Network Security
Elements of Network Security Protocols

The IpSec architecture

Roadmap

- *Architettura di base*
- *Modalità tunnel e client*
- *ESP, AH*
- *Cenni a IKE*

Informazioni generali

- IpSec è una proposta IETF per fare sicurezza al livello IP
  - RFC 2041, 2042, 2046, 2048
- IpSec si basa su IP (raw socket) ed è compatibile con
  - IPv4 (opzionale): è annunciato dal campo *protocol*;
  - IPV6 (obbligatorio): è un *next header*
- IpSec permette di
  - definire canali sicuri end-to-end
  - creare VPN su reti pubbliche

Servizi di sicurezza offerti

- *Integrità dei datagrammi*
- *Autenticazione dell'origine dei dati*
- *Rifiuto dei pacchetti di 'replica'*
- *Confidenzialità*
- *Confidenzialità parziale del flusso di traffico*

Protocolli in IPsec

IPsec è costituito da tre protocolli

- Authentication Header (AH)
  autenticazione dei pacchetti
- Encapsulating Security Payload (ESP)
  confidenzialità ed autenticazione dei pacchetti
- Internet Key Exchange (IKE)
  negoziazione dei parametri di sicurezza, autenticazione e distribuzione delle chiavi

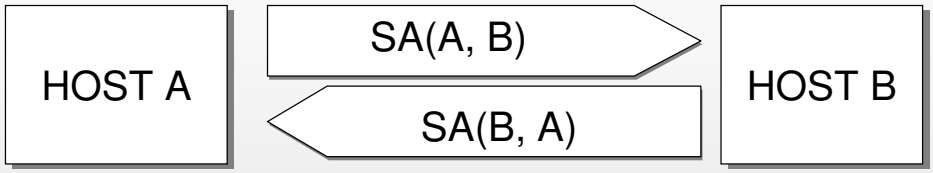
Servizi & Protocolli

	AH	ESP (cifr.)	ESP (cifr. & aut.)
Integrità dei datagrammi	X		X
Autenticazione dell'origine dei dati	X		X
Rifiuto di pacchetti di replica	X	X	X
Confidenzialità		X	X
Confidenzialità parziale del traffico		X	X

Security Association (SA)

- Connessione logica **unidirezionale** tra due host

  (ne occorrono due per avere protezione completa di un canale bidirezionale)



- Una SA è identificata da tre parametri
  - Security Parameter Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier (AH o ESP)

Parametri di una SA

- Sequence number counter
- Sequence counter overflow
- Anti-replay window
- AH information
- ESP information
- Lifetime of this association
- IPSec protocol mode (tunnel, transport, wildcard)
- Path MTU

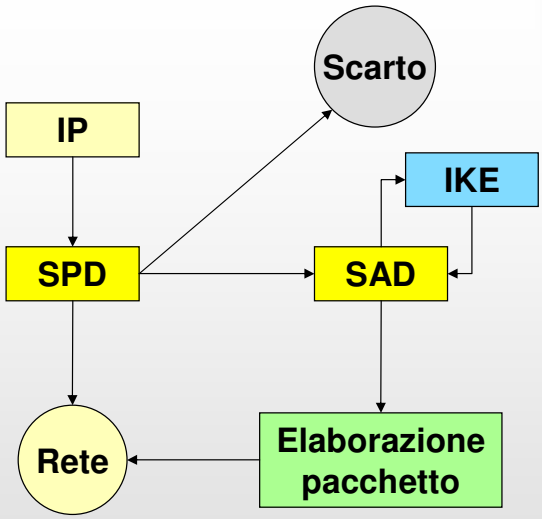
Database di sicurezza

- **Security Association Database**

  SAD definisce i parametri associati a ciascuna SA

- **Security Policy Database**

  SPD mette in relazione una porzione del traffico IP ad SA specifiche (oppure nessuna SA, nel caso al traffico IP sia consentito aggirare I controlli IPSec)



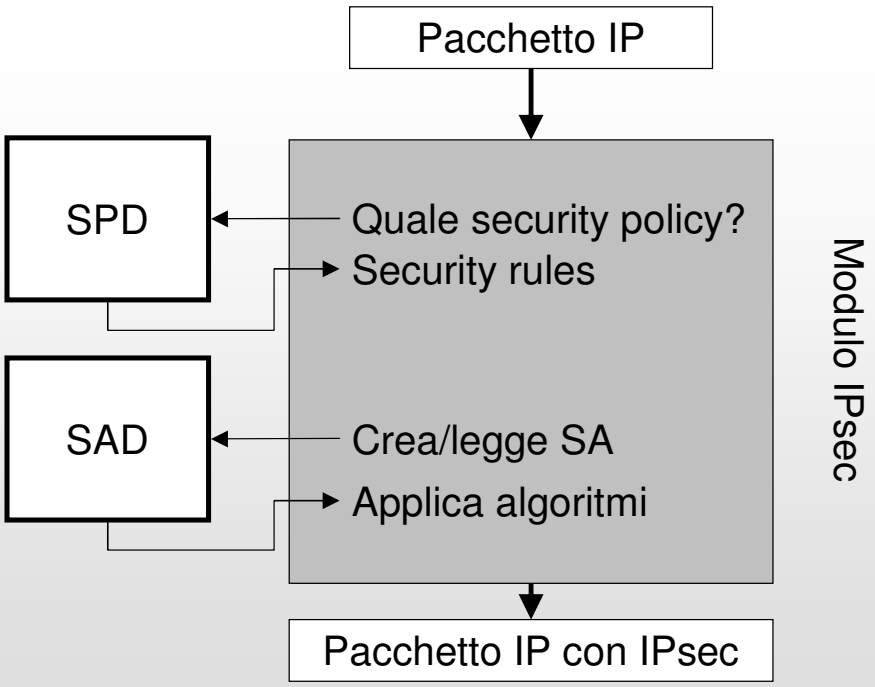
Security policies: examples

- Tutto il traffico verso 192.168.2.3 deve protetto da ESP in modalità trasporto usando DES-CBC
- Tutto il traffico FTP (TCP, porta 20) verso 192.168.2.3 deve essere protetto da ESP in modalità tunnel usando 3DES-CBC
- Tutto il traffico verso 192.168.2.3 non deve essere protetto
- Tutto il traffico verso 192.168.2.3 deve essere scartato

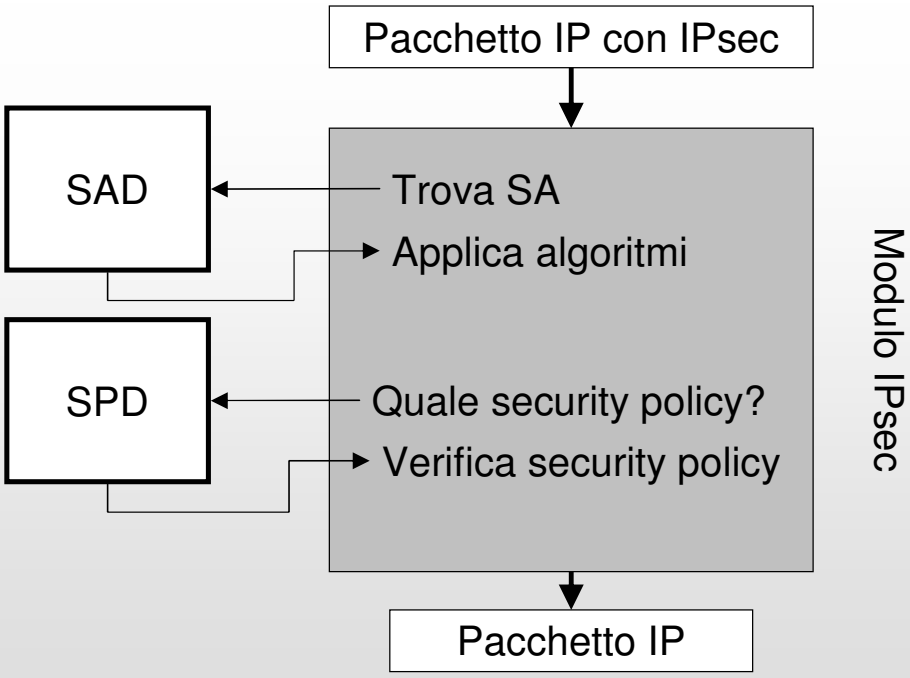
SPD: i selettori IP

- Un SPD contiene un insieme di *politiche* (*policy entries*) ciascuna delle quali specifica una porzione del traffico IP e la SA per quella particolare porzione di traffico
- Una porzione di traffico IP è specificato per mezzo di un insieme di valori detti *selettori* (*selectors*)
  - Destination IP Address
  - Source IP Address
  - Userid
  - Data Sensitivity Level (Classified,…)
  - Transport Layer Protocol
  - Ipsec Protocol
  - Source And Destination Port
  - Ipv6 Class
  - Ipv6 Flow Label
  - TOS, Ipv4 Type Of Service
- Il SPD viene acceduto utilizzando i selettori come chiave

