Introduzione alle VPN

Per rete privata virtuale (Virtual Private Network) si intende un meccanismo per realizzare connessioni sicure tra due o più punti (PC, reti, ecc.) geograficamente distanti.

Una **VPN** permette ai dati di viaggiare su una rete TCP/IP pubblica (es. Internet), grazie alla codifica di tutto il traffico da un punto all'altro.
I dati fra le workstation e il server della VPN vengono infatti inoltrati tramite dispositivi di protezione particolari. Fino a poco tempo fa, quando un'azienda voleva un canale sicuro tra sé e la propria filiale utilizzava una "linea dedicata". Questo tipo di soluzione è notoriamente molto costosa, le VPN si propongono invece come l'alternativa più economica e sicura per le aziende. Sfruttando le reti Internet, stabiliscono una sorta di corsia preferenziale, indipendente ed autonoma, tra l'azienda e la filiale. Questa particolare tecnica viene chiamata "tunneling".

Una rete virtuale può essere realizzata a partire da una infrastruttura molto ampia dalla quale si selezionano alcuni nodi che andranno a far parte della nuova rete virtuale. La nuova rete potrà essere non solo di dimensioni arbitrarie, ma addirittura i membri di questa rete non si renderanno conto di sfruttare una rete fisica sottostante per le loro comunicazioni e crederanno invece di sfruttare una rete limitata geograficamente e nel numero di nodi.

Contrariamente alle tecnologie precedenti, il problema della sicurezza su IP non viene più affrontato da un punto di vista fisico. Storicamente l'infrastruttura pubblica impediva ad utenti non autorizzati di far circolare fisicamente i propri dati su VPN altrui (ad esempio mediante l'utilizzo di circuiti virtuali in emulazione dei circuiti dedicati) garantendo l'isolamento delle VPN senza particolari altri mezzi aggiuntivi. Il protocollo IP, viceversa, non è in grado di fornire isolamento fisico e predispone quindi una serie di meccanismi "logici" (autenticazione, crittografia) in grado di simulare la sicurezza "fisica". Dal momento che un host appartenente ad una VPN può essere una macchina pubblica su Internet, l'appartenenza di un pacchetto alla VPN sarà controllata con determinati protocolli in grado di garantire che solo i dati provenienti da sorgenti "fidate" possano essere elaborati. In altre parole non si impedisce più l'arrivo di dati "esterni", quanto ne si impedisce la loro elaborazione (o il loro inoltro sulla rete privata) grazie ad opportuni meccanismi di mutuo riconoscimento tra i membri della VPN.

I principali problemi che riguardano la sicurezza possono essere schematizzati in:

Confidenzialità: è la capacità di tenere riservata una comunicazione; nel caso di comunicazioni non protette un banale packet sniffer posto su una rete aziendale è in grado di catturare (e visualizzare) tutto il traffico che scorre tra qualunque host, con le ovvie implicazioni sulla privatezza delle comunicazioni. Ovviamente un sistema di questo tipo può entrare in possesso di informazioni riservate quali numeri di carte di credito, password, etc.

Integrità: è la capacità di garantire che in una comunicazione verranno recapitati al destinatario esattamente i dati spediti dal trasmettitore. Questo evita, ad esempio, che una comunicazione venga modificata all'insaputa dei due end-points (ad esempio un pagamento non va al legittimo destinatario ma viene "deviato" su un conto corrente "terzo").

Autenticazione (furto dell'identità): è la capacità di assicurarsi dell'identità dell'altro interlocutore. Il furto dell'identità, ossia lo spacciarsi per qualcun'altro compiendo azioni alla sua insaputa (ad esempio spacciarsi per il sito web di una banca, catturando quindi i dati degli utenti che si rivolgono online per fare un'operazione), è sempre più pericoloso in quanto in una transazione elettronica si hanno pochissimi mezzi per verificare la corretta identità dell'altro interlocutore.

