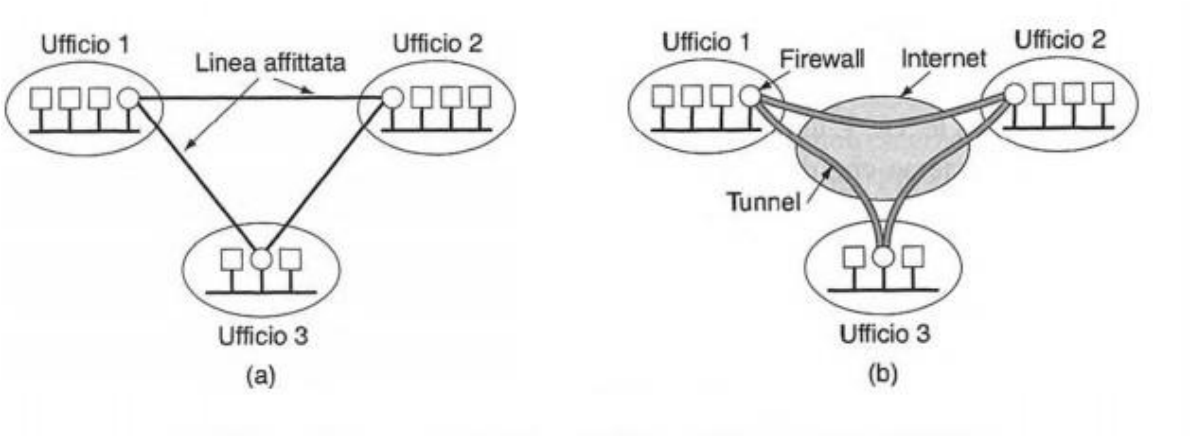
In questo modulo saranno presentate le caratteristiche delle reti VPN e la loro implementazione attraverso il protocollo IPSec.

VPN e IPSEC

Prof. Michele Tarantino

Molte aziende hanno uffici e stabilimenti situati in diverse città, a volte anche in diversi stati. Nel caso in cui i *database* siano posti geograficamente lontani, le informazioni e i dati che viaggiano attraverso internet (che per sua natura è una rete insicura), devono garantiresicurezza e integrità.

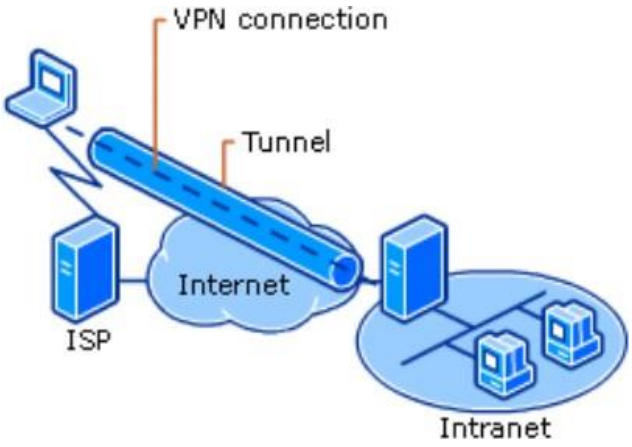
Prima che esistessero le reti pubbliche per i dati, le aziende affittavano dalla compagnia telefonica le linee per collegare fra loro alcune o tutte le loro sedi. Alcune aziende lo fanno ancora. Una rete costruita con i computer aziendali e le linee telefoniche affittate è detta rete privata. Un esempio di rete privata che connette tre siti:



