LA SICUREZZA IP

Corso di Laurea Magistrale in Ingegneria Informatica

A.A. 2015/2016

Prof. Simon Pietro Romano

spromano@unina.it

PANORAMICA SULLA SICUREZZA IP

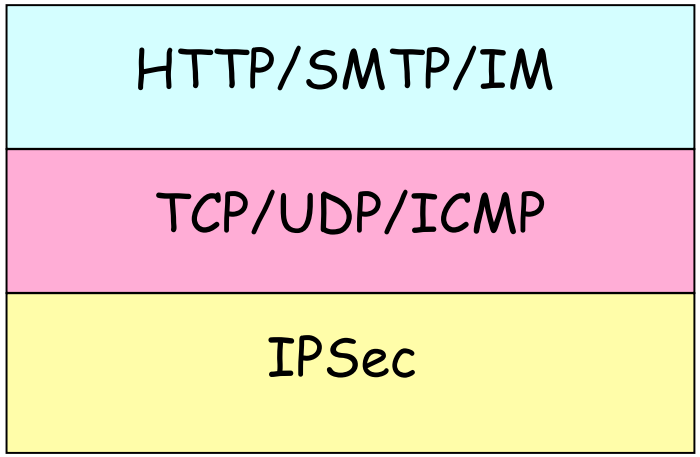
- 1994 – IAB (Internet Architecture Board)
  - "Security in the Internet Architecture" (RFC 1636)
    - Consenso sulla necessità di migliorare il livello di sicurezza di internet
    - Identificazione delle aree chiave per i meccanismi di sicurezza
    - Necessità di evitare monitoraggio non autorizzato del traffico
    - Necessità di rendere sicuro il traffico in transito mediante meccanismi di autenticazione e crittografia
- 2003 – CERT (Computer Emergency Response Team)
  - Più di 137000 incidenti legati alla sicurezza
  - Gravi attacchi perpetrati utilizzando IP spoofing
  - Sfruttamento delle applicazioni che utilizzano l'autenticazione basata su indirizzo IP
  - Lesioni del diritto alla privacy mediante intercettazione del traffico
    - Informazioni di login
    - Contenuto di DB
    - Contenuto di pagine Web

OBIETTIVI

- “Rattoppo” per IPv4
  - Lo Spoofing è un problema serio e concreto
  - Il protocollo non è stato progettato con l’idea dell’autenticazione e della sicurezza
  - Il contenuto dei datagrammi può essere intercettato
  - Il contenuto dei datagrammi può essere modificato
  - Le reti IPv4 possono essere soggette ad attacchi di tipo replay
- Meccanismi di livello rete per IPv4 ed IPv6
  - Non necessariamente tutte le applicazioni devono supportare meccanismi di sicurezza
- Può essere trasparente agli utenti

SICUREZZA “A LIVELLI”

- Link layer: WEP/WPA
- Application layer: PGP (Pretty Good Privacy)
- Transport layer: SSL (Secure Sockets Layer)
- Network layer: IPSec (IP Security)
- Approccio IPSec: gestione sicura della rete per applicazioni “security-unaware”…



CONCETTI ESSENZIALI

- Funzioni di sicurezza per l'estensione di IPv4 & IPv6
- Tre aree funzionali
  - Autenticazione
    - Un datagramma ricevuto è stato realmente trasmesso dalla sorgente indicata nell'intestazione
    - Il datagramma non è stato alterato durante il transito
- Segretezza
  - Crittografia dei messaggi
  - Prevenzione delle intercettazioni
- Gestione delle chiavi
  - Scambio sicuro delle chiavi crittografiche

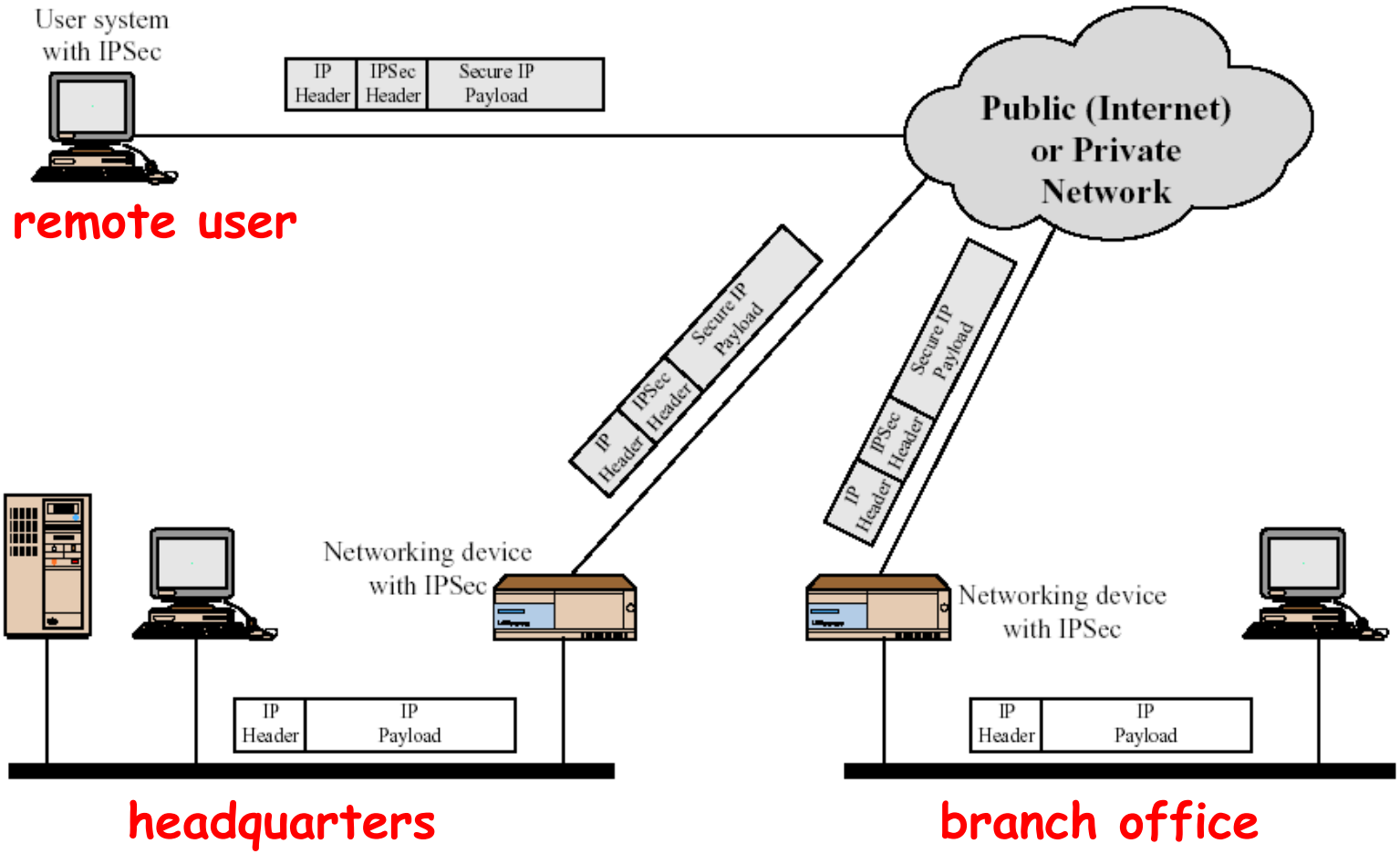
MECCANISMI

- Autenticazione
  - Applicata all'intero datagramma IP → modalità tunnel
  - Datagramma esclusa l'intestazione → modalità transport
- Approcci
  - Encapsulating Security Payload (ESP)
  - Authentication Header (AH)
- Gestione delle chiavi
- Trasparenza alla rete
  - Solo gli end-point della comunicazione devono essere abilitati all'utilizzo di IPSec

APPLICAZIONI DI IPSec

- Connettività sicura delle sedi locali via internet
  - Rete privata virtuale attraverso reti geografiche pubbliche
  - Ridotta necessità di reti private
    - Risparmio in costi di esercizio e gestione della rete
- Accesso remoto sicuro via Internet
  - Un utente finale chiama un ISP locale ed acquisisce un accesso sicuro alla rete aziendale
  - Riduzione dei costi telefonici per tele-lavoratori e dipendenti spesso in viaggio
- Attivazione della connettività extranet e intranet con partner commerciali
  - Comunicazioni sicure con altre aziende e partner commerciali mediante meccanismi di autenticazione, segretezza e scambio di chiavi
  - Miglioramento della sicurezza del commercio elettronico
    - Applicazioni Web utilizzano protocolli interni per la sicurezza

SCENARIO D'USO DI IPSEC



IPSec: VANTAGGI

- Implementato in un firewall o un router fornisce un elevato livello di sicurezza a tutto il traffico che attraversa il perimetro
  - Il traffico interno al perimetro non subisce il sovraccarico dell'elaborazione per la sicurezza
- IPSec in un firewall è difficile da eludere se tutto il traffico proveniente dall'esterno transita su IP ed il firewall è l'unico mezzo di ingresso da Internet
- IPSec è situato sotto al livello trasporto e risulta trasparente alle applicazioni
  - Non sono richieste modifiche ai software degli utenti finali o sui server se IPSec è implementato in un router/ firewall di bordo
  - IPSec implementato negli host terminali non influenza comunque le applicazioni sovrastanti
- IPSec è trasparente agli utenti finali
  - Nessuna necessità di addestramento alla sicurezza
  - Nessuna informazione sulle chiavi e sulla loro esistenza
- IPSec può garantire la sicurezza dei singoli utenti
  - Utile ai lavoratori fuori sede
  - Utile per la configurazione di sottoreti virtuali

SUPPORTO AL ROUTING

- IPSec può fornire garanzie nell'utilizzo di algoritmi di routing
  - Messaggio di pubblicizzazione di un nuovo router proviene da un router autorizzato
  - Messaggio di pubblicizzazione di un neighbor proviene da un router autorizzato
  - Messaggio di redirezione proviene dal router al quale è stato inviato un pacchetto
  - Aggiornamento delle informazioni di routing non falsificato

ARCHITETTURA DI IPSEC

DOCUMENTAZIONE IPSec

- Numerose RFC:
  - RFC 4301: panoramica dell'architettura di IPSec
  - RFC 4302: estensione per l'autenticazione dei datagrammi in IPv4 ed IPv6 (AH)
  - RFC 4303: estensione per la crittografia dei datagrammi in IPv4 ed IPv6 (ESP)
  - RFC 5996: protocollo per lo scambio delle chiavi (IKE – Internet Key Exchange)
  - RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP)
  - RFC 2412: protocollo per la determinazione delle chiavi (Oakley)

DOCUMENTAZIONE IPSec

- Supporto opzionale in IPv4
- Supporto obbligatorio in IPv6
- Funzionalità di sicurezza implementate come extension header immediatamente successivo all'intestazione IP
  - Autentication Header (AH) – extension header per l'autenticazione
  - Encapsulating Security Payload (ESP) – extension header per la crittografia

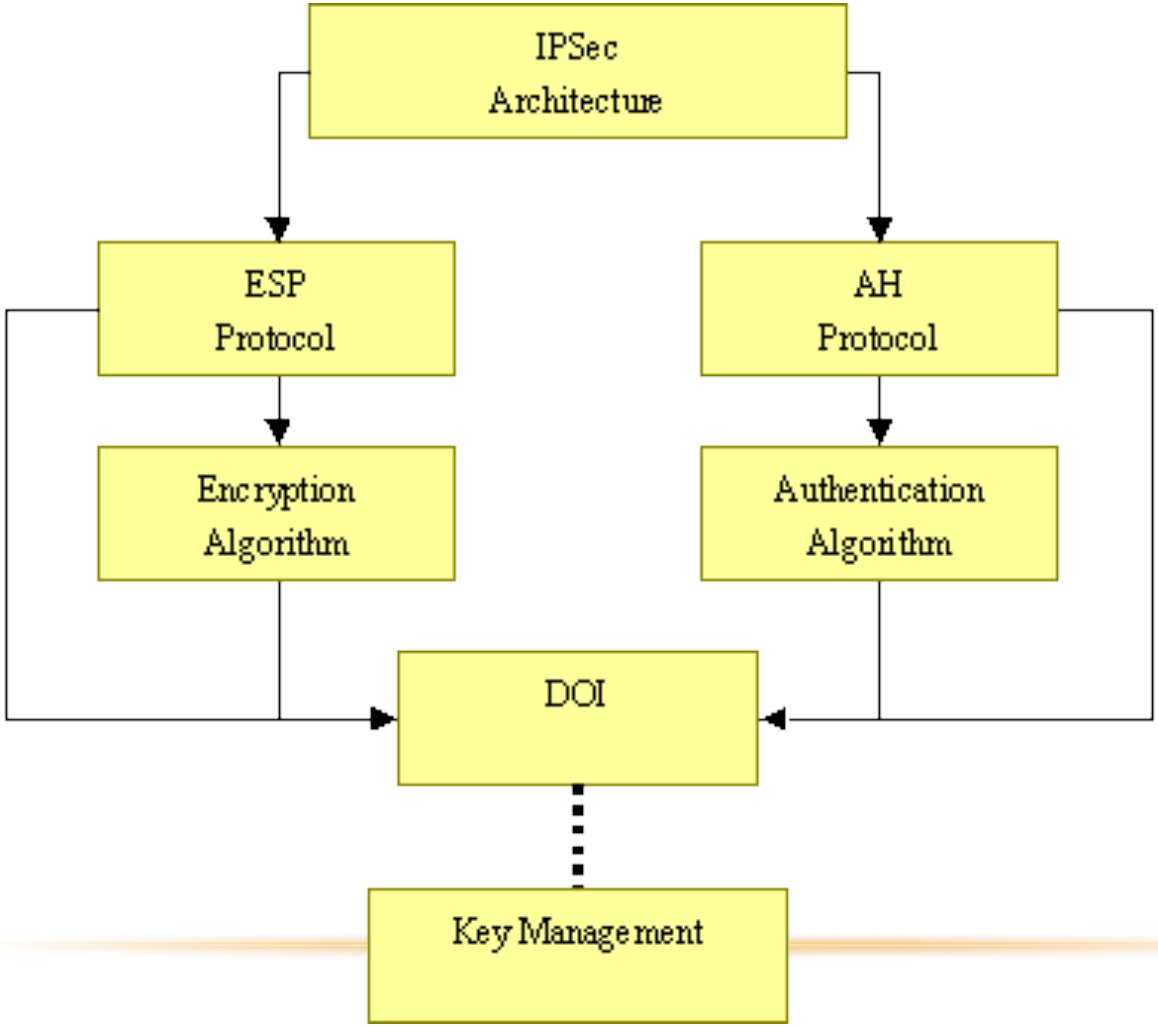
DOCUMENTAZIONE IPSec

- Architettura
  - Concetti generali
  - Requisiti di sicurezza
  - Definizioni e meccanismi
- ESP (Encapsulating Security Payload)
  - Formato del pacchetto
  - Elementi generali di autenticazione e crittografia del pacchetto
- AH (Authentication Header)
  - Formato del pacchetto
  - Elementi generali di autenticazione del pacchetto

DOCUMENTAZIONE IPSec

- Algoritmi di crittografia
  - Utilizzo degli algoritmi di crittografia in ESP
- Algoritmi di autenticazione
  - Utilizzo degli algoritmi di autenticazione in AH ed ESP
- Gestione delle chiavi
  - Descrizione dei meccanismi di gestione delle chiavi
- DOI (Domain Of Interpretation)
  - Relazioni fra i documenti
  - Identificatori per gli algoritmi di crittografia
  - Identificatori per gli algoritmi di autenticazione
  - Parametri operativi
    - Es. durata delle chiavi

DOCUMENTAZIONE IPSec



I SERVIZI DI IPSec

- Possibilità di selezionare i protocolli di sicurezza richiesti
- Determinare gli algoritmi da utilizzare per i servizi
- Determinare gli algoritmi da utilizzare per la gestione delle chiavi

- Authentication Header
  - Autenticazione mediante intestazione del protocollo
- Encapsulating Security Payload
  - Autenticazione e crittografia stabiliti dal formato del pacchetto

I SERVIZI DI IPSec

- Controllo degli accessi
- Integrità dei dati in protocolli connectionless
- Autenticazione dell'origine dei dati
- Rifiuto del replay dei pacchetti
  - Forma di integrità parziale della sequenza
- Segretezza
  - Crittografia
- Segretezza parziale del flusso del traffico

I SERVIZI DI IPSec

	AH	ESP (solo crittografia)	ESP (crittografia ed autenticazione)
Controllo degli accessi	X	X	X
Integrità senza connessione	X		X
Autenticazione origine dei dati	X		X
Rifiuto pacchetti a replay	X	X	X
Segretezza		X	X
Segretezza parziale del flusso		X	X

SECURITY ASSOCIATIONS (SA)

- Una SA è una relazione monodirezionale fra un mittente ed un destinatario
  - Due SA necessarie per uno scambio bidirezionale
- Una SA è utilizzata per AH o per ESP, ma mai per entrambi
- Prima dell'invio dei dati, una connessione virtuale viene stabilita fra due end-point IPSec
  - Stato della connessione ad ogni end-point, come in TCP
  - La connessione è denominata security association (SA)

IP è connectionless; IPSec è connection-oriented!

SECURITY ASSOCIATIONS (SA)

- Una SA è identificata univocamente da tre parametri
  - Security Parameters Index (SPI)
    - Stringa di bit assegnata alla SA
      - Significato esclusivamente locale
    - Trasportato nelle intestazioni AH o ESP per consentire al destinatario la selezione della SA appropriata
  - Indirizzo IP del destinatario
    - Attualmente consentito solo l'impiego di indirizzi unicast
      - Destinazione finale della SA
        - Firewall
        - Router
        - Utente finale
  - Identificatore del protocollo di sicurezza
    - Indica se la SA è di tipo AH o ESP

SECURITY ASSOCIATIONS (SA)

- Per ogni datagramma IPv4 o pacchetto IPv6 l'associazione di sicurezza è identificata univocamente:
  - dall'indirizzo di destinazione nell'intestazione IPv4 o IPv6
  - dal parametro SPI nell'intestazione di estensione AH o ESP
- Meccanismo di gestione della chiave affiancato a meccanismi di autenticazione e privacy tramite il Security Parameters Index
  - Meccanismi di autenticazione e privacy indipendenti dai meccanismi di gestione della chiave

PARAMETRI DI UNA SA

- Security Association Database (SAD):
  - Base dati nominale che definisce i parametri relativi a ciascuna SA
    - La funzionalità deve essere disponibile
    - L'implementazione può variare
- Informazioni chiave:
  - "sequence number counter"
    - Valore a 32 bit contenente un sequence number per l'intestazione AH o ESP (obbligatorio)
  - "sequence counter overflow flag"
    - Indica se un overflow del campo Sequence Number Counter deve generare un evento di audit ed impedire ulteriori trasmissioni sulla SA (obbligatorio)
  - "anti-replay window"
    - Utilizzato per determinare se un pacchetto AH o ESP in ingresso è un replay

PARAMETRI DI UNA SA

- AH information
  - Algoritmo di autenticazione, chiavi, durata delle chiavi, ecc. (obbligatorio per AH)
- ESP information
  - Algoritmo di crittografia ed autenticazione, chiavi, valori di inizializzazione, durata delle chiavi, ecc. (obbligatorio per ESP)
- lifetime
  - Intervallo di tempo o conteggio in byte oltre il quale la SA deve essere sostituita da una nuova SA con un nuovo SPI o chiusa
  - Include l'indicazione dell'azione da eseguire
- IPSec protocol mode
  - Modalità tunnel o trasporto
  - Consente l'utilizzo di wildcard
- path MTU
  - MTU sul percorso

SELETTORI DI SA

- Più SA possono essere combinate per fornire la configurazione desiderata
- Elevato livello di granularità nella distinzione fra traffico protetto da IPSec e traffico non protetto
- Traffico IP associato alle SA mediante il Security Policy Database (SPD)
  - Ogni elemento definisce un sottoinsieme del traffico IP
  - Ogni elemento punta alla SA da applicare al traffico identificato
  - Più voci possono essere collegate alla stessa SA
  - Più SA possono essere relative alla stessa voce nel SPD
  - Ogni voce è definita mediante campi IP e di livello superiore chiamati selettori

TIPI DI SELETTORI

- Destination IP address (single, enumerated list, range, o mask)
- Source IP address (single, enumerated list, range, o mask)
- Transport layer protocol (single, enumerated list, o range)
- Destination port (single, enumerated list, range, o wildcard)
- Source port (single, enumerated list, range, o wildcard)
- UserID ottenuto dal sistema operativo
- Data sensitivity level (secret, unclassified, ...)

