Le VPN e il loro funzionamento

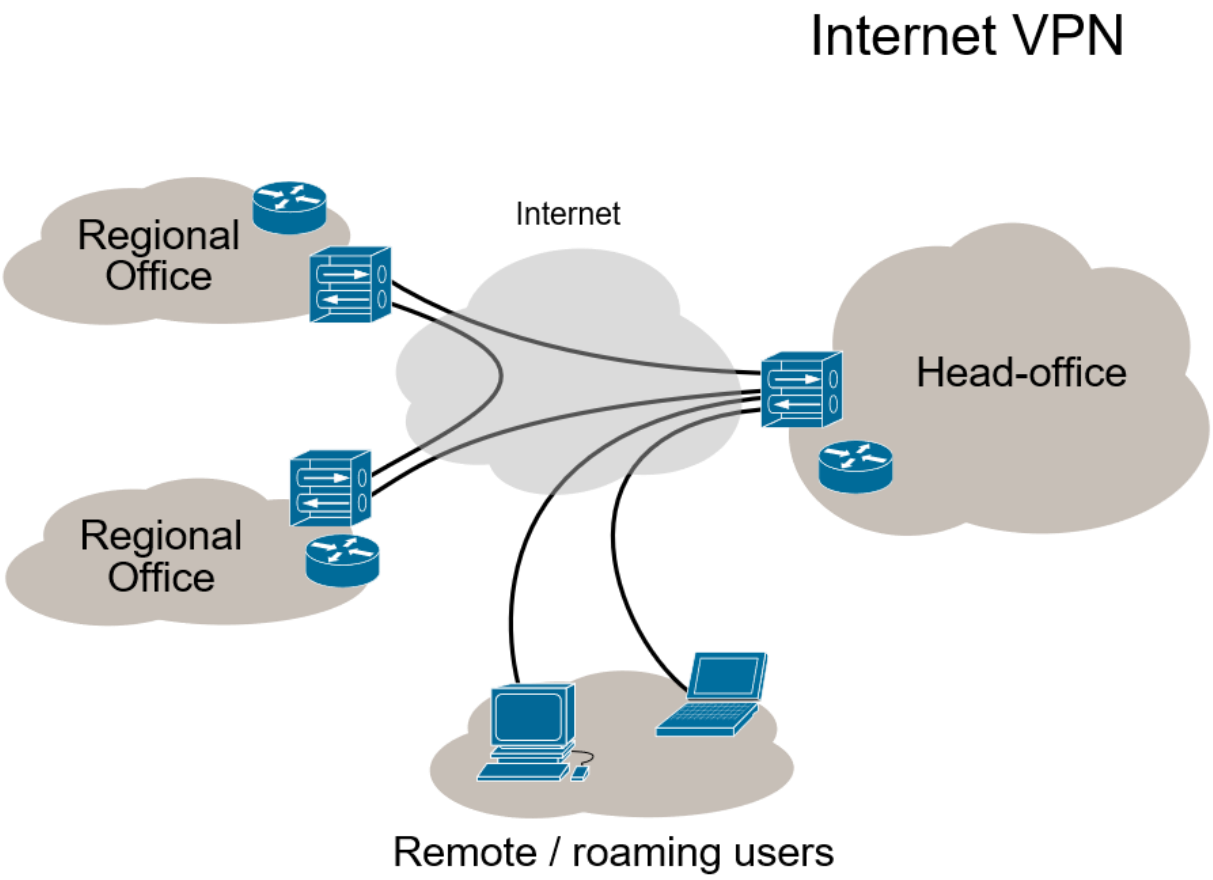
Indice:

1) Caratteristiche delle VPN

Definizione:

La **VPN** (**Virtual Private Network**) è una rete **privata** creata all'interno di un'infrastruttura di rete **pubblica**, come può essere l'Internet.

All'interno di una VPN **l'indirizzamento** è **univoco**, quindi non si possono avere IP uguali, ma si possono trovare connessi differenti tipi di device, l'importante è che abbiano un accesso al web (Pc, tablet, smartphone, TV ecc.).



Come sono nate:

Le VPN nascono in sostituzione **alle reti private fisiche** (canali dedicati che avevano il compito di collegare più siti di un'azienda). Queste reti avevano diversi **vantaggi**, come una larghezza di banda sempre disponibile, nessun problema d'accesso e sicurezza e prestazioni garantite, ma anche numerosi **svantaggi**, come gli alti costi di installazione e manutenzione, tempi lunghi per la configurazione e riconfigurazione e mancanza di

scalabilità.

