VIRTUAL PRIVATE NETWORK

1. Il concetto di Private Network

Le reti privati dedicate sono state progettate per risolvere il problema del collegamento tra sedi remote di una stessa società, o genericamente tra reti LAN remote, con la finalità di garantire un servizio sicuro, affidabile e riservato. In pratica tra la rete LAN della sede centrale e la rete LAN della sede remota veniva stesa una linea di collegamento fisica "point-to-point". Ovvero veniva realizzato un collegamento WAN tra due sedi di tipo circuit permanent. Un circuito che è una connessione fisica permanente "garantita sicura" tra due endpoint. Questo collegamento con le caratteristiche di Sicurezza , Affidabilità e Riservatezza era cioè, un collegamento a prova di intercettazione. Quando le sedi da mettere in comunicazione erano molte, significava realizzare una completa rete WAN sicura, per collegare tutte le LAN remote, e dato che stendere e mantenere una rete WAN per trasmissioni dati riservata, risultava, e risulta ancora, estremamente costoso, le società tipicamente, noleggiavano dalle TelCo nazionali (che funzionavano come carrier) delle linee particolari (di tipo circuit permanent o circuit swiching) che venivano chiamate affittate, dedicate o private. Perciò la sicurezza di una rete Privata classica viene data dal suo "isolamento fisico" rispetto al resto del mondo. La rete privata è una rete fisicamente separata dall'esterno. Addirittura, è possibile che su questa rete privata possano essere utilizzate regole e protocolli completamente diversi da quelli delle normali reti standardizzate. Di contro, la soluzione delle reti private classiche presenta difetti come gli elevati costi di realizzazione, manutenzione e gestione, la difficile scalabilità, la scarsa disponibilità della rete per gli utenti mobili.

2. Introduzione alle VPN - Virtual Private Network

Per ovviare ai problemi della rete privata classica si è cercato il modo di realizzare un tipo di rete che fosse il più diffusa possibile fino al livello più capillare, che fosse adattabile, che fosse economica e che permettesse l'accesso indipendentemente dall'ubicazione, in modo da fornire gli stessi servizi di sicurezza richiesti ad una rete privata. La VPN è la soluzione a tale problema il cui punto di forza risiede nel rendere sicura ed affidabile la trasmissione dei dati su una rete insicura cioè, una rete che è privata solamente in maniera virtuale. L'innovatività è racchiusa nel termine "virtuale" che sta a significare come si possa utilizzare un'infrastruttura già esistente come ad esempio Internet (largamente diffusa ed economica) per realizzare i collegamenti fra gli utenti; d'altro canto Internet come ben sappiano non è stato progettato per essere una rete sicura ma bensì una rete pubblica in cui chiunque può accedervi. Perciò chiunque abbia le conoscenze adatte può intercettare e leggere i dati che vi vengono trasmessi. Per tale ragione le VPN prevedono dei protocolli di sicurezza in modo che le comunicazioni rimangano private, sicure e soprattutto "logicamente separate" dal resto della rete come se si trattasse di una linea riservata. Comunque per garantire la sicurezza è sempre necessario prevedere una "politica di sicurezza" adeguata alla situazione in base alla tecnologia VPN implementata e alle risorse disponibili.

2.1. Definizione

Una VPN è un servizio di comunicazione "logico" **sicuro e affidabile** (cioè che rispetta i principi di riservatezza, integrità e autenticazione) fra due o più apparecchiature realizzata sopra una infrastruttura di rete pubblica potenzialmente non sicura.

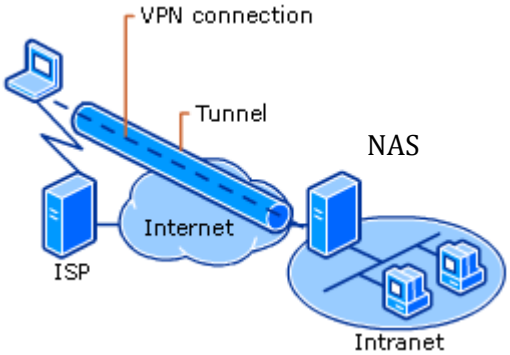
2.2. Vantaggi delle VPN rispetto alle reti private

- **Riducono i costi** – le VPN riducono in maniera profonda i costi di mantenimento di una rete sicura perché usano Internet come infrastruttura di collegamento remoto; la manutenzione è affidata agli ISP.
- **Migliorano le comunicazioni** – ~~gli utenti remoti si possono connettere in sicurezza da qualunque posto 24 ore su 24 alle risorse della rete aziendale o tra di loro~~ ancor più vero nelle PN….
- **Sono flessibili e scalabili** – una infrastruttura VPN può adattarsi con facilità alle necessità di cambiamento o di crescita delle reti. Flessibile in quanto si può realizzare una rete "Privata" non solo tra sedi fisse ma anche tra terminali remoti ma soprattutto perché per impostarle non ci vuole molto; pensare poi alla scalabilità di una PN è quasi ridicolo
- **Sono sicure ed affidabili** – la sicurezza è un concetto intrinseco in una VPN, poiché le VPN utilizzano protocolli di tunneling. ~~L'affidabilità deriva dalla topologia a tunnel, punto-a-punto e quindi estremamente semplice~~. Come sempre può accadere nella storia della cyber security, alcune VPN sono state "bucate"; il consiglio generale è quello di acquistare VPN non gratuite, perché il produttore – in caso di bachi – interviene prontamente a salvaguardare i propri investimenti
- **Sono indipendenti dagli standard tecnologici** dei primi due livelli dalla pila OSI. Questo garantisce che una rete non sia vulnerabile alle caratteristiche di debolezza (insicurezza) dei primi due livelli.