Invio di un messaggio



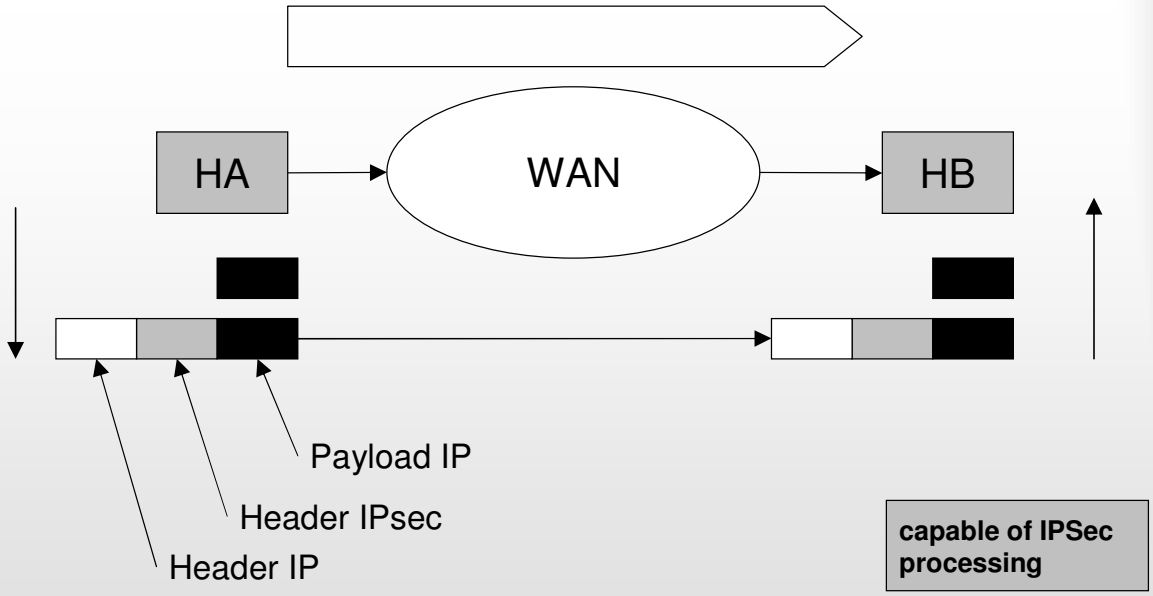
Ricezione di un messaggio



Modalità di incapsulamento

- *Modalità trasporto (transport mode)*
  - L'intestazione (header) del pacchetto originale che deve essere protetto (confidenzialità e/o autenticità) viene utilizzata per instradare il pacchetto protetto
  - Questa modalità di incapsulamento richiede che l'intestazione originale contenga indirizzi instradabili sulla rete pubblica
- *Modalità tunnel (tunnel mode)*
  - Il pacchetto originale (interno) viene trasportato da un pacchetto IP esterno il cui header specifica due gateways
  - Questa modalità di incapsulamento permette di stabilire un VPN che si estende attraverso Internet e che comprende host aventi indirizzi privati
  - La modalità tunnel è la più utilizzata

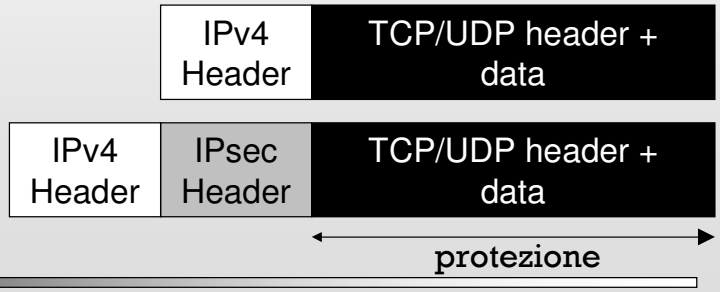
IPsec in modalità Trasporto



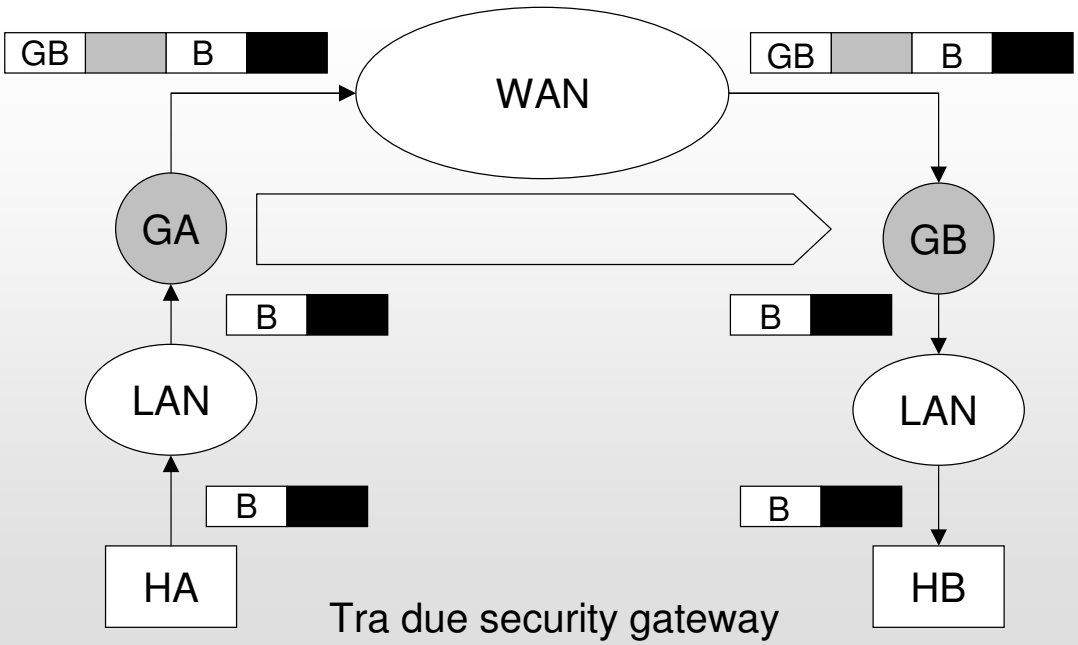
Tra due end-system

IPsec in modalità trasporto

- Fornisce protezione ai pacchetti del livello trasporto (TCP, UDP, SNMP, ICMP) contenuti nel pacchetto IP
  - non protegge i campi variabili dell'header IP
  - non modifica gli indirizzi nell'header IP
- Sicurezza end-to-end
- Non coinvolge i gateway (eccezione: traffico destinato ai gateway)