Vennero così introdotte le **reti private virtuali**, che ebbero successo grazie al fatto che furono **flessibili** e che il **blocco del traffico di rete fosse pressoché nullo** grazie alla grande ridondanza dovuta alla natura stessa della vpn (appoggiata alla rete **pubblica**).

Tale natura però costrinse a dover affrontare 3 grossi problemi:

- La variabilità del tempo di trasferimento
- Il controllo degli accessi
- La sicurezza di trasmissione

2) Tipi di VPN

Le VPN possono essere suddivise in 2 tipologie in base al loro utilizzo e alle componenti fisiche implementate per raggiungere le finalità previste.

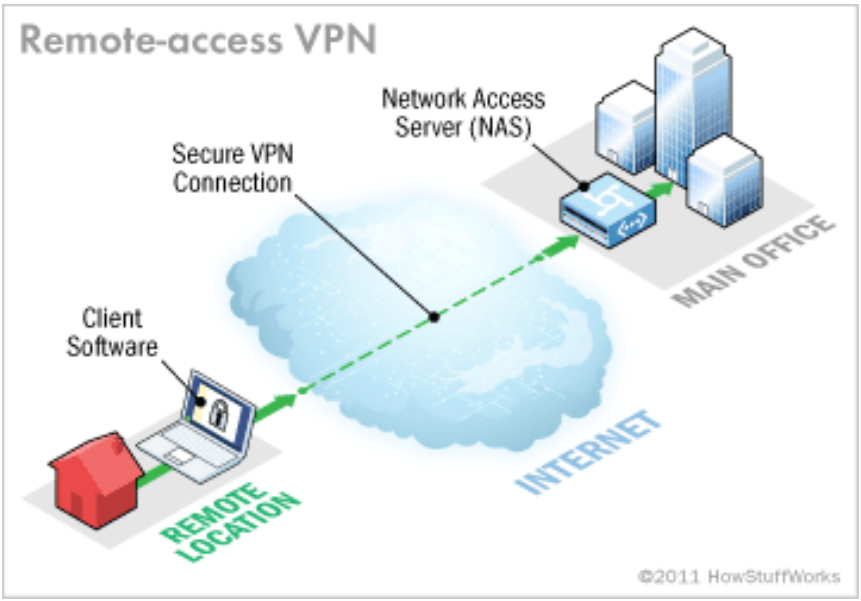
a) Remote-access VPN:

Portano**qualunque** tipo di **dato all'host remoto**. Possono emularne il desktop e sono adatte per i **singoli utenti**.

Consentono ai singoli di effettuare connessioni sicure verso l'esterno.

Le Remot-access possiedono due componenti fisici indispendibili:

- **Server (NAS/AAA):** che permette all'utente di loggarsi e utilizzare la VPN.
- **Software VPN Client:** che permetta l'autenticazione.
- Eventualmente un Firewall per separare la rete privata e l'internet.



b) Site-to-site VPN:

Sono l'alternativa alle WAN Frame Relay e permettono di **estendere le risorse interne verso l'esterno**, connettendo anche differenti LAN dislocate per il mondo, tramite la rete pubblica.

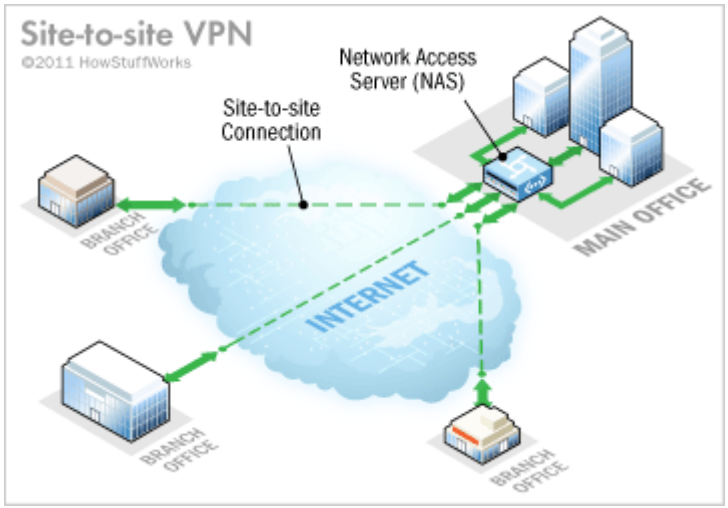
Fondamentale è quindi il concetto di **WAN come insieme di LAN**.