3. Tipologie di VPN

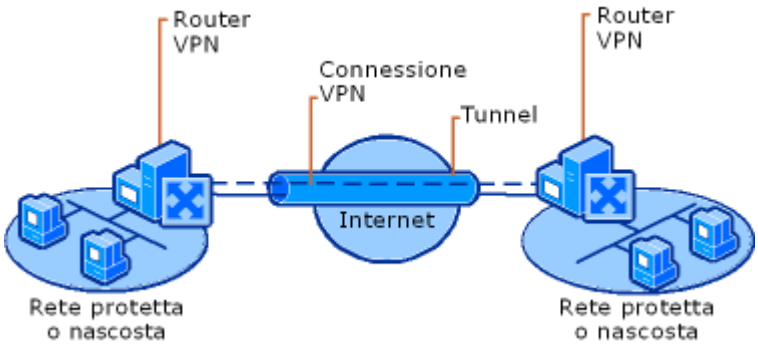
3.1. Remote Access VPN

Le connessioni VPN di accesso remoto consentono agli utenti che lavorano da casa (homeworking) o in movimento (teleworking) di accedere a un server su una rete privata utilizzando l'infrastruttura resa disponibile da una rete pubblica, ad esempio Internet. Dal punto di vista dell'utente, la VPN è una connessione point-to-point tra il computer (il client VPN) e il server di un'organizzazione definito NAS (Network Access Server). L'infrastruttura della rete condivisa è irrilevante, in quanto, dal punto di vista logico, è come se i dati venissero inviati su un collegamento privato dedicato.



3.2. site-to-site VPN

Una connessione VPN da sito a sito connette due parti di una rete privata (dette anche connessioni VPN da router a router) consentendo alle organizzazioni di disporre di connessioni con routing tra uffici distanti o con altre organizzazioni su una rete pubblica e mantenendo al contempo la sicurezza delle comunicazioni. Quando le reti sono connesse su Internet un router inoltra i pacchetti a un altro router tramite la connessione VPN. Per i router, la connessione VPN opera come un collegamento data-link layer.



Il server VPN rende disponibile una connessione con routing alla rete cui è connesso. Il router che esegue la chiamata (il client VPN) si autentica sul router che risponde (il server VPN) e, per autenticazione reciproca, quest'ultimo si autentica sul router chiamante. In una connessione VPN site-to-site ogni host comunica con host di sedi remote senza sapere dell'esistenza del collegamento VPN; tutto il lavoro viene svolto in modo trasparente dai due router VPN che trattano con protocolli speciali solamente i pacchetti IP diretti alle altre sedi remote dell'azienda; gli altri pacchetti (p.e.: quelli verso Internet) sono trattati in modo tradizionale.

A livello concettuale si distingue una rete VPN in "**Intranet**" quando unisce più sedi della stessa azienda o in "**Extranet**" quando la condivisione è con altre aziende o uffici con cui collabora. Nota: i termini Intranet e Extranet non nascono in ambito VPN e quindi sono utilizzati anche in altri contesti; il significato è sempre questo: comunicazioni tra elementi/host della stessa azienda - Intranet , o comunicazioni con elementi appartenenti anche ad altre realtà - Extranet.

4. Principio di funzionamento della VPN

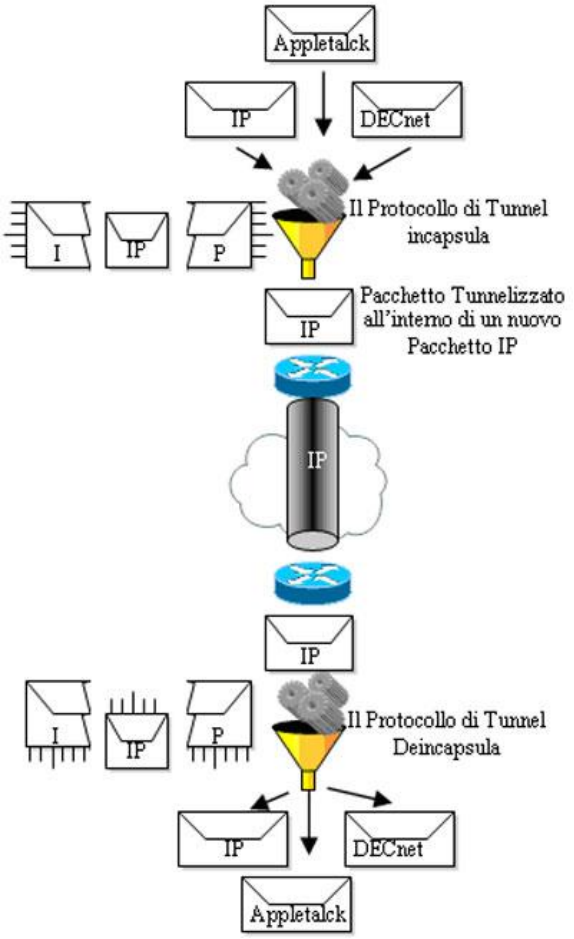
Il metodo di comunicazione di una VPN è molto elaborato perché i dati non si possono inviare direttamente al destinatario dato che i pacchetti transiteranno in chiaro su una rete pubblica non protetta. Per capire i meccanismi con cui una Virtual Private Network instaura una comunicazione sicura attraverso internet è necessario illustrare il **meccanismo di tunneling**.

