparabili): autenticazione/autorizzazione, auditing .

http://en.wikipedia.org/wiki/TACACS TACACS+ (Terminal Access Controller Access Control System) basato su TCP. Le funzioni di autenticazione, autorizzazione e accounting sono separate e possono essere implementate separatamente.

Servizi RADIUS normalmente integrati in directory enterprise (Active Directory)

Rogue Access Point

Wifi Pineapple

https://wifipineapple.com/

Access Point con doppia rete già predisposto per attacco “men in the middle” con software embedded Linux based.
100-200$ a seconda del modello.

Soluzione software basata su WifiPhisher (Open Source)
https://wifiphisher.org/

Rogue Cell Phone Base Station

Stesso principio dei wifi ma applicato alla telefonia cellulare. Sono ripetitori fittizi del segnale cellulare che intercettano gli smartphone delle persone in una certa area.

Richiede attrezzature e complicità disponibili in teoria solamente a livello governativo (e operatori di telefonia mobile un po' consenzienti).

http://www.meganet.com/meganet-products-cellphoneinterceptors.html

Probabilmente usato durante le rivolte della “primavera araba” e dal governo Turco, i “narcos” hanno una loro rete separata ad esempio.

Ma nessun governo forse ha la coscienza pulita …

http://www.csoonline.com/article/2684064/mobile-security/rogue-cell-towers-discovered-in-washington-dc.html

http://www.makeuseof.com/tag/4-things-you-need-know-about-those-rogue-cellphone-towers/

Femtocelle per indoor (10metri)

https://en.wikipedia.org/wiki/Femtocell

Attacchi ai protocolli cellulari

- Oltre ad intercettare il segnale debbo poi attaccare il protocollo.
- Strumenti per intercettare (non si comperano su Amazon) https://en.wikipedia.org/wiki/Stingray_phone_tracker
- Protocollo SS7 (Signaling System 7 1975) per il colloquio fra reti cellulari (vulnerabilità note, poi basta trovare un paese che ti accrediti come carrier “fidato”)
- GSM 2G altamente vulnerabile (colloquio telefono-cella).
- 3G,4G,5G meglio ma esistono vulnerabilità note.
- Poi c’è sempre il problema della portabilità all’indietro (i vecchi telefoni debbono potersi collegare alle nuove antenne e viceversa, quindi il 2G non è ancora morto)

https://www.schneier.com/blog/archives/2020/01/china_isnt_the_.html

Rogue Satelite (GPS spoofing)

Russia 'spoofing' GPS on vast scale to stop drones from approaching Putin, report says

Simulare la presenza di un segnale satellitare con una stazione al suolo. Richiede tecnologie sofisticate (governi).Azioni di guerra mirate al GPS.
https://www.nbcnews.com/news/vladimir-putin/russia-spoofing-gps-vast-scale-stop-drones-approaching-putin-report-n987376
Drone USA fatto atterrare in Iran convinto di essere in Afghanistan
https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident#cite_note-17
GPS Spoofing
https://en.wikipedia.org/wiki/Spoofing_attack#GPS_spoofing
Occhio che economia mondiale vive di GPS
https://qz.com/1106064/the-entire-global-financial-system-depends-on-gps-and-its-shockingly-vulnerable-to-attack/
GPS nasce per scopi militari, per tutti dal 1983 dopo abbattimento aereo di linea coreano per errore.
https://en.wikipedia.org/wiki/Korean_Air_Lines_Flight_007

Virtual Private Network

- Reti nascoste
- Routing protetto
- Protezione crittografica dei pacchetti (OpenVPN, IPSEC)

http://en.wikipedia.org/wiki/Virtual_private_network
Che cosa è una VPN?
Una tecnica (hardware e/o software) per realizzare una rete privata utilizzando canali e apparati di trasmissione condivisi o comunque non fidati.
Tecniche di realizzazione di una VPN:

- mediante reti nascoste (poco efficace, 10.*, non ruotate, ok solo su infrastruttura mia)
- mediante routing protetto (http://en.wikipedia.org/wiki/Tunneling_protocol virtual tunneling protocol, trasporto IP su IP)
- mediante protezione crittografica dei pacchetti (tunnel IP sicuro) http://en.wikipedia.org/wiki/OpenVPN OpenVPN, http://en.wikipedia.org/wiki/IPsec IPSEC. Viene aggiunto un header al pacchetto IP che viene cifrato o autenticato