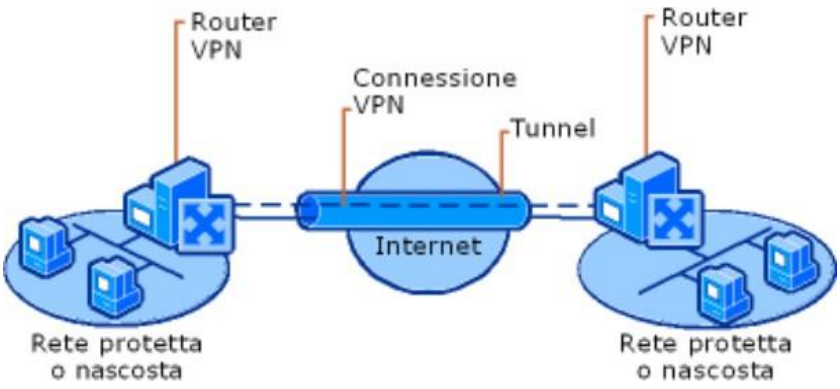
Le reti private funzionano bene e sono molto sicure. Quando le uniche linee presenti sono affittate non è possibile che il traffico di rete possa fuoriuscire dall'azienda, salvo che un intruso riesca a intercettare fisicamente le comunicazioni, il che non è affatto facile. Il problema delle reti private è dato dal loro costo. Quando arrivarono sulla scena le reti pubbliche per i dati, e successivamente Internet, molte aziende vollero spostare il loro traffico dati (e se possibile anche vocale) sulle reti pubbliche, ma senza abbandonare la sicurezza delle linee private.

Questa domanda portò in breve tempo all'invenzione delle VPN (*Virtual Private Network*). Le VPN permettono di sovrapporre delle reti sopra le reti pubbliche, ma senza abbandonare le proprietà di sicurezza tipiche delle reti private. Sono chiamate "virtuali" perché sono una mera illusione, così come i circuiti virtuali non sono veri circuiti e la memoria virtuale non è vera memoria. Virtual Private Network è un modo di utilizzare le reti condivise e pubbliche globali per ampliare in modo controllato e protetto i confini di un major network aziendale privato, ma non significa un unico tipo di tecnologia e di implementazione. Da un punto di vista delle tipologie di VPN possiamo identificarne due tipi, spesso compresenti nella stessa azienda:

- **VPN remote access**: è la tipologia più semplice e comune e prevede esclusivamente la possibilità che alcuni utenti possano connettersi da remoto alla major network dell'azienda.



❖ **VPN site-to-site** permettono di creare tunnel, attraverso reti pubbliche e condivise,fra siti aziendali diversi.



Oltre alle differenze topologie, esistono fra le Virtual Private Network anche diversità in funzione del livello di security e non solo. In particolare le VPN si suddividono in tre principali categorie:

❖ **Trusted VPN**: sono reti private virtuali in cui non è previsto un tunneling crittografato.

❖ **Secure VPN**: hanno il vantaggio principale delle Secure VPN è che i tunnel VPN sono creati utilizzando protocolli di cifratura e sicurezza quali IPsec, TSL/SSL, PPTP(Point to Point Tunneling Protocol) o SSH.

❖ **Hybrid VPN**: consente di coniugare i vantaggi delle Trusted VPN (come il controllo dei percorsi) e delle Secure VPN (la crittografia dei contenuti e dei tunnel).

Una tipica architettura consiste nell'avere un firewall per ogni ufficio e creare dei tunnel attraverso Internet fra tutte le coppie di uffici. Se viene usato *l'IPsec* per il *tunneling*, è possibile aggregare tutto il traffico fra ogni possibile coppia di uffici in una singola SA con autenticazione e cifratura. Questo fornisce controllo dell'integrità, segretezza e anche una considerevole immunità all'analisi del traffico. Ogni coppia di *firewall* deve negoziare allo *startup* i parametri della sua SA: i servizi, le modalità, gli algoritmi e le chiavi. Molti *firewall* sono progettati per gestire le **VPN**, e ciò vale anche per alcuni normali *router*. Visto che i *firewall* sono impiegati principalmente nell'ambito della sicurezza, è naturale che i tunnel delle **VPN** comincino e finiscano su dei *firewall*. In questo modo si realizza una chiara separazione fra Internet e l'azienda.