4.1. Tunneling

La VPN usa il concetto di tunneling per creare una rete privata attraverso Internet. Concettualmente, è come se un tunnel sicuro venisse costruito tra due apparecchiature finali abilitate a realizzare VPN end-to-end. I dati possono essere spediti dall'origine verso la fine del tunnel, avendo la certezza che arriveranno alla fine del tunnel. Fisicamente non esiste alcun tunnel e il termine indica un processo "logico" di collegamento punto-a-punto attraverso una rete IP connectionless. I due punti finali del tunnel, anche se sono distanti e collegati attraverso molti nodi, durante il processo logico diventano "adiacenti".

Il termine “tunneling” si riferisce a un insieme di tecniche per cui un protocollo (passenger protocol) viene incapsulato in uno o più protocolli (carrier protocol) dello stesso livello o di livello differente e viaggiare così “nascosto” da questi.

Il Tunneling compie un **incapsulamento multiprotocollo dei dati**. Questo termine significa che i pacchetti di dati, anche se sono di protocolli differenti ad esempio: DECnet, Appletalk, IP privato (non instradabile, tipo 192.168.x.x), IP globale unico, IPX, NetBeui una volta giunti davanti l’entrata del tunnel (interfaccia d’entrata del tunnel), vengono imbustati nuovamente dal protocollo di tunneling all’interno di un secondo pacchetto IP e vengono spediti sulla rete con un nuovo header IP e così trasportati verso la fine del tunnel (interfaccia d’uscita del tunnel). Una volta giunti alla fine del tunnel vengono spogliati dell’imbustamento (header) supplementare aggiunto dal protocollo di tunnel e instradato verso la sua destinazione. Essenzialmente, il tunneling è un processo che incapsula il pacchetto di dati all’interno di un altro pacchetto; ovvero, i dati vengono imbustati due volte per far sì che essi siano trasmessi solamente ai destinatari finali autorizzati.



4.2. Sicurezza del tunneling

Le tecniche utilizzate per l'implementazione del tunneling sono diverse; emerge il problema della mancanza di uno standard. Tali tecniche, comunque, sono tutte atte a trattare i dati in maniera riservata e protetta. Un protocollo di tunneling deve garantire la sicurezza della rete VPN rispettando i seguenti criteri:

- **Autenticazione ~~e Autorizzazione~~** Possibilità di autenticare il mittente della comunicazione. Il destinatario deve poter verificare il mittente (la sorgente) delle informazioni.
- **Integrità (Integrity).** Il destinatario deve avere dei meccanismi per comprendere se le informazioni arrivate a destinazione sono realmente quelle spedite dal mittente.
- **Riservatezza (Confidentiality).** Il mittente non può inviare un’informazione sulla rete in chiaro, ha necessità di cifrarla affinché se fosse intercettata non sia interpretabile da un soggetto esterno al destinatario.

In conclusione, per garantire questi criteri, il tunneling tra le sue funzionalità implementa:

- **Tecnica di autenticazione**
- **Metodo di cifratura sui dati**

4.3. Autenticazione

L'**autenticazione** è una procedura che un sistema di telecomunicazioni come la VPN utilizza per accertarsi dell'identità del mittente/destinatario; ciò consente di:

- consentire l'accesso alla rete
- assicurare che i dati possano essere letti solo dal destinatario corretto
- garantire al destinatario la certezza sulla sorgente (il mittente)

Si adotta pertanto uno **schema di autenticazione** che può andare dal semplice utilizzo di una coppia username/password per accedere al sistema alle forme più evolute basate su diversi sistemi di crittografia e/o multifactoring; dipende dalla procedura/protocollo che si è deciso di adottare per implementare il tunneling.

I protocolli utilizzati per l'autenticazione nelle VPN sono:

Protocolli/algoritmi per autenticazione e sintesi (digest)	**Protezione**
AH Authentication header	***Media***
CHAP *Challenge Handshake Authentication Protocol*	***Alta***
EAP - *Extensible Authentication Protocol* **EAP-TLS -** *EAP-Transport Level Security*. **EAP-MD5 Challenge** - *Message Digest 5 Challenge.* **EAP-PEAP** - Protected Extensible Authentication Protocol	***Alta***
MS-CHAP-MS-CHAPV2 -*Microsoft Challenge Handshake Authentication Protocol*.	***Alta***
PAP - *Password Authentication Protocol*	***Bassa***
RADIUS Remote Access Dial-In User Service	***Alta***
SPAP - *Shiva Password Authentication Protocol*	***Media***

4.4. Cifratura

La Cifratura assicura che i messaggi non possano essere letti da nessuno oltre il destinatario intenzionale. La riservatezza delle informazioni viene garantita da una cifratura robusta. La Cifratura trasforma quindi le informazioni in chiaro (plain text) in un testo cifrato (cipher text) che risulta incomprensibile, non decodificabile a chi non è autorizzato. L'operazione di decifratura ripristina l'originale plain-text, in forma comprensibile al destinatario. A seconda del protocollo di comunicazione prescelto vengono adottati diverse cifrature dei dati.