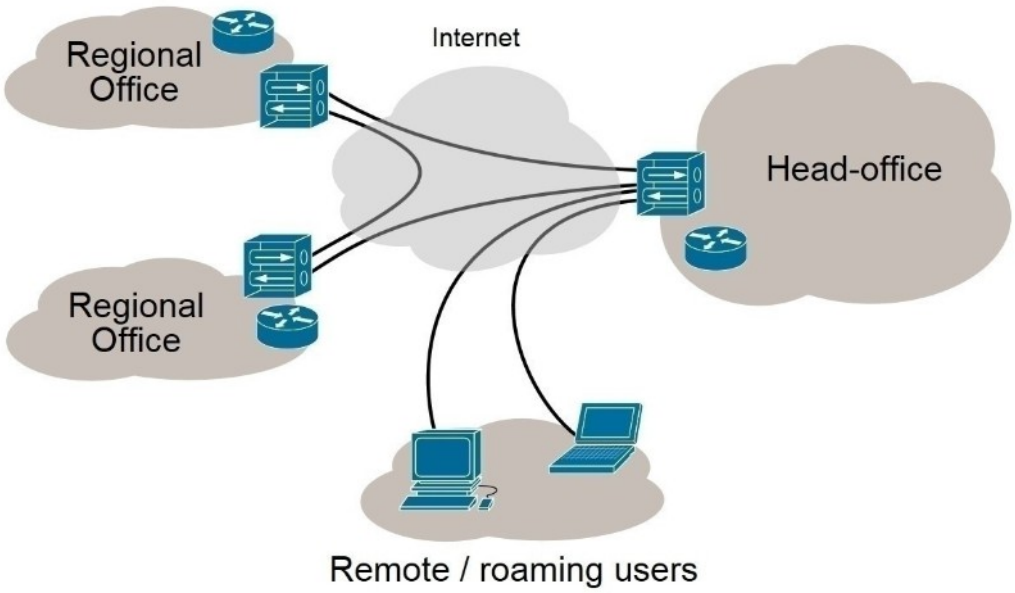
Architetture di VPN

- Remote access o Client To Site
- Site To Site
- Site to Extranet
- Personal VPN

Architetture di VPN

- Remote access o Client To Site
  Un utente singolo che si collega a una sede (telelavoro, mobile)
- Site To Site
  Collega due sedi diverse (sostituisce le linee dedicate)
- Site to Extranet
  Collega una sede a una terza parte, community o cloud infrastructure (es. Google Apps, Office365)
- Personal VPN (uso personale, mi collego al server di un fornitore di servizio VPN per proteggere il mio traffico in transito su reti wifi non sicure, mi debbo ovviamente fidare del provider VPN)

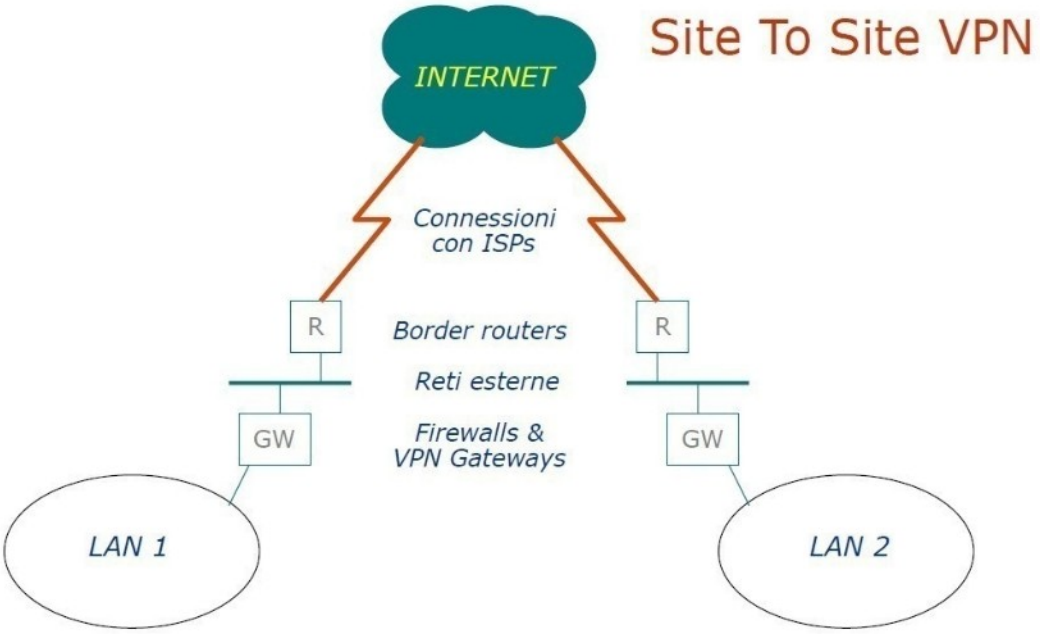
VPN



"Virtual Private Network overview" by Ludovic.ferre (talk · contribs) - Own work. Licensed under GFDL via Wikimedia Commons -