FUNZIONE DEI SELETTORI

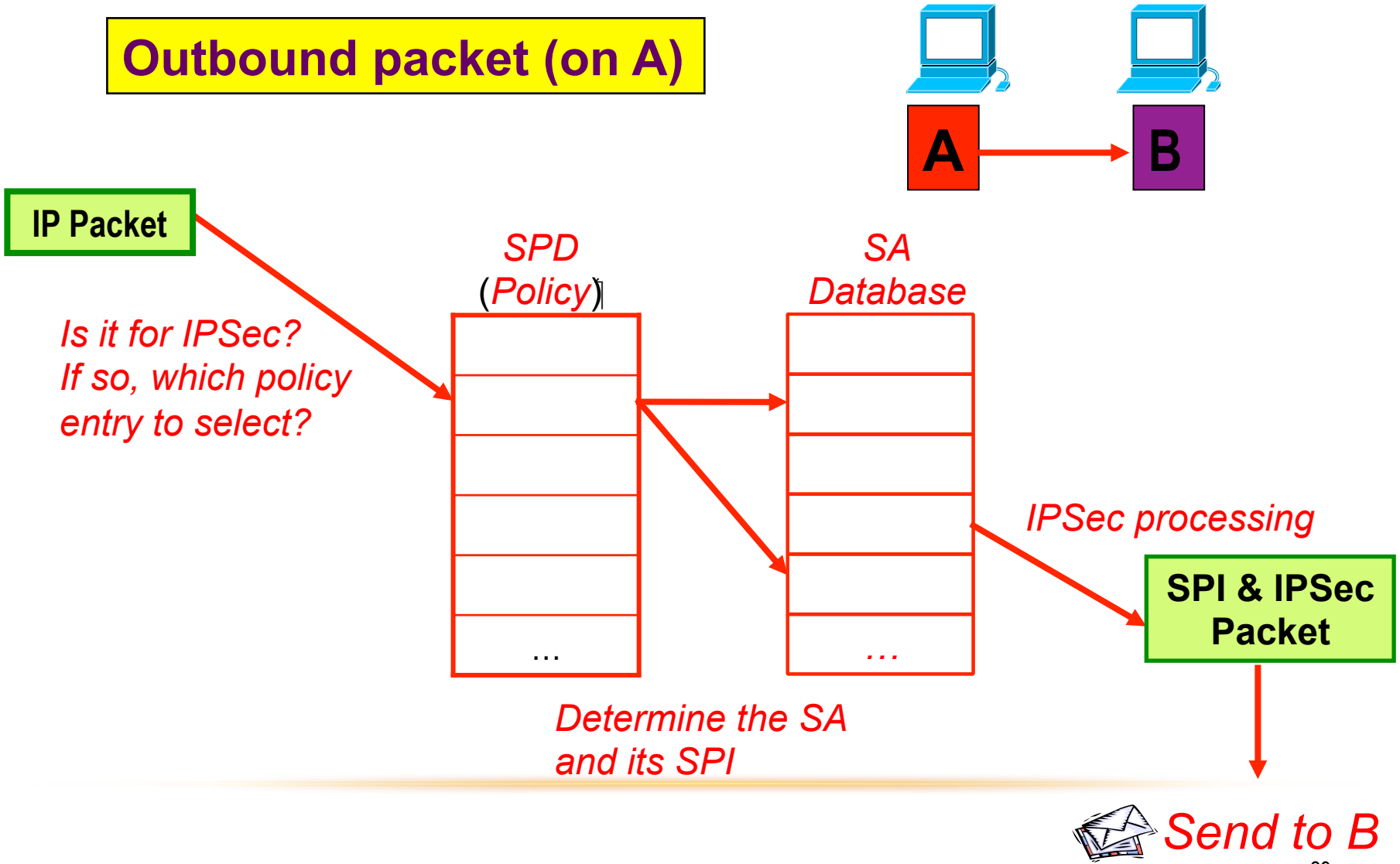
- I selettori consentono di filtrare il traffico in uscita ed associarlo ad SA
  - Confrontare i campi del pacchetto con quelli del SPD
  - Determinare l'eventuale SA ed il corrispondente SPI
  - Svolgere l'elaborazione richiesta per il pacchetto (AH o ESP)

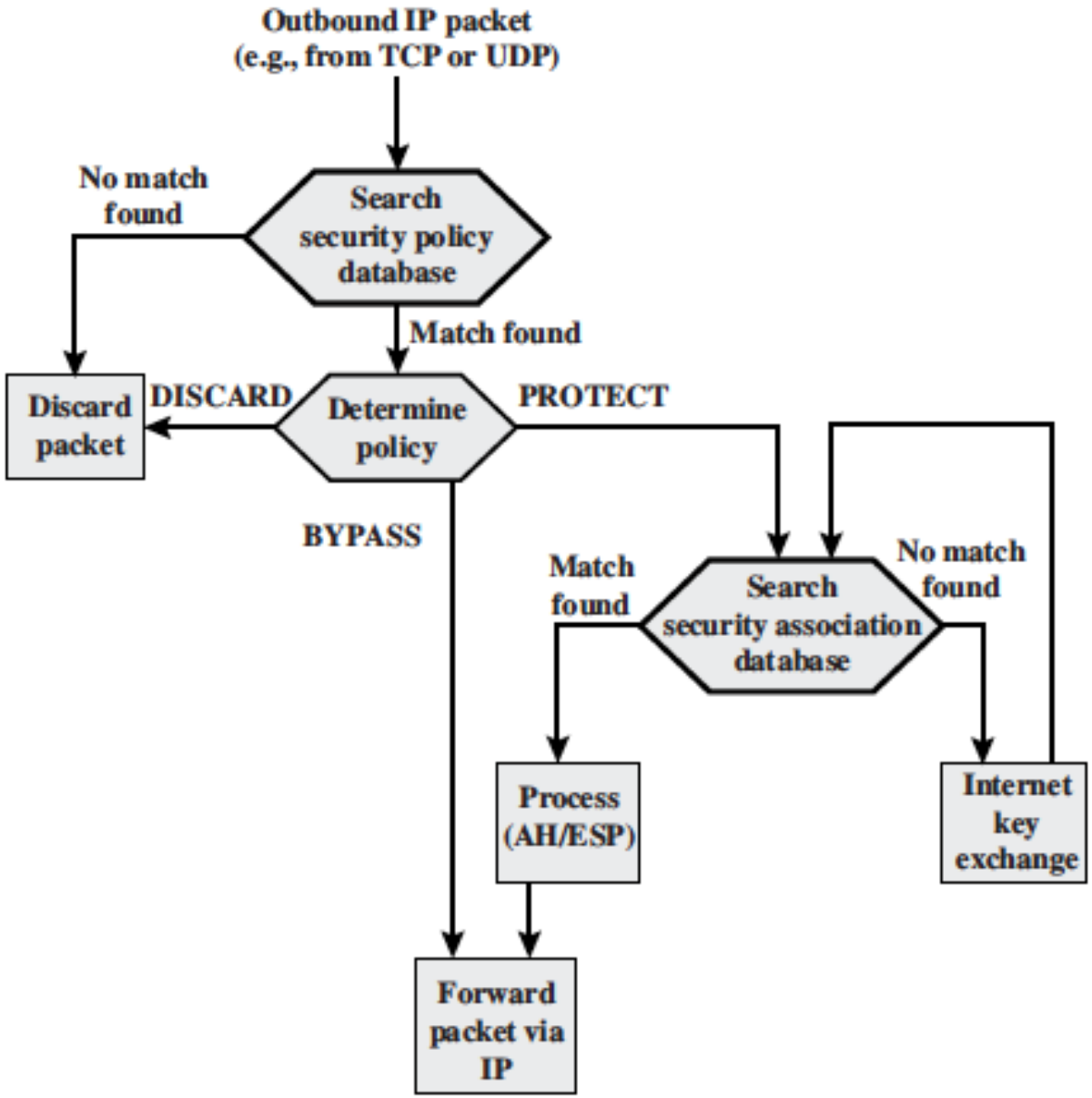
SPD: UN ESEMPIO

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

OUTBOUND PROCESSING

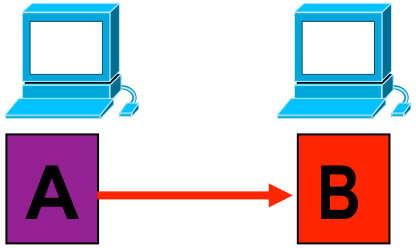
Outbound packet (on A)

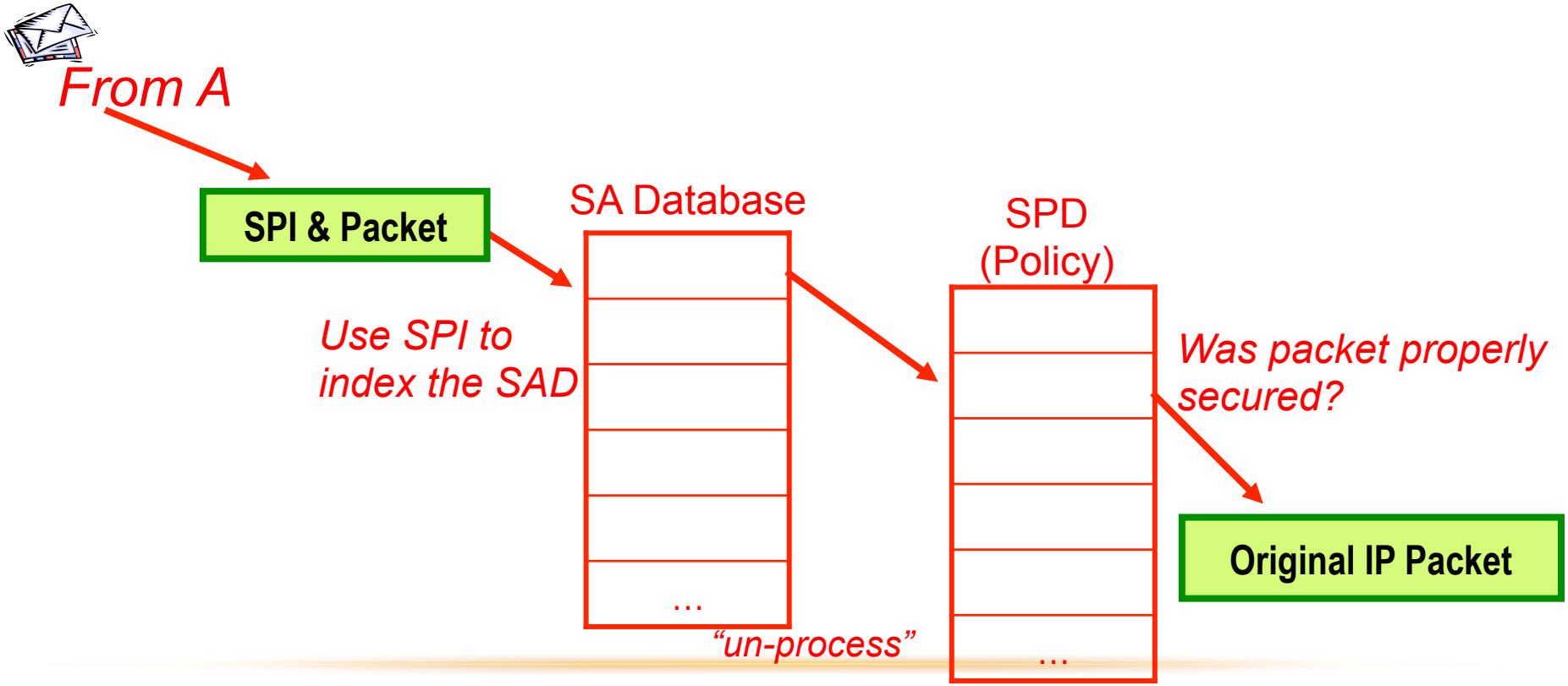


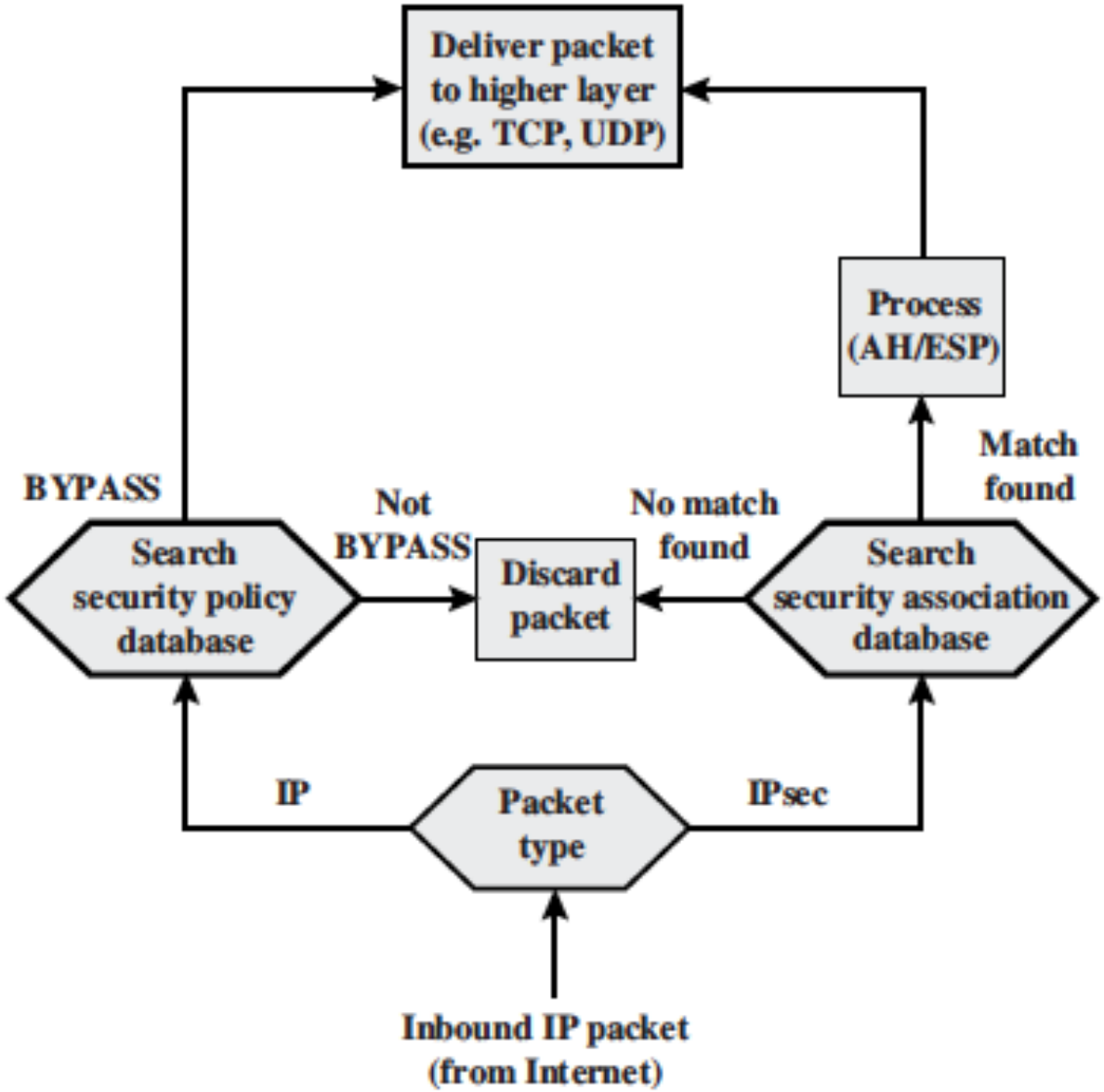

Outbound IP packet
(e.g., from TCP or UDP)
Search security policy database
No match found
Match found
Discard packet
DISCARD
Determine policy
PROTECT
BYPASS
Search security association database
Match found
No match found
Process (AH/ESP)
Internet key exchange
Forward packet via IP

INBOUND PROCESSING

Inbound packet (on B)






Deliver packet to higher layer (e.g. TCP, UDP)
Process (AH/ESP)
Match found
BYPASS
Not BYPASS
No match found
Search security policy database
Discard packet
Search security association database
IP
Packet type
IPsec
Inbound IP packet (from Internet)

MODALITÀ DI FUNZIONAMENTO

- AH ed ESP supportano due modalità operative:
  - Transport
  - Tunnel

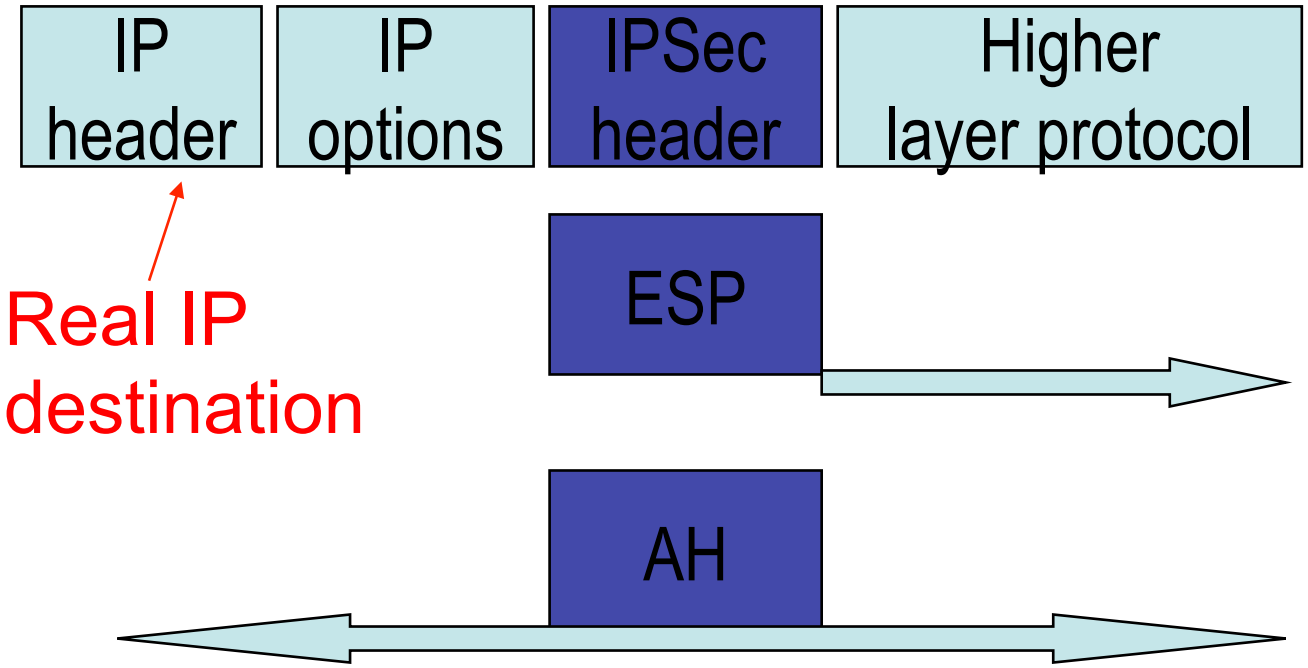
MODALITÀ TRANSPORT

- Protezione di protocolli di livello superiore
- Relativa al payload del pacchetto IP
  - Segmenti TCP
  - Datagrammi UDP
  - Pacchetti ICMP
  - …
- Generalmente utilizzata per le comunicazioni end-to-end fra due host
- Payload IPv4
  - Dati successivi all'intestazione IP
- Payload IPv6
  - Dati successivi all'intestazione IP ed eventuali intestazioni di estensione
    - Eccezione: opzioni di destinazione possono essere incluse nella protezione

MODALITÀ TRANSPORT

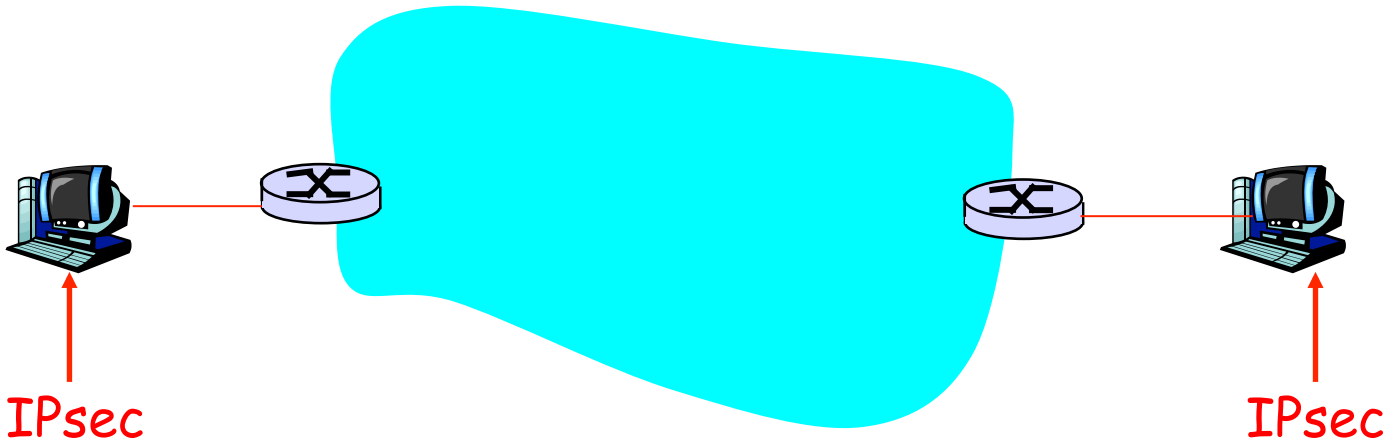
- AH
  - Autentica il payload IP e determinate parti dell'intestazione IP
- ESP
  - Esegue la crittografia
  - Opzionalmente:
    - autentica il payload IP, ma non l'intestazione!