Firewall*, VPN e *IPsec su ESP in modalità tunnel costituiscono una combinazione naturale e molto usata nella pratica. Il traffico comincia a scorrere dopo che sono state stabilite le SA. Per un router su Internet, un pacchetto che viaggia attraverso un tunnel VPN non è altro che un normale pacchetto. I firewall impostano e gestiscono le SA. L'unica persona che è al corrente di queste impostazioni è l'amministratore di sistema che deve configurare e gestire i firewall. Per tutti gli altri utenti, è come se ci fosse una rete privata su linea dedicata.

Internet Protocol Security (IPSec)

È possibile implementare nelle VPN IPsec per lacreazione del tunnel. IPSec è un *frameworks* che opera a livello rete (livello 3 modello ISO/OSI). Implementato sul classico protocollo IP ma pur trovandosi allo stesso livello, è orientato alla connessione: prima della trasmissione di qualsiasi

tipo di dato, si deve stabilire una connessione logica o fisica end-to-end. Al classico protocollo IP si aggiungono molteplici servizi, algoritmi e granularità. I servizi principali offerti sono quindi:

- **segretezza**: garantire che il pacchetto arrivi a destinazione senza che venga letto da utenti o host non autorizzati;

- **integrità dei dati:** garantire che il pacchetto non venga alterato durante la trasmissione;

- **protezione dagli attacchi di tipo "ripetizione" (attacchi DOS – *Denial Of Service*)**:il pacchetto deve essere inviato una sola volta o eventualmente inviato nuovamente a seconda dell'accettazione del pacchetto stesso.

Tutti questi servizi sono basati sulla crittografia a chiave simmetrica, in quanto le prestazioni sono cruciali. La motivazione nell'utilizzo di più algoritmi è data dal fatto che un algoritmo che si crede ad oggi sicuro, potrebbe essere forzato in futuro. IPSec è indipendente dall'algoritmo e quindi l'infrastruttura può sopravvivere anche se un particolare algoritmo viene forzato. Prevedendo diverse complessità degli algoritmi è possibile proteggere una singola connessione TCP, tutto il traffico tra due host o tutto il traffico fra due router sicuri. Per trasferire, quindi, dati in modo sicuro c'è bisogno dell'IPSec solo agli estremi della connessione (*Socket*): in tale contesto, la *Socket* prende il nome di *Security Association* (SA), cioè una connessione *simplex* (unidirezionale) fra due estremi con un identificatore di sicurezza associato. Se è necessario stabilire un traffico bidirezionale sicuro sono necessarie due SA. Gli identificatori di sicurezza sono trasportati da pacchetti che viaggiano su queste connessioni sicure e vengono usati all'arrivo dei pacchetti per la ricerca delle chiavi.

I parametri caratteristici delle SA sono:

- **l'identità** (indirizzo IP) dei due host che partecipano alla comunicazione;

- **il *security protocol*** (**AH** o **ESP**), un algoritmo di *hashing* (una funzione iniettiva che prende in ingresso una stringa di n bit e la converte in modo univoco in un'altrastringa che può avere dimensione diversa) e un algoritmo di crittografia (solo se vieneusato ESP);

- **la chiave condivisa** dagli algoritmi di *hashing* e crittografia per la durata dellaconnessione;

- descrizione del flusso di traffico protetto, specificato tramite IP e il port number (numero di porta che identifica l'applicazione su un host con un determinato IP) protetto;