Gli algoritmi di cifratura più utilizzati nelle VPN sono:

Algoritmi di cifratura
AES Advanced Encrypton Standard

DES Data Encryption Standard
ESP Encapsulated Security Payload
MPE Microsoft Point-to-Point Encryption
~~**RC4 – RC5**~~
SHA Secure Hash Algorithm
MD5 Message Digest algorithm 5

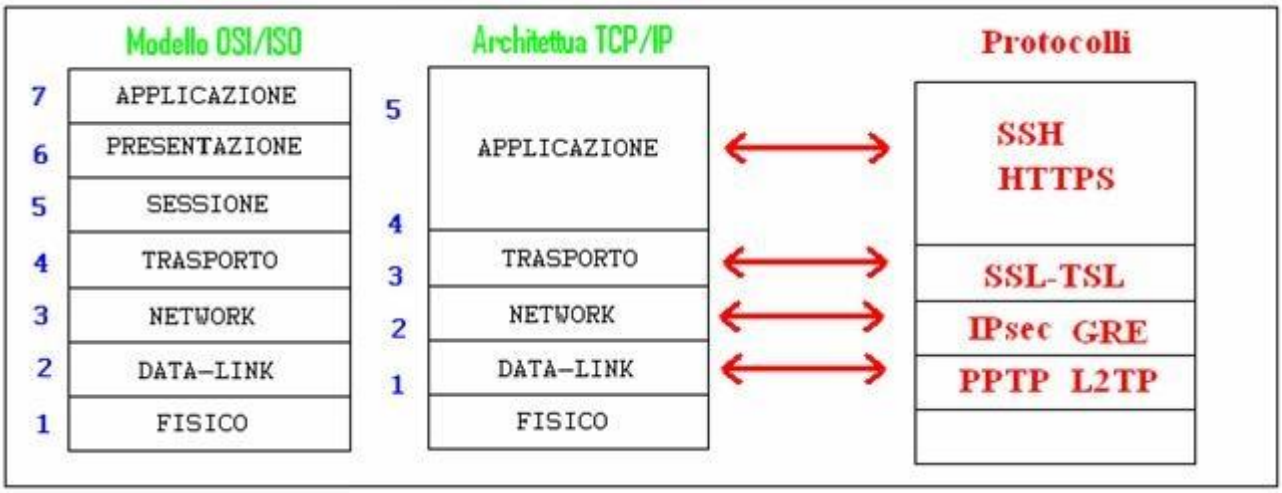
4.5. Processo di comunicazione

Per instaurare una connessione VPN, ad esempio tra un client VPN e un server (VPN client-to-Lan), i passi che sono richiesti possono essere riassunti in linea generale con i seguenti:

1. Il client VPN contatta il Server
2. Il Server se presente notifica la sua presenza
3. Il ***client*** si presenta e ***richiede*** di essere ***autenticato*** (cioè il client richiede al server di identificarlo)
4. Il server esegue la procedura di ***autenticazione*** ~~***e autorizzazione***~~ (ovvero il server verifica che il tentativo di ***connessione*** tra client e server sia permesso dopo che il processo di autenticazione sia riuscito)
5. Il server risponde alla richiesta di autenticazione
6. Il Client può comunicare con la rete (o il singolo client) in base alle autorizzazioni a lui concesse
7. Inizia la comunicazione tra le due entità

5. Protocolli per reti VPN

Per poter realizzare la sicurezza delle trasmissioni mediante VPN esistono diversi protocolli di sicurezza, a vari livelli nella rete. In sostanza è possibile realizzare una VPN praticamente su ogni livello della pila OSI. La scelta di utilizzare un protocollo piuttosto che un altro dipende dai requisiti di sicurezza delle applicazioni e dalle necessità di sicurezza dell'utente, il quale deve decidere a che livello della pila deve essere implementata la sicurezza nelle trasmissioni su VPN. In alcuni casi, ha senso offrire alcuni di questi servizi/capacità ad un livello della pila e altri servizi/capacità ad un livello differente. Servizi e funzionalità che devono necessariamente essere implementate in alcuni livelli e non in altri, proprio per poter garantire la sicurezza e per la correzione degli errori.



Attenzione: i protocolli evidenziati sulla sinistra in rosso non sono da intendersi come "pila" di protocolli da usare per la sicurezza VPN; a seconda dei requisiti si adotterà una sicurezza tipicamente in un solo strato, e gli altri strati restano "normali"; per fare un esempio: IPsec non incapsula TSL, o usi IPsec o usi TSL.

I protocolli di tunneling più utilizzati sono i seguenti:

Protocollo	Livello	Cifrato
PPTP Point to Point Tunneling Protocol	Data-Link	*
L2TP (Layer two Tunneling Protocol) / L2F (Layer 2 Forwarding)	Data-Link	
GRE (Generic Routing Encapsulation)	Network	
IPSec (IP security)	Network	*
SSL-TSL (Secure Sockets Layer – Transport Layer Security)	Transport	*
SSH Secure Shell	Application	*

In ogni caso questi protocolli, ognuno con la propria tecnologia di sicurezza, utilizzano tutti dei meccanismi di tunneling e cifratura che incapsulano il pacchetto di dati creandogli attorno una protezione durante la trasmissione e lo de-incapsulano in ricezione. Tra questi il più sicuro è IPSEC, un protocollo completo per la comunicazione VPN; altri protocolli come L2TP e GRE non offrono servizi di cifratura e autenticazione perciò per garantire la sicurezza vengono usati in combinazione con IP Security (L2TP/IPSEC e GRE/IPSEC).

6. IPsec: la soluzione standard alla sicurezza IP

6.1. Introduzione

IPsec (IP Security) non è, ad esser precisi, un protocollo, ma è un insieme di protocolli che fornisce sicurezza a livello di rete (strato 3). E' un oggetto piuttosto complesso, descritto in oltre una dozzina di

RFC. Prima di entrare nelle specifiche di IPSec, facciamo qualche passo indietro e consideriamo cosa significa fornire sicurezza allo strato di rete.