Questo tipo di VPN si suddivide a sua volta in due sotto-categorie: le **intranet-based**, in cui le diverse LAN condividono ogni risorsa interna, e le **extranet-based**, dove le varie LAN condividono solo l'extranet senza però mettere in comunione le risorse interne.

A differenza delle remote-access, le site-to-site **eliminano la barriera per cui i singoli utenti debbano utilizzare ognuno un software per collegarsi alla VPN.**

Per farlo, nelle StS si utilizzano i seguenti dispositivi:

- **VPN Concentrator**: Sostituisce il server AAA, stabilisce il tunnel VPN e gestisce un elevato numero di connessioni contemporanee.
- **VPN Router**: è un router che permette di instradare pacchetti con i protocolli delle VPN.
- **VPN Firewall**: filtro che permette di gestire il traffico di rete tramite i protocolli delle VPN.
- **VPN Client**: Software in esecuzione su un dispositivo dedicato che funge da tunnel-interfaccia ed evita che su ognu macchina sia installato un software VPN client. Ogni host quindi passerà da lui per poter interfacciarsi col web.



3) La sicurezza nelle VPN

Poiché le VPN si appoggiano a una rete pubblica, hanno bisogno di **criteri di sicurezza** per rendere i dati protetti da eventuali rischi del web, ed è quindi per

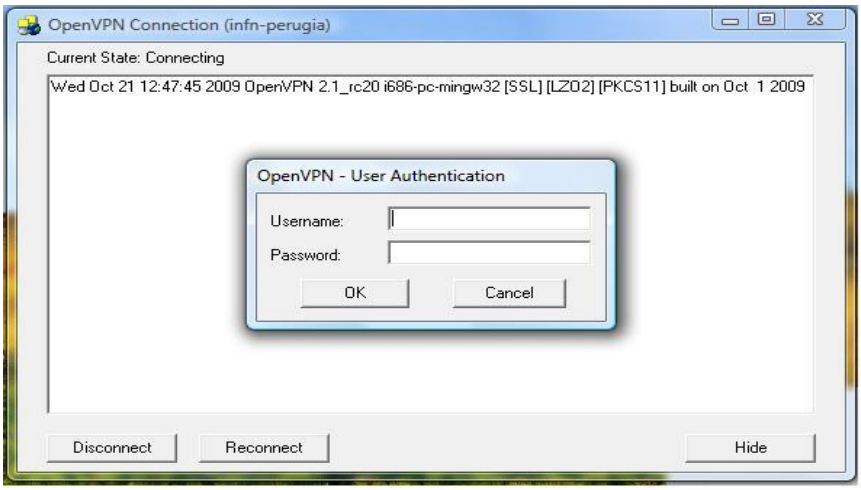
questo che quando si parla di sicurezza nelle Virtual Private Network, ci si riferisce a:

a) Autenticazione:

Processo per il quale un **utente verifica la propria, o per lo meno presunta, identità digitale**, al fine di poter utilizzare un applicativo software in totale sicurezza con le adeguate autorizzazioni.

L'autenticazione viene richiesta poiché si sta parlando di una rete private, e quindi non aperta al pubblico, e dunque che richiede una email/username e password per accedervi.

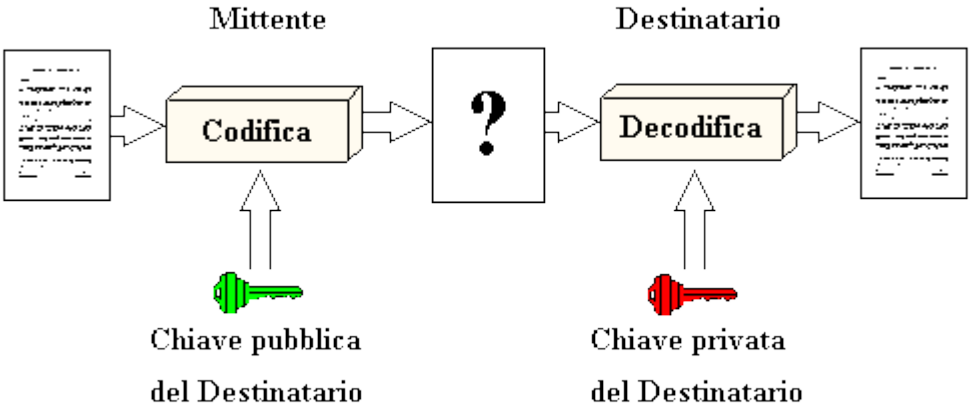
La porta di accesso nelle VPN è il server (NAS o AAA) e talvolta le autenticazioni possono essere anche due, come nel caso di alcune università dove prima si effettua un'autenticazione "di gruppo" e poi dopo un'autenticazione personale.



