



UNIVERSITA' DEGLI STUDI DI PARMA  
Dipartimento di Ingegneria dell'Informazione

## Security Protocols: IPSec

Luca Veltri

(mail.to: luca.veltri@unipr.it)

Corso di Sicurezza nelle reti di telecomunicazioni, a.a. 2006/2007

<http://www.tlc.unipr.it/veltri>



Università degli Studi di Parma  
Dipartimento di Ingegneria dell'Informazione

IPSec

### Introduzione ad IPSec (1/2)

- IPSec rappresenta un'architettura aperta definita dall'IPSec Working Group dell'IETF (RFC 2401) come framework per garantire la security al network layer e/o ai protocolli di livello superiore dello stack TCP/IP
- Fornisce una serie di funzionalità (Security Services) orientate a garantire la Sicurezza su traffico di tipo IP
- Il supporto di IPSec è raccomandato per IPv4, mandatorio per IPv6
- IPSec può essere utilizzato per proteggere uno o più percorsi tra coppie di host, di router o coppie miste host/router, o VPN (Virtual Private Network)
  - può essere implementato sia su un host che su un router (security gateway)

2



Università degli Studi di Parma  
Dipartimento di Ingegneria dell'Informazione

IPSec

### Introduzione ad IPSec (2/2)

- Gli standard IPSec specificano separatamente:
  - L'architettura di base ed i suoi componenti: **Security Services**, **Security Association**
  - Security protocols: **Authentication Header (AH)**, **Encapsulation Security Payload (ESP)**
  - Key Management (Internet Key Management, IKE o ISAKMP/OAKLEY): protocolli per la **negoiazione dei Security protocols**, degli **algoritmi di encryption** e per lo scambio delle chiavi
  - Algoritmi per l'authentication e l'encryption: possibilità di utilizzare algoritmi diversi, più o meno potenti; apertura verso nuovi e futuri algoritmi

3



Università degli Studi di Parma  
Dipartimento di Ingegneria dell'Informazione

IPSec

### Caratteristiche generali

- L'implementazione di IPSec può avvenire:
  - IP stack
    - mediante modifica del codice sorgente IP
  - Bump-in-the-stack
    - strato IP inalterato; IPSec viene implementato nello stack tra il protocollo IP ed il local network driver
  - Bump-in-the-wire
    - viene impiegata una scheda con crypto processor separata
- IPSec permette di offrire sicurezza della comunicazione in modo trasparente
  - trasparenza rispetto ai nodi intermedi ai nodi IPSec
  - trasparenza rispetto alle applicazioni e ai protocolli di trasporto
    - molto utile in presenza di applicazioni legacy
    - servizio offerto contemporaneamente a tutte le applicazioni
  - trasparenza rispetto ai nodi terminali, nel caso IPSec sia router-to-router o router-to-host
    - molto utile in presenza di nodi legacy
    - 1 nodo IPSec può proteggere contemporaneamente più host terminali

4

## I Security Services offerti da IPSec

- Data Origin Authentication
  - **verifica l'autenticità del mittente di ciascun datagramma IP**
- Data integrity
  - **verifica che il contenuto di ciascun datagramma non sia stato modificato (deliberatamente o a causa di errori di linea) durante il transito tra sorgente e destinazione**
- Data confidentiality
  - **nasconde il testo in chiaro contenuto in un messaggio mediante l'impiego della crittografia**
- Replay protection
  - **assicura che se venga intercettato un datagramma IP, non sia possibile a posteriori rispedirlo a destinazione per qualche scopo illecito**

5

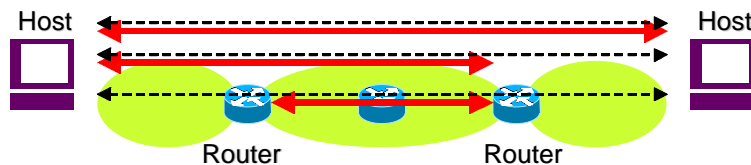
## Principali protocolli

- IP Authentication Header (AH)
  - **protocollo utilizzato per lo scambio di dati tra sorgente e destinazione che fornisce:**
    - data origin authentication
    - data integrity
    - opzionalmente replay protection
- IP Encapsulating Security Payload (ESP)
  - **protocollo utilizzato per lo scambio di dati tra sorgente e destinazione che fornisce:**
    - data confidentiality
    - opzionalmente data origin authentication, data integrity e replay protection
- Internet Key Exchange/Internet Security Association and Key Management Protocol (IKE/ISAKMP)
  - **meccanismo di scambio di messaggi di controllo/configurazione tra nodi IPSec che permette di:**
    - instaurare automaticamente connessioni IPSec (SA) tra sorgente e destinazione
    - gestire le chiavi di crittografia associate