Lo strato della rete riuscirebbe a garantire una certa sicurezza se tutti i dati trasportati da tutti i datagram IP fossero cifrati. Questo significa che ogni volta che un host vuole inviare un datagram, esso dovrebbe cifrare il campo dati del datagram prima di inviarlo nella rete. Ovviamente, riuscendo a cifrare l'intero datagram (header compresi) si otterrebbe una sicurezza ancor maggiore nascondendo così anche le informazioni riguardanti l'origine e la destinazione della comunicazione. Il campo dati potrebbe essere un segmento UDP, un messaggio ICMP, e così via. Se questo servizio di rete fosse disponibile, tutti i dati inviati dagli host (comprese e-mail, pagine web, comandi e messaggi di gestione come SNMP) risulterebbero nascosti a qualsiasi intrusore interessato ad intercettarli dalla rete.

Oltre alla **segretezza** (**confidenzialità**), si potrebbe desiderare che lo strato della rete fornisca l'**autenticazione** della sorgente. In tal caso, quando un "destinatario" riceve un datagram IP, dovrebbe autenticare il "mittente" verificando l'effettiva corrispondenza tra il pacchetto ricevuto e il mittente stesso. Possiamo dire che lo standard IPSec fornisce i seguenti servizi:

1. confidenzialità dei dati (crittografia)
2. ~~confidenzialità delle parti effettivamente coinvolte nel flusso del traffico~~ **???**
3. integrità dei dati
4. autenticazione del mittente
5. protezione contro gli attacchi di replay

Per fare ciò IPSec si serve di un protocollo a scelta tra: **AH** (Autentication Header) o **ESP** (Encapsulating Security Payload). Il protocollo AH fornisce l'autenticazione della sorgente e l'integrità dei dati ma non la segretezza; l'ESP fornisce l'integrità dei dati, l'autenticazione e la segretezza, per questo è maggiormente utilizzato. Fornendo più servizi, il protocollo ESP è più complicato e richiede più elaborazioni rispetto ad AH. Ma non basta.

6.2. Security Association (SA)

Sia nel caso di AH che nel caso di ESP, prima di inviare datagram "sicuri" sul canale, l'host sorgente e quello destinazione devono prima avviare una fase di handshake (negoziazione), detta connessione logica, che stabilisce i parametri di sicurezza: algo di crittografia, chiavi, protocollo, hashing, …

Questa connessione logica è detta **Security Association** (**SA**). ~~IPSec trasforma il tradizionale strato della rete "connectionless" di Internet in uno strato connection-oriented~~. La connessione logica definita da una SA è simplex, cioè unidirezionale. Se entrambi gli host vogliono scambiarsi datagram sicuri devono stabilire due SA, una per ciascuna direzione. Una SA è unicamente identificata da:

- il protocollo di sicurezza (AH o ESP)
- l'indirizzo IP destinazione ~~per una connessione simplex~~
- un identificatore a 32 bit della connessione: **SPI**, Security Parameter Index

Ogni datagram IPSec ha un campo speciale che ospita il SPI. Tutti i datagram di una stessa SA useranno lo stesso valore SPI.

Per un buon funzionamento di IPSec, è necessario uno schema SA automatico per la gestione delle chiavi. Per fare questo si utilizzano principalmente due protocolli:

- il protocollo **IKE** (Intenet Key Exchange) RFC 2409 per lo scambio delle chiavi. IKE è di livello 7 e si appoggia su UDP, ma gestisce in proprio la connessione logica: se un datagramma si perde ne richiede la trasmissione. Esiste IKEv2 (RFC 7296)
- ~~il protocollo Internet per la gestione delle associazioni per la sicurezza e delle chiavi **ISAKMP** (Internet Security Association & Key Management Protocol) il quale definisce le procedure per stabilire e interrompere le SA. ISAKMP prevede due fasi per la contrattazione: una prima fase in cui gli end-points della comunicazione si autenticano e si accordano su un insieme di funzioni crittografiche per lo scambio dei dati e una seconda fase in cui avviene lo scambio vero e proprio delle SA~~

In generale le chiavi associate alle SA sono valide per un periodo di tempo limitato, scaduto il quale si stabilisce una nuova SA

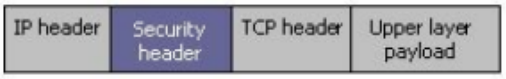
6.3. Security Association modes (modalità SA)

IPSec può essere utilizzato in due modalità: trasporto e tunnel. Nella modalità trasporto, i campi di IPSec (si tratta di AH o ESP) sono inseriti nel datagram IP, tra l'header IP e l'header superiore, tipicamente TCP o UDP. Questo tipo di soluzione può essere necessaria nel caso di comunicazioni end-to-end. In tutti gli altri casi è obbligatorio utilizzare la modalità tunnel. In questo caso il pacchetto IP viene inglobato in quello IPSec al quale, a sua volta, viene aggiunto un nuovo header IP con gli indirizzi dei security gateways che stanno ai due capi del tunnel.

Da questa immagine si vede chiaramente come i campi dell'header IP non siano assolutamente protetti nel caso della modalità trasporto, mentre la protezione è totale per quanto riguarda la modalità tunnel.

6.3.1. SA in transport mode

Si utilizza nel caso di connessione tra due hosts. In IPv4 l'header del protocollo di sicurezza si trova subito dopo l'header IP con le relative opzioni e prima dei protocolli di livello superiore (TCP o UDP).



Nel caso in cui stia utilizzando ESP, una SA in transport mode fornirebbe sicurezza ai protocolli di livello superiore ma non all'header IP. Nel caso di AH, la protezione è estesa anche a porzioni selezionate dell'header IP.