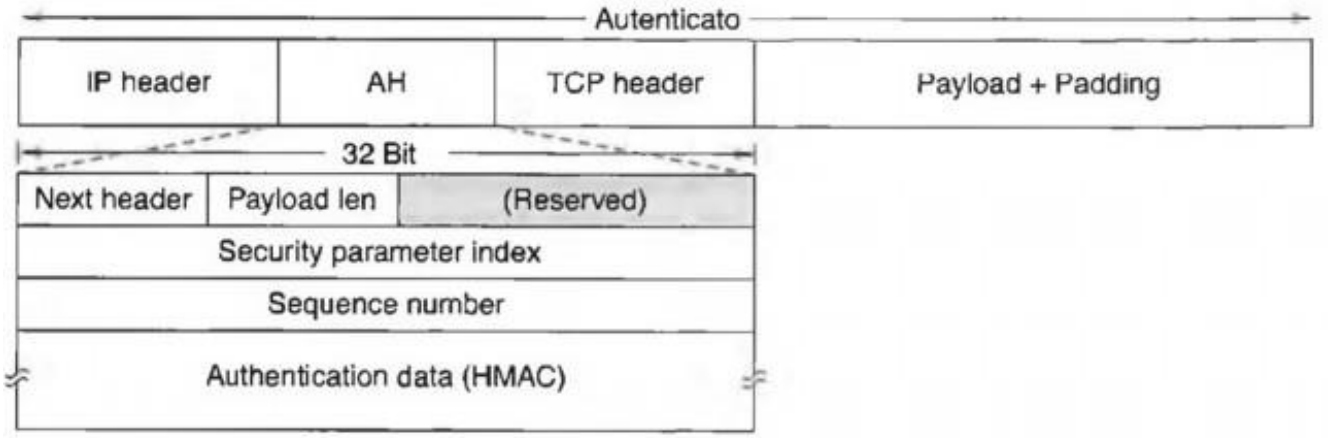
- numero che identifica la SA, chiamato *Security Parameter Index* (**SPI**);

- timer e contatori che registrano il **TTL** (*Time To Live*) della SA, utilizzati per determinare quando una connessione e le chiavi utilizzate diventano vecchie e quindi occorre aggiornarle;

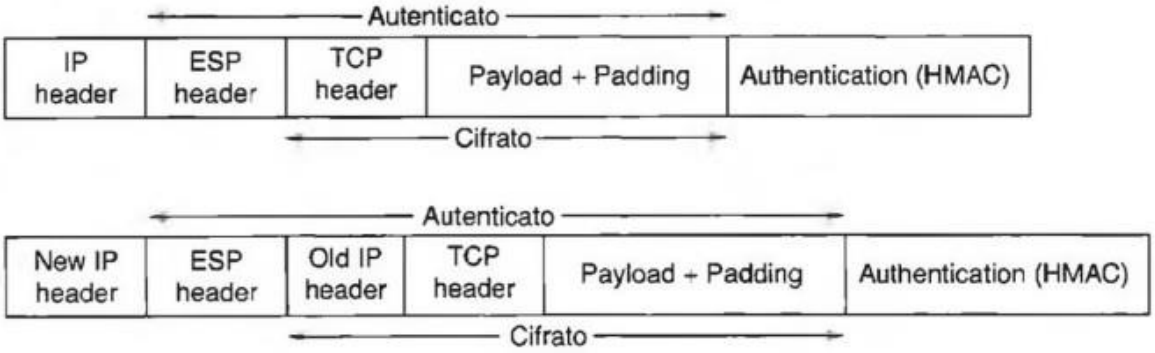
- **Sequence number**, utilizzati per l'individuazione di attacchi "***replay***" (a ripetizione).

Il protocollo IPSec comprende due metodi che collaborano insieme per inviare e ricevere dati in modo sicuro:

Il protocollo AH (*Authentication Header*): fornisce i servizi di autenticazione, integrità e sicurezza contro attacchi di ricezione ma non comprende la cifratura e quindi non rientra nelle restrizioni all'esportazione che riguardano il *software* crittografico. Nellaschematizzazione seguente è rappresentato il pacchetto IPSec.