MODALITÀ TRANSPORT



MODALITÀ TRANSPORT

- Datagramma IPSec trasmesso e ricevuto dagli end-system
- Protezione dei protocolli di livello superiore



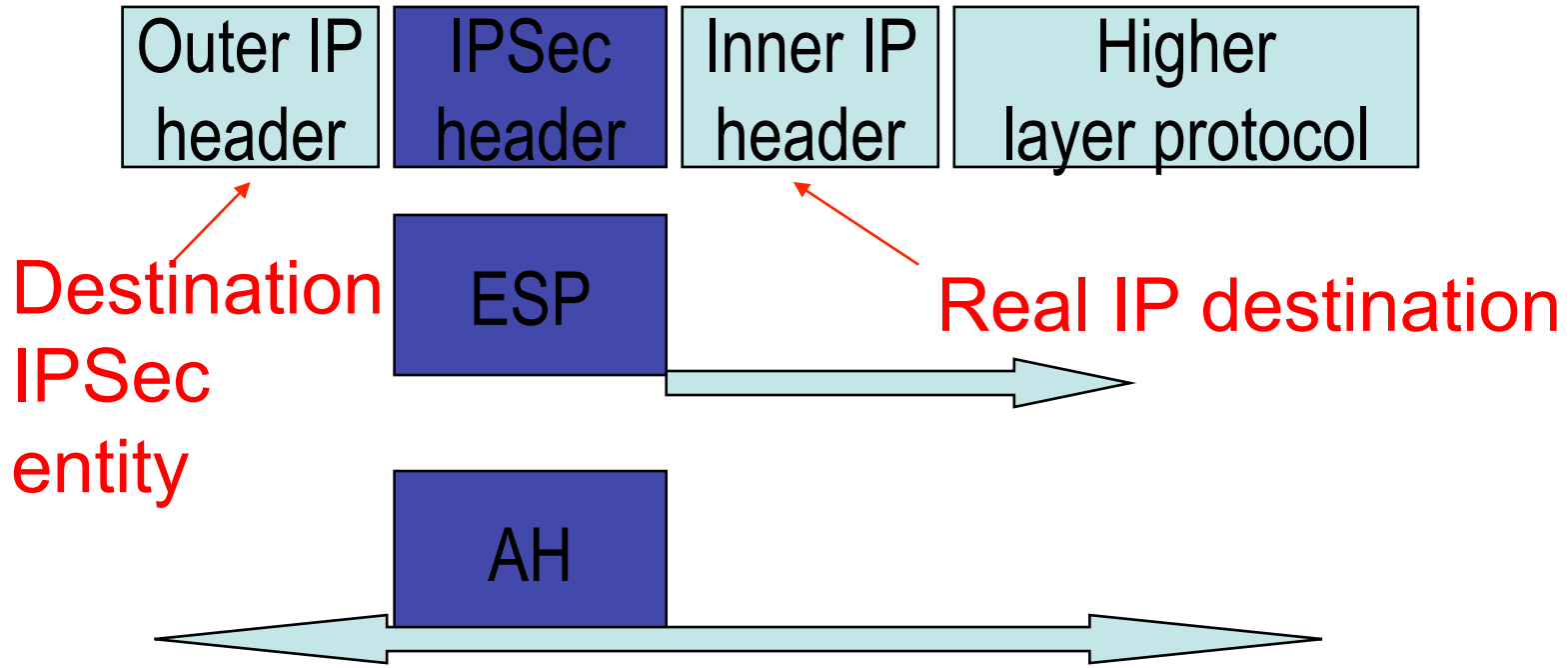
MODALITÀ TUNNEL

- Protezione dell'intero pacchetto IP
- Vengono aggiunti i campi AH o ESP
- L'intero pacchetto così ottenuto viene trattato come il payload di un nuovo pacchetto IP con una nuova intestazione
- Il pacchetto originario viaggia in un tunnel
- Nessun router sarà in grado di esaminare l'intestazione interna
- Indirizzi IP esterni potenzialmente diversi da quelli originari

MODALITÀ TUNNEL

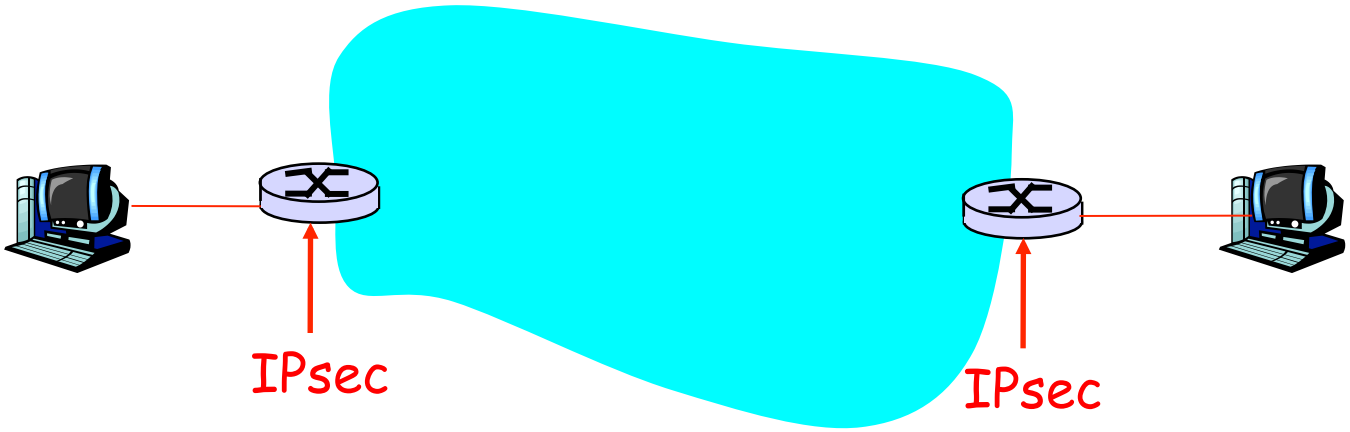
- AH
  - Autenticazione dell'intero pacchetto IP interno ed alcune parti dell'intestazione IP esterna
- ESP
  - Crittografia e (opzionalmente) autenticazione dell'intero pacchetto IP interno, compresa l'intestazione IP interna

MODALITÀ TUNNEL



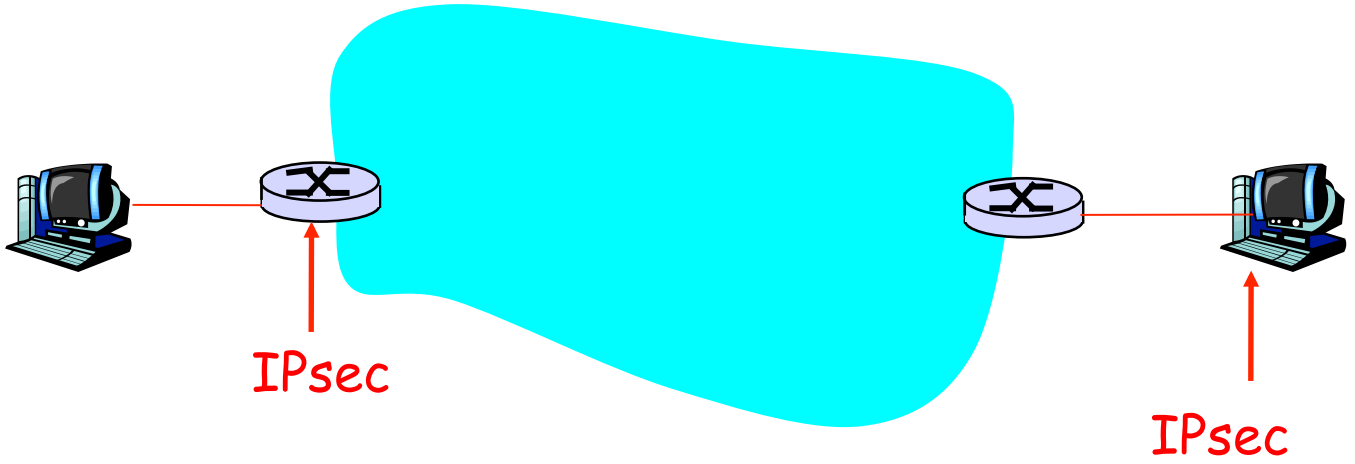
MODALITÀ TUNNEL

- End router sono IPSec-aware
- Host inconsapevoli

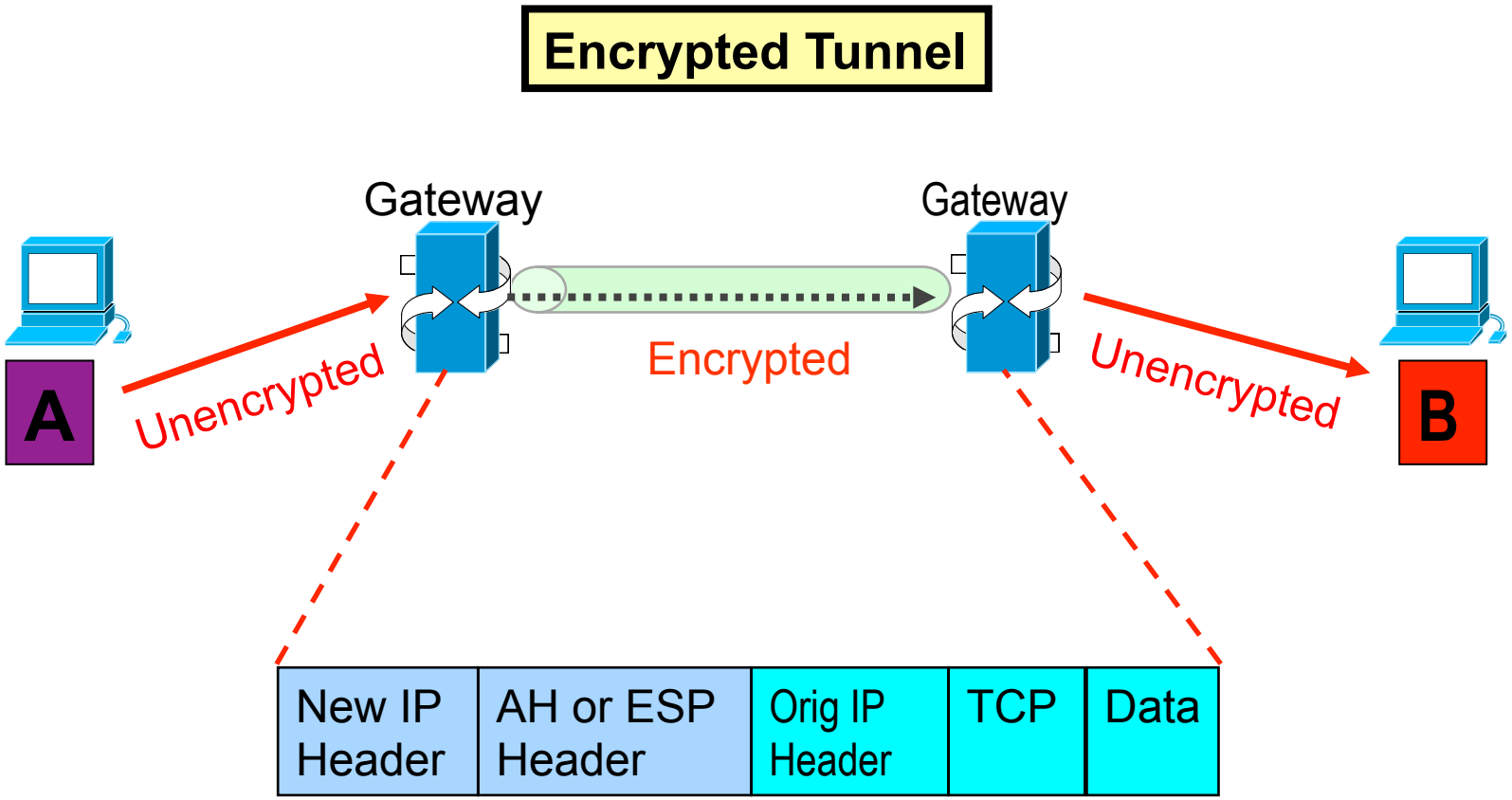


MODALITÀ TUNNEL

- Tunneling verso un host IPSec



MODALITÀ TUNNEL

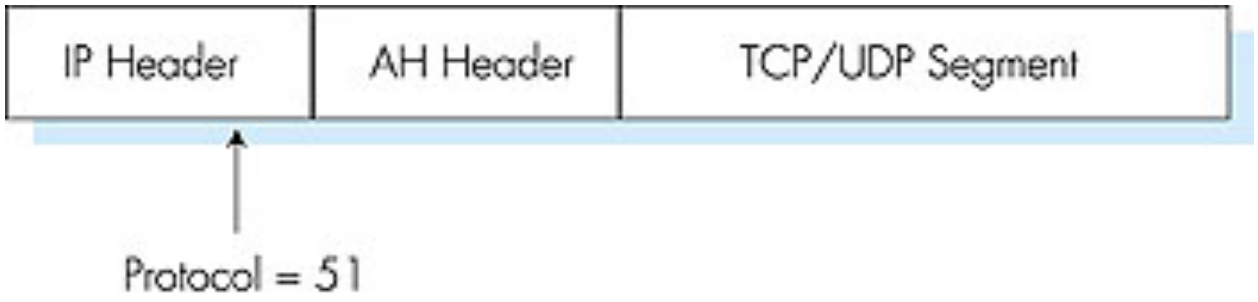


RIASSUMENDO…

	Modalità transport	Modalità tunnel
AH	Autentica il payload IP e determinate parti dell'intestazione IP e delle estensioni in IPv6	Autentica l'intero pacchetto IP interno più determinate parti dell'intestazione IP esterna e delle intestazioni di estensione IPv6 esterne
ESP	Esegue la crittografia del payload IP e di ogni intestazione di estensione IPv6 che segue l'intestazione ESP	Esegue la crittografia del pacchetto IP interno
ESP con autenticazione	Esegue la crittografia del payload IP e di ogni intestazione di estensione IPv6 che segue l'intestazione ESP. Autentica il payload IP ma non l'intestazione IP	Esegue la crittografia del pacchetto IP interno. Autentica il pacchetto IP interno

AUTENTICATION HEADER

STRUTTURA DEL PACCHETTO IP ESTERNO

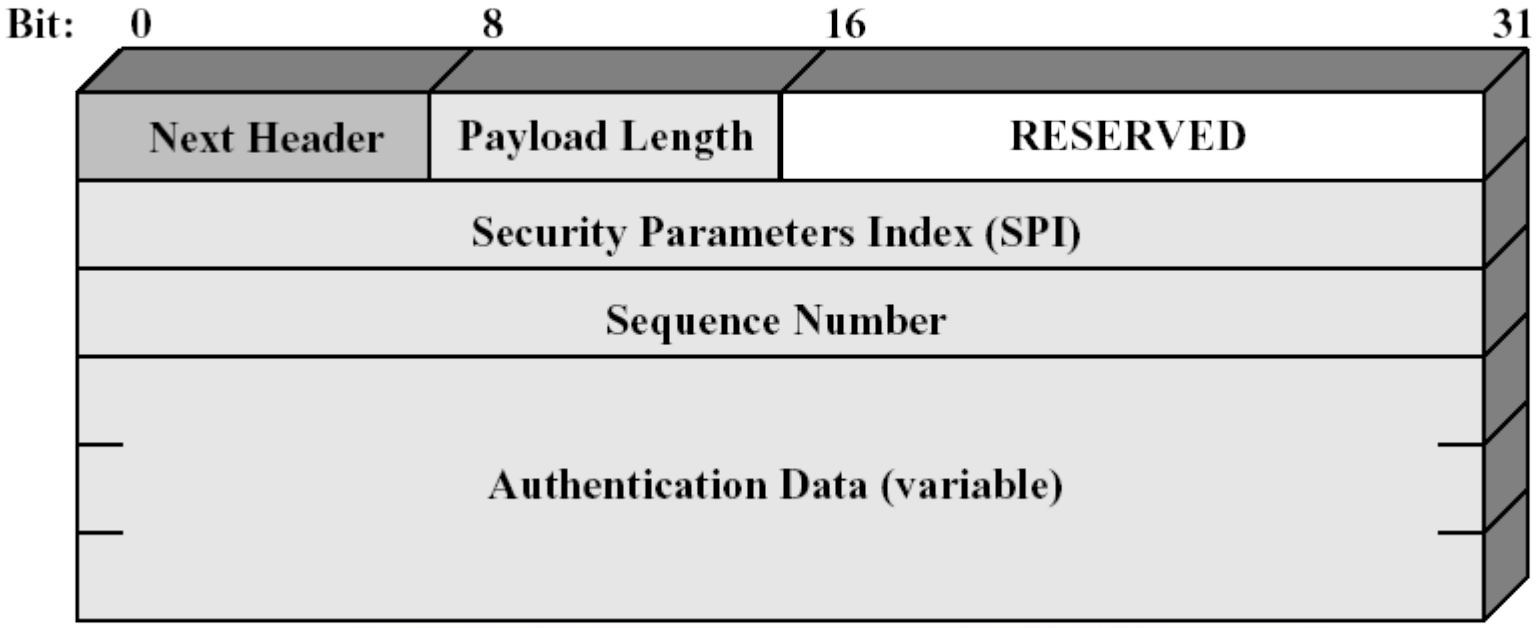


PROPRIETÀ

- Supporto per l'integrità dei dati
  - Impossibile modificare il contenuto del pacchetto in transito senza che tale operazione venga rilevata
- Supporto per l'autenticazione dei pacchetti IP
  - Autenticazione dell'utente o dell'applicazione
  - Filtraggio del traffico non autenticato
  - Prevenzione IP spoofing
- Prevenzione di attacchi replay
- Autenticazione basata su MAC (Message Authentication Code)
  - Le due parti devono condividere una chiave segreta

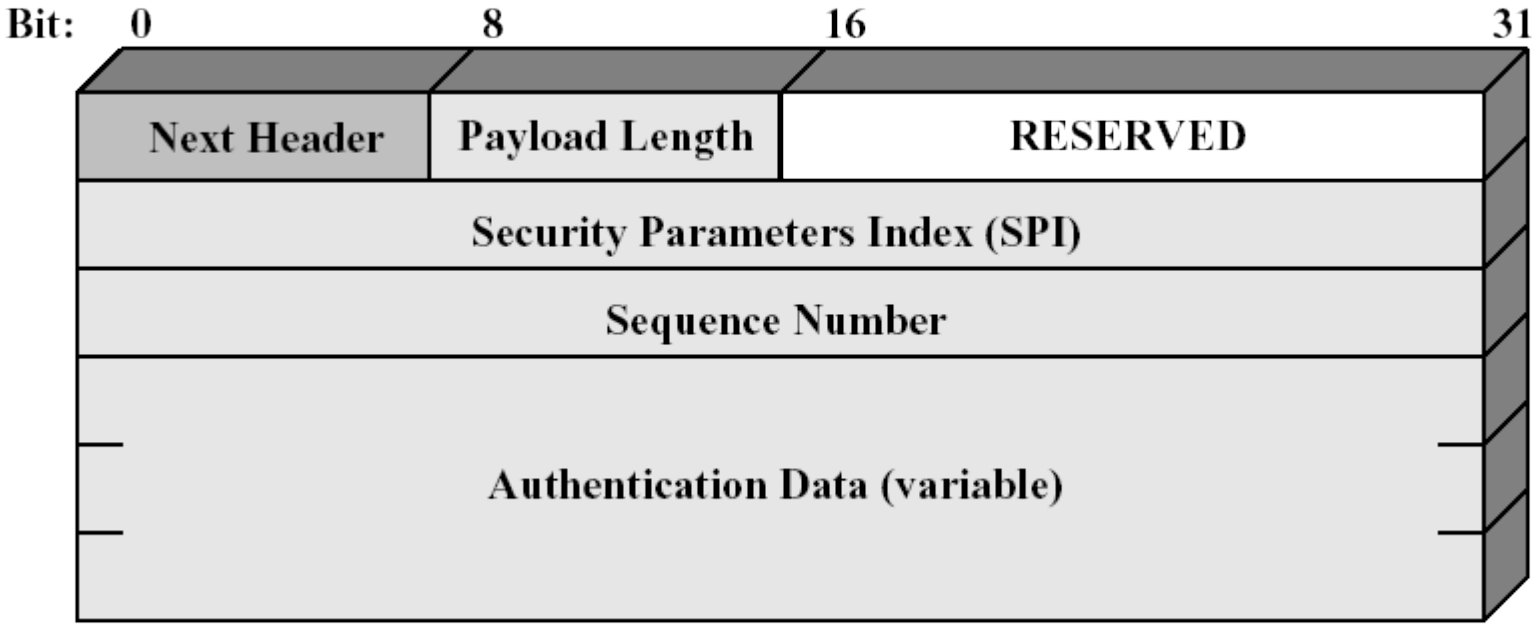
FORMATO DELL'INTESTAZIONE IN AH

- Next header (8 bit)
  - Tipo di intestazione che segue questa intestazione (TCP, UDP, ICMP, …)