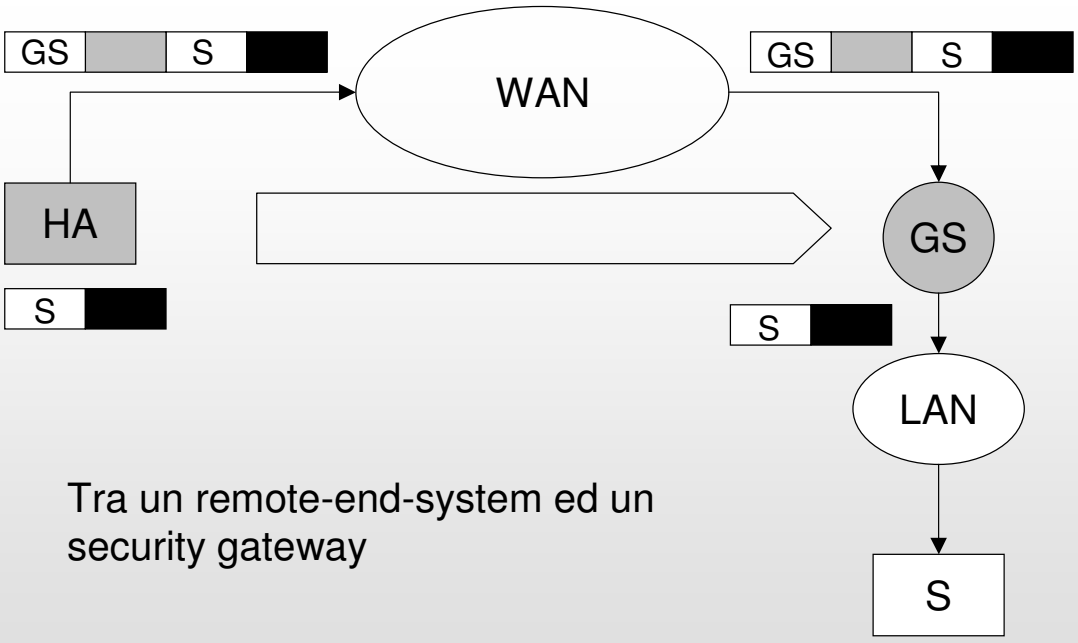


IPsec in modalità Tunnel



Tra due security gateway

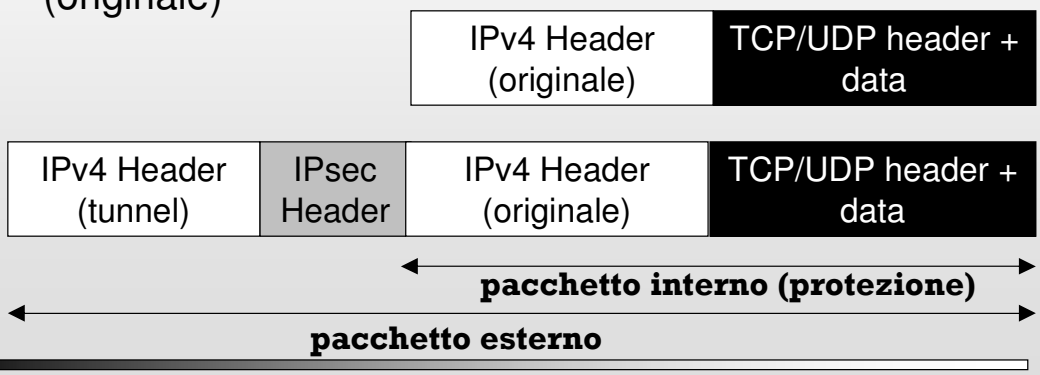
IPsec in modalità Tunnel



Tra un remote-end-system ed un security gateway

IPsec in modalità Tunnel

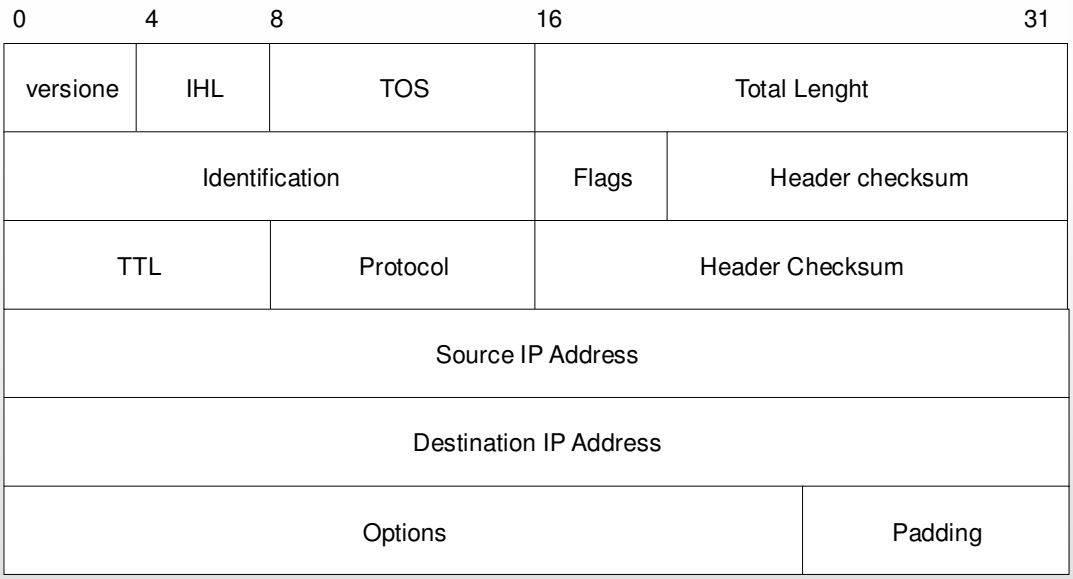
- Utilizzato sempre quando uno degli host è un gateway
- Fornisce protezione all'intero pacchetto IP (originale)
- Protegge i campi variabili del pacchetto originale
- Gli indirizzi nell'header del pacchetto esterno possono essere diversi da quelli nell'header IP interno (originale)



Funzionalità

	modalità trasporto	modalità tunnel
AH	Autentica il payload e porzioni selezionate dell'header IP e degli extension header IPv6	Autentica l'intero pacchetto IP interno e porzioni selezionate del pacchetto esterno
ESP	Cifra il payload IP e gli extension header IPv6	Cifra il pacchetto interno
ESP con autenticazione	Cifra il payload IP e gli extensione header IPv6. Autentica il payload IP ma non l'header IP	Cifra il pacchetto interno. Autentica il pacchetto interno

Header IPv4



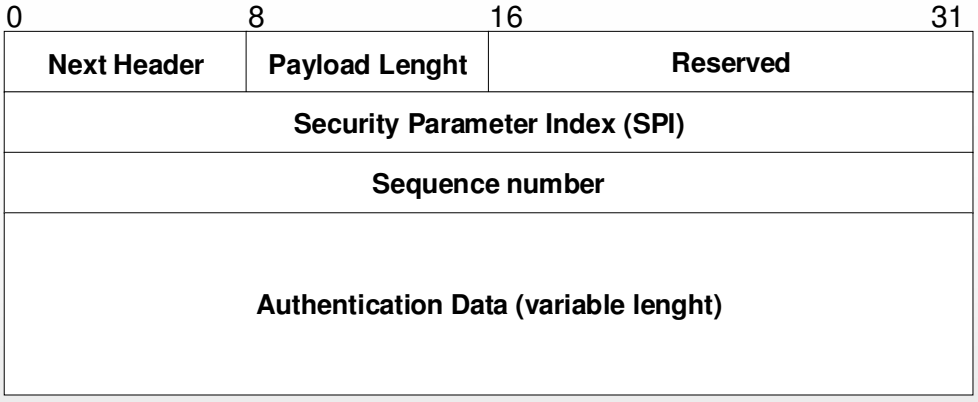
Header IPv4

- Indirizzi IP del mittente e del destinatario (32 bit)
- Internet Header Length (IHL) in 32 bit word
- Type Of Service (TOS)
- Length: numero di byte del pacchetto IP
- Identification: ID del pacchetto (per i frammenti)
- Flags: may/don't fragment; last/more fragments
- Time To Live (TTL): number of hops
- Protocol: protocollo usato dal payload
- ...*altri campi*...