b) Cifratura:

Quando si parla di cifratura, o crittografia dei dati, ci si riferisce a tutte le **tecniche utilizzate per**, appunto, **cifrare il traffico di rete e non renderlo "chiaro"** agli occhi di eventuali intercettazioni da parte di persone non autorizzate.Nelle VPN la cifratura è obbligatoria, e ci sono differenti tecniche utilizzate, tra queste **IKE** e altre, la cui spiegazione la potete trovare seguendo il link del capitolo 4.

Gli algoritmi per la cifratura dei dati prevedono due chiavi, e queste, assieme allo stesso accordo di utilizzo di un determinato algoritmo, vengono scambiate tra i due host su una **connessione sicura**, in modo da non poter essere intercettate/alterate.



c) Tunneling:

Il tunneling è il procedimento utilizzato nelle VPN per **aggiungere uno strato di sicurezza aggiuntivo**, col fine di proteggere il pacchetto di dati nel suo percorso in internet.

Con il termine Tunneling ci si riferisce quindi al **processo di incapsulamento di un protocollo in un secondo protocollo di pari livello o superiore**.

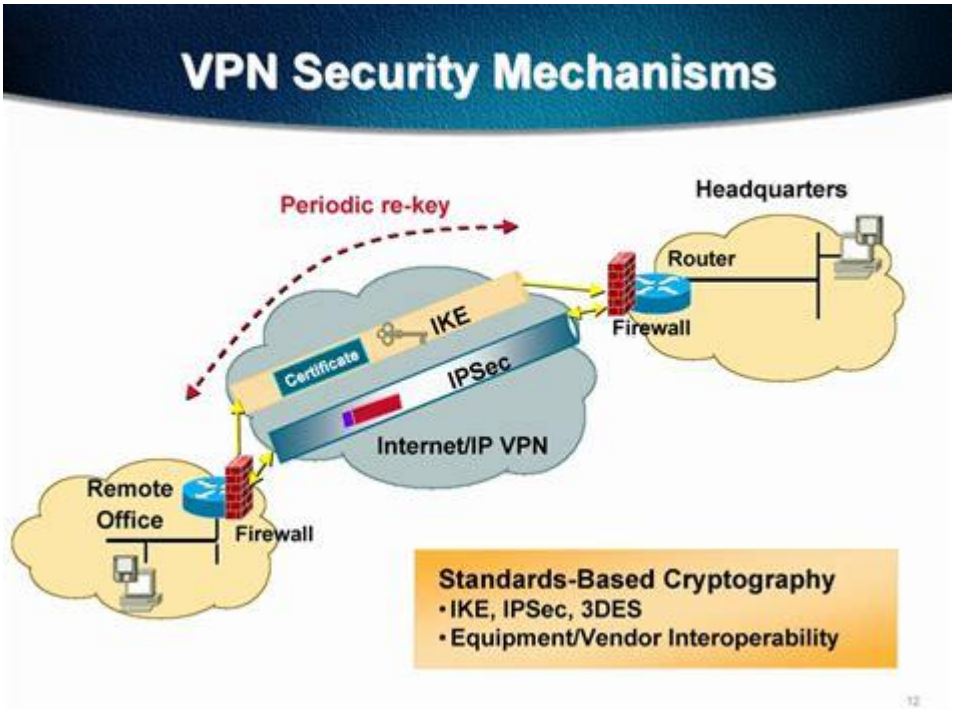
I protocolli usati per il tunneling sono diversi, tra di questi:

