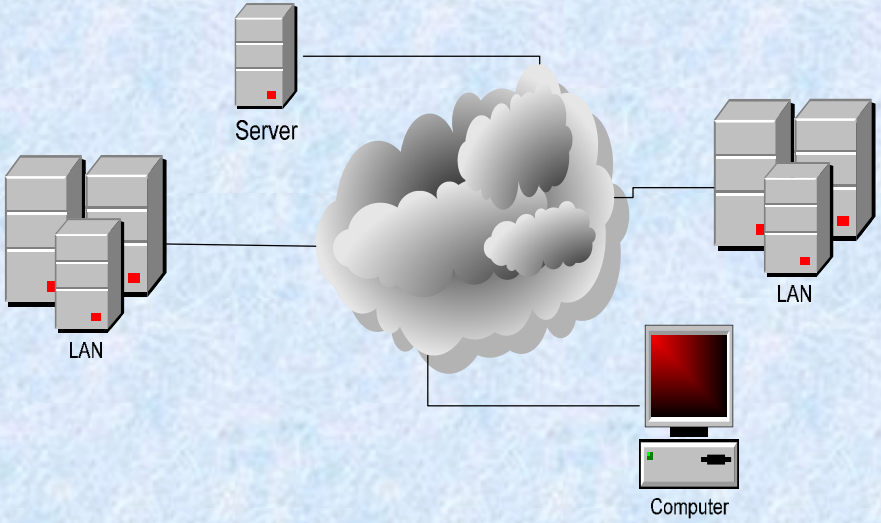
Università di Pisa – Facoltà di Informatica
Corso di Tecnologie di convergenza su IP
a.a. 2005/2006

# **VPN**
# Virtual Private Network

Gaspare Sala

# Introduzione

- Una rete pubblica è un insieme di sistemi indipendenti che si scambiano dati tra di loro più o meno liberamente.
- Una rete privata è composta da computer appartenenti ad una stessa organizzazione che condividono informazioni e risorse, non visibili da utenti all'esterno del gruppo.
- Necessità di interconnettere reti private con altre reti private o con utenti senza ricorrere a linee dedicate (costose e poco flessibili)
- Simulare una rete privata e sicura sulla rete pubblica




**Application layer security**
- Security e-mail (S-MIME)
- DNS security extensions
- SSH(Secure SHell)

**Transport layer security**
- SSL (Secure Socket Layer)

**Network layer security**
- IPSec
- PPTP, L2TP

# Introduzione

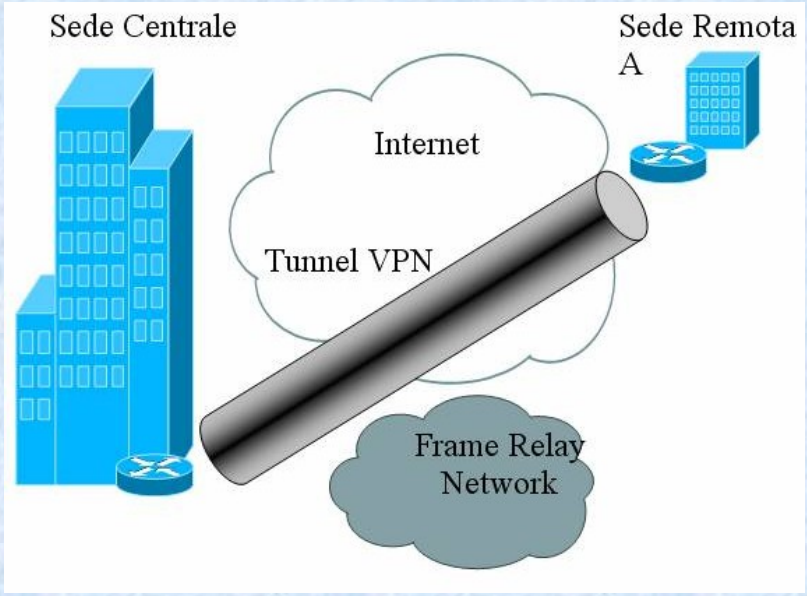
**Firewall**

- Il limite tra una rete pubblica e una privata sta di solito in un Gateway router, in cui viene inserito un firewall che filtra gli accessi da Internet verso l'interno e viceversa.
- Rendere sicura la rete privata come se fosse isolata creando uno o più *perimetri di sicurezza*.
- Permettere la connessione verso un'altra rete privata di quel gruppo
- Condizione necessaria prima di creare una VPN.