Authentication Header (AH)

- Estensione di IPv4/IPv6 per l'autenticazione dei pacchetti (IP protocol 51, RFC-2402)
- Servizi offerti: autenticazione del pacchetto
  - integrità dei dati
  - autenticazione dell'origine dei dati
  - anti-replay
- Algoritmi utilizzati: HMAC
  - HMAC-MD5-96
  - HMAC-SHA-1-96

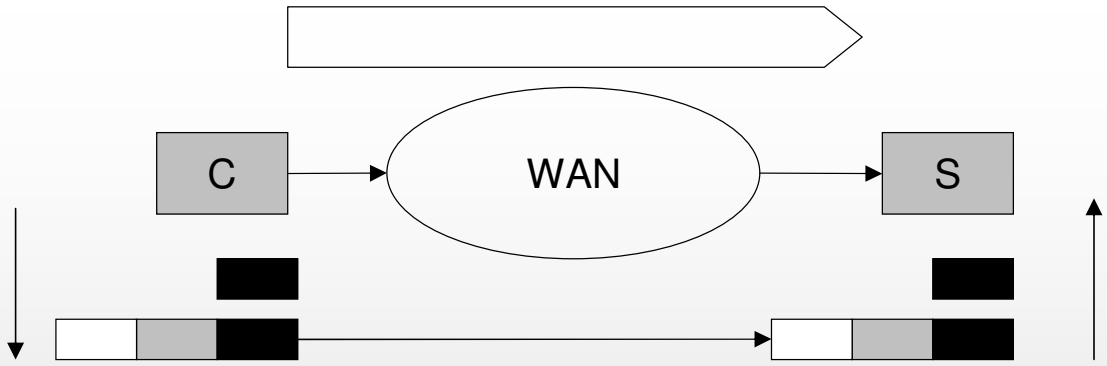
Formato di AH

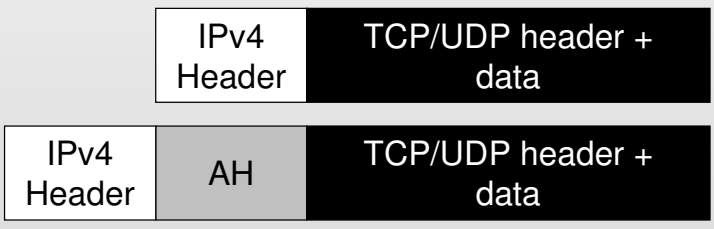


Formato di AH

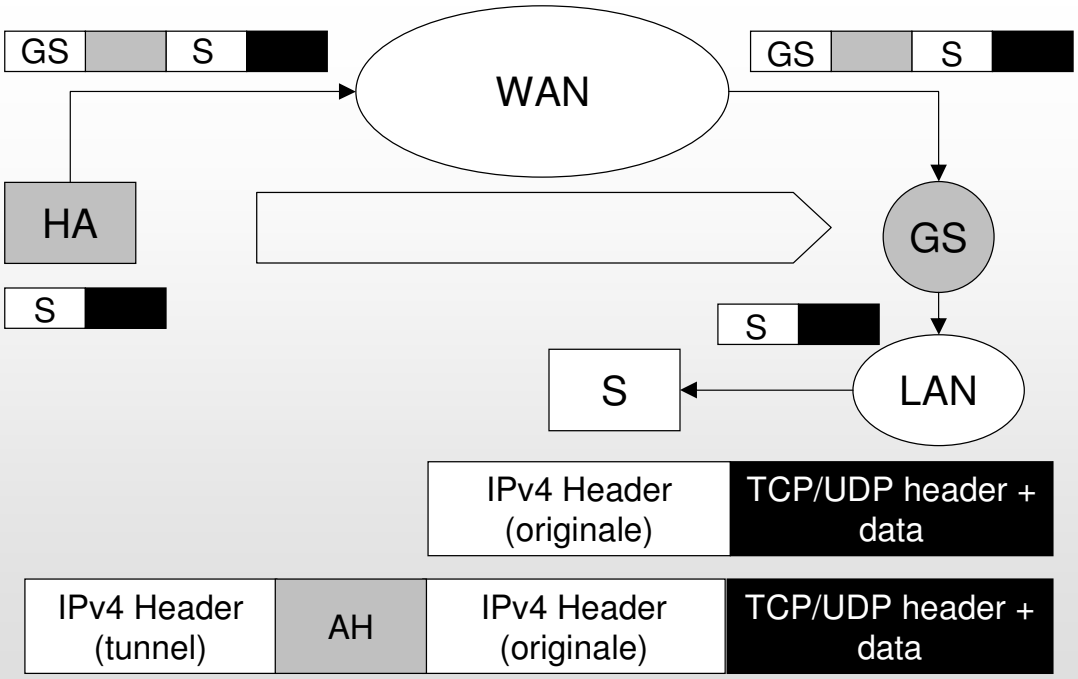
- *Next Header* (8 bit) indica il tipo di intestazione che segue
- *Payload Length* (8 bit) lunghezza di AH espressa in word di 32 bit meno due
- *Reserved* (16 bit) riservato per usi futuri
- *SPI* (32 bit) identifica una SA
- *Sequence number* (32 bit) numero di sequenza
- *Authentication data* contiene il valore per la verifica dell'integrità (Integrity Check Value)
  - campo di lunghezza variabile, multiplo di 32 (default 96 bit)
  - MAC o una sua versione tronca (96 bit)