6.3.2. SA in tunnel mode

Si deve utilizzare quando uno dei due o entrambi gli estremi della comunicazione è un security gateway, per evitare potenziali problemi relativi alla frammentazione/riassemblaggio di pacchetti IPSec, e in situazioni dove esistono percorsi multipli (dopo un gateway) per raggiungere la stessa destinazione. **???**

Per una SA in tunnel mode esiste un header IP esterno, che specifica il security gateway che elaborerà IPsec, e un IP header interno che specifica la destinazione finale (host) a cui è diretto il pacchetto. L'header del protocollo di sicurezza utilizzato si trova tra i due.

6.3.3. SA bundle

L'insieme dei servizi di sicurezza offerti da una SA dipende dal protocollo selezionato, dalla modalità dell'SA, dai punti terminali dell'SA e dalla scelta di servizi opzionali all'interno del protocollo.

Quando una politica di sicurezza richiede la combinazione di più servizi, può non essere sufficiente l'uso di una singola SA. Queste possono essere combinate tra loro (SA bundle) in due modi: **transport adjacency mode** e **iterated tunneling mode**.

Transport adjacency mode

Applico più di un protocollo di sicurezza allo stesso pacchetto IP senza invocare tunneling. E' possibile combinare AH ed ESP una sola volta; ulteriore annidamenti non porterebbero nessun beneficio. L'esempio più frequente è costituito da un pacchetto che viene autenticato tramite AH, ma cifrato con ESP, in modo tale da godere dei vantaggi di entrambi i protocolli.

Iterated tunneling mode

Applicando la tecnica del tunneling posso utilizzare più livelli di annidamento, in quanto ogni tunnel può avere origine o terminare su differenti siti lungo il percorso che implementano IPsec.

6.4. Databases

Per assicurare interoperabilità e facilitare la gestione, IPsec standardizza alcuni aspetti. Si è giunti ad un modello che fa uso di due databases: **SPD** (Security Policy Database) e **SAD** (Security Association

Database). Il primo specifica le politiche che gestiscono il traffico IP in arrivo o in partenza da un host o da un security gateway. Il secondo contiene i parametri di ogni SA attiva. Ogni interfaccia, per la quale è abilitato IPSec, richiede l'uso di database separati per il traffico entrante (inbound) o uscente (outbound), a causa della direzionalità di molti dei campi, usati come **selectors**. **???**

6.4.1. SPD: Security Policy Database

Quando arriva un pacchetto IP si esamina l'indirizzo e si stabilisce di quale trattamento ha bisogno il pacchetto. L'SPD deve essere consultato durante l'elaborazione di tutto il traffico (entrante o uscente), incluso quello non sottoposto a IPsec. Per questo motivo sono richiesti record differenti per il traffico in entrata e in uscita. Si può immaginare ciò come due SPD separati. Per ogni pacchetto entrante o uscente sono possibili tre scelte:

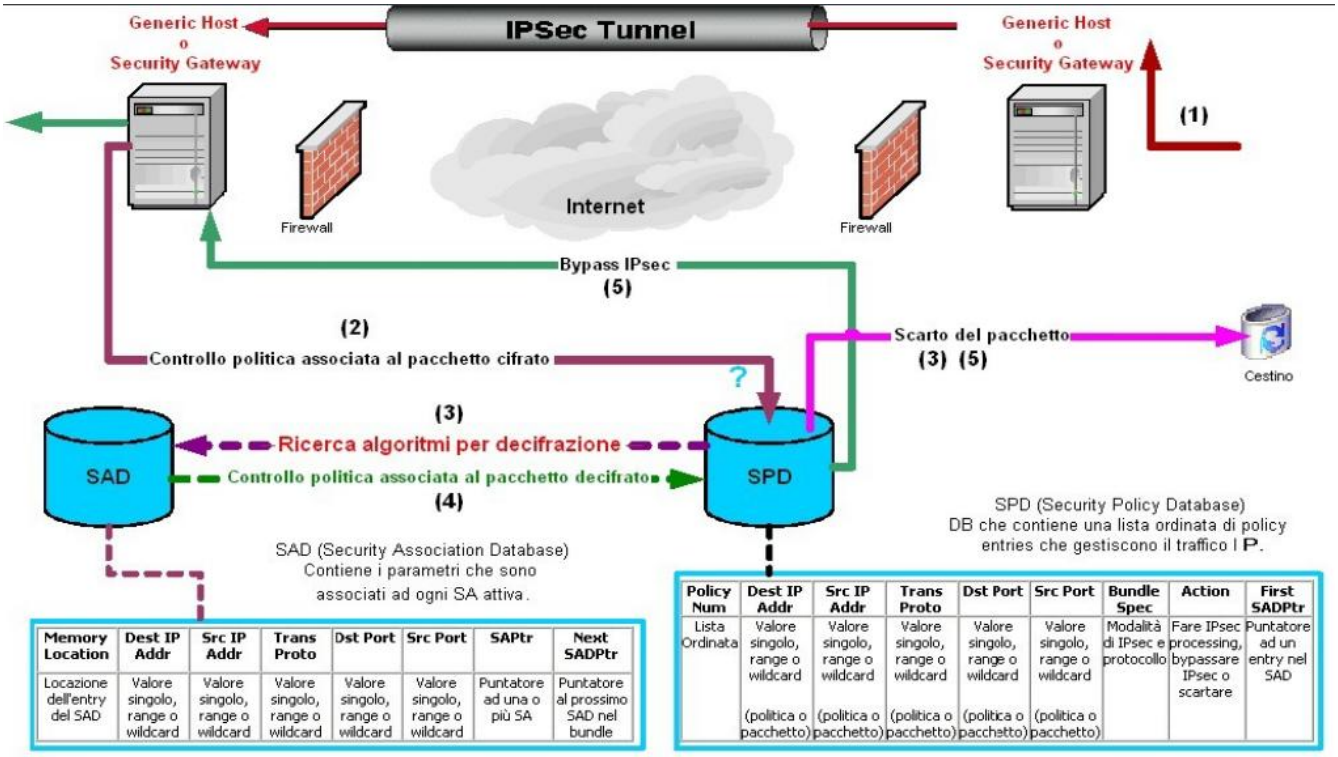
1. scarto del pacchetto, che quindi non può lasciare l'host, non può attraversare il security gateway o essere consegnato ad una applicazione
2. bypass di IPsec (il pacchetto può transitare senza che gli venga fornita protezione da IPsec)
3. utilizzo di IPsec