# Introduzione

**Tunneling**

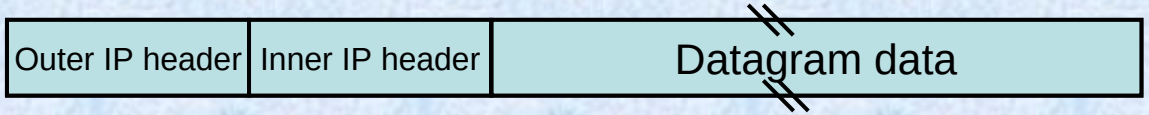
- Creazione di una rete virtuale in cima ad una rete fisica, attraverso l'incapsulamento di dati appartenenti ad un protocollo dentro il campo dati di un altro protocollo di uguale o più alto livello.
- Simula un collegamento diretto tra due o più sistemi
- Il traffico nel tunnel non interferisce con il traffico della rete Internet e quindi con il routing.
- Permette di trasportare pacchetti di un protocollo incompatibile con la rete su cui si trasmettono.
- Di per se non garantisce autenticazione o segretezza dei dati incapsulati.



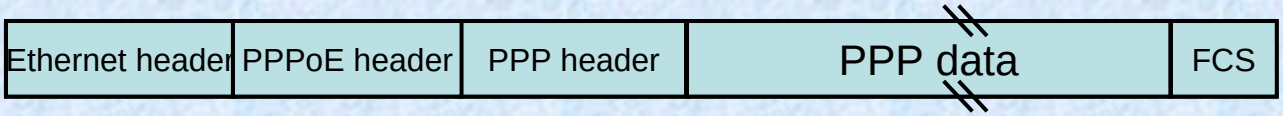
# Introduzione

**Tunnels**

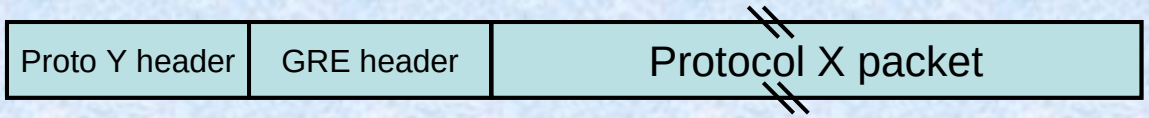
- **IP-in-IP**




- **PPPoE**

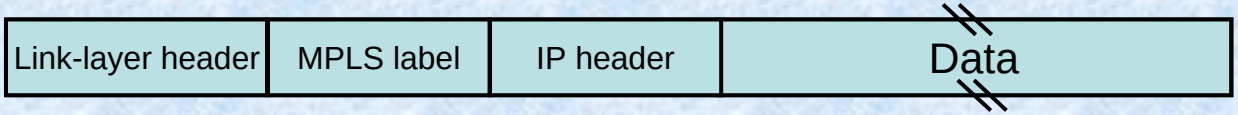



- **GRE**




– si evita di implementare codice specifico per l'incapsulamento per ogni coppia di protocolli (X,Y)

- **MPLS**




– Multiprotocollo: incapsula qualsiasi tipo di pacchetti di livello network che, nel tunnel, sono "opachi" ai router

# Introduzione

**Identification & Authentication**

- Assicurare che le parti coinvolte nella comunicazione scambiano informazioni con il corretto utente o host.
- Shared Key System o RSA.
- Effettuata all'inizio e casualmente durante ogni sessione.
- Può eventualmente assicurare l'integrità dei dati.