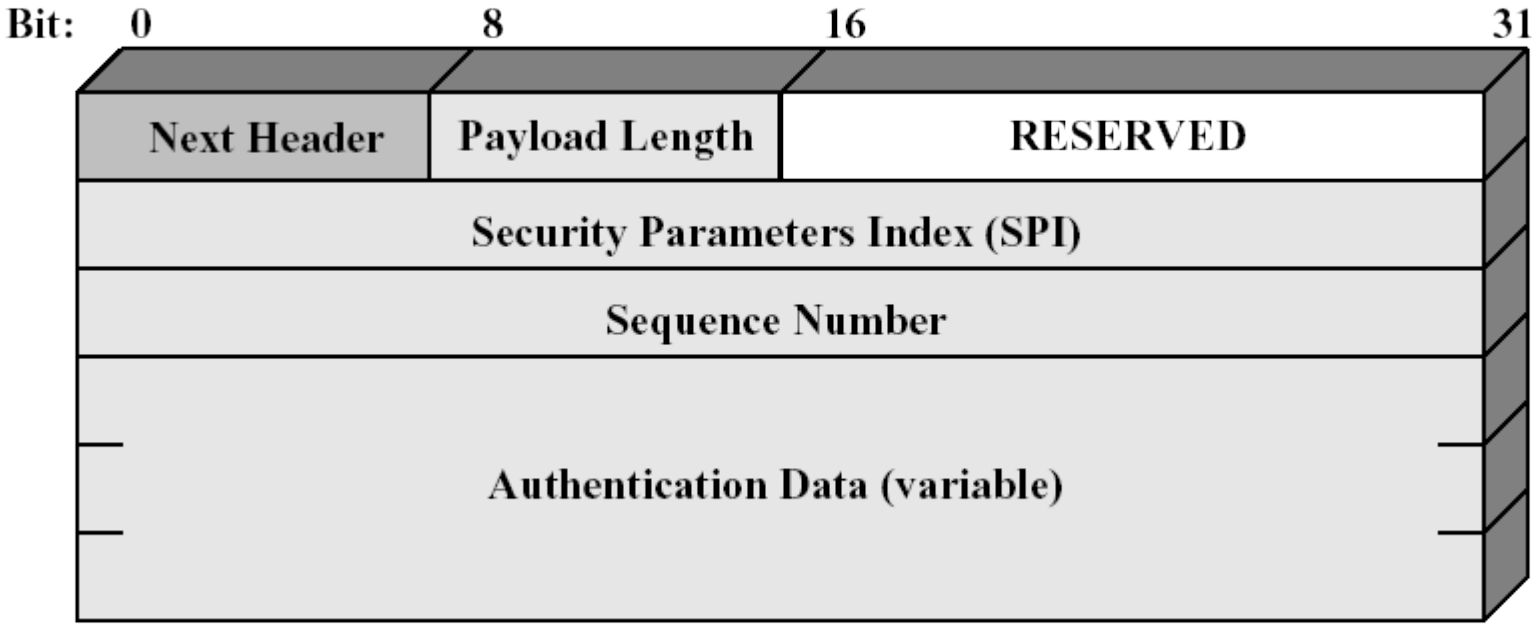
FORMATO DELL'INTESTAZIONE IN AH

- Payload length (8 bit)
  - Lunghezza di Authentication Header in word di 32 bit



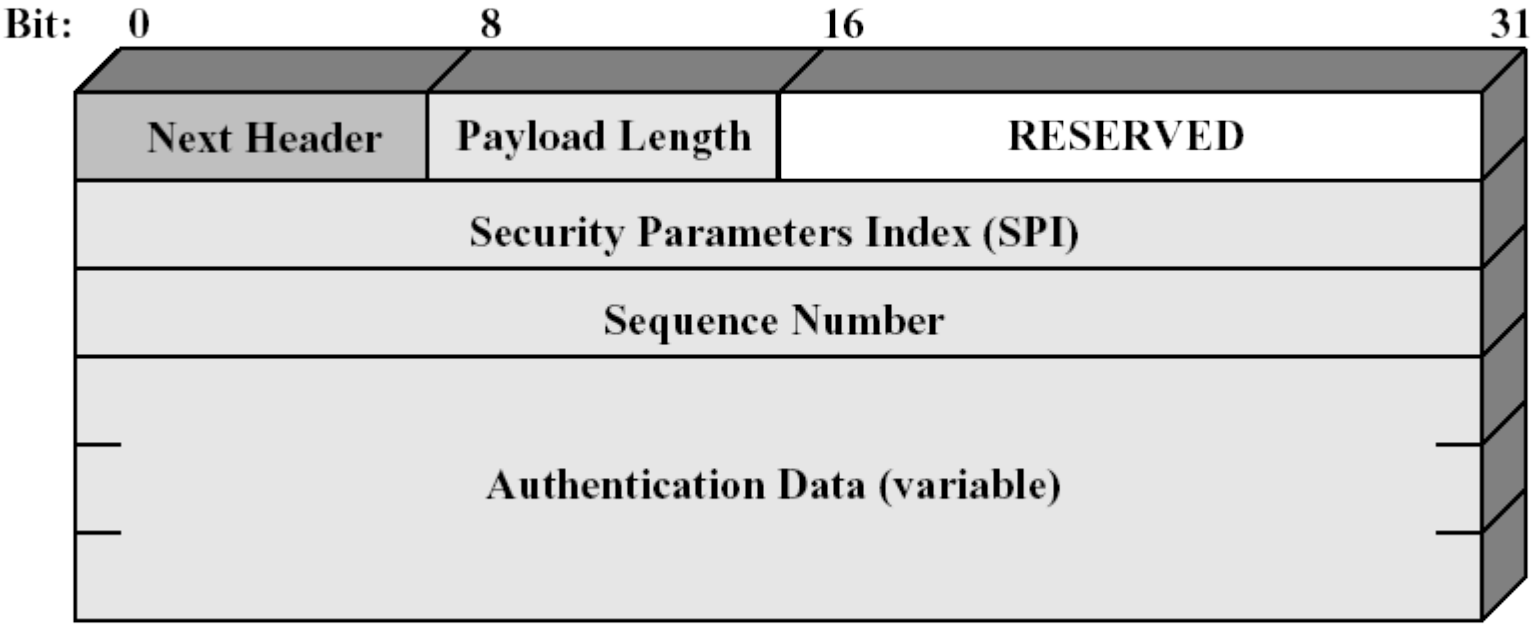
FORMATO DELL'INTESTAZIONE IN AH

- Reserved (16 bit)
  - Riservato per utilizzi futuri



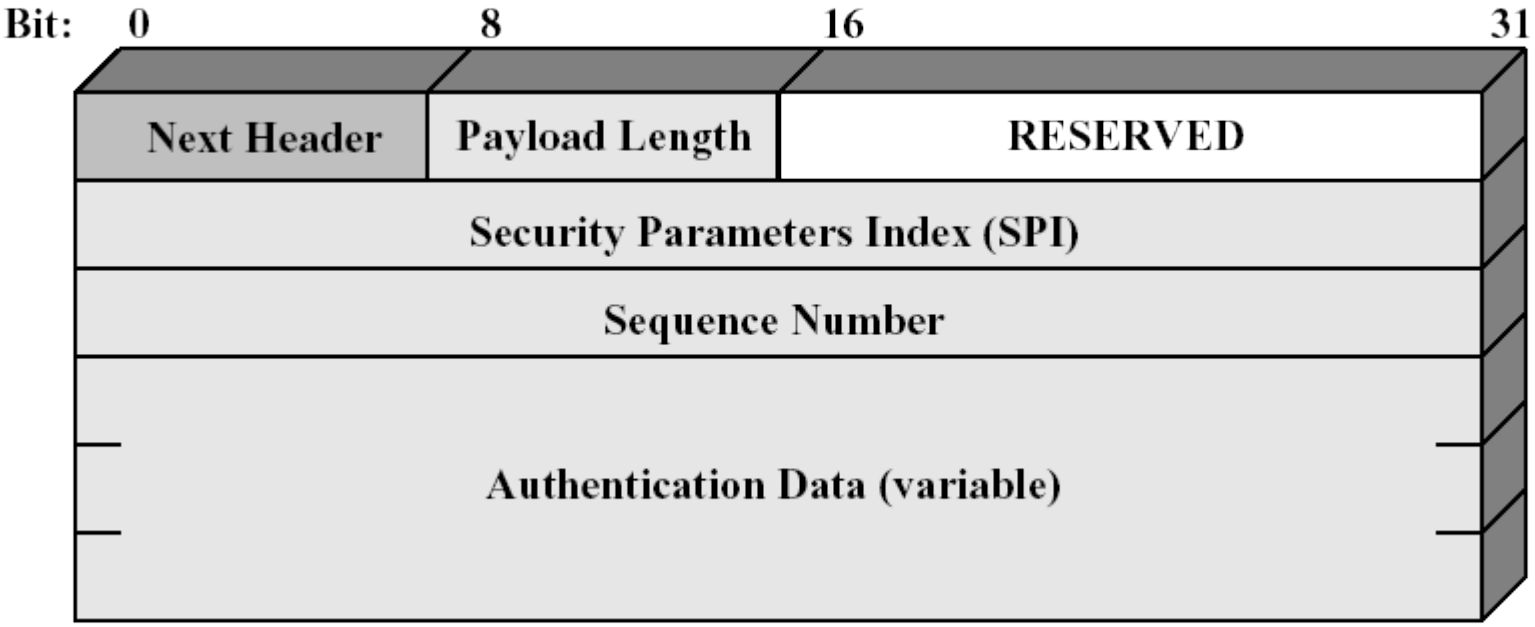
FORMATO DELL'INTESTAZIONE IN AH

- Security Parameters Index (32 bit)
  - Identifica una security association



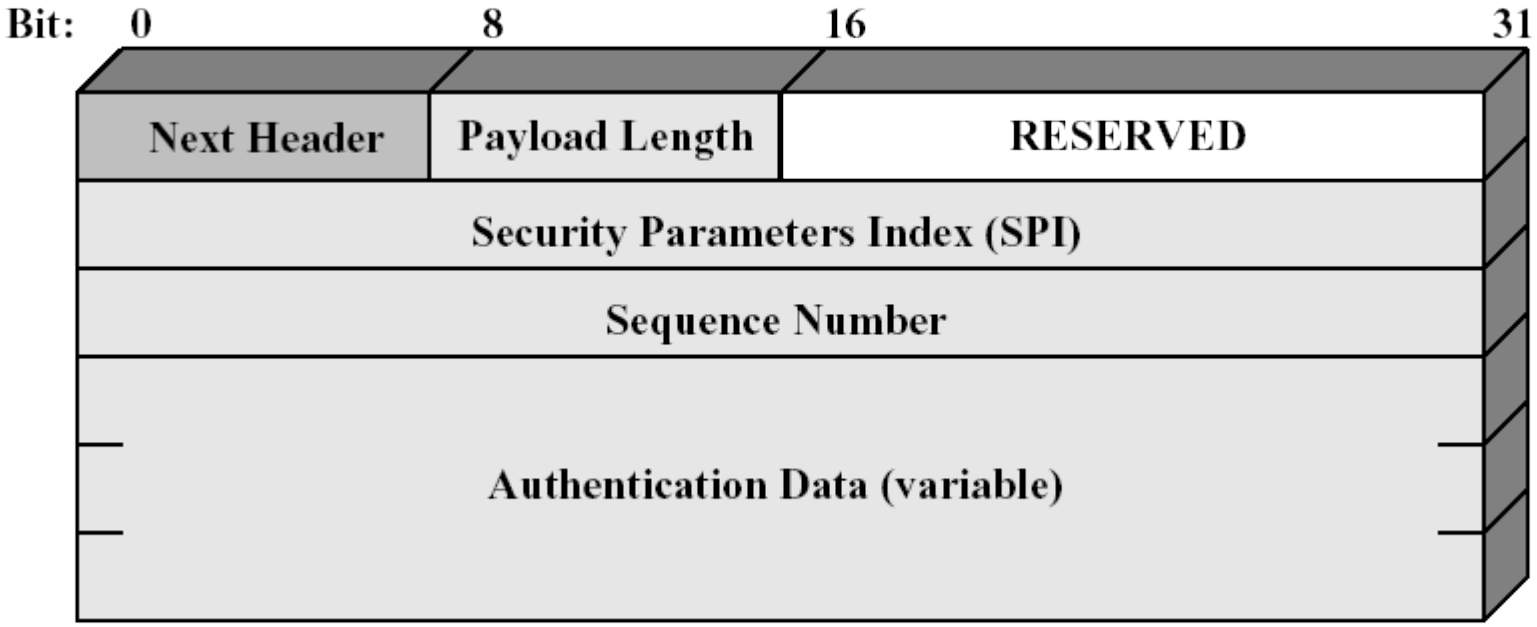
FORMATO DELL'INTESTAZIONE IN AH

- Sequence number (32 bit)
  - Contatore incrementale monotono



FORMATO DELL'INTESTAZIONE IN AH

- Authentication data (variabile)
  - Campo di lunghezza variabile (multiplo di word di 32bit) che contiene il valore ICV (Integrity Check Value) o MAC (Message Authentication Code)



ATTACCO REPLAY

- Un estraneo ottiene copia di un pacchetto autenticato
- Trasmette successivamente tale copia alla destinazione prevista
- Pacchetti autenticati duplicati possono minare il corretto funzionamento della rete
- Il campo “Sequence Number” serve ad evitare questo genere di attacchi

PACCHETTO IN USCITA – LATO MITTENTE

- Alla creazione di una nuova SA il mittente inizializza un contatore a 0
- Ad ogni pacchetto inviato in una SA il mittente incrementa il contatore ed inserisce il valore nel campo Sequence Number
  - Il primo valore è pari ad 1
- La difesa da attacchi replay è attiva di default
  - Il mittente non deve consentire che i numeri di sequenza ricomincino ciclicamente dopo ($2^{32} - 1$) incrementi…
  - …al raggiungimento di questo valore, la SA viene chiusa, e ne viene aperta una nuova

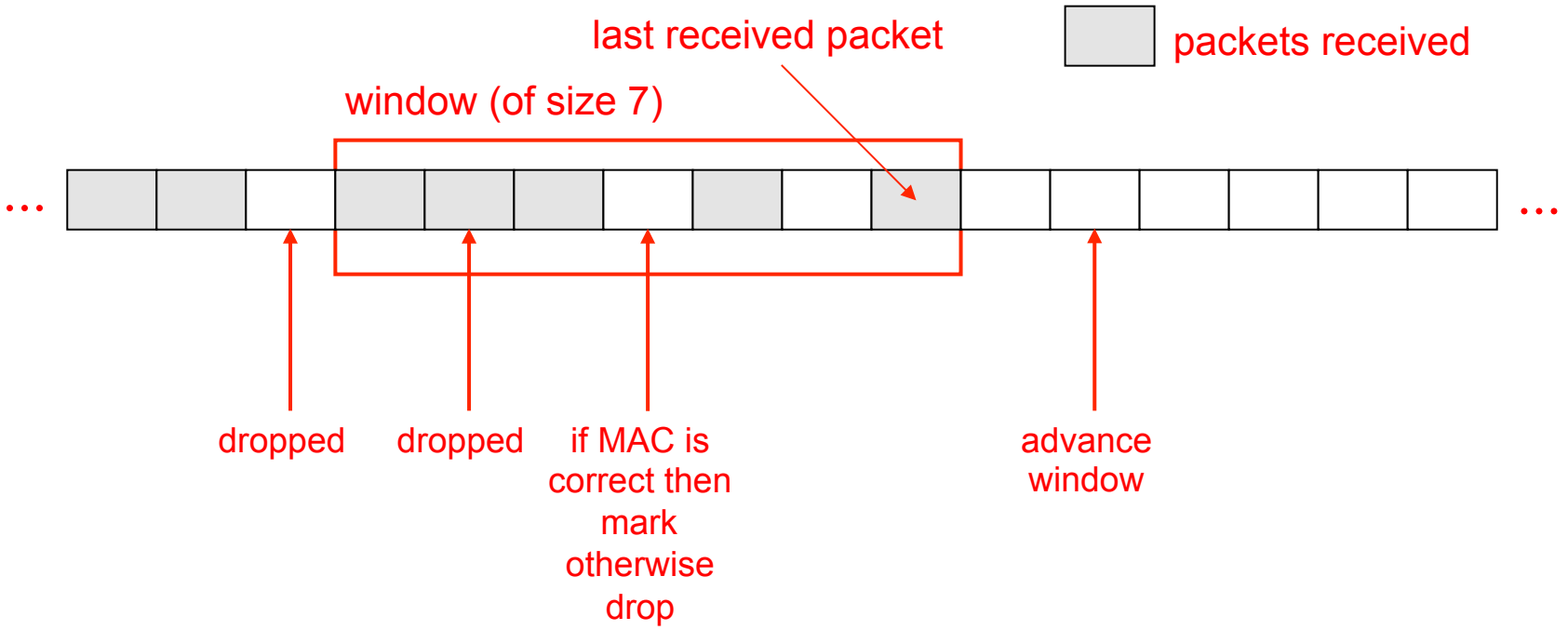
PACCHETTO IN INGRESSO – LATO DESTINATARIO

- IP è connectionless, inaffidabile, best effort
  - La consegna dei pacchetti non è garantita
  - La consegna in ordine dei pacchetti non è garantita
- Il ricevitore implementa una finestra di dimensione W = 64 (tipicamente)
- Pacchetto con numero sequenziale compreso fra “N-W+1” ed “N” ricevuto correttamente
  - Posizione corrispondente nella finestra contrassegnata

ALGORITMO DI RICEZIONE

- Pacchetto nuovo rientra nella finestra
  - Controllo codice MAC
  - Contrassegnata la posizione dei pacchetti correttamente autenticati
- Pacchetto nuovo alla destra della finestra
  - Controllo codice MAC
  - Pacchetto correttamente autenticato
    - Avanzamento finestra
    - Posizione corrispondente contrassegnata
- Pacchetto alla sinistra della finestra o non correttamente autenticato
  - Pacchetto eliminato
  - (opzionalmente) Evento registrato ai fini dell'auditing

FINESTRA DI RICEZIONE ANTI-REPLAY

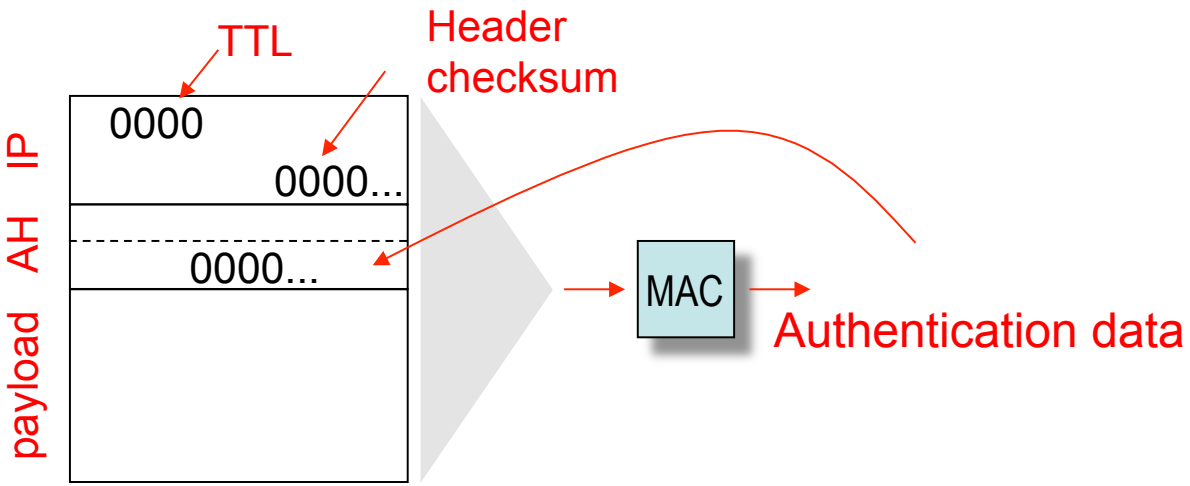


INTEGRITY CHECK VALUE

- Contenuto nel campo Authentication Data
- Codice di autenticazione del messaggio
  - Può essere una versione troncata di un codice prodotto da un algoritmo MAC
- Implementazioni devono supportare
  - HMAC-MD5-96
    - Algoritmo HMAC
    - Codice hash MD5
  - HMAC-SHA1-96
    - Algoritmo HMAC
    - Codice hash SHA1
- Calcolo HMAC completo
- Troncamento a 96 bit

CALCOLO DEL MAC

- Campi utilizzati
  - Campi dell'intestazione IP che non cambiano durante la trasmissione
  - Campi dell'intestazione IP che hanno un valore prevedibile al punto terminale della SA AH
  - Campi variabili o non prevedibili vengono considerati 0
  - Intestazione AH tranne Authentication Data
  - Authentication Data viene considerato 0
  - Tutti i dati dei protocolli di livello superiore