AH in modalità Trasporto

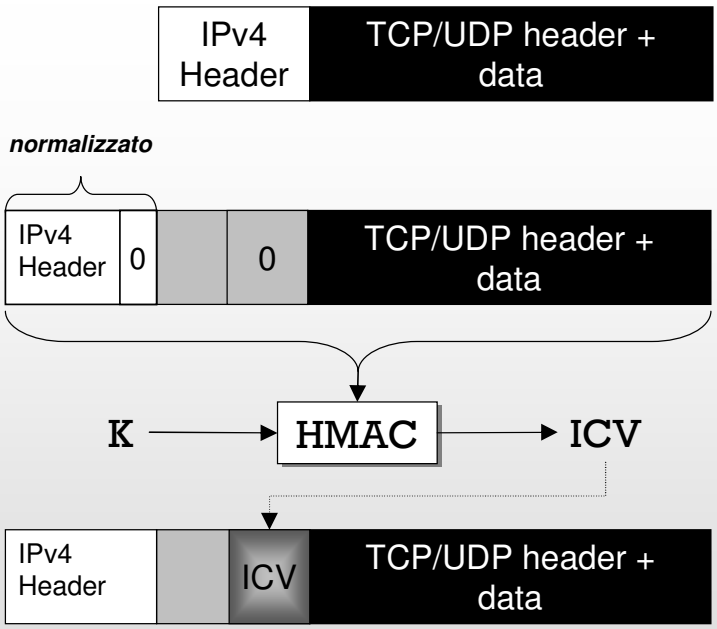




AH in modalità Tunnel



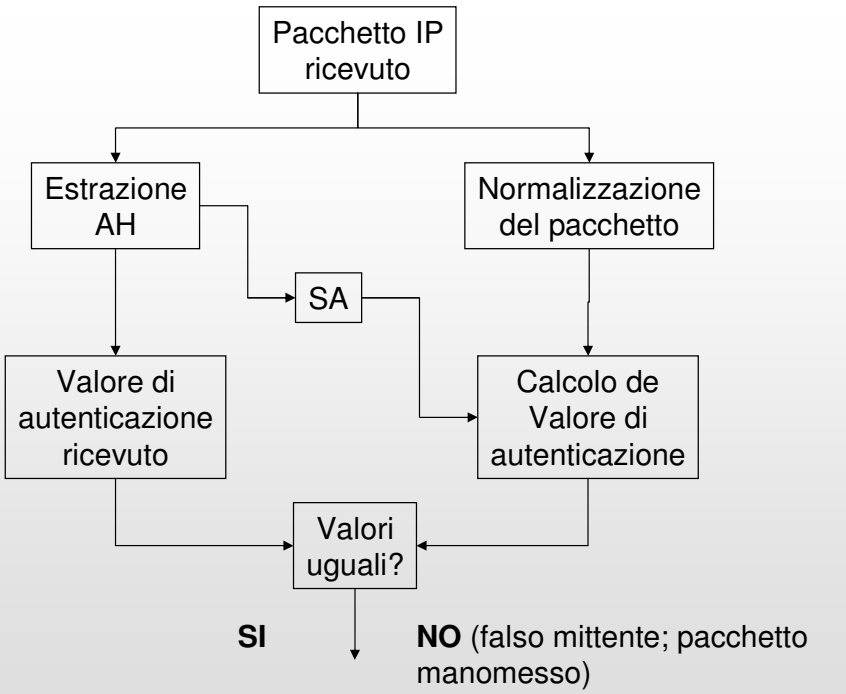
Costruzione di un pacchetto AH



Costruzione di un AH

1. Costruire l'header AH con Authentication Data inizialmente impostato a zero
2. Appendere il payload
   - modalità trasporto: pacchetto del livello di trasporto
   - modalità tunnel: pacchetto IP originale
3. Prependere l'header IP *normalizzato* (i campi mutabili sono impostati a zero)
   - I campi *mutabili* (es. TTL, hop count) sono poi ripristinati dopo il calcolo del MAC
4. Calcolare l'ICV (il MAC) su l'header IP normalizzato, l'header AH ed il payload
5. Copiare l'ICV nel campo Authentication Data

Autenticazione dei dati e del mittente



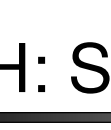
Livello di protezione di AH

- In modalità trasporto, l'autenticazione copre
  - l'intero pacchetto IP (originario), ad eccezione dei campi mutabili della intestazione originaria che sono posti a zero
- In modalità tunnel, l'autenticazione copre
  - l'intero pacchetto IP interno (originario) e
  - l'intestazione del pacchetto IP esterno, ad eccezione dei suoi campi mutabili che sono posti a zero

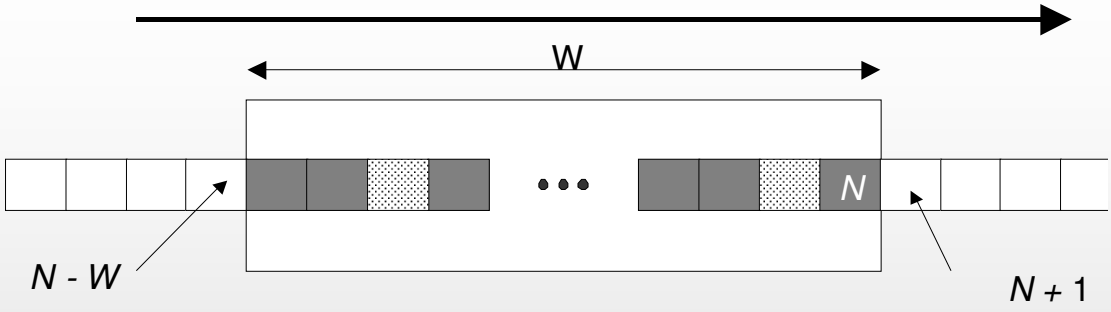
Servizio Anti-Replay

- Quando una SA viene creata, il mittente inizializza a zero il contatore (32 bit)
- Prima di inviare un pacchetto, il mittente incrementa il valore del contatore di uno e lo copia nel campo Sequence Number
  - Quando il contatore raggiunge il valore $2^{32} - 1$, il mittente deve terminare o rinegoziare la SA
- IP non garantisce né la consegna né l'ordine di consegna, perciò il ricevente deve realizzare un meccanismo a finestra
  - Dimensione di default è 64

AH: Servizio Anti-replay



La finestra viene spostata se si riceve un pacchetto valido che cade a destra della finestra; il pacchetto diventa l'estremo superiore



messaggio valido ricevuto

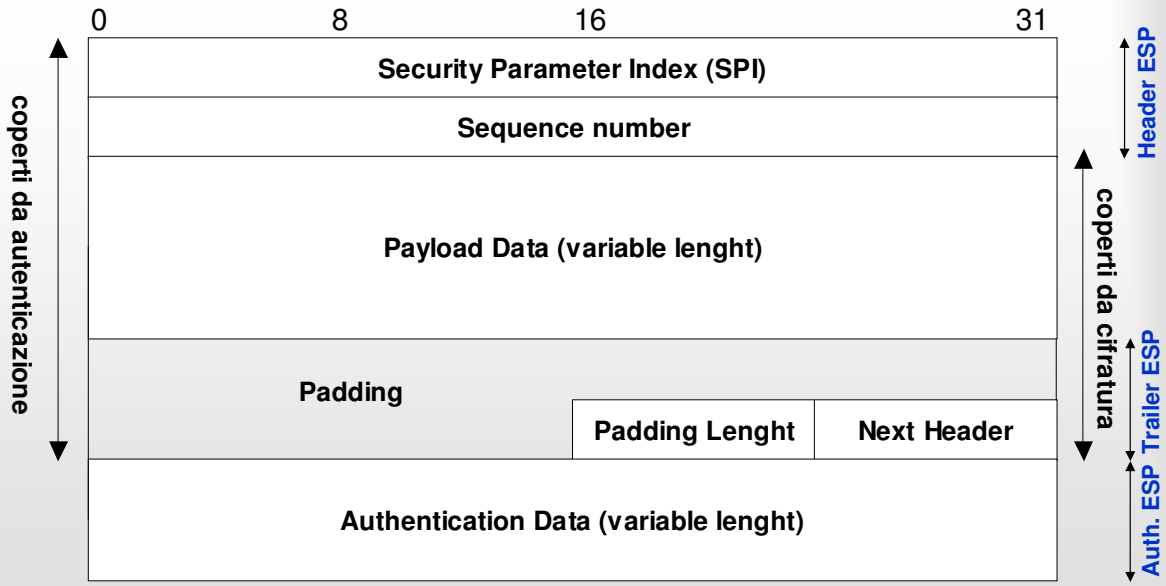
messaggio valido non ancora ricevuto

Un pacchetto non-valido o un pacchetto che cade a sinistra della finestra viene scartato

Encapsulating Security Payload (ESP)

- Estensione di IPv4/IPv6 per la cifratura dei pacchetti (IP protocol 50, RFC-2406)
- Servizi offerti
  - Confidenzialità del contenuto dei pacchetti
  - Parziale riservatezza del flusso di traffico
  - Autenticazione opzionale e limitata al payload
- Algoritmi utilizzati
  - DES in modalità CBC (richiesto)
  - 3DES, RC5, IDEA, 3IDEA, CAST, Blowfish (opzionali)
  - HMAC-MD5-96, HMAC-SHA-1-96