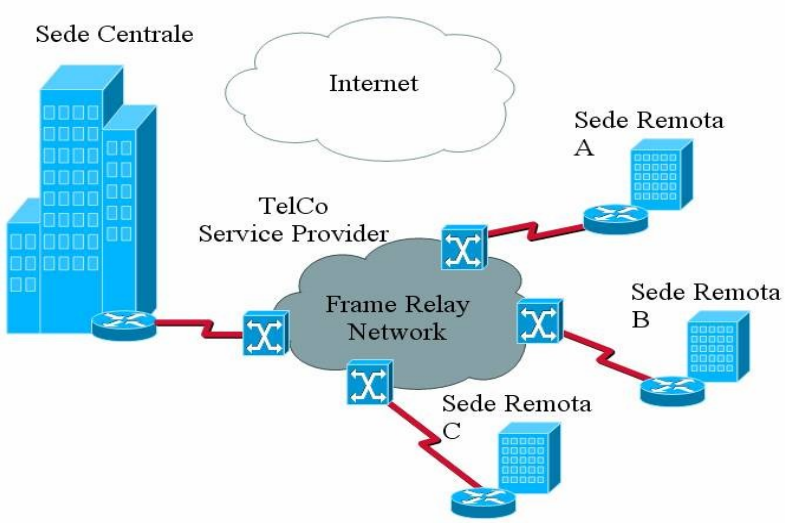
**Encryption** 

- Impacchettare i dati dentro un contenitore sicuro.
- Private or public key encryption.

# Classificazioni

Sostanzialmente una rete privata può essere distinta sia per la tecnologia:

• **Trusted**: sfrutta uno o più circuiti noleggiati da un fornitore di telecomunicazioni. ⇒ **WAN, RAS**




• **Secure**: utilizza mezzi di comunicazione pubblici e mantiene la riservatezza di quanto trasportato mediante l'uso di crittografia e specifiche procedure di sicurezza. ⇒ **VPN**

# Classificazioni

che per l'impiego che se ne fa:

- **Remote access**: accesso remoto ad una struttura condivisa da parte di un utente(ISDN, PSTN, cable modem, DSL**)** ⇒ **PPTP, L2TP,SSH**
- **Intranet**: Collega la sede aziendale principale a uffici remoti,filiali,… ⇒ **IPsec**
- **Extranet**: Collega alla rete aziendale clienti o comunità di interesse ⇒ **IPsec**

Una VPN mantiene le stesse politiche e prestazioni di una rete privata, ma:

- permette di ridurne i costi totali di gestione
- migliora le connettività
- è flessibile e scalabile
- è sicura ed affidabile

# IPsec

- Proposto nell'Ottobre 1993 per introdurre funzioni di sicurezza in IP senza alterarne la struttura [RFC 2401]
- Tecnologia VPN standard per IETF definita per TCP/IP.
- Obiettivi:
  - flessibilità nella configurazione della VPN
  - integrazione con lo stack TCP/IP e quindi con i meccanismi di routing
- Indipendente dagli algoritmi crittografici utilizzati
- Può essere applicato ad una comunicazione senza modificare le applicazioni o gli apparati intermedi che forniscono la connettività.

# IPsec

Consiste di 3 protocolli principali:

- **AH** che fornisce autenticazione dell'origine, integrità dei dati e protezione da attacchi replay[RFC 2402]
- **ESP** fornisce gli stessi servizi di AH più segretezza dei dati[RFC 2406]
- **IKE** fornisce, in alternativa alla gestione manuale, funzioni di gestione e scambio tra i sistemi dei parametri di comunicazione e di sicurezza [RFC 2409]

AH ed ESP determinano l'incapsulamento e possono operare in 2 modalità:

- **Transport** fornisce sicurezza (end-to-end) ai protocolli dal livello trasporto in su nel datagram IP.
- **Tunnel** fornisce sicurezza (non solo end-to-end) all'intero datagram IP cioè all'intero tunnel ma richiede maggiore banda.

La combinazione e la manipolazione di questi meccanismi fornisce una comunicazione che può essere orientata a:

- **client to network**
- **network to network**
- **client to client**

# Security Associations

Per costruire una VPN c'è bisogno di uno stato condiviso e quindi di sincronizzazione tra i punti terminali del tunnel.

Questo stato condiviso è contenuto in una struttura dati chiamata appunto SA che è composta da tutti i dati necessari ai terminali per mantenere una connessione VPN :

- Indirizzo IP di ciascun terminale e/o IPsec Gateway
- Algoritmo crittografico e le sue chiavi
- Algoritmo di autenticazione e le sue chiavi
- Il numero di sequenza corrente
- Il ciclo di vita dello stesso SA
- Il Security Parameter Index(SPI), un numero identificativo assegnato dal terminale di destinazione.