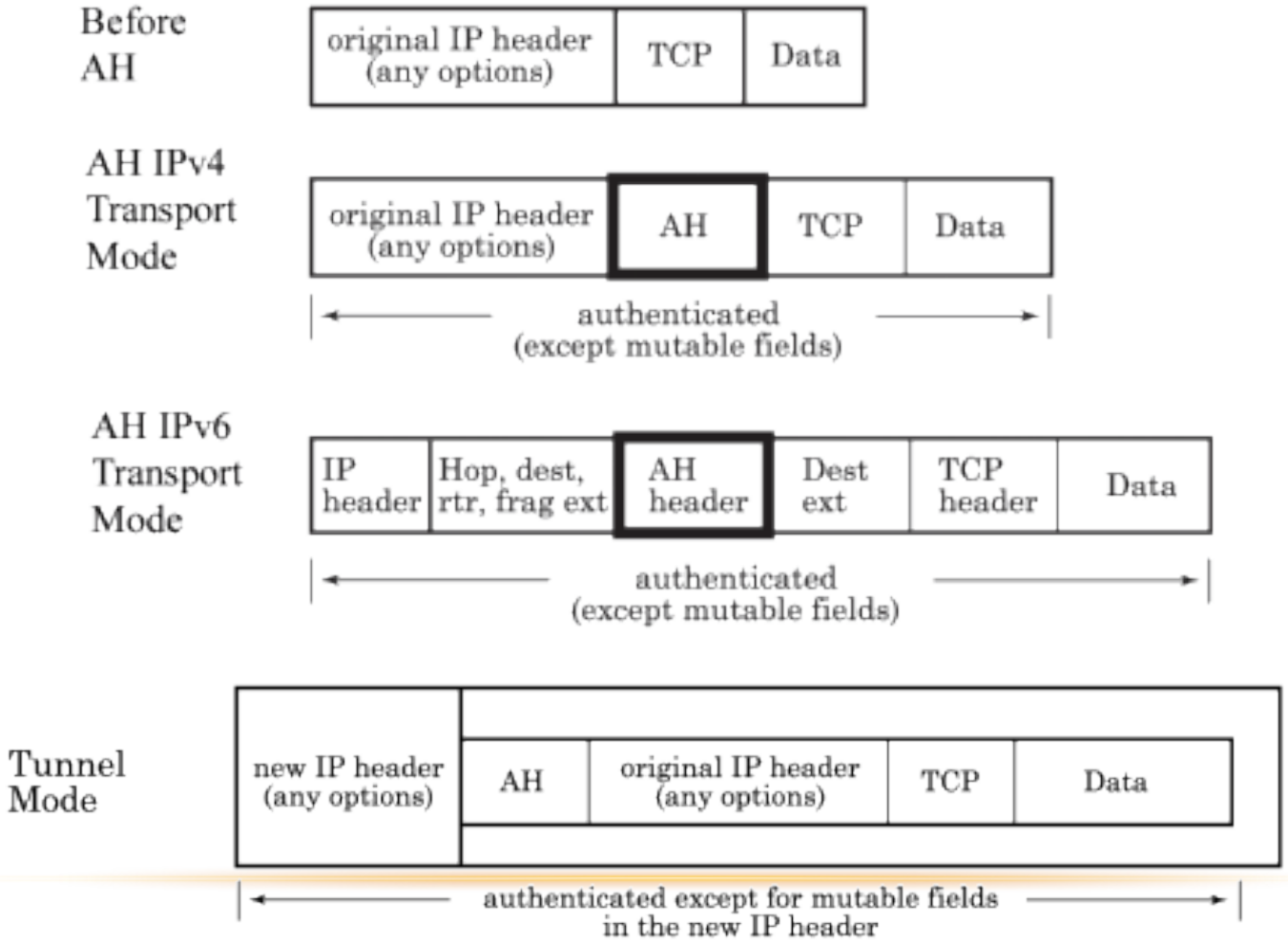
CALCOLO DEL MAC PER IPv4

- Campi immutabili
  - Internet Header Length
  - Source Address
- Campi mutabili ma prevedibili
  - Destination Address
- Campi mutabili (azzerati)
  - Time to Live
  - Header Checksum
- Src IP e Dst IP protetti per evitare spoofing

CALCOLO DEL MAC PER IPv6

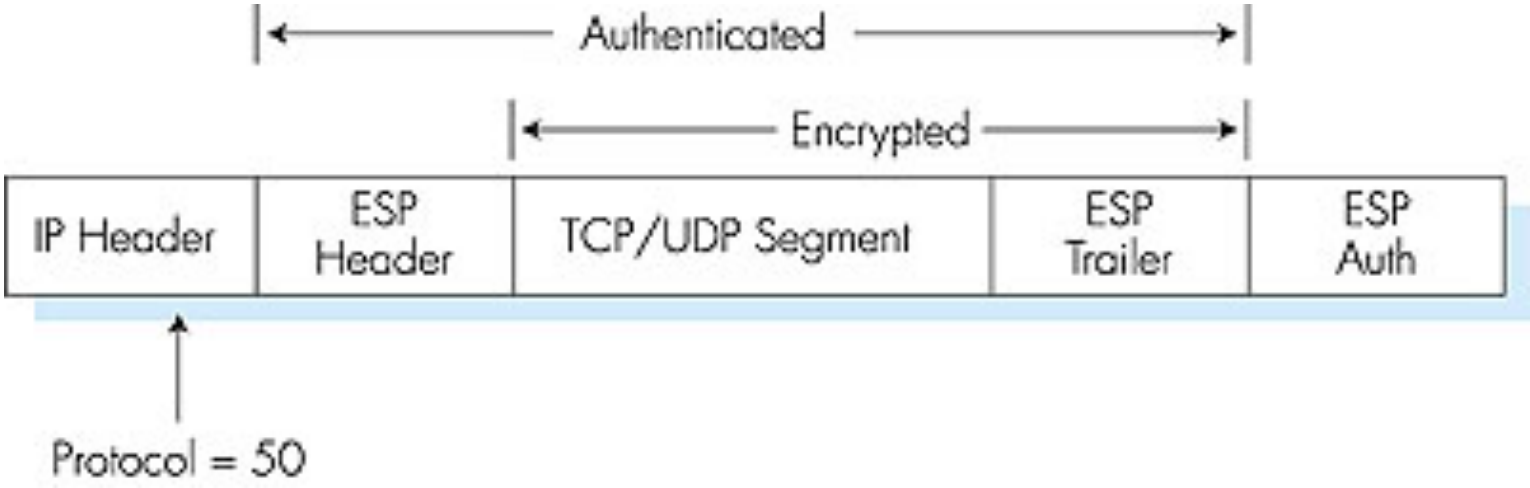
- Campi immutabili
  - Version
- Campi mutabili ma prevedibili
  - Destination Address
- Campi mutabili (azzerati)
  - Flow Label

STRUTTURA DEI DATAGRAMMI IPSec



ENCAPSULATING SECURITY PAYLOAD

STRUTTURA DEL PACCHETTO IP ESTERNO

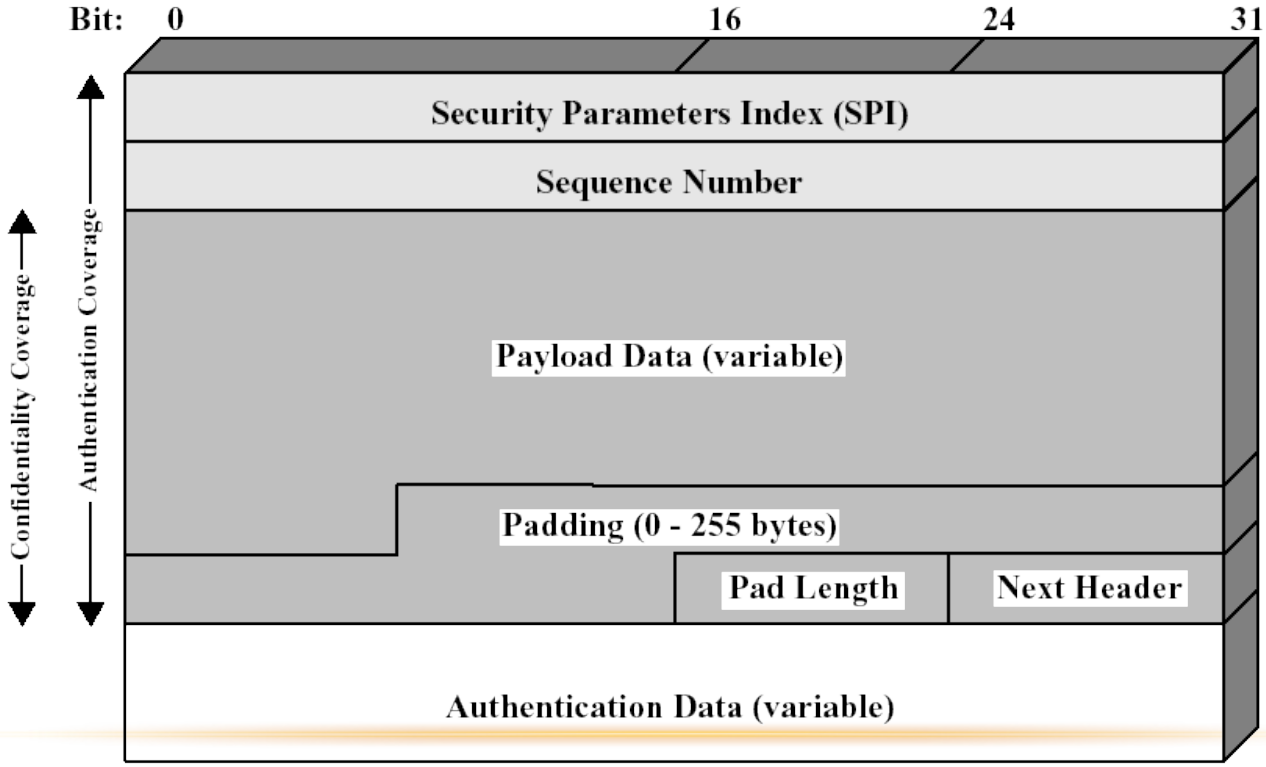


PROPRIETÀ

- Servizi di segretezza del contenuto del messaggio
- Servizi di segretezza parziale del flusso di traffico
- Servizio opzionale di autenticazione

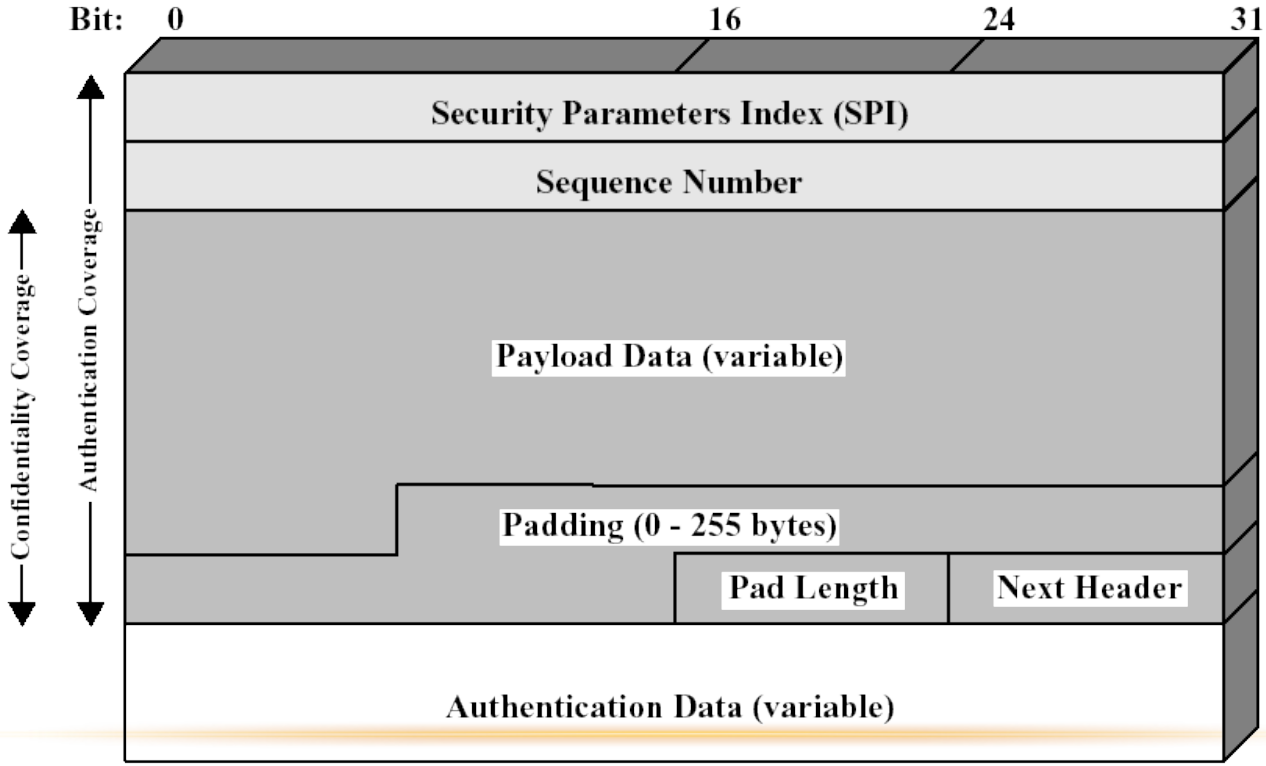
FORMATO DELL'INTESTAZIONE IN ESP

- Security Parameters Index (SPI) – 32 bit
  - identifica una SA



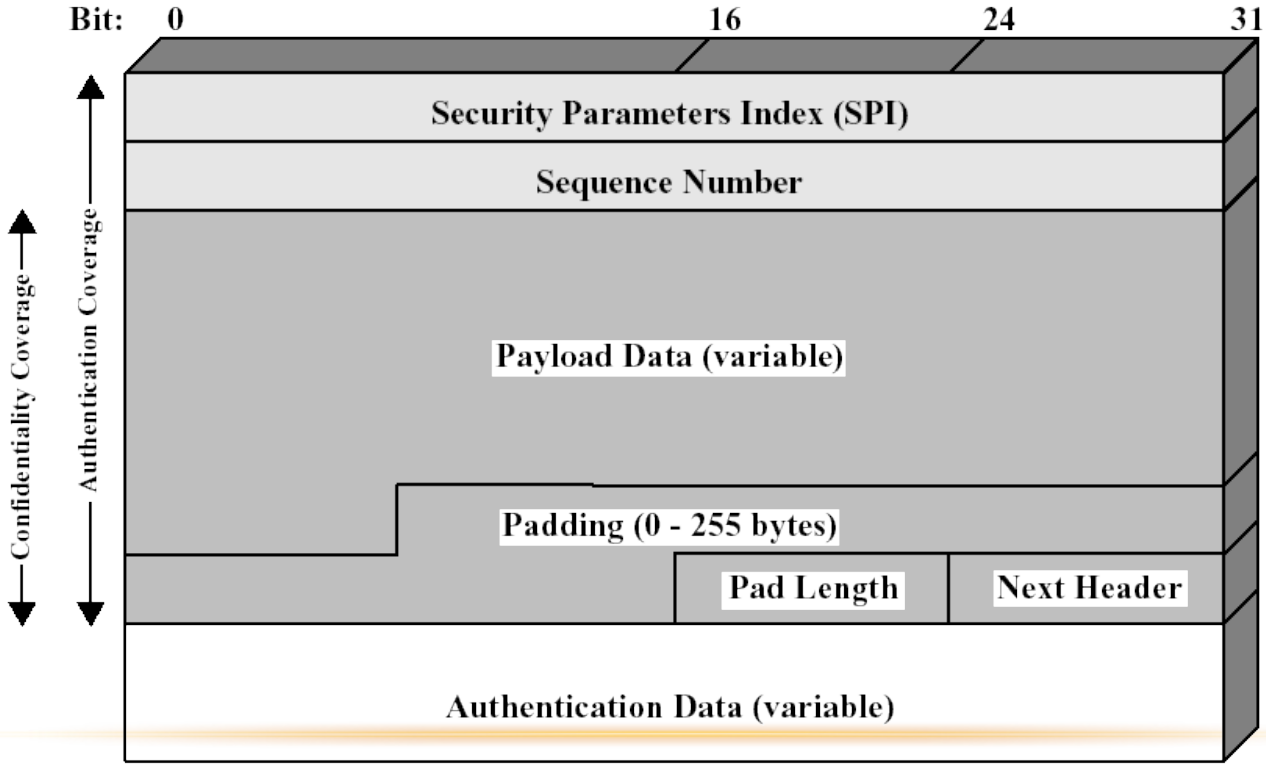
FORMATO DELL'INTESTAZIONE IN ESP

- Sequence number (32 bit)
  - Contatore incrementale monotono per la funzione anti-replay



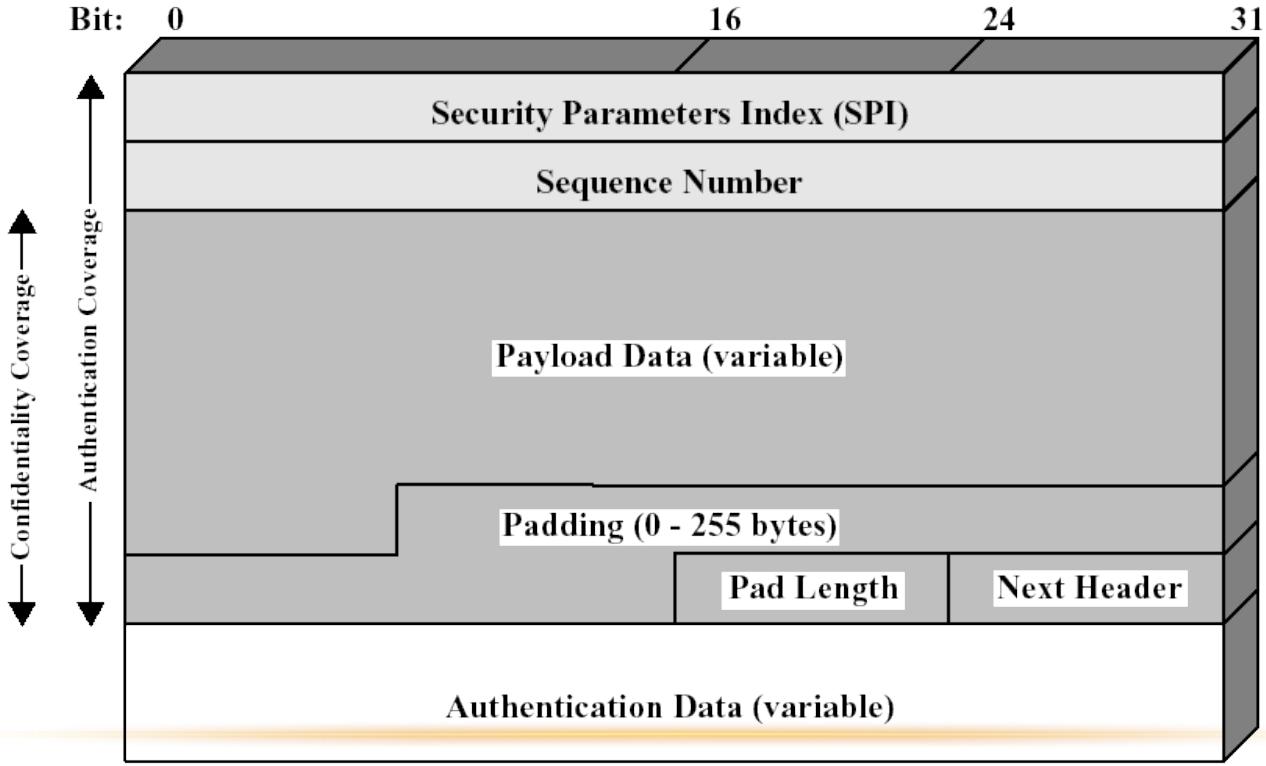
FORMATO DELL'INTESTAZIONE IN ESP

- Payload data (variabile)
  - Segmento di dati (transport) o pacchetto IP (tunnel) protetto



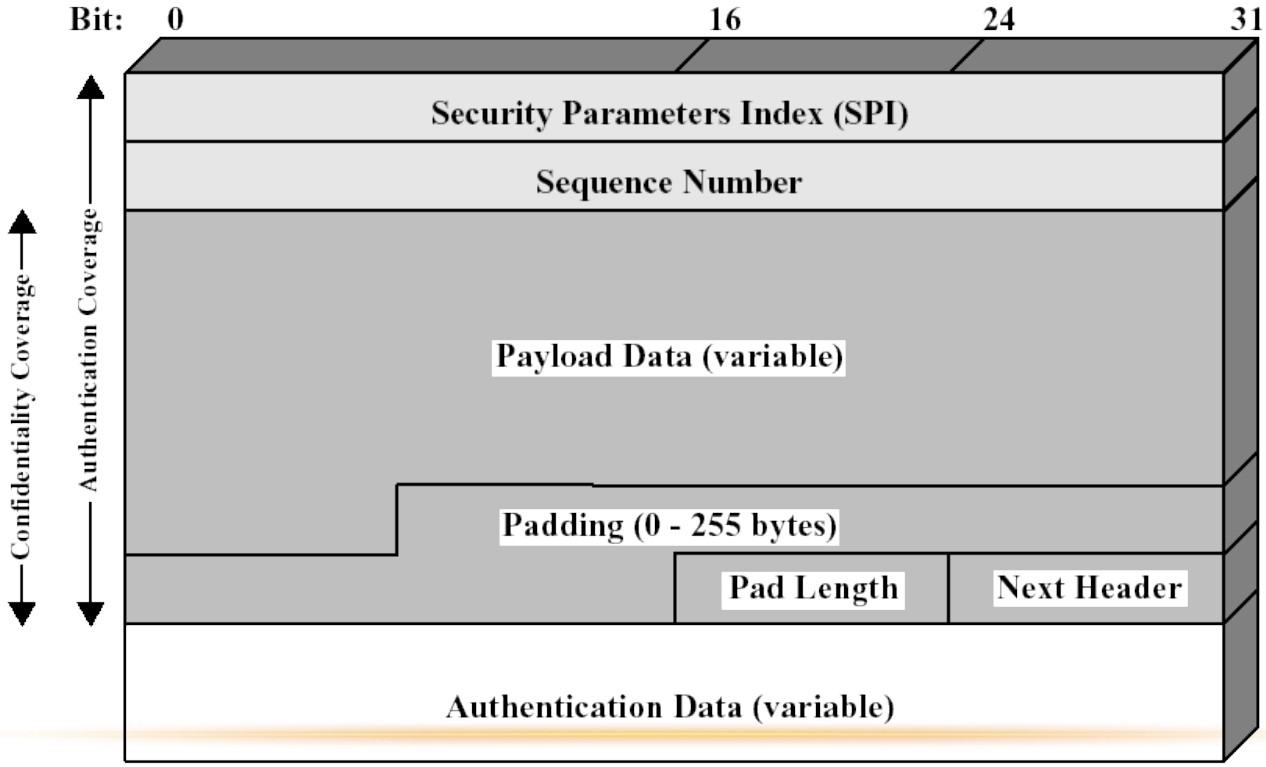
FORMATO DELL'INTESTAZIONE IN ESP

- Padding (0-255 byte)