6

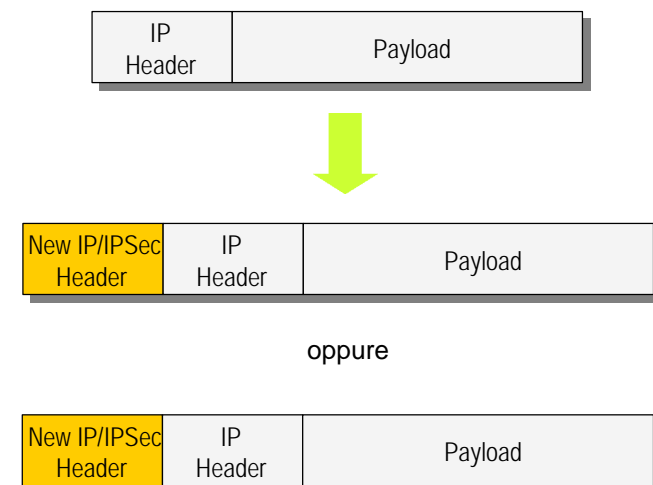
## IPSec

- IPSec (AH ed ESP) può essere impiegato per creare comunicazioni "sicure" di tipo
  - **host-to-host**
    - scenario end-to-end, in alternativa a soluzioni a livello applicativo/trasporto
  - **host-to-router**
    - scenario host-to-network, spesso riferito come "road-warrior"
  - **router-to-router**
    - scenario network-to-network, spesso riferito come VPN/IPSec



7

## IPSec basics: Tunneling



8

## Security Association (SA)

- Le SA sono essenziali in IPSec, sia con AH che ESP
- Una SA identifica univocamente tutti i parametri necessari per una comunicazione sicura fra due parti qualsiasi
  - identità dei partecipanti, tipo di protocollo (AH, ESP), algoritmi di crittografia ed autenticazione utilizzati, etc.
- Rappresenta una connessione logica unidirezionale (simplex) tra due sistemi IPSec
  - nel caso di comunicazione bidirezionale è necessario instaurare almeno due SA



9

## Security Association (SA)

- Una SA è identificata da 3 parametri:
  - SPI (Security Parameter Index)
  - IP address di destinazione
  - Sec protocol (AH, ESP)
- Una SA è caratterizzata dai seguenti parametri:
  - AH info (algo, IV, keys)
  - ESP info (algorithms, IV, keys)
  - IPSec mode
  - sequence number
  - anti-replay window
  - lifetime
  - max MTU
- E' stato standardizzato un protocollo di creazione e gestione delle SA detto Internet Security Association and Key Management Protocol (ISAKMP)

10

## Authentication Header (AH)

## Authentication Header

- L'Authentication Header fornisce l'integrità e l'autenticazione dei datagrammi IP
  - Si ottiene calcolando una funzione hash sul datagramma IP ed usando una chiave segreta di autenticazione
- Le informazioni di autenticazione sono calcolate utilizzando tutti i campi del datagramma IP che non cambiano durante il trasporto (o che cambino in maniera prevedibile)
- Due modalità di impiego: Transport Mode e Tunnel Mode
  - La modalità "Tunnel" protegge l'IP header originale mascherando gli indirizzi IP di sorgente e di destinazione

12

## AH: Security Services offerti

- Data integrity
  - viene assicurata in maniera connectionless (pacchetto per pacchetto) generando un Integrity Check Value che protegge l'intero datagramma IP eccetto alcuni campi mutevoli dell'header
- Data origin authentication
  - viene garantita firmando in maniera digitale l'Integrity Check Value
- Replay protection
  - è opzionale ed è realizzata impiegando un campo sequence number nell'header del pacchetto AH
- Nella terminologia IPSec le tre distinte funzioni vengono comunemente riferite con il termine "Authentication"
- Osservazione:
  - la mancanza di confidenzialità consente anche l'uso di IPSec su Internet anche nei paesi dove l'esportazione, l'importazione o l'uso della crittografia è regolato da leggi restrittive