La tripla **< SPI, destination address, protocol >** identifica univocamente un SA su un host

Ogni terminale VPN deve avere una coppia(input/output) di SA per ogni protocollo(AH/ESP), contenuta in un Security Associations Database(SAD)

# IPsec processing

- È possibile stabilire regole chiamate **policies,** che specificano le azioni da compiere su ogni datagram uscente da o entrante in un terminale VPN

Il security policy database(**SPD**) è un insieme *ordinato* delle policies di un nodo

- I campi del datagram usati per stabilire se un datagram rispetta la policy viene detto **selettore**.

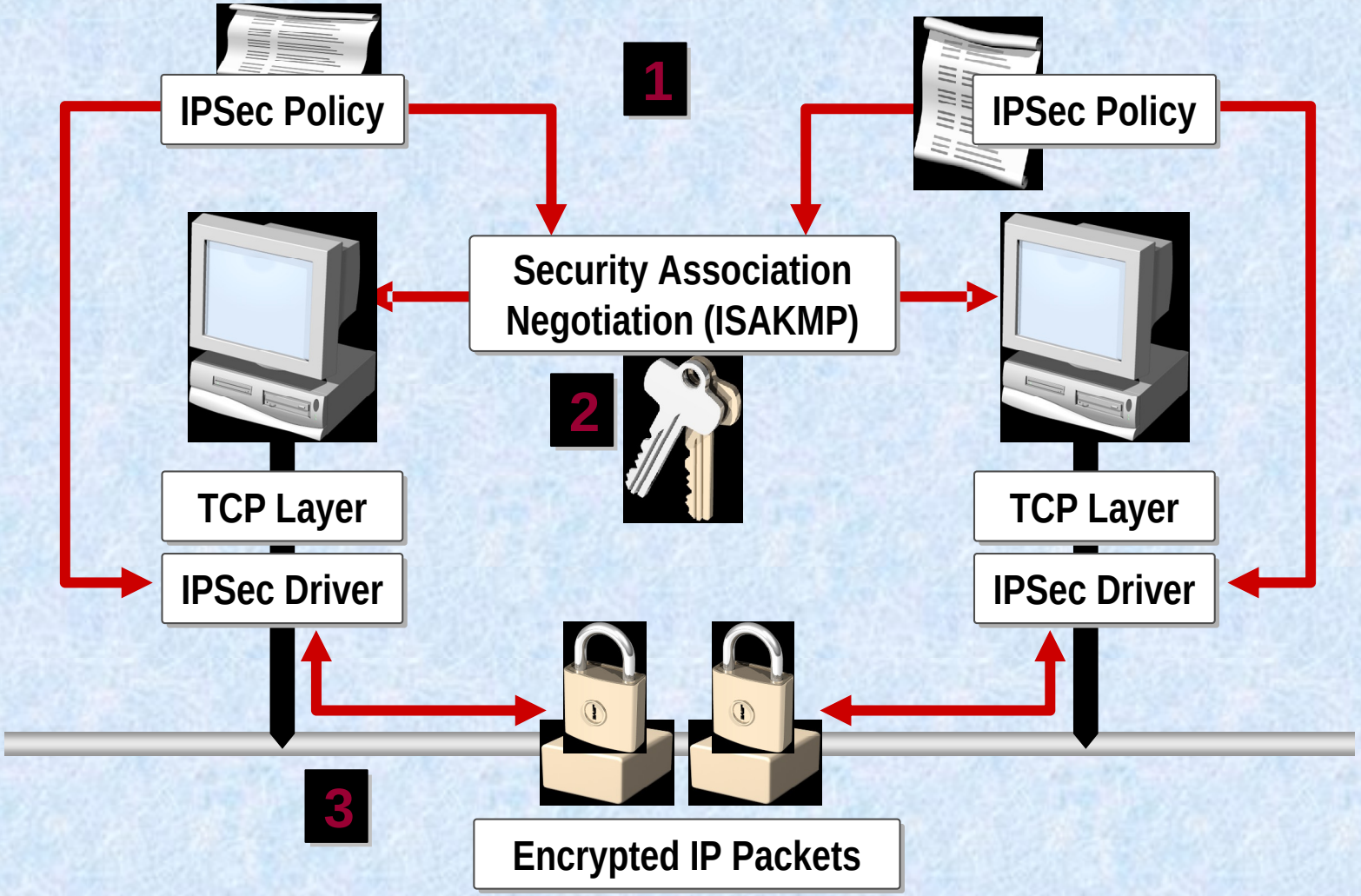
**Outbound processing:**

1. Confronta ogni selettore del datagram uscente con quello contenuto nelle policies nel SPD. Compie azioni a seconda se la policy:
   - specifica che deve essere scartato
   - specifica che deve essere bypassato e trasmesso normalmente
   - specifica che deve essere applicato un protocollo di IPsec
   - non esiste allora negozia nuovo SA con il peer
2. Cerca il primo SA in SAD e applica il corrispondente servizio IPsec al datagram

**Inbound processing:**

1. Controlla se il datagram in entrata contiene un header IPsec.