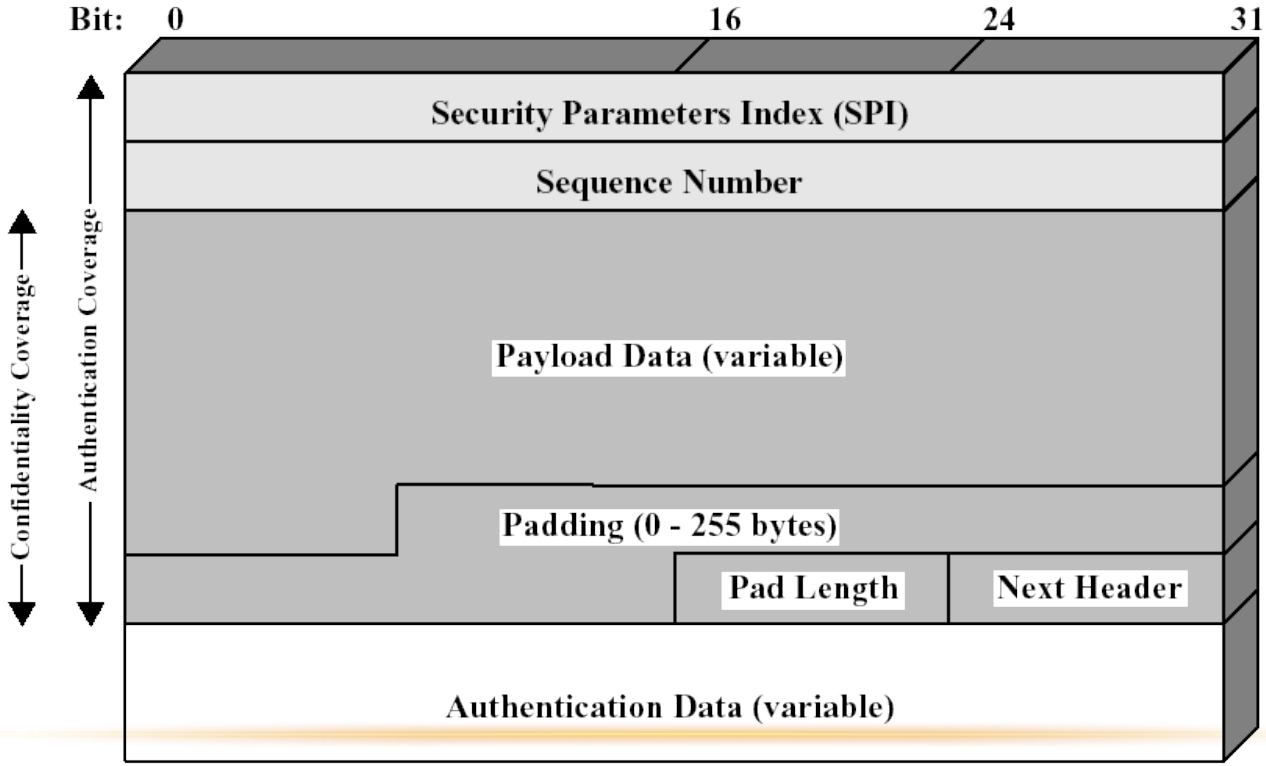
FORMATO DELL'INTESTAZIONE IN ESP

- Pad length (8 bit)
  - Numero di byte di riempimento nel campo precedente



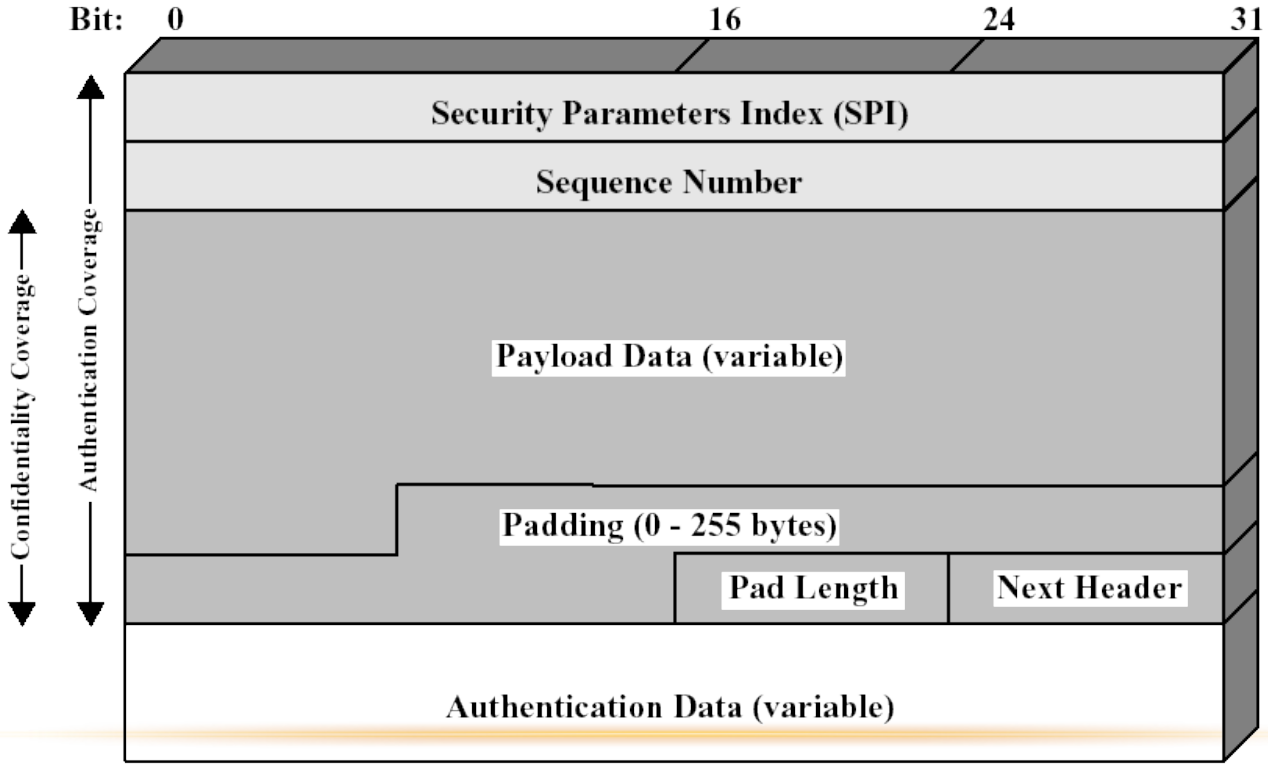
FORMATO DELL'INTESTAZIONE IN ESP

- Next header (8 bit)
  - Tipo di dati contenuti in payload data, identificato puntando alla prima intestazione



FORMATO DELL'INTESTAZIONE IN ESP

- Authentication data (variabile)
  - Costituito da un numero intero di word di 32 bit. Contiene il valore Integrity Check Value calcollato su ESP, escluso il campo AD stesso



CRITTOGRAFIA E AUTENTICAZIONE

- Payload data, padding, pad length e next header sono crittografati dal servizio ESP
- Se sono richiesti dati di sincronizzazione crittografica, devono essere presenti all'inizio del campo Payload Data
- Se esiste, il vettore di inizializzazione non viene crittografato
  - Viene comunque implicitamente considerato parte del testo cifrato

ALGORITMI DI CRITTOGRAFIA

- Algoritmi utilizzabili definiti nel documento DOI (Domain Of Interpretation)
  - Triple DES a tre chiavi
  - RC5
  - IDEA
  - Triple IDEA a tre chiavi
  - CAST
  - Blowfish

ALGORITMI DI AUTENTICAZIONE

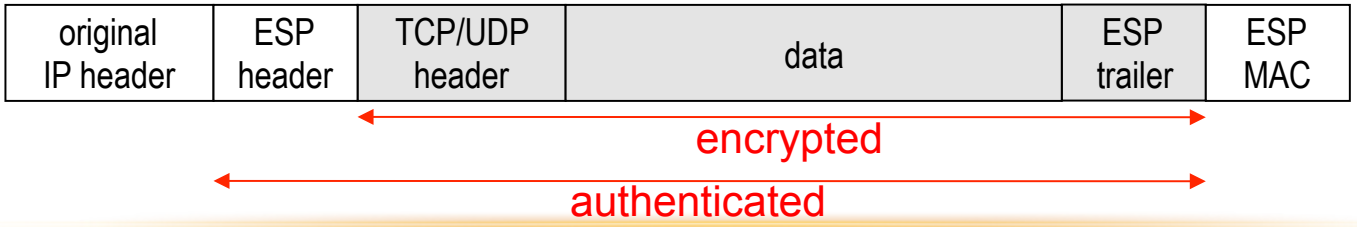
- Supporto per codice MAC con lunghezza standard di 96 bit
- Requisiti per un'implementazione compatibile
  - HMAC-MD5-96
  - HMAC-SHA-1-96
- Il MAC è calcolato su
  - Security Parameters Index
  - Sequence Number
  - Payload Data
  - Padding
  - Pad Length
  - Next Header
- Diversamente da AH, il MAC non copre l'header IP precedente

PADDING

- Dimensione del testo in chiaro multiplo di un determinato numero di byte
  - Consente di espandere il testo in chiaro (Payload Data, Padding, Pad Length, Next Header) fino alla lunghezza desiderata
- ESP richiede che Pad Length e Next Header siano allineati a destra all'interno di una word di 32 bit
  - Il testo cifrato deve essere un multiplo intero di 32 bit
- Ulteriore riempimento per garantire la segretezza parziale del flusso del traffico
  - Nasconde l'effettiva lunghezza del payload

ESP IN MODALITÀ TRANSPORT

- Crittografia dei dati trasportati da IP
- Autenticazione opzionale dei dati trasportati da IP
- IPv4
  - Inserimento intestazione ESP immediatamente prima dell'intestazione di livello trasporto
  - Coda ESP (Padding, Pad Length e Next Header)
  - Se è richiesta autenticazione dopo la coda ESP viene aggiunto il campo ESP Authentication Data
  - Vengono crittografati l'intero segmento di livello trasporto più la coda ESP
  - L'autenticazione copre tutto il testo cifrato più l'intestazione ESP



ESP IN MODALITÀ TRANSPORT

- IPv6
  - ESP considerato come un payload end-to-end
  - Nessuna elaborazione effettuata dai router intermedi
- Intestazione ESP posta dopo:
  - l'intestazione IPv6
  - gli extension header relativi al funzionamento hop-by-hop, al routing ed alla frammentazione
    - NB: l'extension header delle opzioni di destinazione può trovarsi sia prima che dopo l'intestazione ESP, a seconda della semantica
- L'intero segmento di livello trasporto, più la coda ESP sono coperti dalla crittografia
  - Anche l'header delle opzioni di destinazione, nel caso si trovi dopo l'intestazione ESP

PACCHETTO IN USCITA – LATO MITTENTE

- Coda ESP e segmento di livello trasporto crittografati alla sorgente
  - Testo in chiaro sostituito dal testo cifrato per formare il pacchetto IP
  - Autenticazione aggiunta opzionalmente
- Il pacchetto viene instradato verso la destinazione
  - Ogni router esamina l'intestazione IP ed eventuali estensioni IP in chiaro
  - I router non hanno necessità di esaminare il testo in chiaro

PACCHETTO IN INGRESSO – DESTINATARIO

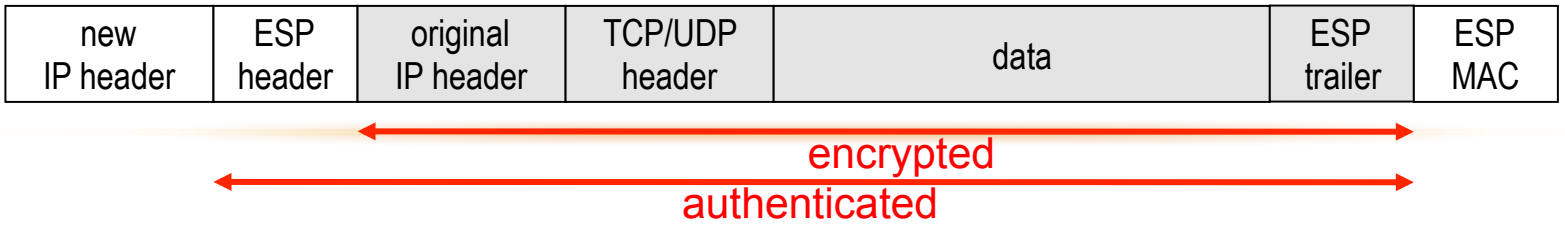
- Elaborazione intestazione IP
  - Elaborazione eventuali estensioni in chiaro
  - In base al campo SPI (Security Parameters Index):
    - viene decrittografata la parte rimanente del pacchetto
    - si recupera il segmento di livello trasporto

UTILIZZO DI ESP IN MODALITÀ TRANSPORT

- Funzionalità di segretezza fornite a qualsiasi applicazione
  - Le applicazioni non devono implementare meccanismi di sicurezza singolarmente
- La lunghezza del pacchetto IP aumenta di poco
- Resta comunque possibile analizzare il traffico costituito dai pacchetti trasmessi
  - Supporto solo parziale al mascheramento delle proprietà del flusso

ESP IN MODALITÀ TUNNEL

- Utilizzato per crittografare un intero pacchetto IP
- L'intestazione ESP precede il pacchetto
- Vengono crittografati pacchetto e coda ESP
  - Possibile elusione dell'analisi del traffico
- L'intestazione IP contiene informazioni relative agli indirizzi IP di mittente e destinatario e talvolta direttive di source routing ed opzioni hop-by-hop
  - Necessario incapsulare l'intero blocco con una nuova intestazione IP
- Utile in presenza di firewall o security gateway
- Host interni non devono utilizzare IPSec
- Numero di chiavi ridotte
- Impedisce l'analisi del traffico basata sull'osservazione della destinazione



PACCHETTO IN USCITA – LATO MITTENTE

- SCENARIO:
  - Host esterno tenta di comunicare con un host protetto da firewall
  - ESP implementato nell'host esterno e nel firewall

1. Preparazione pacchetto IP (interno) con indirizzo destinazione dell'host dietro firewall
2. Aggiunta dell'intestazione ESP
3. Crittografia del pacchetto e della coda ESP
   - Con eventuali dati "Authentication Data"
4. Incapsulamento del blocco prodotto con nuova intestazione IP
   - IP destinazione = IP del firewall
5. Pacchetto esterno instradato verso firewall di destinazione
   - I router elaborano solo l'intestazione IP esterna più eventuali extension header

PACCHETTO IN INGRESSO –DESTINATARIO

- Il firewall di destinazione esamina ed elabora l'header IP
  - Elaborazione delle eventuali intestazioni opzionali
- Sulla base del campo SPI contenuto nell'intestazione ESP esegue la decrittografia della parte rimanente del pacchetto
- Il pacchetto decrittografato viene trasmesso nella rete interna
- Il pacchetto viene inoltrato da zero o più router nella rete interna, fino alla sua destinazione finale

COMBINAZIONE DI SECURITY ASSOCIATIONS

MOTIVAZIONE

- Una singola SA può utilizzare il protocollo AH o ESP, ma non entrambi
- Determinati flussi di traffico richiedono servizi forniti da entrambi i protocolli
- Determinati flussi possono richiedere particolari servizi end-to-end fra gli host e servizi differenti fra i gateway di sicurezza o i firewall

- È necessario impiegare diverse SA per lo stesso flusso di traffico

SOLUZIONE

- Viene creato un gruppo di associazioni di sicurezza rispetto alle quali il traffico deve essere elaborato per fornire il particolare insieme di servizi IPSec desiderato
- Le SA per tale gruppo possono terminare negli stessi punti o in punti differenti
- Due strategie di combinazione
  - Adiacenza di trasporto
  - Tunnel iterato
- I due approcci possono essere combinati fra loro

TRASPORTO vs TUNNEL

- Adiacenza di trasporto
  - Allo stesso pacchetto IP si applicano più protocolli di sicurezza senza usare la modalità tunnel
  - Offre un solo livello di combinazione
  - Ulteriori nidificazioni non offrono vantaggi, poiché l'elaborazione viene svolta su una sola istanza di IPSec, a destinazione
- Tunnel iterato
  - Applicazione di diversi livelli di protocolli di sicurezza tramite tunnel IP
  - Consentiti più livelli di nidificazione
  - Possibili origini e terminazioni differenti per i tunnel

AUTENTICAZIONE E SEGRETEZZA

- ESP con opzione di autenticazione
- ESP applicato ai dati da proteggere
- Campo dei dati di autenticazione aggiunto in coda
- Modalità transport
  - Autenticazione e crittografia applicate al payload
  - Intestazione IP non protetta
- Modalità tunnel
  - Autenticazione applicata all'intero pacchetto IP consegnato alla destinazione esterna dove viene effettuata l'autenticazione
  - L'intero pacchetto IP interno è protetto
- L'autenticazione si applica al testo cifrato, e non al testo in chiaro

ADIACENZA DI TRASPORTO

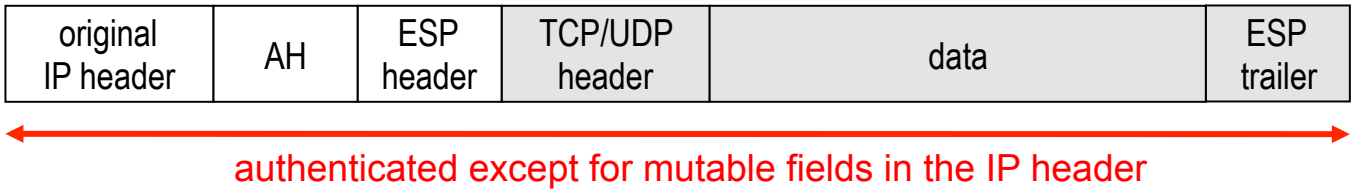
- Utilizzo di due associazioni di sicurezza in modalità transport
  - ESP su SA interna
    - Utilizzato senza autenticazione
  - AH su SA esterna
- Crittografia applicata al payload IP
  - Autenticazione applicata all'intestazione ESP più l'intestazione IP originale ed eventuali estensioni
- Più campi coperti da autenticazione rispetto al caso precedente
  - IP sorgente
  - IP destinazione
  - …
- Sovraccarico dovuto all'impiego di due SA

RAGGRUPPAMENTO TRANSPORT-TUNNEL

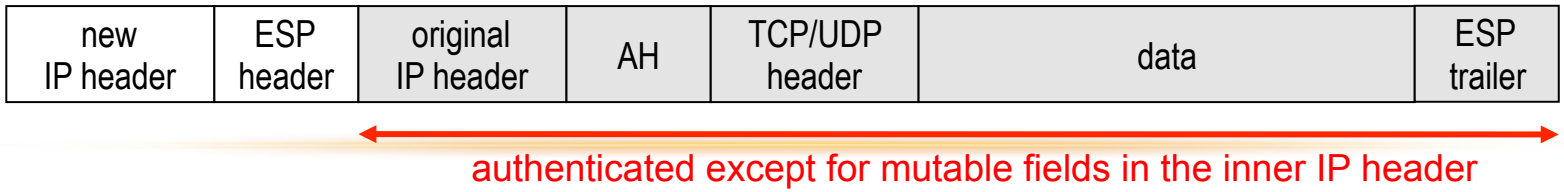
- Autenticazione prima della crittografia
  - Dati di autenticazione protetti da crittografia
  - Informazioni di autenticazione memorizzate col messaggio
    - Utile per riferimenti futuri
    - Più comodo operare su dati non crittografati
      - In caso contrario il messaggio dovrebbe essere decrittografato e ricrittografato per verificare l'autenticazione
- SA con AH interna in modalità transport
- SA con ESP esterna in modalità tunnel
- Autenticazione applicata al payload ed all'intestazione IP ad esclusione dei campi mutevoli
- Il pacchetto risultante viene elaborato in modalità tunnel da ESP
  - Il pacchetto interno (autenticato) viene crittografato
  - Viene aggiunta una nuova intestazione IP

COMBINAZIONI DI SA

- Combinazione ESP-AH
  1. ESP in modalità transport senza autenticazione
  2. AH in modalità transport



- Combinazione AH-ESP
  1. AH in modalità transport
  2. ESP in modalità tunnel senza autenticazione