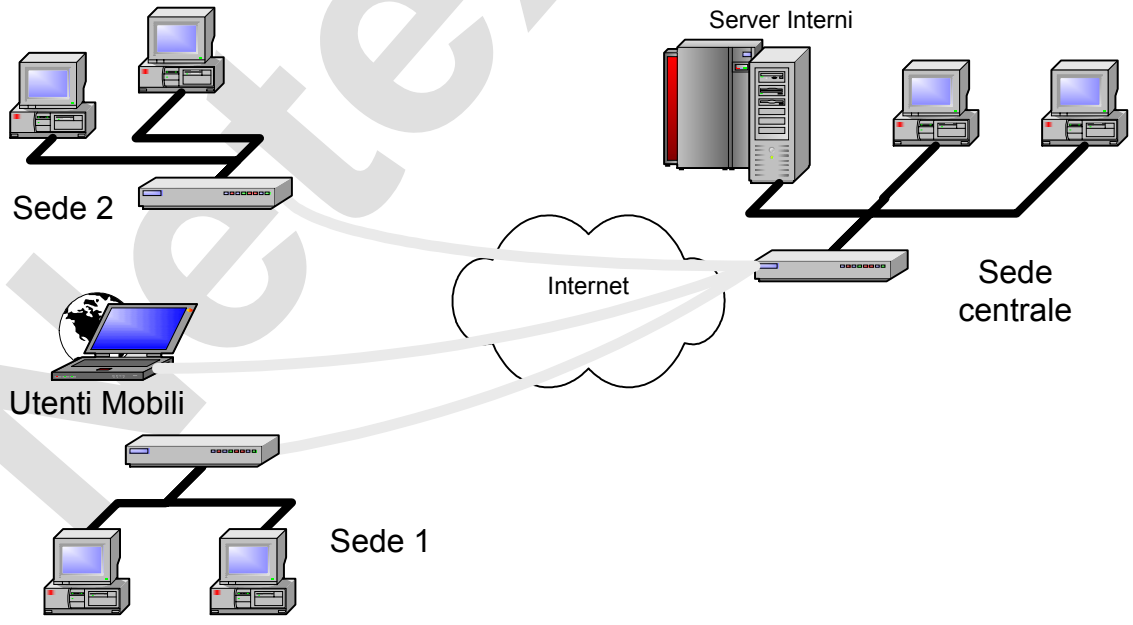
Denial of Service: è l'ultima frontiera degli attacchi su Internet, ossia disturbare (o addirittura annullare) il servizio fornito da una determinata entità; questo può essere ad esempio l'oscuramento di un sito di commercio elettronico, impedendo ai potenziali acquirenti di collegarsi a causa dell'altissimo traffico di disturbo generato.

Altro problema legato all'uso delle VPN su Internet è la definizione e il rispetto di un'opportuna garanzia di servizio. A differenza delle reti precedenti dove i parametri banda-ritardo erano spesso garantiti dall'infrastruttura fisica, IP fornisce garanzie più blande, soprattutto in presenza di VPN distribuite su più gestori.

Architettura di una VPN

Le VPN sono essenzialmente di due tipi

- Host-to-Net: collegamento di un end-system con organizzazioni intere, ad esempio per consentire ad un utente mobile (venditore) di potersi collegare ai server aziendali per la lettura di dati come se fosse fisicamente sulla rete interna dell'azienda
- Net-to-Net: collegamento di organizzazioni intere, ad esempio due stabilimenti di una stessa azienda i quali necessitano di scambiarsi informazioni (ad esempio quelle relative alla produzione)



Esempio di rete privata virtuali "ibrida"

I protocolli utilizzati con le VPN

I protocolli di tunneling vengono utilizzati dai client e dai server VPN per gestire i tunnel e inviare dati in modalità protetta. Di seguito sono riportate le descrizioni dei protocolli maggiormente usati.

Generic Routing Encapsulation (GRE)
Il protocollo GRE specifica un generico meccanismo di incapsulamento per il trasporto di qualunque protocollo X su Y. Il protocollo prevede che il pacchetto originale sia imbustato con un header GRE, e a sua volta inbustato nel protocollo (solitamente IP) che ne garantirà il trasporto alla destinazione.
L'header GRE include infatti un campo Protocol Type, con la stessa codifica prevista per Ethernet, che indica il protocollo trasportato. A sua volta, GRE risponde al Protocol Type IP (codice 47). Non sono previsti particolari meccanismi di autenticazione, etc, ed è possibile sfruttare per questo IPSec.