2. Seleziona il SA associato, se non lo trova scarta il datagram.
3. Esegue la decifratura e/o autenticazione specificata nel SA e verifica che i selettori del datagram risultante matchano con la policy corrispondente a quel SA.
4. Invia il datagram decapsulato al prossimo hop se non ha ancora raggiunto la destinazione

# IPsec processing



# IKE

- Protocollo ibrido derivante da tre protocolli:
  - ISAKMP
  - OAKLEY
  - SKEME
- Crea una coppia di SA quando si stabilisce una sessione IPsec
- Mantiene lo stato della VPN, negoziando nuove SA quando è necessario
  - usa Diffie-Hellman per ottenere una chiave segreta condivisa
  - crittografia a chiave pubblica per firmare lo scambio di chiavi

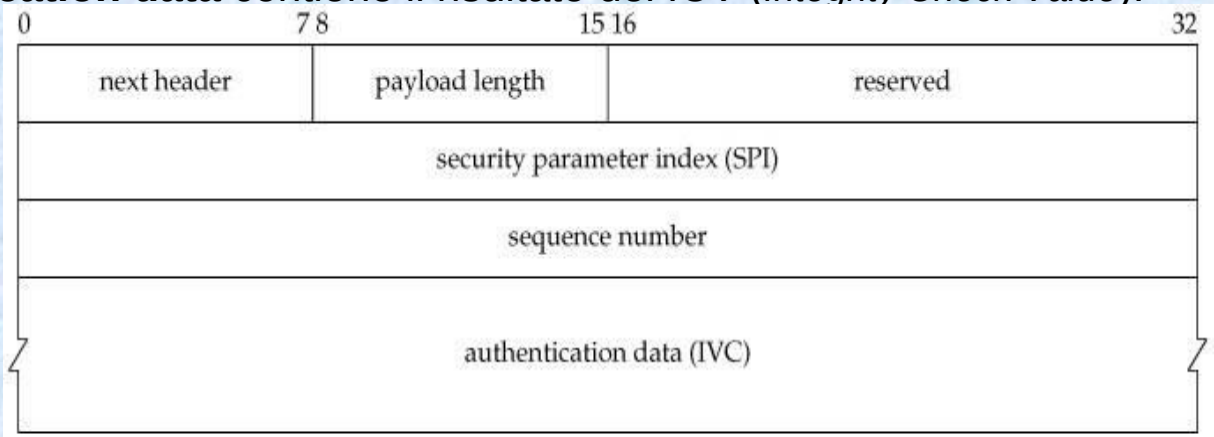
Con questa tecnica, ogni peer si scambia in modo protetto dati per la cifratura e l'autenticazione nella connessione IPsec

- Certificati digitali per validare le chiavi pubbliche
- DES, 3DES, RC5 per cifrare i dati
- SHA1, MD5 per l'autenticazione

# AH

Il protocollo AH garantisce autenticazione e integrità dei dati sia per l'intestazione IP che per i dati utilizzando una funzione di hash (no encryption)