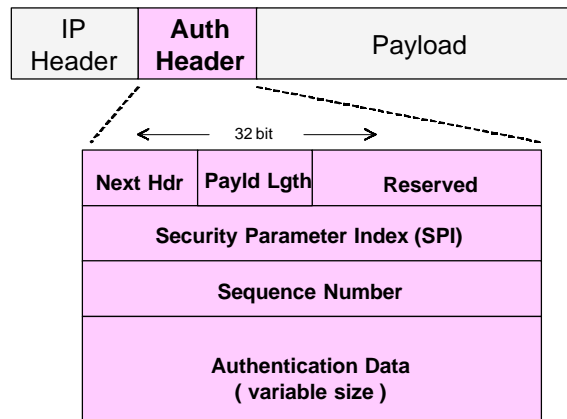
13

## Informazione protetta da AH

- AH protegge anche tutti i campi dell'intestazione IP immutabili o mutabili in maniera prevedibile
- Immutable IP header fields (IPv4):
  - Version
  - Internet Header Length
  - Total Length
  - Identification
  - Protocol (This should be the value for AH.)
  - Source Address
  - Destination Address (without loose or strict source routing)
- Mutable but predictable IP header fields (IPv4):
  - Destination Address (with loose or strict source routing)
- Mutable IP header fields (IPv4) - zeroed prior to ICV calculation of AH:
  - Type of Service (TOS)
  - Flags
  - Fragment Offset
  - Time to Live (TTL)
  - Header Checksum

14

## Authentication Header



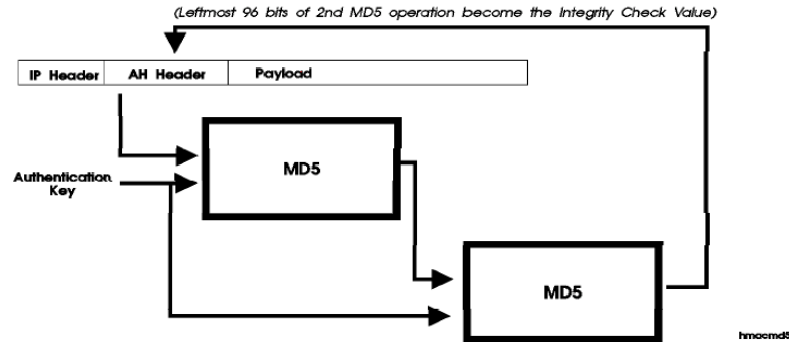
15

## Descrizione del AH

- Next header
  - indica il tipo di protocollo trasportato nel campo payload
- Payload length
  - campo di 8 bit che specifica la lunghezza del pacchetto AH in 32 bit word, meno due (compatibilità vecchia specifica di AH)  
e.g. se authentication data = HMAC-md5-96, allora PL= 3+3-2=4
- Reserved
  - campo riservato per scopi futuri ed attualmente riempito di zeri
- Security Parameter Index (SPI)
  - identificativo numerico a 32 bit che identifica una SA e tutti i suoi attributi (security protocol, algoritmi utilizzati, le chiavi e la durata di validità delle chiavi)
- Sequence number
  - contatore che viene incrementato ogni volta che un pacchetto viene spedito alla medesima destinazione usando la stessa SA
- Authentication data
  - contiene un Integrity Check Value (ICV) calcolato sulla parte rimanente del pacchetto e sulla parte fissa dell'header del datagramma IP (header originale/transport mode o nuovo header/tunnel mode)
  - può includere un padding per riportare la lunghezza dell'header del pacchetto AH ad un multiplo intero di 32 bit (IPv4) o 64 bit (IPv6)

16

## Generazione dell'ICV (esempio HMAC-MD5)



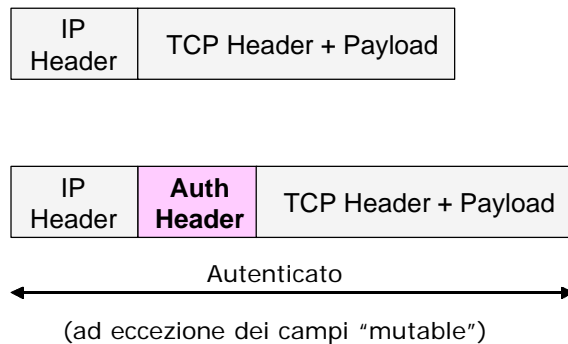
17

## AH - Transport Mode

- viene mantenuto l'header del datagramma IP originale, seguito dall'AH header e dal payload originale
- l'intero datagramma IP, eccetto alcuni campi dell'header, viene autenticato
- qualsiasi modifica al contenuto del datagramma, eccetto quelle che avvengono nei campi mutevoli dell'header IP, viene rilevata
- le informazioni vengono trasportate dal datagramma in chiaro