Per ogni implementazione di IPsec, ci deve essere un'interfaccia di amministrazione che permetta al system administrator di gestire il SPD. **???**

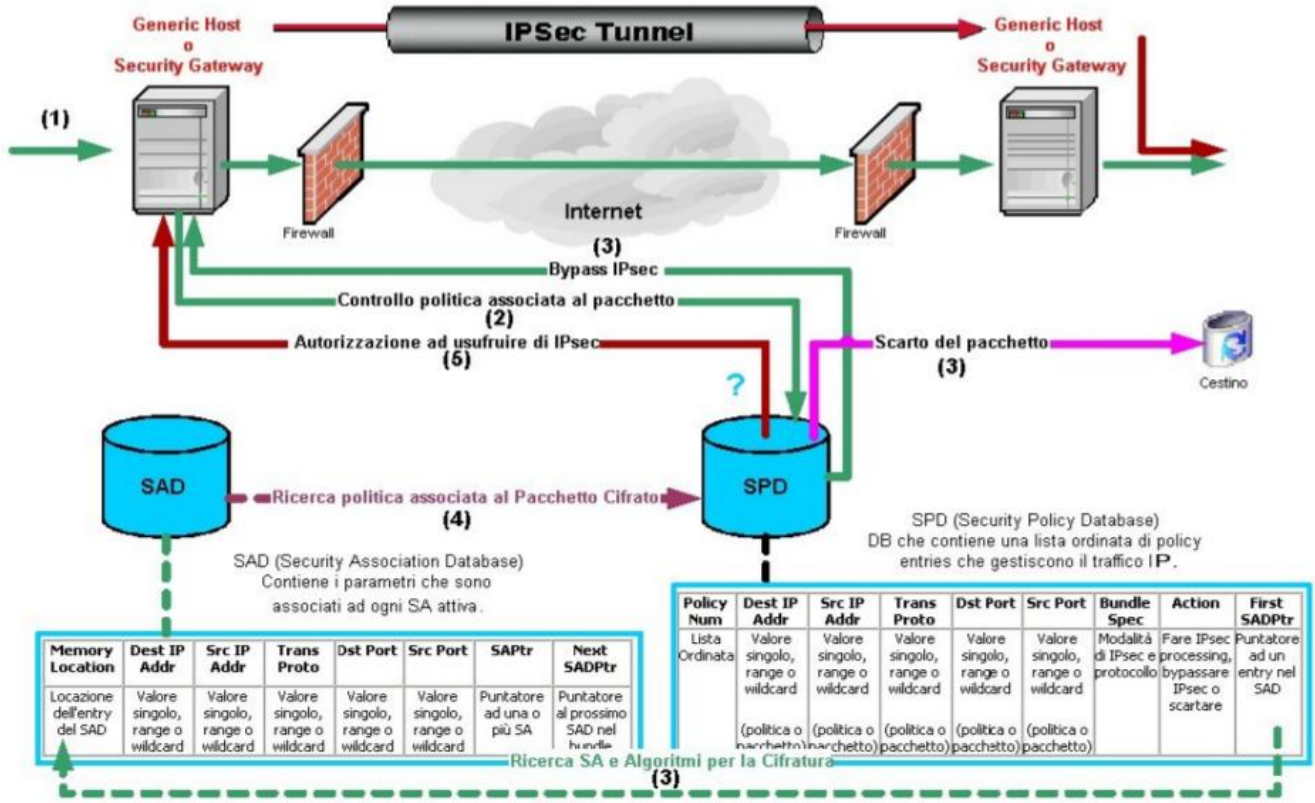
6.4.2. SAD: Security Association Database

Ogni record definisce i parametri associati ad una SA; di conseguenza ogni SA deve avere un record nel SAD. Per l'elaborazione del traffico uscente, i record sono puntati da quelle presenti nel SPD. Nel caso in cui una entry nel SPD non faccia riferimento a nessuna SA, IPSec dovrà creare una SA appropriata e collegare l'entry dell'SPD con quella del SAD. Per l'elaborazione del traffico IPSec entrante invece, ogni entry nel SAD è sicuramente indicizzata dalla tripla *<indirizzo IP di destinazione, protocollo IPsec, SPI>*, altrimenti il pacchetto viene scartato.