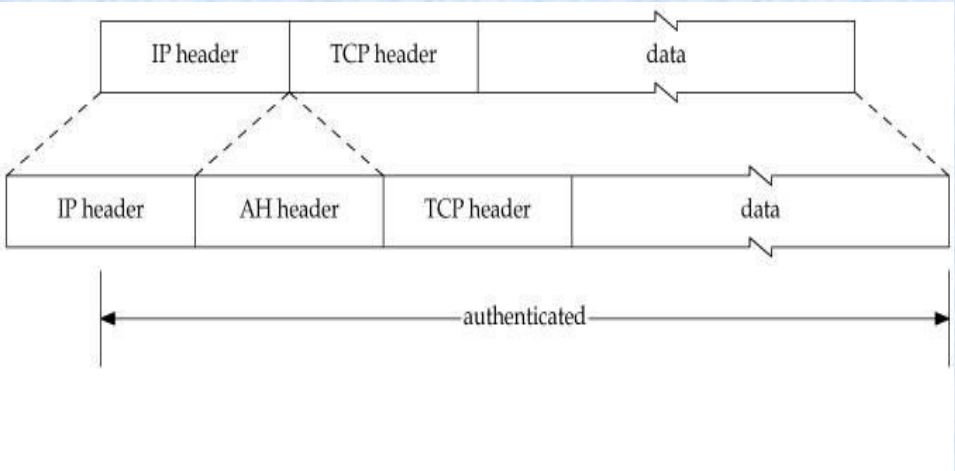
- Il campo **next header** è un numero che identifica il protocollo contenuto nel payload di AH.
- Il campo **payload length** è la lunghezza dell'header di AH
- Il **security parameter index**, insieme all'indirizzo di destinazione e all'identificatore del protocollo(AH) identifica il SA a cui si applica questo datagram AH.
- Il **sequence number** è un contatore,inizialmente con valore 1, che si incrementa di una unità per ogni datagram AH inviato da un host ad un SA. L'host ricevente lo usa per scoprire datagram ripetuti.
- Il campo **authentication data** contiene il risultato del ICV (*Integrity Check Value*).

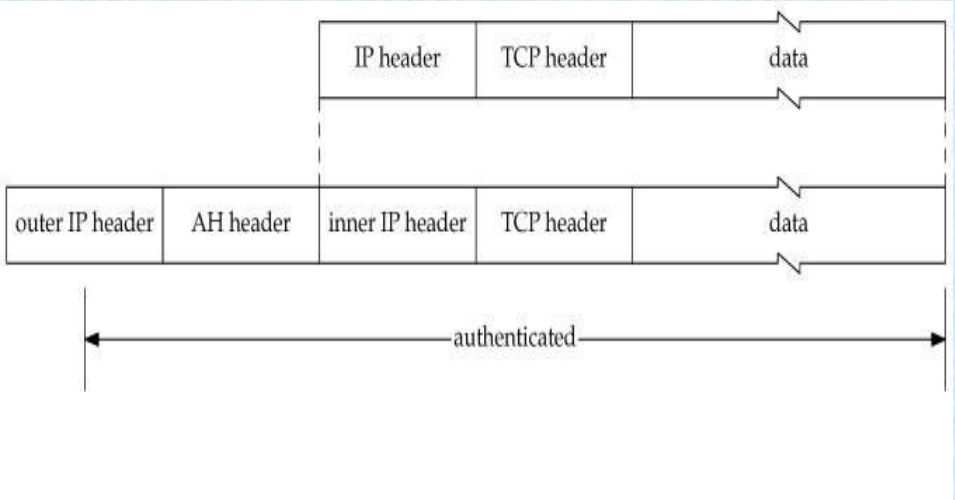


# AH

AH può essere implementato:

- nella modalità *Transport Mode*, in cui solo la parte fissa dell'header IP viene autenticata(compreso il source address)
  - Non può essere usato con un NAT o PAT esterno. L'indirizzo sorgente e le porte fanno parte dell'ICV
    → datagram scartato
- nella modalità *Tunnel Mode*, in cui l'intero pacchetto IP originario viene autenticato ed incapsulato in un nuovo pacchetto:
  - NAT non necessario perchè all'header IP esterno del datagram viene assegnato l'indirizzo del Gateway