18

## AH - Transport Mode



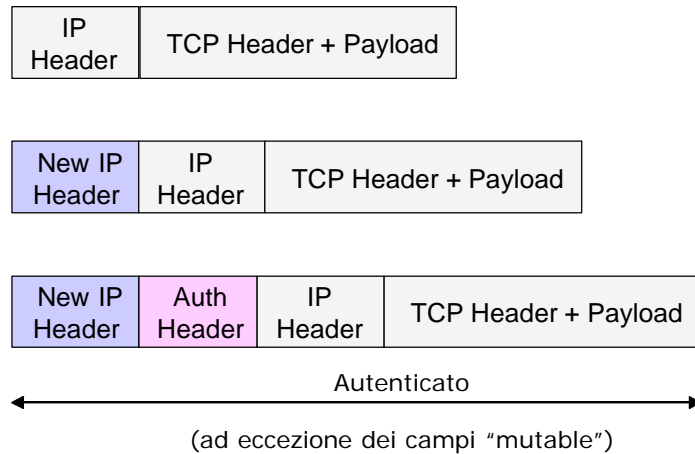
19

## AH - Tunnel Mode

- viene utilizzato un nuovo header IP con Source e Destination address in genere differenti da quelli originari (tipicamente gli indirizzi dei security gateway)
- il nuovo header è seguito dall'AH header e dall'intero datagramma IP originale
- l'intero nuovo datagramma IP, eccetto alcuni campi del nuovo header, viene autenticato
- qualsiasi modifica al contenuto del nuovo datagramma, eccetto quelle che avvengono nei campi mutevoli dell'header IP, viene rilevata
- le informazioni vengono trasportate dal datagramma in chiaro

20

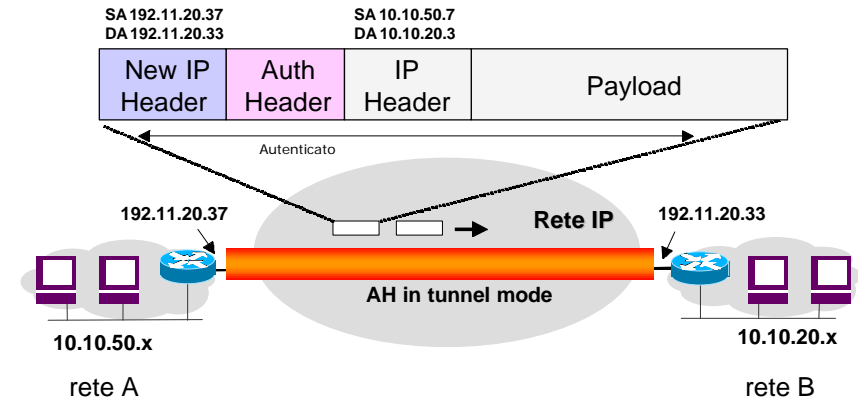
## AH - Tunnel Mode



21

## AH- Tunnel Mode: Esempio

- AH in tunnel mode
- Due gateway autenticano tutto il traffico trasportato



22

## Encapsulating Security Payload (ESP)

## Encapsulating Security Payload

- Non è specificato un particolare algoritmo di cifratura
- Due modalità di impiego: Transport mode e Tunnel Mode
- La modalità "Tunnel" protegge l'IP header originale mascherando gli indirizzi IP di sorgente e di destinazione

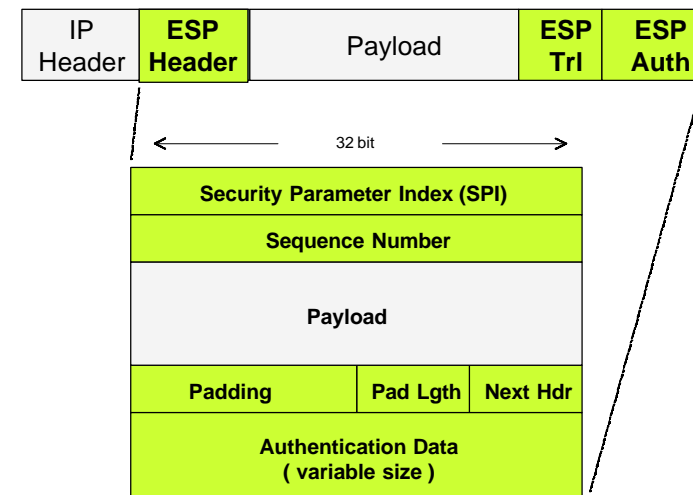
24

## ESP: Security Services offerti

- **data confidentiality**: viene assicurata mediante meccanismi di encryption/decryption dei dati trasmessi, avvalendosi dell'impiego di una chiave simmetrica utilizzata da entrambi gli attori della comunicazione
- **data integrity**: è opzionale, come in AH viene assicurata in maniera connectionless (pacchetto per pacchetto) generando un Integrity Check Value, ma copre una porzione differente del datagramma IP
- **data origin authentication**: è opzionale, come in AH viene garantita firmando in maniera digitale l'Integrity Check Value
- **replay protection**: è opzionale ed utilizza un sequence number