http://commons.wikimedia.org/wiki/File:Virtual_Private_Network_overview.svg#/media/File:Virtual_Private_Network_overview.svg

VPN

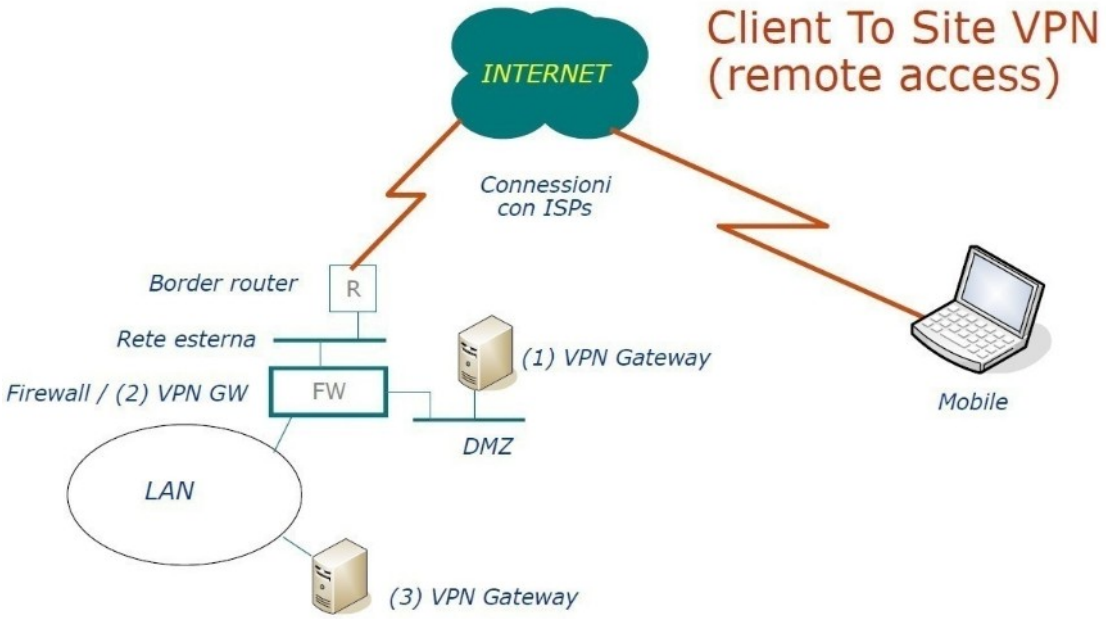


Architetture di VPN

- Site To Site

  Collega due sedi diverse (sostituisce le linee dedicate)

VPN



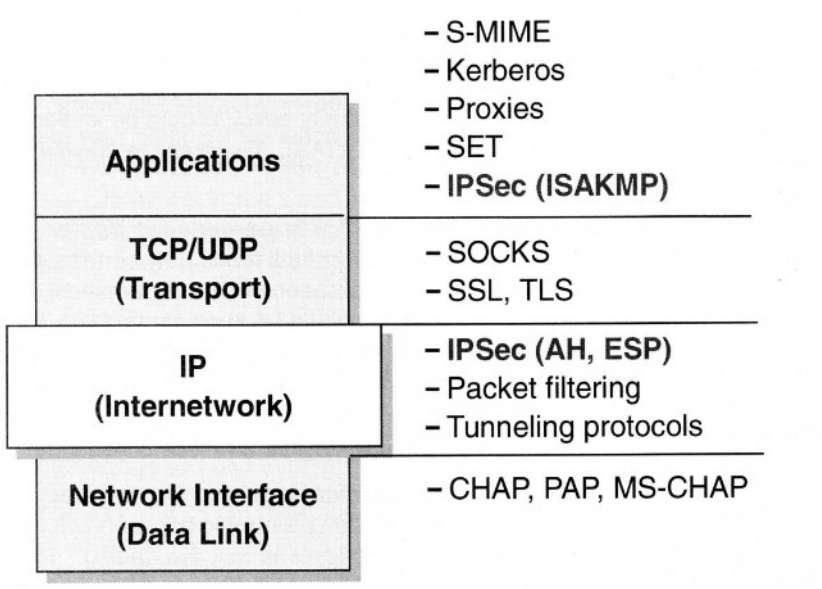
Architetture di VPN

- Remote access o Client To Site
  Un utente singolo che si collega a una sede (telelavoro, mobile)

VPN

Personal VPN, viaggio protetto fino al provider del servizio poi da lì sembra che stia navigando lui.