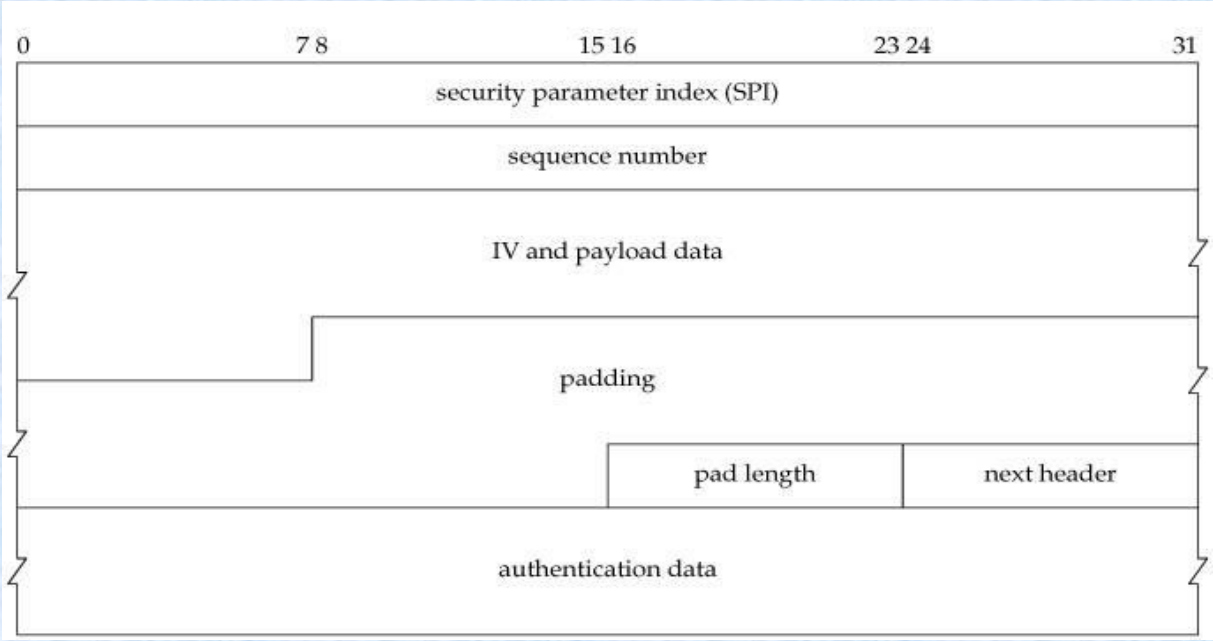


# ESP

Garantisce anche la confidenzialità dei dati scambiati(encryption):

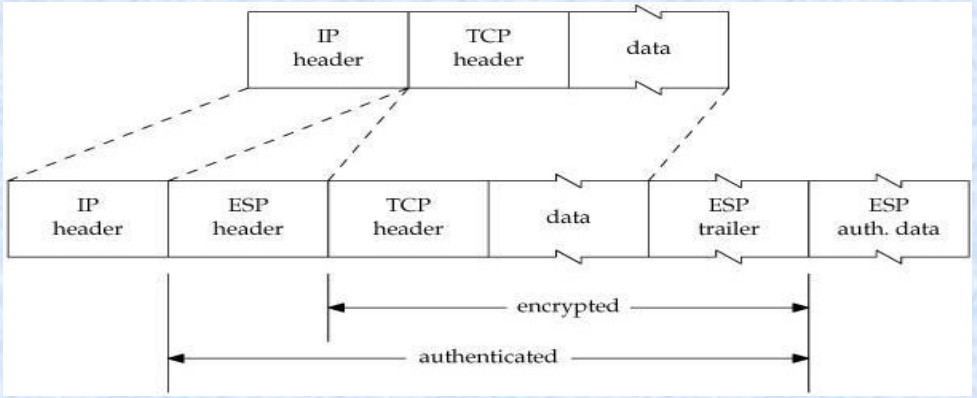
- Se l'algoritmo crittografico richiede esplicitamente un *initialization vector* allora viene incluso nel campo **IV and payload data**.
- Gli algoritmi di cifratura a blocchi richiedono che il testo in chiaro abbia una dimensione multiplo della dimensione del blocco. Allora, se necessario, viene inserito un certo **padding** immediatamente dopo il payload.
- La lunghezza del padding sta nel campo **pad length**.
- Il campo **next header** indica il tipo di dati contenuti nel campo IV and payload data
- Il campo **authentication data** contiene un controllo di integrità per il pacchetto ESP.