25

## Encapsulating Security Payload



26

## Formato del pacchetto ESP

- Security Parameter Index (SPI)
  - identificativo numerico a 32 bit che identifica una SA e tutti i suoi attributi (security protocol, algoritmi utilizzati, le chiavi e la durata di validità delle chiavi)
- Sequence number
  - contatore che viene incrementato ogni volta che un pacchetto viene spedito alla medesima destinazione usando la stessa SA
- Payload data
  - rappresenta l'area destinata al trasporto dei dati (protocollo di livello superiore/transport mode o datagramma IP/tunnel mode)
- Padding
  - (0-255 bytes) riempimento di lunghezza variabile necessario ad alcuni algoritmi che richiedono che i dati da criptare abbiano una lunghezza multipla di un valore fissato
- Pad length
  - indica la lunghezza del campo riempimento
- Next header
  - indica il tipo di protocollo trasportato nel campo payload
- Authentication data
  - campo opzionale che contiene un Integrity Check Value (ICV) calcolato sulla rimanente parte del pacchetto ESP dopo che lo stesso è stato criptato
  - la lunghezza varia a seconda dell'algoritmo di autenticazione utilizzato

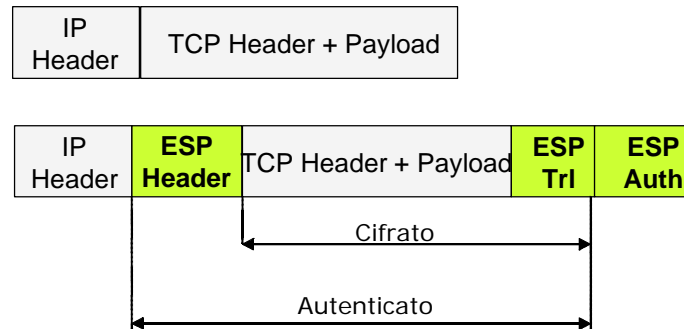
27

## ESP - Transport Mode

- viene mantenuto l'header del datagramma IP originale, seguito dall'ESP Header, dal Payload originale, l'ESP Trailer e l'ESP Auth
- vengono crittati esclusivamente il Payload del datagramma IP originale e l'ESP Trailer
- vengono autenticati l'ESP Header, l'IP Payload e l'ESP Trailer
- l'header IP non viene né crittato né autenticato, gli indirizzi IP sorgente e destinazione originali restano in chiaro nel transito e visibili da un eventuale hacker

28

## ESP - Transport Mode



**Nota:** in modalità Trasporto l'header IP originario non è cifrato né autenticato

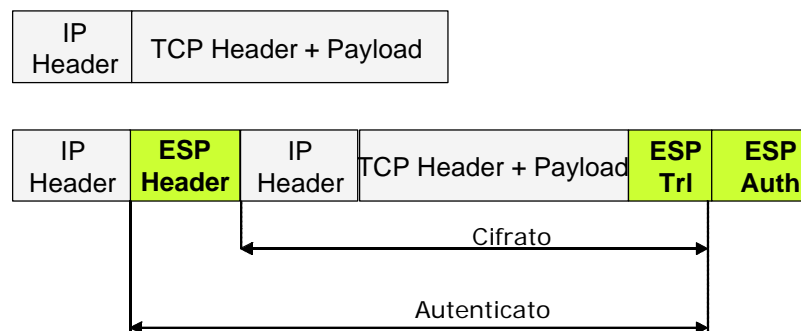
29

## ESP - Tunnel Mode

- viene utilizzato un nuovo Header IP con Source e Destination address in genere differenti da quelli originali
- l'intero datagramma IP originale (IP Header ed IP Payload) e l'ESP Trailer vengono crittati
- l'autenticazione viene applicata all'ESP Header, all'intero datagramma IP originale e all'ESP Trailer
- Un tipico impiego di ESP in tunnel mode è quello di nascondere gli indirizzi IP sorgente e destinazione originali realizzando un tunnel tra una coppia di security gateway (firewall/router)