PPTP
PPTP è un protocollo di rete che permette il trasferimento sicuro di dati da un computer remoto ad un server attraverso un circuito virtuale privato costruito su di una rete TCP/IP come ad esempio Internet.

Gli utenti remoti accedono al server usando una rete pubblica come Internet, ed il protocollo PPTP si incarica di mantenere la riservatezza del canale virtuale cifrando i dati in transito. Una volta connessi, si possono usare tutti i protocolli standard come IP, IPX, e NetBEUI per accedere alle risorse della rete locale.

In tal modo si elimina la necessità di chiamare direttamente il server con telefonate a lunga distanza o di creare una costosa rete dedicata per l'accesso al server.
PPTP è uno standard proposto da compagnie come Microsoft, Ascend Communications, 3Com e USR Robotics ed è supportato da diversi sistemi operativi, sia per il lato client che per il lato server.

L2TP
L2TP è un protocollo di tracking standard IETF ormai affermato e ampiamente implementato. L2TP effettua l'incapsulamento dei frame PPP (Point-to-Point Protocol) da inviare sulle reti IP, X.25, Frame Relay o ATM (Asynchronous Transfer Mode). Dopo aver configurato il protocollo L2TP per l'utilizzo di IP come trasporto, è possibile adottarlo come protocollo di tunneling VPN in Internet.
Quando i tunnel L2TP vengono visualizzati come pacchetti IP, essi sfruttano la protezione IPSec standard utilizzando la modalità di trasporto IPSec per integrità, risposta, autenticità e protezione della privacy avanzate. L2TP è stato progettato appositamente per le connessioni client ai server di accesso remoto e per le connessioni tra gateway. Grazie all'impiego di PPP, L2TP acquisisce il supporto multiprotocollo per protocolli quali IPX e Appletalk. PPP rende inoltre disponibile una vasta gamma di opzioni per l'autenticazione dell'utente, quali CHAP, MS-CHAP, MS-CHAPv2 e EAP (Extensible Authentication Protocol), in grado di supportare i meccanismi di autenticazione di token card e smart card. L2TP/IPSec implementa quindi funzionalità di tunneling ben definite e interoperabili, con sicurezza IPSec avanzata e interattiva.

IPSEC

Una delle principali soluzioni ai problemi di Confidenzialità, Integrità e Autenticazione descritti in precedenza è costituita dal protocollo proposto in ambito IETF: lo standard IPSec.
IPSec è una soluzione che si pone ad un livello di protezione intermedio tra l'IP e i protocolli di livello 4, permettendo la gestione della sicurezza su tutto il payload IP e alcuni campi del pacchetto IP stesso. IPSec risolve alcuni problemi presenti in altre soluzioni quali SSL, che invece lavorano a livello "applicativo" (sopra il livello 4) ad esempio nel caso del protocollo TCP. Infatti il protocollo TCP non è a conoscenza del livello SSL soprastante e i due livelli chiaramente non si parlano. E' quindi possibile, per un attaccante, spedire un pacchetto TCP fasullo che verrà ricevuto dalla macchina attaccata e riconosciuto come valido (basta che i campi del TCP siano corretti e che il Sequence Number sia compatibile con i restanti pacchetti della connessione).
Il risultato è che il TCP passerà questo pacchetto al livello SSL, il quale si renderà conto dell'attacco e scarterà questi dati. Il problema è che non ha modo di informare che quel pacchetto dati era fasullo, quindi il vero pacchetto del flusso, con quel Sequence Number, verrà scartato in quanto il TCP crede di aver già ricevuto questi dati. Questo problema è tipico di TCP/SSL e questo spiega l'importanza degli algoritmi che generato un numero casuale per il Sequence Number all'instaurazione della connessione TCP.

IPSec, posizionandosi sotto il TCP, evita questo problema. Inoltre, come SSL, non richiede alcuna modifica sulla rete core in quanto i pacchetti IPSec sono ancora pacchetti IP e l'unico problema può essere per quanto riguarda la QoS in quanto i campi interni del pacchetto possono essere invisibili dai routers del backbone.