Formato di ESP



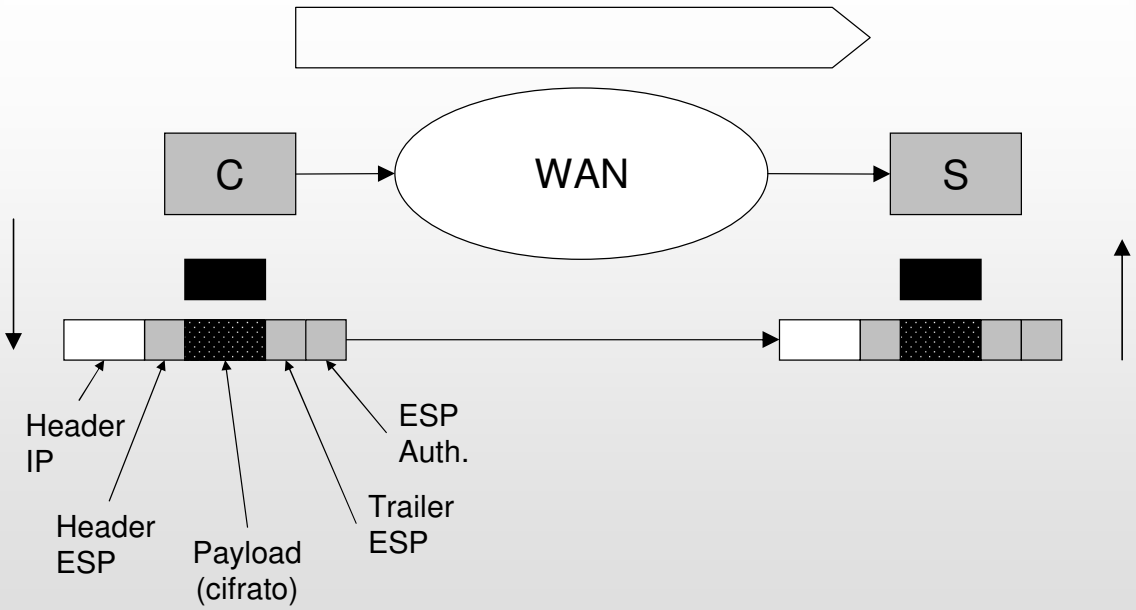
Formato di ESP

- *Security Parameters Index* (SPI): 32 bit
- *Sequence number* (32 bit): servizio anti-replay
- *Payload data* contiene i dati cifrati
  - Un eventuale vettore di inizializzazione è contenuto in forma esplicita all'inizio del campo
- *Padding* (0 – 255 byte) byte di completamento
- *Padding length* numero di byte di completamento
- *Next Header* (8 bit): Tipo di dati contenuti nel payload
- *Authentication Data* contiene il valore ICV

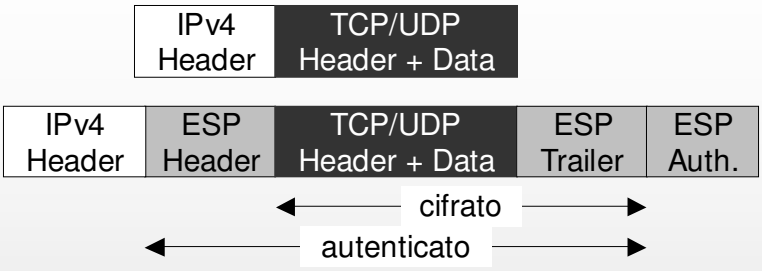
Formato di ESP

- *Header ESP* è formato dai campi
  - SPI
  - Sequence Number
- *Trailer ESP* è formato dai campi
  - Padding,
  - Padding Lenght
  - Next Header
- *Authentication* ESP è formato dal campo
  - Authentication Data

ESP in modalità Trasporto

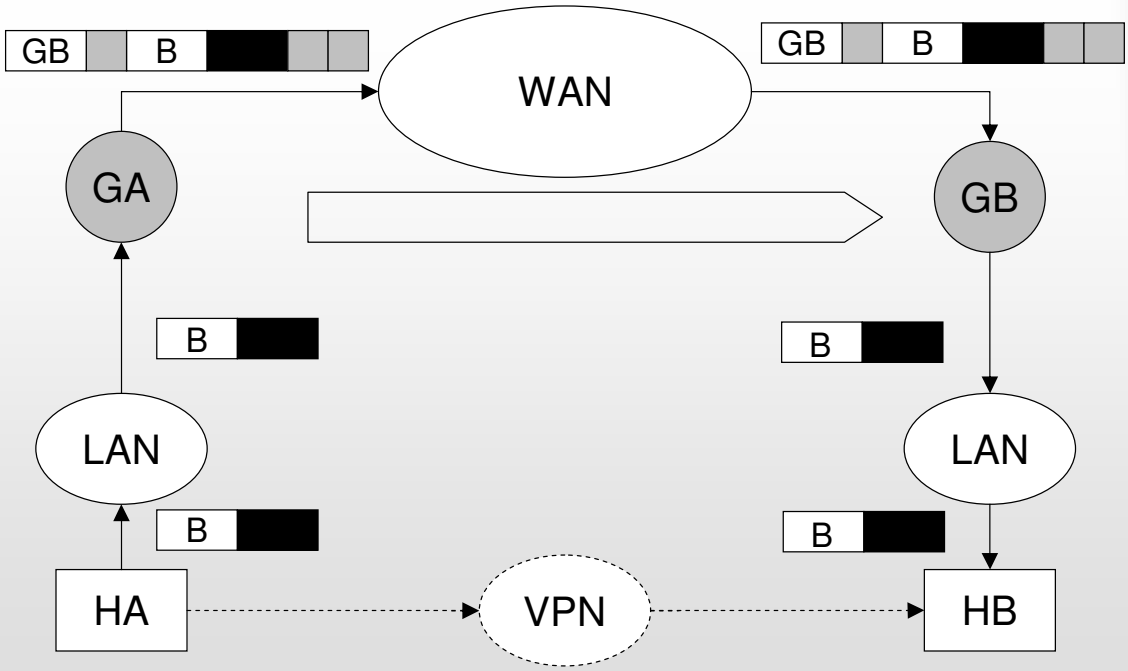


ESP in modalità Trasporto

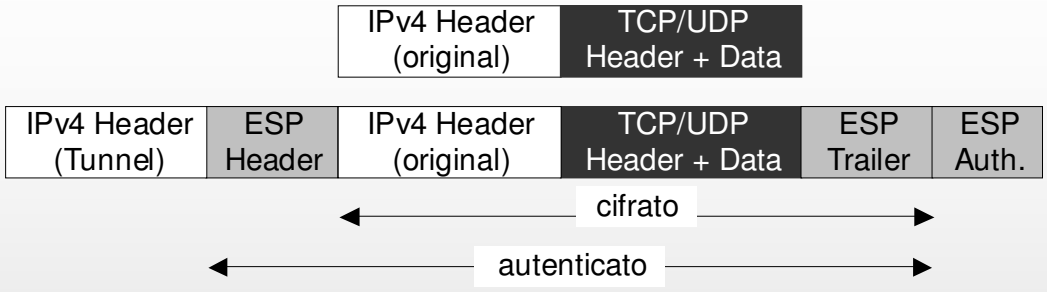


- L'autenticazione non copre l'header IP
- Rispetto ad AH, ESP offre una minore copertura

ESP in modalità Tunnel

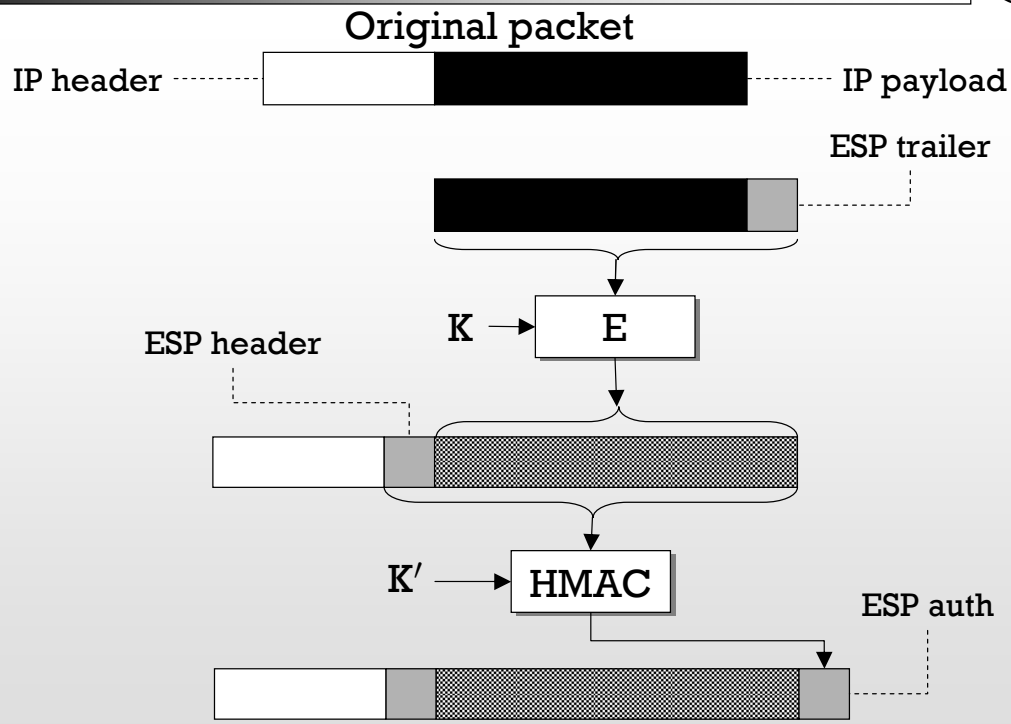


ESP in modalità Tunnel



- L'autenticazione non copre l'header IP (tunnel)
- Rispetto ad AH, ESP offre una minore copertura