IPSEC: suite di protocolli



IPSEC è una suite di protocolli a vari livelli dello stack IP.
ESP, Encapsulating Security Payload
AH, Authentication Header
IKE, Internet Key Exchange
ISAKMP,

Interoperabile e indipendente dai protocolli di crittografia.
Doveva essere standard in IPV6 ma non è così.
Due concetti chiave: SA Security Association e modalità di trasporto.

VPN

IPSEC: Security Association
Una connessione logica unidirezionale (simplex) fra due sistemi IP caratterizzata da tre valori:
- Security Parameter Index
- IP destination
- Security Protocol

IPSEC: Security Association (SA)
Una connessione logica unidirezionale (simplex) fra due sistemi IP caratterizzata da tre valori:
- Security Parameter Index (identifica la connessione a parità di IP e protocollo)
- IP destination
- Security Protocol (può essere AH o ESP)

Ne servono almeno due per completare la connessione.
Elenco mantenuto nel Security Association Database.

VPN

IPSEC: Modalità operativa
- Transport Mode
- Tunnel Mode

ISAKMP/Oakley
Framework per lo scambio di chiavi crittografiche e la negoziazione di Security Association

IPSEC: Modalità operativa
- Transport Mode (host to host, viene cifrato solo il payload, protetti solo con hash i livelli trasporto e applicativo, non cambia IP e porta, problemi con NAT, bisogna usare NAT-Traversal)
- Tunnel Mode (network tunneling mode, viene protetto tutto il pacchetto originale aggiungendo davanti un IP header, viene usato per le VPN)

ISAKMP/Oakley (Internet Security Association and Key Management Protocol)
Framework per la generazione, lo scambio e il refresh di chiavi crittografiche e la negoziazione di Security Association.
Tutto automatico, fondamentale in chiave enterprise.
IKE (Internet Key Exchange)= sottinsieme
Supporta PSK, chiavi pubbliche, RSA ecc.

VPN

OpenVPN:

- Basata su OpenSSL, SSLv3 e TLSv1
- Open Source, implementazioni per tutti i sistemi operativi
- Tunnelling layer 2 e 3
- Push di configurazioni (DHCP ecc.)
- Supporta PSK, certificati, username/password
- Supporto NAT, firewall ecc.