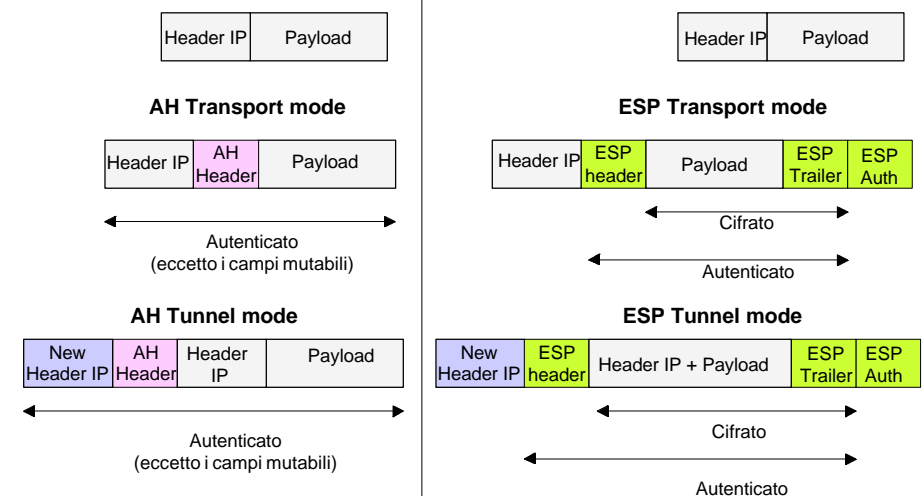
30

## ESP - Tunnel Mode



31

## AH ed ESP: riepilogo



32

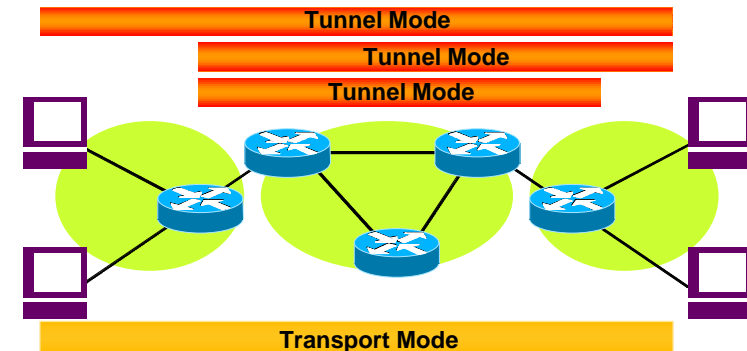


## Transport & Tunnel Mode (1/3)

- Transport mode:
  - fornisce protezione ai protocolli di livello superiore a IP
  - è impiegato tra i due end point di una comunicazione fornendo quindi una protezione da estremo a estremo lungo l'intero percorso
- Tunnel mode:
  - fornisce protezione a livello IP (tunneling IP) e ai protocolli di livello superiore
  - è normalmente impiegato tra due macchine di cui almeno una non rappresenta l'end point della connessione (firewall to firewall, client to firewall) fornendo quindi una protezione su di un singolo segmento del percorso

33

## Transport & Tunnel Mode (2/3)



- Il transport mode può essere impiegato soltanto quando sia la sorgente che la destinazione implementano IPSec
- Comunemente IPSec viene utilizzato in tunnel mode tra router intermedi in quanto non richiede modifiche al OS o alle applicazioni sui nodi terminali

34

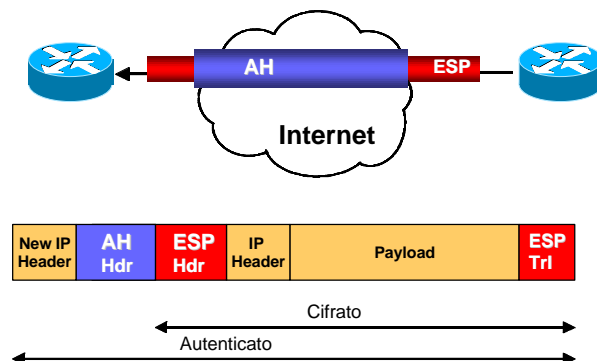
## Transport & Tunnel Mode (3/3)