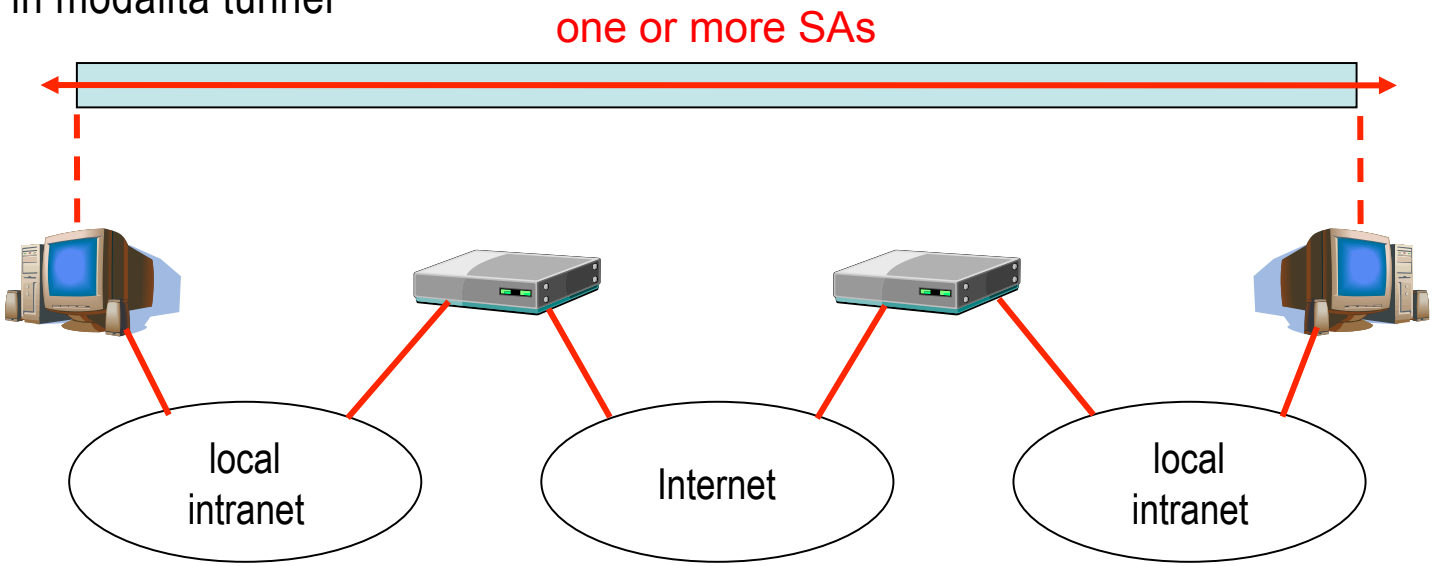


COMBINAZIONE DI SA

- Il documento IPSec Architecture elenca 4 esempi di combinazioni di SA che devono essere supportate da qualsiasi implementazione
- Si considerano la connettività fisica e la connettività logica (SA nidificate)
- Le SA possono essere di tipo AH ed ESP
- Per le SA fra host si possono usare le modalità transport e tunnel
- Negli altri casi si considera solo la modalità tunnel

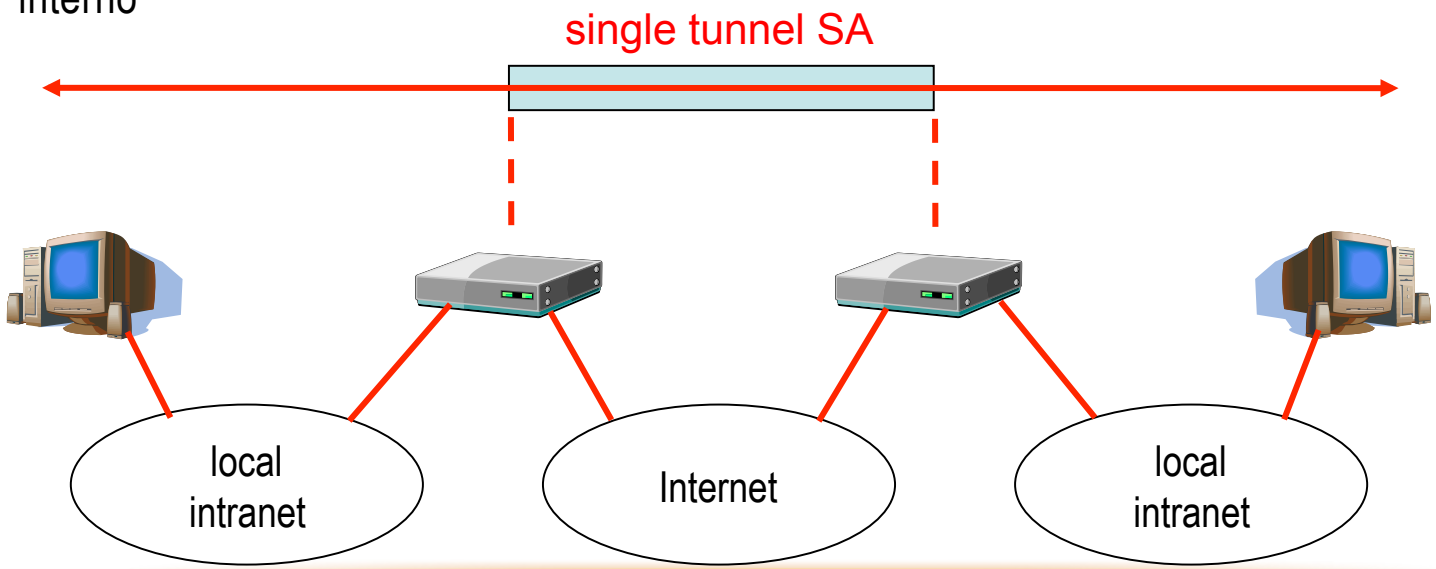
CASO 1: HOST-TO-HOST SECURITY

- Sicurezza fornita dai sistemi terminali che implementano IPSec
- Necessità di condividere chiavi segrete
- Possibili combinazioni: AH in modalità transport, ESP in modalità transport, ESP all'interno di AH in modalità transport, uno dei casi precedenti all'interno di AH o ESP in modalità tunnel



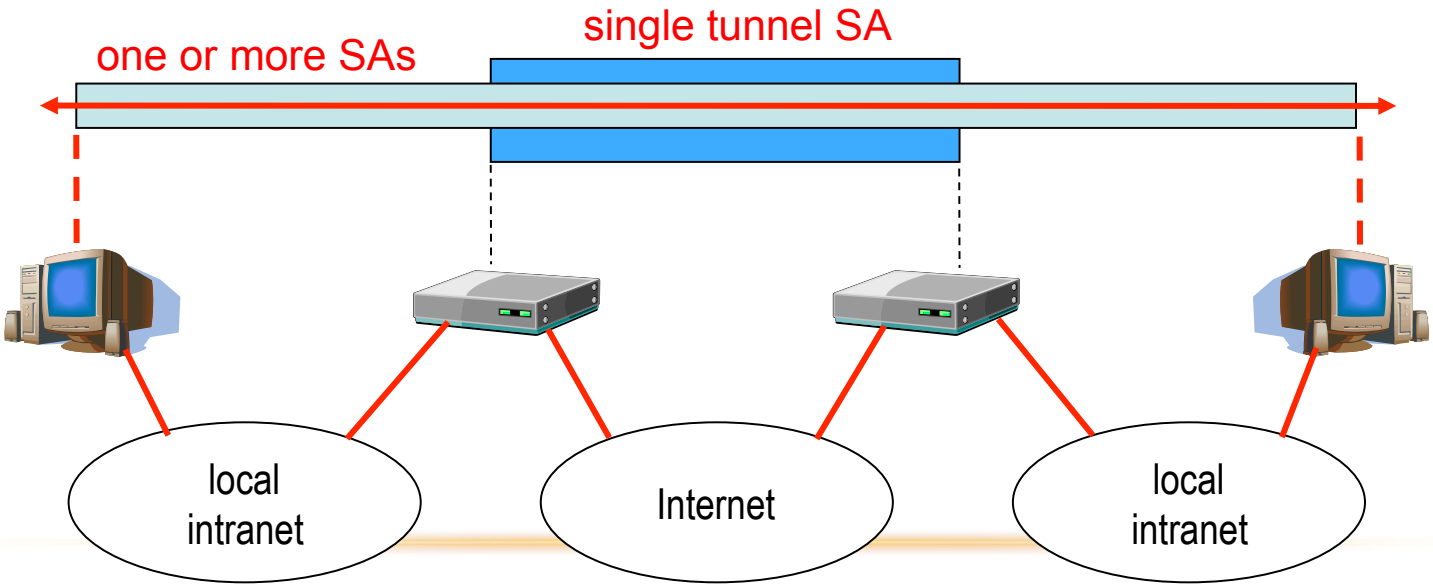
CASO 2: GATEWAY-TO-GATEWAY SECURITY

- Nessun host implementa IPSec
- Supporto di una semplice VPN
- Necessaria un'unica SA in modalità tunnel: AH, ESP, ESP con autenticazione
- Non è necessario usare tunnel nidificati: I servizi IPSec si applicano all'intero pacchetto interno



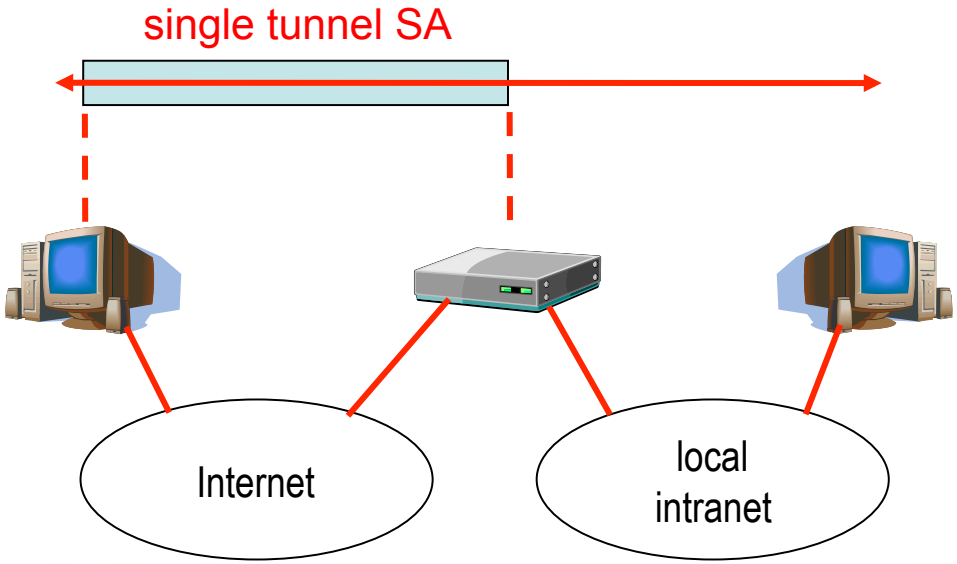
CASO 3: SICUREZZA END-TO-END

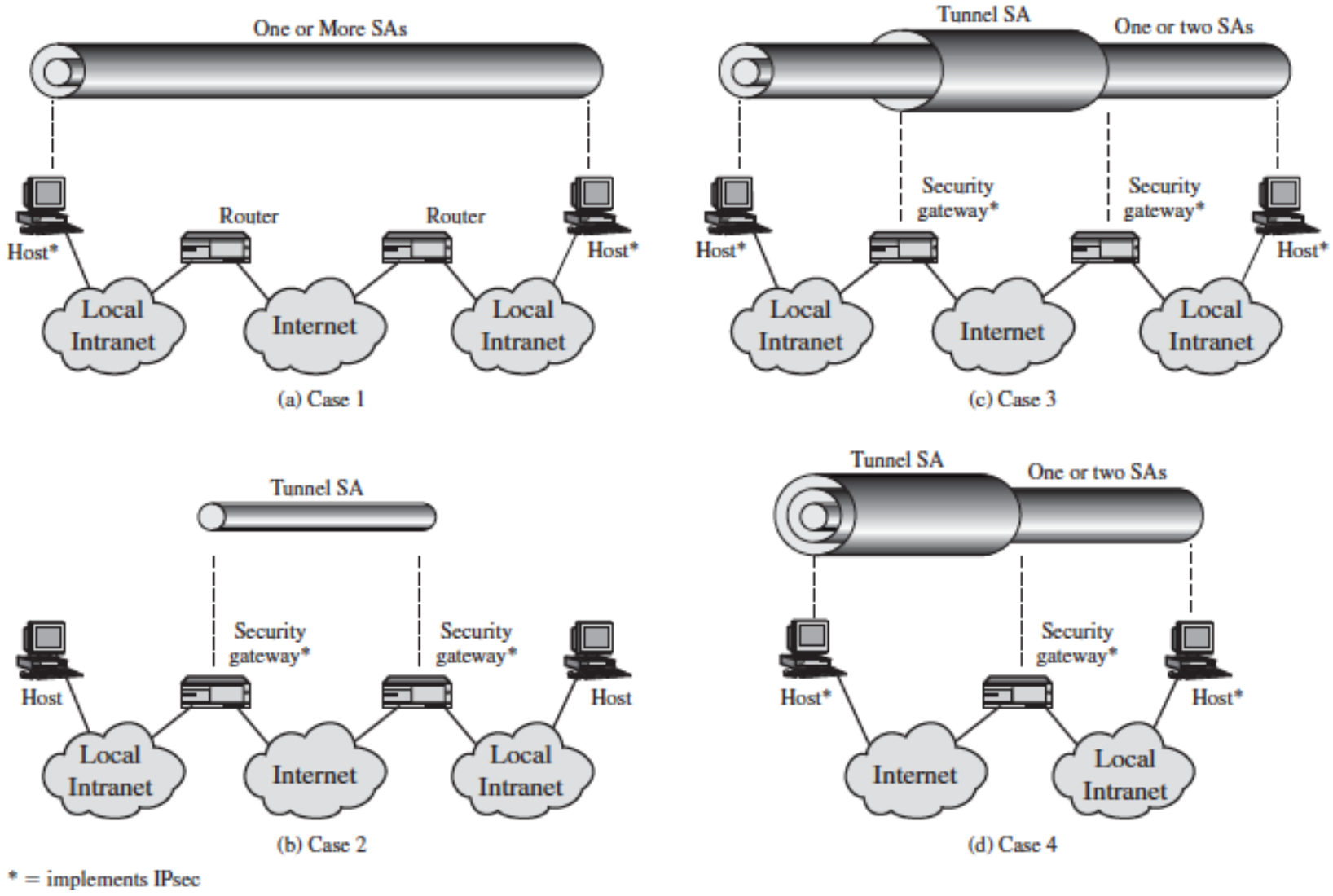
- Stesse combinazioni dei casi 1 e 2
- Tunnel gw-gw fornisce l'autenticazione e/o la segretezza per tutto il traffico fra i terminali
- Se il tunnel GW-GW è ESP fornisce anche il supporto per la segretezza del traffico
- Singoli host possono implementare servizi IPSec aggiuntivi per determinate applicazioni o utenti mediante SA end-to-end



CASO 4: HOST-TO-GATEWAY SECURITY

- Supporto per un host remoto che usa internet per raggiungere il firewall di un'azienda per poi accedere a server o workstation protetti
- Modalità tunnel fra host remoto e firewall
- Fra host remoto e locale possono essere utilizzate una o due SA




One or More SAs
Router
Router
Host*
Host*
Local Intranet
Internet
Local Intranet
(a) Case 1
Tunnel SA
One or two SAs
Security gateway*
Security gateway*
Host*
Host*
Local Intranet
Internet
Local Intranet
(c) Case 3
Tunnel SA
Security gateway*
Security gateway*
Host
Host
Local Intranet
Internet
Local Intranet
(b) Case 2
Tunnel SA
One or two SAs
Security gateway*
Host*
Host*
Internet
Local Intranet
(d) Case 4
* = implements IPsec

GESTIONE DELLE CHIAVI

CARATTERISTICHE DEL PROBLEMA

- Necessità di scegliere e distribuire le chiavi segrete
- Quattro chiavi richieste per la comunicazione fra applicazioni
  - Due coppie in ricezione e trasmissione
- Richiesto il supporto a due tipi di gestione
  - Manuale
    - Ciascun sistema è configurato manualmente con le proprie chiavi e quelle di altri sistemi
    - Ambienti piccoli e statici
  - Automatica
    - Creazione su richiesta delle chiavi per le SA
    - Sistemi dinamici di grandi dimensioni

ELEMENTI DEL PROTOCOLLO STANDARD

- Oakley key determination protocol
  - Protocollo per lo scambio di chiavi basato sull'algoritmo Diffie-Hellman
- ISAKMP (Internet Security Association and Key Management Protocol)
  - Fornisce una struttura per la gestione delle chiavi
  - Fornisce il supporto per la negoziazione degli attributi di sicurezza
    - Formati da utilizzare
  - Non impone un algoritmo specifico
  - È un insieme di tipi di messaggi che consentono di usare vari algoritmi per lo scambio per le chiavi
  - Inizialmente Oakley era obbligatorio

IL PROTOCOLLO DIFFIE-HELMAN

1. Accordo iniziale fra A e B sui parametri globali
   - q
   - Numero primo esteso
   - Alfa (radice primitiva di q)
2. A trasmette a B la sua chiave pubblica
3. B trasmette ad A la sua chiave pubblica
4. I due end-point calcolano la chiave privata di sessione
5. Le chiavi segrete vengono create solo quando necessario
6. Lo scambio non richiede infrastrutture preesistenti, ma solo l'accordo sui parametri iniziali

PUNTI DEBOLI DI DIFFIE-HELMAN

- Nessuna informazione sull'identità delle parti
- Vulnerabile all'attacco man-in-the-middle
  - C si finge B mentre comunica con A
  - C si finge A mentre comunica con B
  - A e B negoziano la chiave con C
  - C ascolta ed inoltra il traffico
- È computazionalmente oneroso
  - Vulnerabile all'attacco clogging in caso di richieste di numeri elevati di chiavi

L'ALGORITMO OAKLEY

- Mantiene i vantaggi di D-H
- Evita i punti deboli di D-H
- Impiega il meccanismo dei cookie per evitare gli attacchi clogging
  - Invio e riscontro di una sequenza pseudocasuale nel primo messaggio di scambio di chiavi
  - Nel caso di IP Spoofing nessuna risposta sarà ottenuta dall'attaccante
  - Il cookie deve dipendere dalle specifiche parti
  - Nessuno deve poter generare cookie accettabili dall'entità emettitrice
    - Utilizzo di informazioni segrete locali
  - Metodi veloci per la generazione e la verifica dei cookie
- Consente di negoziare un gruppo, specificando i parametri globali dello scambio delle chiavi
  - Definizione dei parametri globali
  - Identità dell'algoritmo

L'ALGORITMO OAKLEY

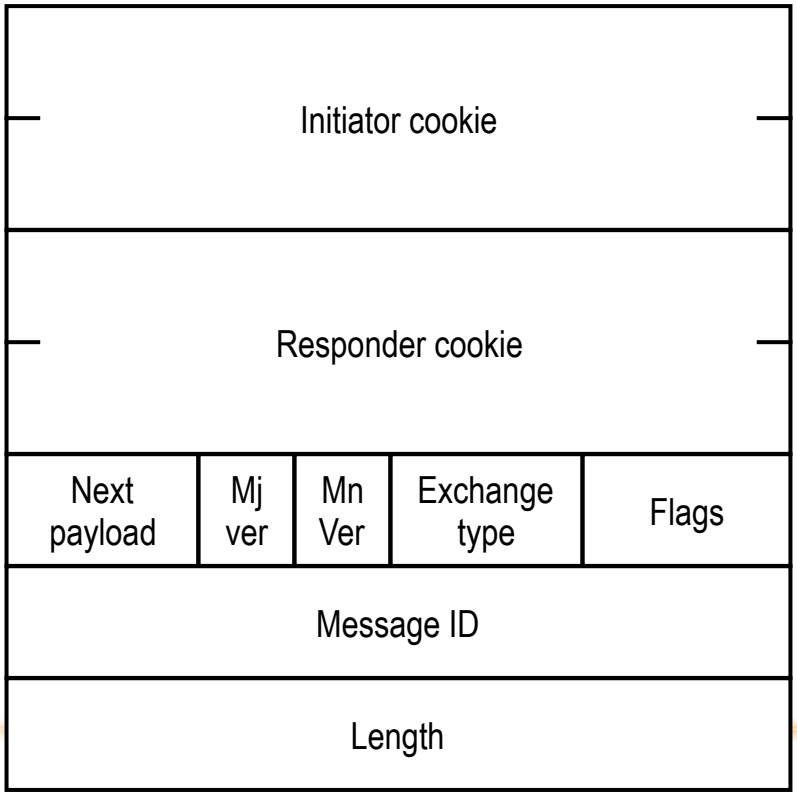
- Usa meccanismi per la difesa di attacchi a replay (nonce)
  - Ciascun nonce è un numero pseudocasuale generato localmente
  - I nonce compaiono nelle risposte e vengono crittografati in specifiche fasi dello scambio
- Consente lo scambio delle chiavi D-H
- Autentica lo scambio per evitare l'attacco man-in-the-middle
  - Firme digitali
    - Autenticazione mediante firma di un codice hash ottenibile vicendevolmente
    - Codice hash generato includendo il codice utente ed i valori nonce
  - Crittografia a chiave pubblica
    - Crittografia di parametri sensibili (codice utente, nonce) mediante la chiave privata del mittente
  - Crittografia a chiave simmetrica
    - Chiave ottenuta mediante meccanismi fuori banda (telefono, email, …)