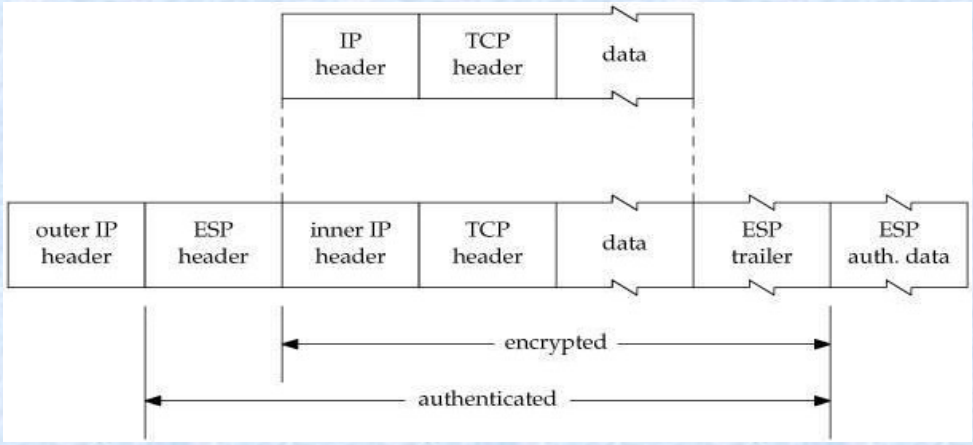


# ESP

ESP può essere implementato:

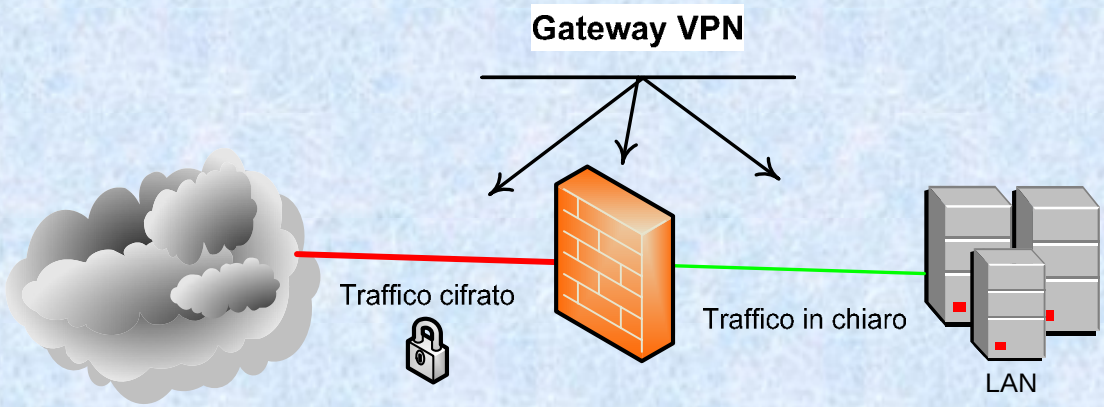
- nella modalità *Transport Mode,* in cui:
  - ESP header non è crittato altrimenti il ricevente non saprebbe l'SPI e non potrebbe decrittare il pacchetto
  - Il ricevente è sicuro dell'autenticità del mittente perché soltanto loro due posseggono le chiavi.
  - Può essere usato con NAT
  - No PAT esterno → l'header di livello trasporto è cifrato
- nella modalità *Tunnel Mode*, in cui l'intero pacchetto IP originario viene incapsulato in un nuovo pacchetto:
  - Il ricevente è sicuro che il pacchetto originale non è stato modificato
  - Protezione contro analisi del traffico
  - NAT non necessario




Si usa combinare AH con ESP in modo da autenticare anche l'indirizzo di origine contenuto nell'header IP esterno

# VPN Gateway e Firewall




- Interno
  - Nessun controllo sul traffico VPN
  - Gateway VPN protetto dal firewall
- Esterno
  - Gateway protetto solo dall'access router
  - Controllo su traffico
- Integrato
  - Flessibilità massima

# FINE