- E' possibile combinare le due modalità utilizzando ricorsivamente più istanze del medesimo protocollo (AH o ESP) o combinazioni dei due
  - adiacenze di trasporto
  - tunnel iterato
- Tramite combinazioni delle due modalità e dei due protocolli (AH e ESP) è possibile selezionare maggiormente il livello di granularità offerto dai Security Services, esempi:
  - adiacenze di trasporto AH e ESP:
    - (end-to-end) per autenticare anche header IP
  - transport-tunnel:
    - singolo tunnel AH per trasportare il traffico tra una coppia di security gateway
    - ESP transport per crittare il traffico di ciascuna connessione TCP tra coppie di host separati dai security gateway

35

## Transport & Tunnel Mode: esempio

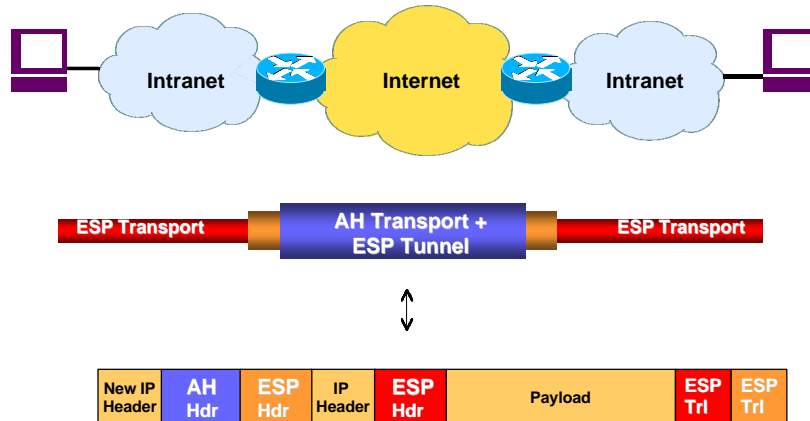
- AH ed ESP possono essere combinati in vari modi
  - Es: ESP in Tunnel Mode + AH in Transport mode



36

## Transport & Tunnel Mode: esempio

- Esempio End-to-End



37

## IPSec e la crittografia

- IPSec implementa lo stato dell'arte della crittografia avvalendosi dei comuni algoritmi standard
- Rimane aperto a futuri sviluppi
- Ciascun algoritmo è impiegato nell'ambito più opportuno
  - Crittatura simmetrica a chiave segreta per il data bulk
  - Crittatura a chiave pubblica (RSA) per lo scambio della chiave di sessione
  - Diffie-Hellmann per la generazione di chiavi di sessione
  - Trasformazioni Hash

38

## Distribuzione delle chiavi

- In generale per una comunicazione bidirezionale tra due nodi sono necessarie 4 chiavi segrete
  - **AH e ESP in entrambe le direzioni**
- La negoziazione e la distribuzione delle chiavi può essere effettuata attraverso due modalità:
  - **distribuzione manuale delle chiavi**
    - soluzione non scalabile
  - **distribuzione automatica delle chiavi**
    - tramite protocollo ISAKMP/IKE

39

## Problemi con IPSec

- L'impiego di funzionalità di NAT (Network Address Translation) è incompatibile con l'utilizzo del protocollo AH in quanto sostituendo l'indirizzo IP il datagramma non verrebbe più autenticato
- L'impiego di firewall di tipo packet filtering tradizionali (stateless/stateful inspection) è incompatibile con l'utilizzo del protocollo ESP:
  - **ESP nella modalità transport mode critta il payload del datagramma IP rendendo impossibile un controllo di tipo stateful**
  - **ESP nella modalità tunnel mode critta l'intero datagramma IP rendendo impossibile un controllo di tipo stateful o stateless**

40

## IKE ISAKMP/OAKLEY Protocols

- IPSec necessita la realizzazione tra gli end-point di una Security Association (SA):
  - una SA contiene tutte le informazioni per l'elaborazione del traffico IPSec:
    - l'algoritmo di cifratura
    - l'algoritmo di autenticazione
    - chiavi
    - etc.
- IKE (RFC 2409) è un meccanismo per la negoziazione negoziazione/creazione automatica di una SA tra 2 nodi IPsec
  - **permette la creazione delle chiavi e di altro materiale di crittografico in modo protetto**
  - **definisce le modalità di utilizzo e gestione delle stesse**
- IKE deriva dalla congiunzione 2 protocolli ISAKMP e Oakley