Nel campo "*IP header*" sono contenute tutte le informazioni che riguardano la versione del protocollo IP, l'indirizzo IP del mittente del messaggio e del destinatario, il *Time To Live* (TTL - identifica la scadenza del pacchetto). Nell'intestazione "AH", si trovano ulteriori sotto-campi: - "*Next header*" identifica l'indirizzo IP originale prima dell'utilizzo del protocollo AH; - "*Payload length*" contiene il numero di parole a 32 bit in AH; - "*Security Parameter Index*" identifica la connessione ed è inserito dal mittente. Indica uno specifico record che contiene la chiave condivisa usata per la connessione nel *database* del ricevente; "*Sequence Number*" attribuisce un numero a tutti i pacchetti inviati, compresi quelli ritrasmessi, che dovranno avere un numero diverso. Viene utilizzato per evitare attacchi a ripetizione; - "*Authentication data*" è un campo a lunghezza variabile che contiene la firma del *payload*. L'algoritmo di firma elettronica è deciso quando viene stabilita la SA ed utilizza una chiave privata poiché gli algoritmi a chiave pubblica sono troppo lenti. Il mittente e il destinatario stabiliscono una chiave comune prima di cominciare la connessione. Si calcola poi, tramite **HMAC** (*Hashed Message Authentication Code* - Messaggio univoco di autenticazione), *l'hash* sui contenuti del pacchetto e della chiave insieme, ovviamente non trasmettendo la chiave. - Il protocollo ESP (*Encapsulating Security Payload* – Carico di sicurezza crittografato): ha le stesse funzioni di AH, con l'aggiunta del mantenimento della segretezza dei dati.



L'intestazione ESP è composta da due word a 32 bit, che costituiscono i campi "*Security Parameters Index"* e "*Sequence Number*", con funzioni simili ad AH. Il controllo dell'integrità con HMAC è fatto in coda al *payload*, in quanto si possono trasmettere i dati all'interfaccia di rete mentre si calcola HMAC, rendendo più efficiente la trasmissione. I due host prima di iniziare la comunicazione, devono accordarsi su: - algoritmo di cifratura dei dati da utilizzare; - algoritmo da utilizzare per verificare l'integrità dei dati; - scelta del metodo di autenticazione delle connessioni (se usare una chiave pubblica o una chiave privata

condivisa). IPSec può essere utilizzato in due modalità: - modalità trasporto: in cui l'intestazione IPSec viene inserita subito dopo quella dell'IP. Il campo "*Protocol*" nell'intestazione IP è cambiato in modo da indicare che un'intestazione IPSec segue quella solita dell'IP (prima dell'intestazione TCP). L'intestazione IPSec contiene le informazioni di sicurezza: principalmente l'identificatore SA, un nuovo numero di sequenza ed eventualmente un controllo di integrità del campo "*payload*". Questa modalità è utilizzata tipicamente nelle connessioni *host-to-host* VPN, la quale non fornisce sicurezza sul flusso di dati, quindi il traffico tra due host può essere facilmente analizzato anche se si codificano le informazioni, in quanto gli indirizzi di sorgente e destinazione rimangono intatti e sono in chiaro nell'intestazione del pacchetto. - modalità tunnel: in cui l'intero pacchetto IP comprensivo anche dell'intestazione, viene incapsulato nel corpo di un nuovo pacchetto IP con un'intestazione completamente diversa. La modalità tunnel è utile quando il tunnel è collegato in una *socket* diversa dalla sua destinazione finale. In alcune situazioni, il tunnelpuò arrivare ad un host con un *gateway* sicuro (ad esempio il firewall di un'azienda):operando in questo modo, il *firewall* incapsula e rimuove l'incapsulamento dei pacchetti che lo attraversano e gli host presenti sulla LAN non devono essere a conoscenza dell'IPSec; soloil *firewall* ne è a conoscenza. In questa modalità viene creato il "*Security header*" AH/ESP, che viene posto all'inizio del pacchetto criptato creando una nuova intestazione IP chepermette di inviare il pacchetto al *gateway* appropriato. Questa soluzione viene utilizzatanelle connessioni *network to network* VPN. Lo svantaggio di questa modalità è dato dal fatto che vengono aggiunti molte intestazioni IP, aumentando di molto le dimensioni del pacchetto.

Resta connesso e informato sui prossimi eventi, corsi e seminari:

Web
www.profmicheletarantino.com

Email
profmicheletarantino@gmail.com

Telefono
349 83 54 521

Facebook
@micheletarantinodocente

Instagram
@profmicheletarantino

Hai bisogno di un modulo personalizzato? Non esitare a contattarmi!