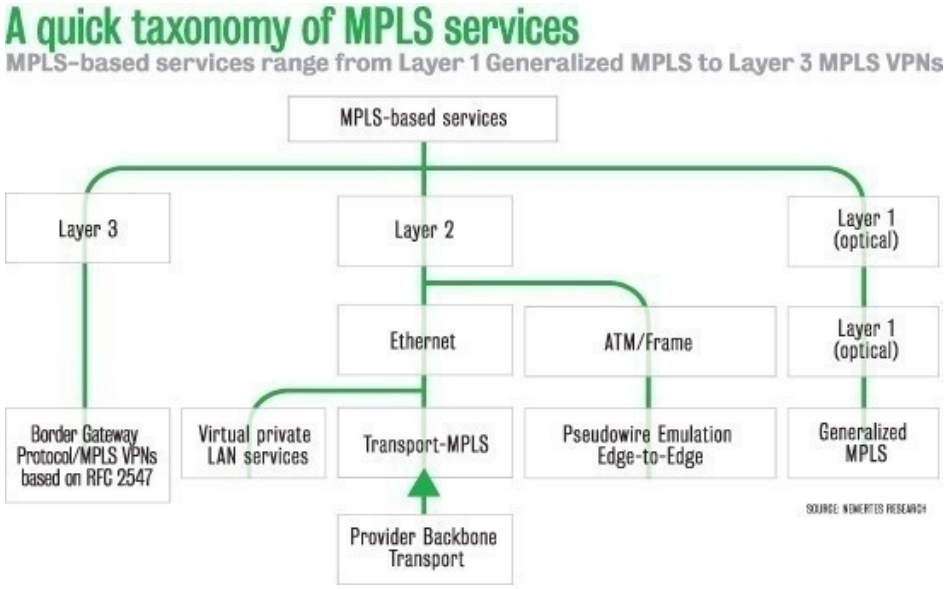
VPN outsourcing

Virtual Private Circuit

VPN outsourcing, a volte dette Virtual Private Circuit.
http://en.wikipedia.org/wiki/Virtual_circuit
Alternativa alla costruzione e gestione delle VPN via Internet: acquistarle da qualcuno che poi le gestisce.
I provider oggi offrono sempre “reti private” sotto forma di VPN, come servizio che rivendono ai clienti che hanno acquistato la connettività presso di loro.
Le tecnologie attuali sono principalmente di tipo MPLS https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching (MultiProtocol Label Switching), di derivazione Ethernet.
Instradamento tramite label invece che routing in base all'indirizzo.
Sono reti che normalmente i Provider stessi tengono logicamente separate dalla connettività Internet tradizionale, per poter costruire offerte con SLA garantiti.

VPN

MPLS

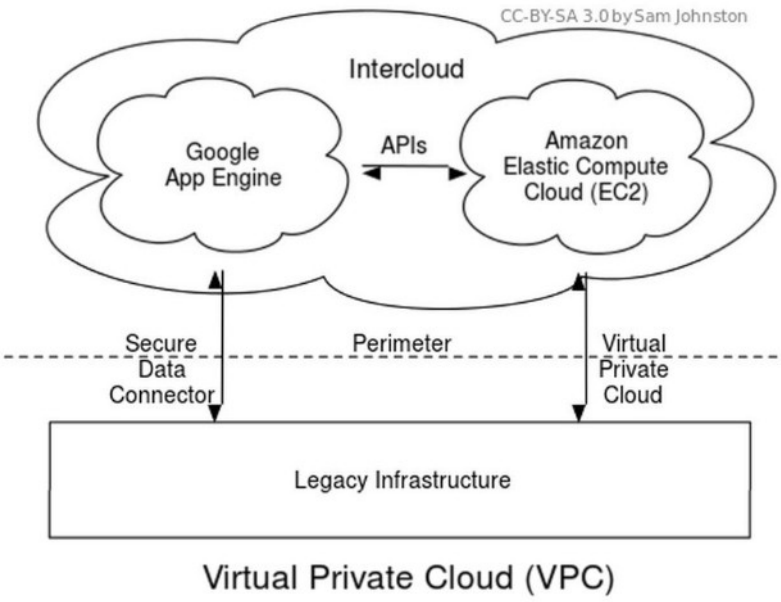


Il concetto fondamentale è l'etichettatura dei pacchetti, che avviene al momento dell'immissione del pacchetto nella rete. Nel normale routing IP, ogni router prende una decisione per ogni pacchetto, che dipende solamente dall'header L3 contenuto.

Nell'MPLS, quando un pacchetto entra nella rete è assegnato a una specifica FEC (Forwarding Equivalence Class), appendendo al pacchetto una stringa di bit apposita (label). Questo primo router effettua anche il lookup del percorso (Label Switched Path) necessario a raggiungere l'ultimo router di destinazione.

Ogni altro router della rete MPLS utilizza la Label per effettuare il forwarding; quindi, eccettuato il primo, i router non effettuano più l'analisi degli header per prendere la decisione di forwarding, ma mandano il pacchetto al prossimo router seguendo il percorso predeterminato all'ingresso dal primo router.

VPN



Virtual Private Cloud (VPC)

http://en.wikipedia.org/wiki/Virtual_private_cloud

Si parla di VPC quando alcuni (o tutti i) servizi sono esterni e stanno presso un “Cloud Provider” (es. Amazon, Google App Engine, Microsoft Azure, VMWare Vcloud).

Nella “nuvola” viene creata una “bolla” privata ospitata in un’infrastruttura virtuale multi-tenant, gestita da un fornitore e accessibile in modo efficiente a livello globale.

Ciascun sito di un'organizzazione diventa dunque una rete-ad-accesso-remoto ai servizi contenuti nella VPC, che sono raggiunti nello stesso modo anche dai singoli utenti remoti.

Non è sempre applicabile: è facile spostare nel cloud le applicazioni web, la posta elettronica, la collaboration.

E' difficile per applicazioni ad alto flusso di dati (es. CAD) o di tipo Client-Server.