IKE – INTERNET KEY EXCHANGE

- Definisce le procedure ed i formati dei pacchetti necessari per attivare, negoziare, modificare e cancellare le SA
- Nell'attivazione di una SA definisce il payload per lo scambio dei dati di generazione ed autenticazione delle chiavi
- Formato del payload indipendente
  - Dal protocollo di scambio delle chiavi
  - Dall'algoritmo di crittografia
  - Dal meccanismo di autenticazione

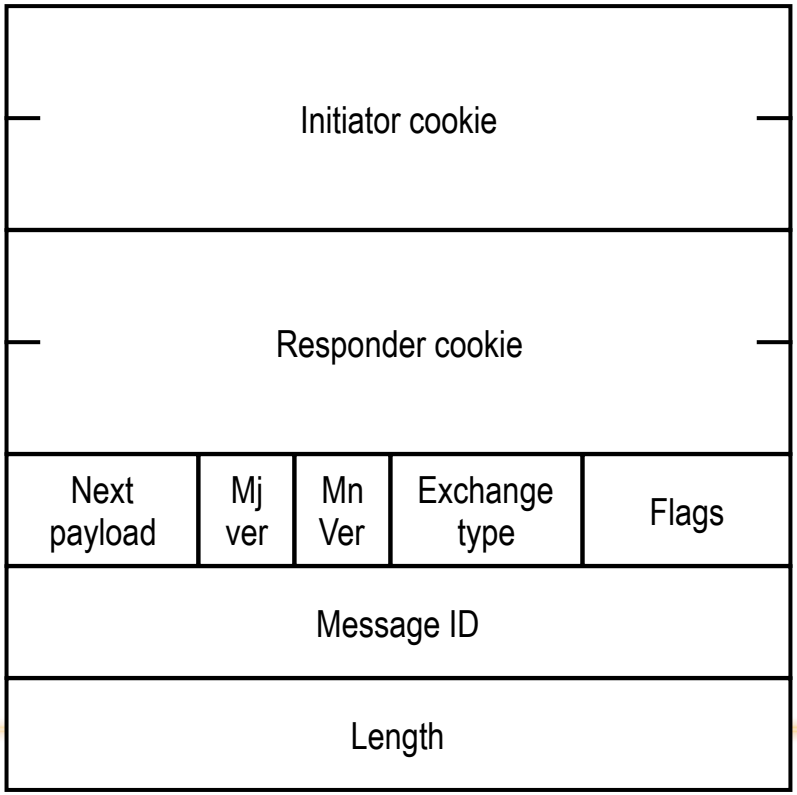
FORMATO DELL'INTESTAZIONE IKE

- Initiator cookie (64 bit)
  - SPI dell'entità che inizia l'attivazione, la notifica o la cancellazione della SA



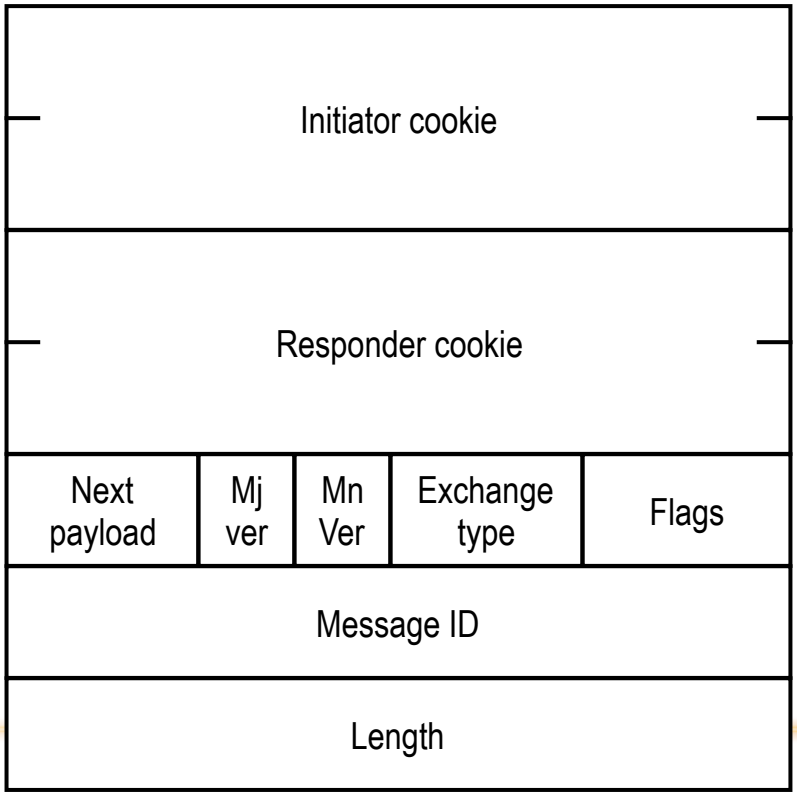
FORMATO DELL'INTESTAZIONE IKE

- Responder cookie (64 bit)
  - SPI dell'entità rispondente ("null" nel primo messaggio)



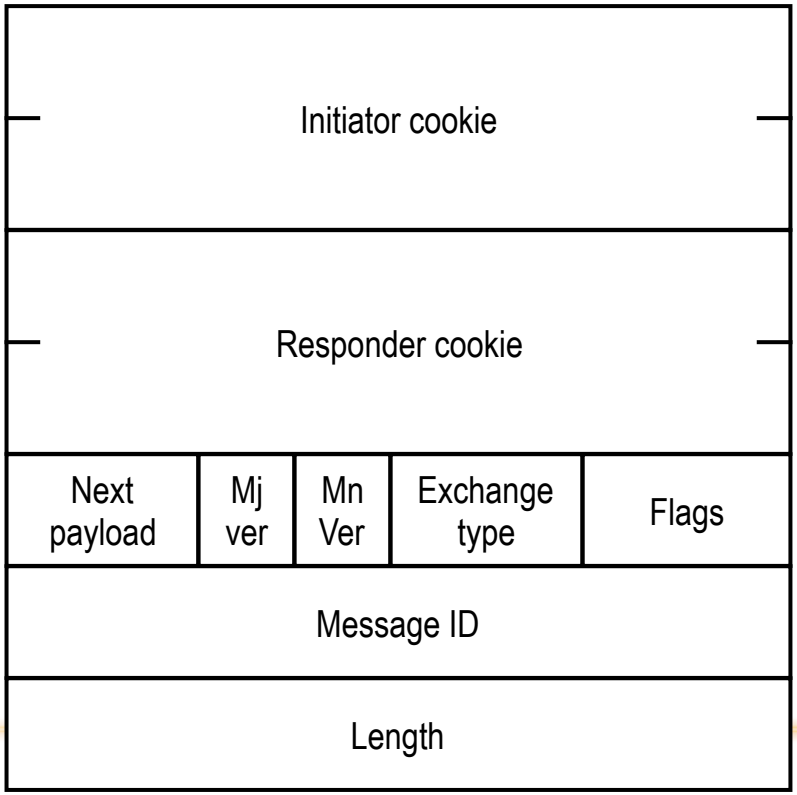
FORMATO DELL'INTESTAZIONE IKE

- Next Payload (8 bit)
  - Tipo del primo payload del messaggio



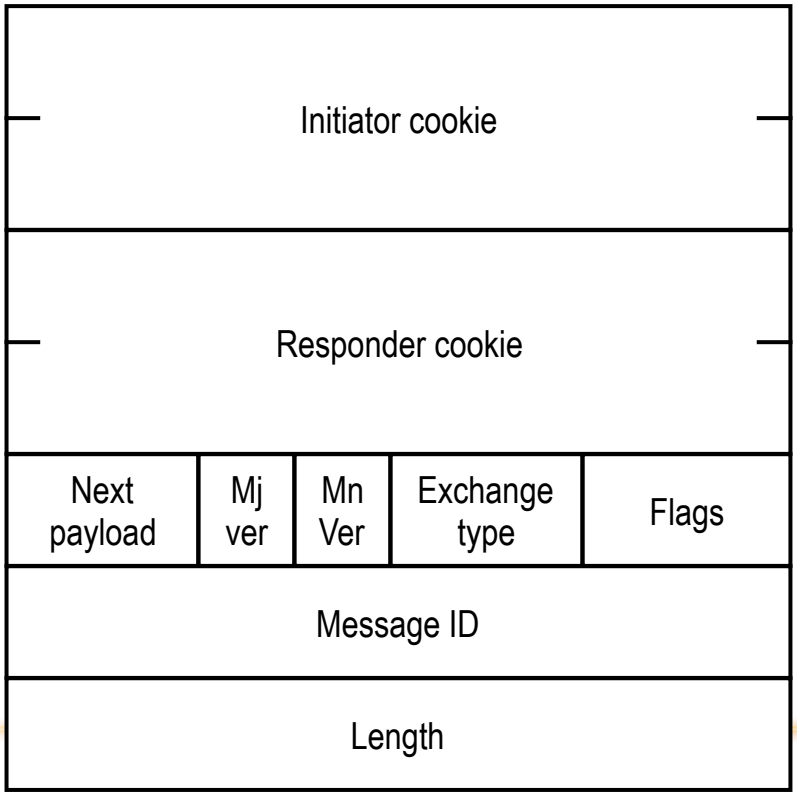
FORMATO DELL'INTESTAZIONE IKE

- Major version (4 bit)
  - Versione major di ISAKMP utilizzata



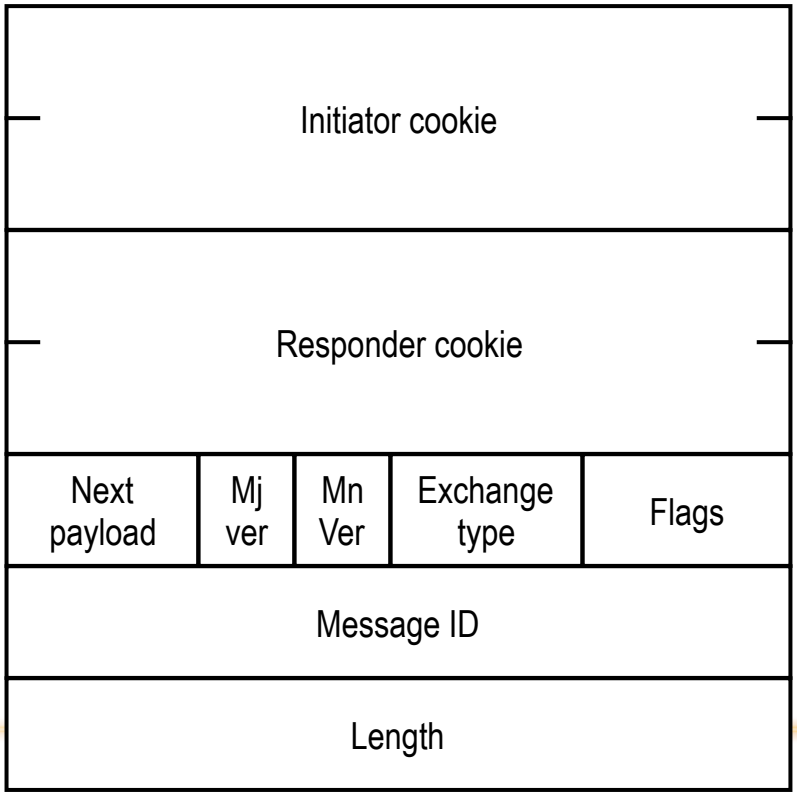
FORMATO DELL'INTESTAZIONE IKE

- Minor version (4 bit)
  - Versione minor di ISAKMP utilizzata



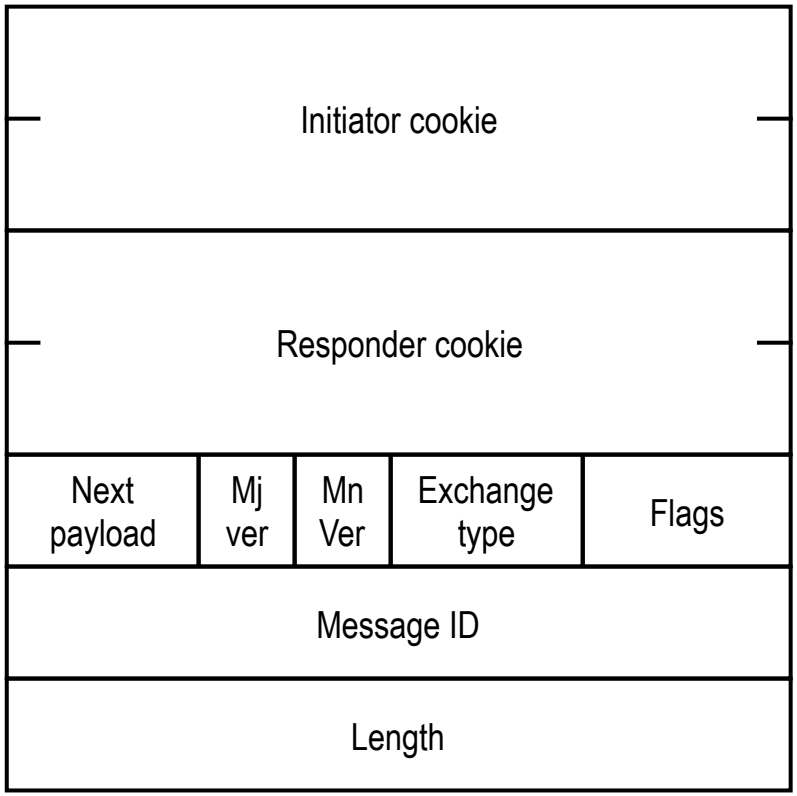
FORMATO DELL'INTESTAZIONE IKE

- Exchange type (8 bit)
  - Tipo di scambio effettuato



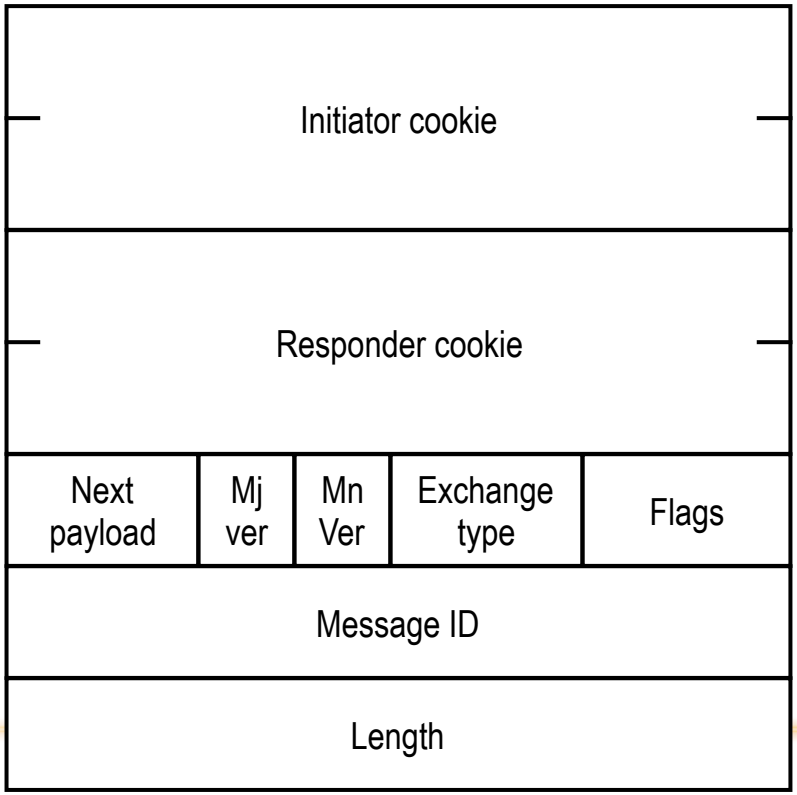
FORMATO DELL'INTESTAZIONE IKE

- Flags (8 bit)
- Opzioni impostate per lo scambio:
  - encryption se tutti i payload seguenti sono crittografati usando l'algoritmo di crittografia della SA
  - commit per garantire che il materiale crittografato venga ricevuto solo dopo l'attivazione della SA



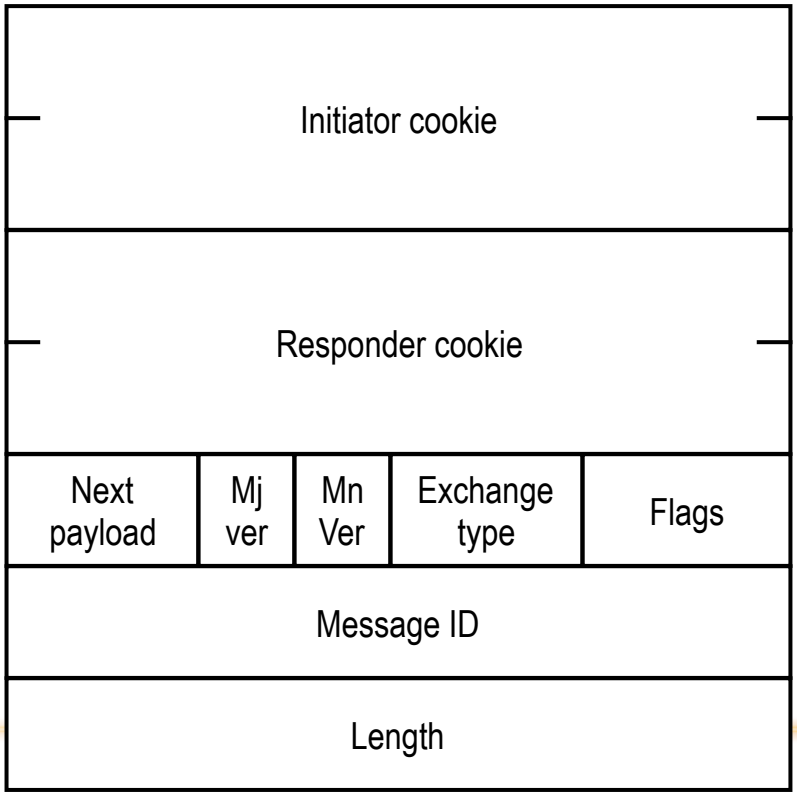
FORMATO DELL'INTESTAZIONE IKE

- Message ID (32 bit)
  - Identificativo univoco del messaggio



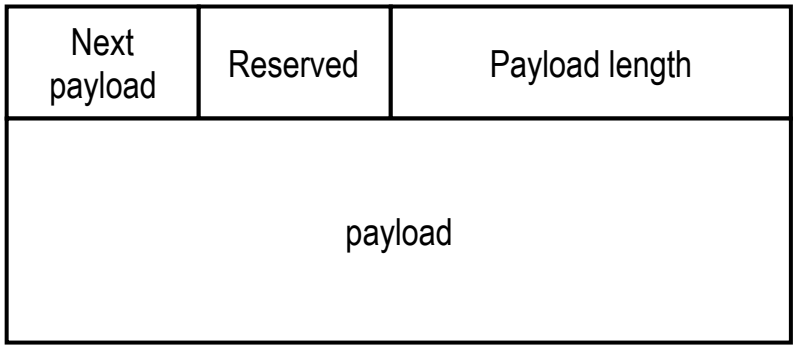
FORMATO DELL'INTESTAZIONE IKE

- Length (32 bit)
  - Lunghezza totale del messaggio (header + payload) misurata in ottetti



TIPI DI PAYLOAD IKE

- Next payload
  - 0 per l'ultima intestazione
  - Valore associato al payload successivo
- Payload length
  - Lunghezza in ottetti del payload + intestazione generica



TIPI DI PAYLOAD IKE

- Security Association (SA)
  - used to begin the setup of a new SA; carries various attributes
- Proposal (P)
  - used during SA setup; indicates protocol to be used (AH or ESP) and number of transforms
- Transform (T)
  - used during SA setup; indicates transform (e.g., DES, 3DES) and its attributes
- Key exchange (KE)
  - used to carry key exchange data (e.g., Oakley)
- Identification (ID)
  - used to exchange identification information (e.g., IP address)
- Certificate (CR)
  - carries a public key certificate (PGP, X.509, SPKI, …)
- Hash (HASH)
- Signature (SIG)
- Nonce (NONCE)
- Notification (N)
  - contains error or status information
- Delete (D)
  - indicates one or more SAs that the sender has deleted from its database (no longer valid)

SCAMBI IKE

- Base exchange
  - Riduce il numero di scambi
  - Non protegge l'identità

1. I → R : SA; NONCE
2. R → I : SA; NONCE
3. I → R : KE; IDi; AUTH
4. R → I : KE; IDr; AUTH

- Identity protection exchange
  - Estende il caso Base
  - Scambio di chiavi con nonce

1. I → R : SA
2. R → I : SA
3. I → R : KE; NONCE
4. R → I : KE; NONCE
5. I → R : IDi; AUTH
6. R → I : IDr; AUTH

SCAMBI IKE

- Authentication only exchange
  - Reciproca autenticazione senza scambio di chiavi
    - I → R : SA; NONCE
    - R → I : SA; NONCE; IDr; AUTH
    - I → R : IDi; AUTH
- Aggressive exchange
  - Riduce il numero di scambi ma non garantisce la protezione dell'identità
    - I →R : SA; KE; NONCE; IDi
    - R → I : SA; KE; NONCE; IDr; AUTH
    - I → R : AUTH
- Informational exchange
- Trasmissione monodirezionale di informazioni per la gestione della SA
  - I → R : N/D

DOMANDE?