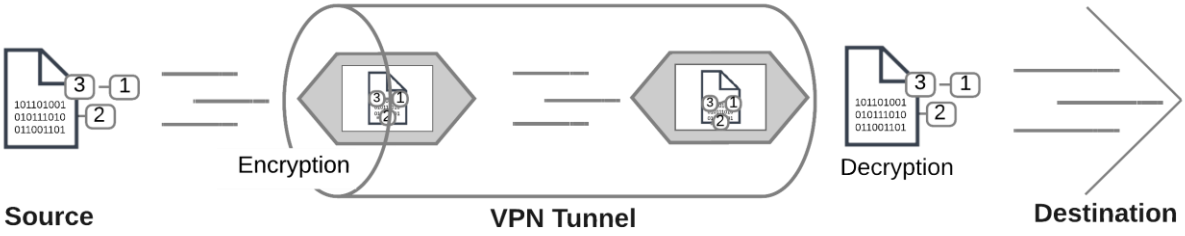
- IPsec
- SSL/TLS
- PPTP
- IEEE 802.1Q
- SSH
- L2TP
- …

Il funzionamento del tunneling, da un punto di vista pratico, è il seguente, e per quanto possano cambiare i protocolli, la logica è sempre la stessa:

il pacchetto di dati principale (**Passenger Protocol**), deve essere trasferito attraverso il web. Per fare ciò, bisogna apporre una preventiva sicurezza al pacchetto, e quindi la **Tunnel interface** (estrmità del "tunnel" in cui il pack viaggerà in sicurezza)incapsula il dato dentro un livello aggiuntivo (**Encapsulating Protocol**). Questo, una volta spedito nel web, verrà ancora

incorporato in un terzo livello, dettato dal protocollo di trasporto (**Carrier Protocol**), fino al raggiungimento del destinatario, dove il pacchetto incontrerà l'altra estremità del tunnel (**seconda Tunnel interface**), che con la stessa logia di incapsulamento della prima interfaccia, eseguirà il processo inverso e otterrà quindi il dato in chiaro.
Per tutto il tragitto, il dato viaggia in una "matriosca" formata da 3 livelli, rendendo così il dato sicuro.





d) Sicurezza globale:

Questa sezione non riguarda una vera e propria metodologia per garantire la sicurezza dei dati, ma analizza da un punto di vista teorico le VPN e i concetti intrinsechi di garanzia di protezione e prevenzione dei dati da esse trasportati.
Le VPN prima di tutto devono garantire **l'integrità** e **autenticità** dei dati dei dati, cioè che i pacchetti rivenuti non siano stati **alterati** e che provengano da una **fonte certa**. La soluzione a tutto ciò è adottare meccanismi di **firmadigitale** e **certificati digitali**.
Per verificare che non siano state effettuate azioni non desiderate o non autorizzate, è necessario prevedere anche meccanismi di **accounting**, cioè delle procedure volte a misurare e documentare le risorse concesse a un utente durante l'accesso. In poche parole quindi si tratta di impostare dei meccanismi per la registrazione e visualizzazione dei cosiddetti file di **log**, misurare la **durata della sessione** di navigazione ecc.
Infine, dal punto di vista dei fornitori, si deve garantire la **confidenzialità**, quindi che i propri dati, conservati dai fornitori, siano ben protetti e riservati dalla fruizione di terza parti.

4) I protocolli usati

Le VPN per garantire la sicurezza dei dati e incapsularli, utilizzano differenti protocolli.
Per vedere il funzionamento di alcuni di questi, scaricare la seconda parte del manuale al seguente link:
[DOCUMENTO IN FASE DI STESURA]

5) Fiducia VS Sicurezza

In base al grado di sicurezza garantito e ai protocolli utilizzati, le VPN si dividono in **3 categorie**:

- **Trusted VPN**: Non utilizzano cifratura e tunneling, ma la riservatezza dei dati trasmessi è affidata a un ISP, che garantisce la QoS (qualità del servizio) assegnando alle VPN in maniera univoca percorsi e canali dedicati. Le tecnologie utilizzate sono: circuiti di rete ATM e MPLS, su 2 e 3 livelli.
- **Secure VPN**: Utilizzano cifrature e tunneling per la protezione dei dati. Possono utilizzare uno o più tunnel, sempre con 2 estremità. Utilizzano

tutte le metodologie descritte precedentemente e i protocolli utilizzati sono: IPSec (ESP, AH, IKE), SSL/TLS, PPTP, SOCK4/5, L2TPv2/3 e altri.

- **Hybrid VPN**: Sono l'unione tra le Secure e le Trusted.