Costruzione di un pacchetto ESP



Costruzione di un pacchetto ESP

1. Costruire l'header ESP
2. Appendere il payload
   - in modalità trasporto: il pacchetto del livello di trasporto
   - in modalità tunnel: il pacchetto IP originale
3. Costruire il trailer ESP ed appenderlo al payload
4. Cifrare il payload ed il trailer ESP
5. Se richiesto, calcolare il MAC su header ESP ed il testo cifrato ed appendere l'ICV al testo cifrato (ESP Authentication)

Utilizzi del padding

- L'algoritmo di cifratura richiede che il testo in chiaro sia un multiplo di un certo numero di byte
- La specifica di ESP richiede che i campi Padding Length e Next Header siano allineati al byte più significativo all'interno di una parola di 32 bit
- Può essere inserito per non rivelare l'effettiva lunghezza del payload

Combinazione di SA

- Ad una stessa porzione di traffico si possono associare più SA
- Una bundle SA è una sequenza di SA tramite la quale viene elaborata una porzione di traffico
- Per formare un bundle, le SA possono essere combinate in due modi
  - transport adiacency – consiste nell'applicare allo stesso pacchetto IP più protocolli di sicurezza senza invocare il tunnelling
  - iterated tunnelling – consiste nell'applicare più protocolli di sicurezza tramite la modalità tunnel

Autenticazione & Riservatezza

- ESP con opzione di autenticazione
  - modalità trasporto: l'autenticazione e la cifratura si applicano al payload del pacchetto IP; l'intestazione del pacchetto IP non viene protetta
  - modalità tunnel: l'autenticazione e la cifratura sono applicate all'intero pacchetto IP interno e sono elaborate dal destinatario esterno
  - in entrambi i casi l'autenticazione si applica al testo cifrato

Autenticazione & Riservatezza

- Transport adiacency.
  - bundle trasporto-trasporto. Bundle costituita da una SA ESP (interna) in modalità trasporto senza opzione di autenticazione seguita da SA AH (esterna) in modalità trasporto

    Rispetto al caso ESP con autenticazione, ha il vantaggio che è protetto l'ESP ma anche le intestazioni originarie
  - bundle trasporto-tunnel. SA AH (interna) in modalità trasporto seguita da una SA ESP (esterna) in modalità tunnel

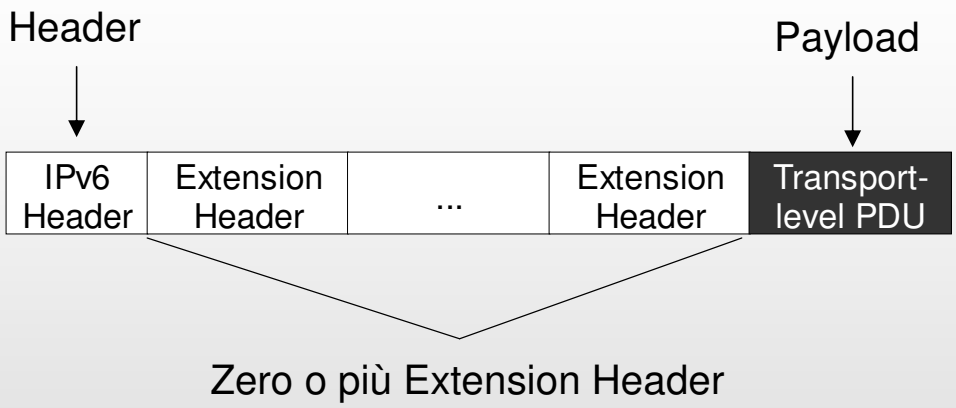
    Rispetto ai casi precedenti l'autenticazione si applica al testo in chiaro

IPSec nei...

- Sistemi Operativi
  - Unix, Windows 2000
- Router
  - Cisco, 3COM, Nortel
  - Tipicamente: canali protetti tra i router
  - Cisco supporta certificati X.509
- Firewall
  - IBM, Checkpoint

IPv6

Struttura di un pacchetto IPv6



IPv6 ed IPsec

Tipi di Extension Header:

1. Hop-by-hop options header
2. Routing header
3. Fragment header
4. Authentication Header
5. Encapsulating Payload Header
6. Destination options header

Internet Key Exchange (IKE)

Internet Key Exchange (IKE) – RFC 2409

IKE svolge le seguenti funzioni

- negoziazione dei parametri di sicurezza
- autenticazione
- scambio delle chiavi
- gestione delle chiavi (dopo lo scambio)

Suite di protocolli in IKE

IKE è costituito da tre protocolli

- SKEME
  protocollo di autenticazione basato sulla crittografia a chiave pubblica
- OAKLEY
  meccanismo di distribuzione delle chiavi basato su Diffie-Hellman
  Scelta obbligatoria per la versione iniziale di ISAKMP
- Internet Security Association and Key Management Protocol (ISAKMP)
  specifica un'architettura per lo scambio di messaggi tra IPSec peer
  compreso il formato dei pacchetti e le transizioni di stato
  UDP, port = 500

Le due fasi di IKE

- Uno dei peer genera o riceve traffico su una interfaccia configurata per iniziare una sessione di traffico IPsec
- Gli IPsec peer attivano IKE
  - IKE – PHASE 1: i peer negoziano un canale sicuro ed autentico su cui comunicare nella fase successiva
  - IKE – PHASE 2: i peer negoziano 2 SA
- I peer generano traffico IPsec

IKE Phase 1: main/aggressive mode

- IKE PHASE 1
  - funzionalità
    - negoziazione dei parametri per autenticare i due peer (e per cifrare una porzione del traffico del main mode)
    - autenticazione dei due peer l'uno rispetto all'altro
    - distribuzione di uno o più segreti da cui sono successivamente generate tutte le chiavi
  - possibili implementazioni
    - main mode, 6 messaggi
    - aggressive mode, 3 messaggi

IKE Phase 2: quick mode

- IKE PHASE 2
  - funzionalità
    - negoziazione dei parametri delle Security Associations che si stabiliscono tra i peer
  - implementazione
    - quick mode, 3 messaggi

Implementazioni di main/aggressive mode

principali implementazioni

- main mode using preshared key authentication
- main mode using digital signature authentication
- aggressive mode using preshared key authentication

ma anche

- main mode using encrypted nonces authentication
- aggressive using digital signature authentication

Protocollo Diffie-Hellman

- L'algoritmo Diffie-Hellman ha i seguenti **vantaggi**:
  - le chiavi segrete sono create solo quando necessario
  - lo scambio non richiede alcuna infrastruttura pre-esistente ad eccezione dell'accordo sui parametri globali
- L'algoritmo Diffie-Hellman ha i seguenti **svantaggi**:
  - non fornisce garanzie sull'identità dei soggetti coinvolti
  - è soggetto ad attacchi di tipo man-in-the-middle
  - è oneroso dal punto di vista computazionale

Protocollo Oakley

- Il protocollo Oakley è stato progettato per mantenere i vantaggi di Diffie-Hellman superandone le debolezze
- Il protocollo ha le seguenti caratteristiche
  - utilizza il meccanismo dei cookie per contrastare attacchi di clogging (DoS)
  - consente alle parti di negoziare un gruppo
  - utilizza i nonce per contrastare il replay
  - consente lo scambio DH di chiavi pubbliche
  - autentica lo scambio DH contrastando gli attacchi man-in-the-middle