Traffico Entrante



Traffico uscente

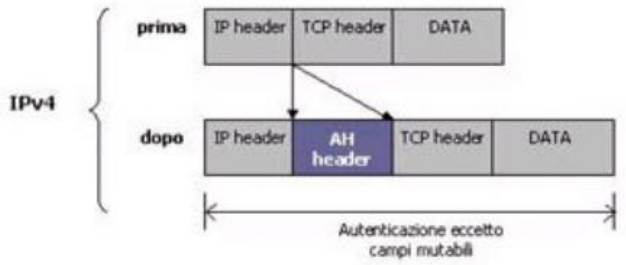


6.5. AH (Authentication Header) RFC 2402

Come già detto, il protocollo AH fornisce l'autenticazione dell'host sorgente e l'integrità dei dati ma non la segretezza. Quando un determinato host sorgente vuole inviare uno o più datagram utilizzando IPSec, prima stabilisce una SA con la destinazione, dopo di che può iniziare a spedire effettivamente i datagram sicuri verso di essa. Come abbiamo visto nei paragrafi precedenti esistono due modalità con cui è possibile implementare i protocolli IPSec, la modalità "Trasporto" e la modalità "Tunnel".

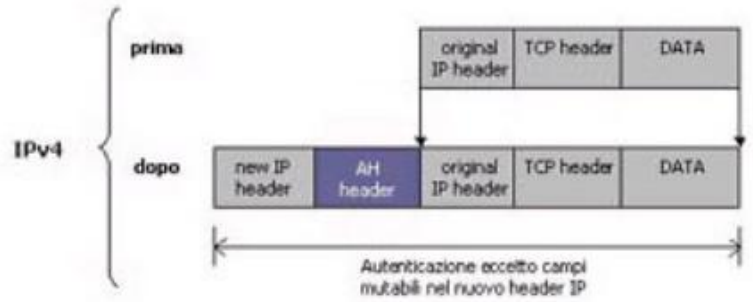
6.5.1. AH (Modalità Trasporto)

In questa modalità i datagram IPsec comprendono l'intestazione AH, che è inserita fra i dati del datagram IP originale (per esempio un segmento TCP) e l'intestazione IP, come mostrato in figura. L'header IP del pacchetto originale subisce una modifica nel campo "protocol" nel quale viene inserito il valore 51 per indicare che il datagram sta incapsulando un'intestazione AH. Quando l'host di destinazione riceve il datagram IP, esso si accorge del valore 51 presente nel campo protocollo ed elabora il datagram usando il protocollo AH. I router intermedi elaborano i datagram come hanno sempre fatto: esaminano l'indirizzo IP di destinazione e instradano i datagram in funzione di questo indirizzo.



6.5.2. AH (Modalità Tunnel)

La modalità Tunnel invece, prevede la creazione, da parte del mittente, di un pacchetto IP ausiliario utilizzato per ospitare l'originario datagram IP. Quest'ultimo viene messo in sicurezza mediante incapsulamento in un pacchetto AH. Come è possibile osservare dalla figura, grazie a questa modalità, il pacchetto IP originario viene interamente protetto (Header + Dati), mentre nella modalità Trasporto poteva esserlo solo in parte (l'header IP restava fuori dalla protezione di AH).

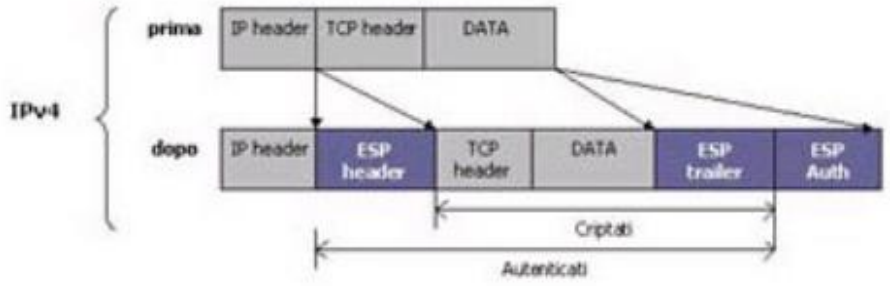


6.6. ESP (Encapsulating Security Payload) RFC 2406

Il protocollo ESP fornisce la segretezza a livello di rete, ma può fornire anche autenticazione dell'host così come AH. I servizi offerti da ESP sono mutuamente esclusivi e oltre a quelli già citati vi può essere anche il controllo dei duplicati (opzionale), il quale, se presente, deve essere accompagnato dall'autenticazione della sorgente. Nel caso di modalità trasporto è necessario indicare il valore 50 nel campo protocol del datagram IP originario, per indicare che il datagram contiene un pacchetto ESP. Quando l'host di destinazione, ricevuto il datagram IP, vede il valore 50, elabora il datagram usando tale protocollo.

6.6.1. ESP (modalità Trasporto)

ESP in modalità trasporto può essere applicato solo a comunicazioni host-to-host e vengono protetti solo i dati relativi ai protocolli superiori, non l'header IP del pacchetto stesso. In modalità di trasporto, ESP è inserito dopo l'header IP e prima dei protocolli di livello superiore (TCP, UDP, ICMP, ...) e di qualsiasi altro header IPsec precedentemente inserito. Vediamo in dettaglio le caratteristiche della modalità trasporto. Come mostra la seguente figura, un datagram sicuro è creato circondando il campo dati del datagram IP originale con l'intestazione e il trailer del pacchetto ESP, e quindi reinserendo il tutto sotto l'header del datagram IP originale.



6.6.2. ESP (Modalità Tunnel)

Nella modalità Tunnel invece, il datagram sicuro è creato circondando l'intero datagram IP originale con i campi intestazioni e trailer del pacchetto ESP, e quindi inserendo il tutto, questa volta, in un nuovo pacchetto IP. Così come mostrato dalla seguente figura.