Il problema del clogging

Denial of service

- L'algoritmo Diffie-Hellman

$$\begin{array}{|ll|}\hline A \rightarrow B: & A, g^a \bmod p \\ B \rightarrow A: & B, g^b \bmod p \\ \hline\end{array}$$

- Un avversario (Mallet) abusa dell'indirizzo di Alice ed induce Bob ad eseguire *ripetutamente* DH *saturandone* così le risorse computazionali

$$\begin{array}{|ll|}\hline A[M] \rightarrow B: & A, X \\ B \rightarrow A: & B, g^b \bmod p \\ \hline\end{array}$$

Cookie: meccanismo anti-clogging

un cookie è una quantità fresca ed imprevedibile

i calcoli sono eseguiti solo se viene ricevuto il cookie di risposta

$$A \to B: \quad cookie_A$$
$$B \to A: \quad cookie_B$$
$$A \to B: \quad A, cookie_A, cookie_B, \left(g^a \bmod p\right)$$
$$B \to A: \quad B, cookie_A, cookie_B, \left(g^b \bmod p\right)$$

un avversario può solo indurre un processo a comunicare il proprio cookie ma non ad eseguire DH

$$A[M] \to B: \quad cookie_A$$
$$B \to A: \quad cookie_B$$
$$A[M] \to B: \quad A, cookie_A, \overset{?}{cookie}_B, \left(g^a \bmod p\right)$$
$$B \to A: \quad B, cookie_A, cookie_B, \left(g^b \bmod p\right)$$

ISAKMP RFC raccomanda che un cookie sia una quantità di 8 byte cosí fatta:
cookie = h(*IP*$_{dest}$, *IP*$_{source}$, *Port*$_{dest}$, *Port*$_{source}$, *random number, time stamp*)

Main mode using preshared key auth.

Scambio chiavi basato su Diffie-Hellman

1. $A \to B: \quad c_a$
2. $B \to A: \quad c_b$
3. $A \to B: \quad c_a, c_b, X_a, N_a$
4. $B \to A: \quad c_a, c_b, X_b, N_b$
5. $A \to B: \quad c_a, c_b, \left\{A, h\left(SKEYID\_a, c_a, c_b, PSK_{ab}, prev.msg., A\right)\right\}_{SKEYID\_e}$
6. $B \to A: \quad c_a, c_b, \left\{B, h\left(SKEYID\_a, c_a, c_b, PSK_{ab}, prev.msg., B\right)\right\}_{SKEYID\_e}$

$cookie\ c_a, c_b$; pre-shared key: PSK_{ab}

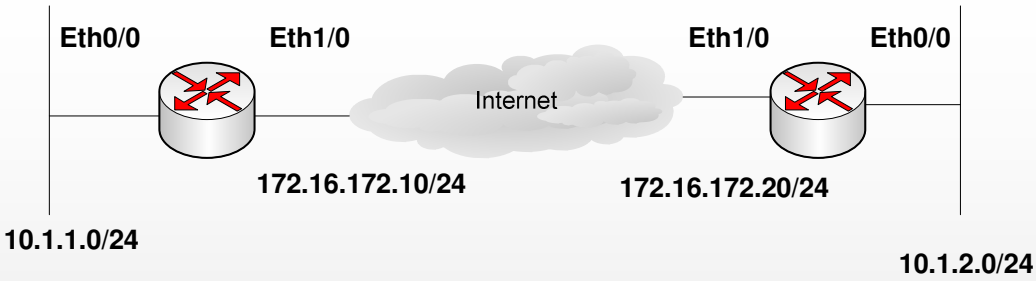
$$SKEYID = PRF\left(PSK_{ab}, N_a, N_b\right)$$
$$SKEID\_d = PRF\left(SKEYID, g^{ab}, c_a, c_b, 0\right)$$
$$SKEID\_a = PRF\left(SKEYID, SKEYID\_d, g^{ab}, c_a, c_b, 1\right)$$
$$SKEID\_e = PRF\left(SKEYID, SKEYID\_d, g^{ab}, c_a, c_b, 2\right)$$

Quick mode

Scambio chiavi basato su Diffie-Hellman

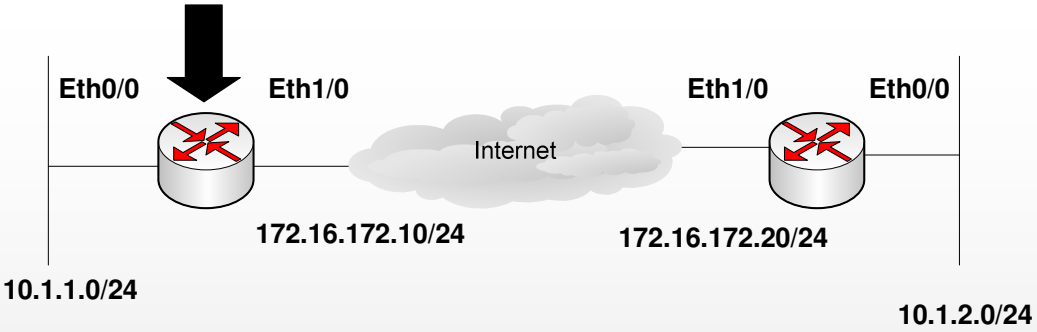
1. $A \rightarrow B: \quad c_a, c_b, \left\{ \begin{matrix} h(SKEYID\_a, 1, N'_a, X'_a, rest\ of\ msg), \\ N'_a, X'_a, A, B, rest\ of\ msg \end{matrix} \right\}_{SKEYID\_e}$
2. $B \rightarrow A: \quad c_a, c_b, \left\{ \begin{matrix} h(SKEYID\_a, 2, N'_a, N'_b, X'_b, rest\ of\ msg), \\ N'_b, X'_b, A, B, rest\ of\ msg \end{matrix} \right\}_{SKEYID\_e}$
3. $A \rightarrow B: \quad c_a, c_b, \{h(SKEYID\_a, 3, N'_a, N'_b)\}_{SKEYID\_e}$

Example: LAN-to-LAN VPN



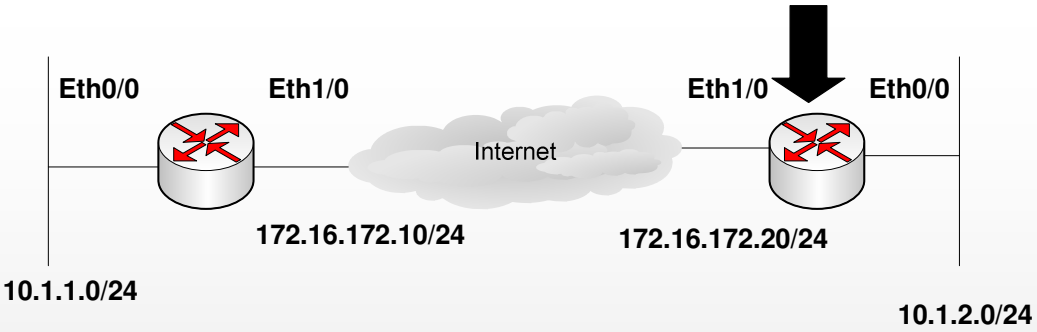
- Authentication method: ***preshared keys***

Example: *configuration of router* 1



1. ISAKMP policy: **(3des, sha, pre-shared key)**
2. Security association: **(tunnel mode, esp-3des esp-md5-hmac)**
3. IpSec peer: **address = 172.16.172.20**
4. Pre-shared key: **key = jw4ep9846804ijl; address = 172.16.172.20**
5. Security policy: **permit ip 10.1.1.0/24 10.1.2.0/24**

Example: *configuration of router* 2



1. ISAKMP policy: **(3des, sha, pre-shared key)**
2. Security Association: **(tunnel mode, esp-3des esp-md5-hmac)**
3. IpSec peer: **address = 172.16.172.10**
4. Pre-shared key: **key = jw4ep9846804ijl; address = 172.16.172.10**
5. Security policy: **permit ip 10.1.2.0/24 10.1.1.0/24**