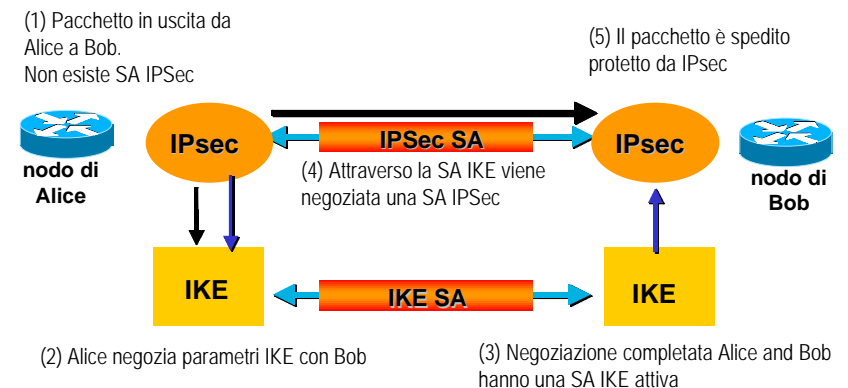
42

## IKE: ISAKMP/Oakley

- ISAKMP (Internet Security Association Key Management Protocol) è il protocollo di instaurazione della SA e di creazione delle chiavi
  - **negoziare la SA e definizione dei meccanismi di sicurezza**
  - **generazione iniziale di tutte le master key necessarie alla generazione delle chiavi di encryption**
  - **supporto allo scambio di messaggi per un successivo refresh delle chiavi**
- Oakley è l'algoritmo di scambio delle chiavi utilizzato all'interno di ISAKMP
  - **è un raffinamento di Diffie-Hellman**
- L'impiego di ISAKMP/ Oakley rende automatiche o semiautomatiche tutte le operazioni di bootstrap consentendo la realizzazione di VPN scalabili

43

## IKE: modello



- Periodicamente le SA vengono rinegoziate per modificare le chiavi
- La rinegoziazione comincia poco prima che scadano le SA attualmente in vigore

44

## IKE: Phase 1 and Phase 2

- IKE/ISAKMP coinvolge due o più end point system di una SA in fase di instaurazione secondo un approccio strutturato in due fasi:
  - **Phase I:** avviene la negoziazione di una “master secret” dalla quale dovranno successivamente (Phase II) essere derivate le chiavi per proteggere il traffico IP. Vengono stabilite una ISAKMP SA e le chiavi per proteggere i messaggi ISAKMP scambiati nella Phase II
    - Poiché la comunicazione in questa fase avviene su connessioni ancora insicure, per lo scambio di messaggi si fa utilizzo di crittografia a chiave pubblica
  - **Phase II:** avviene la negoziazione della SA e delle chiavi necessarie alla protezione del traffico di dati (IPSec o altro protocollo)
    - La negoziazione avviene per mezzo di messaggi ISAKMP protetti dalla SA generata nella Phase I
    - entrambe le parti possono iniziare la negoziazione (la ISAKMP SA è bidirezionale)

45

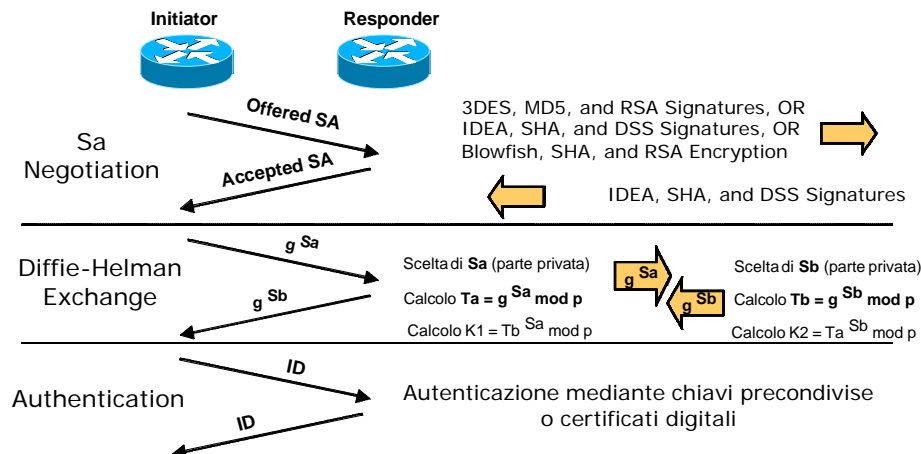
## IKE: Phase 1 and Phase 2

- Phase I:
  - richiede il computo di un maggior numero di operazioni crittografiche e quindi un maggior onere in termini di carico di CPU in quanto deve essere scambiata una “master secret” in maniera sicura su link potenzialmente insicuri
  - supporta successive e multiple istanze della Phase II e quindi viene eseguita non di frequente (1 volta al giorno o alla settimana)
- Phase II:
  - richiede uno sforzo computazionale inferiore
  - a seguito di una unica Phase I, più sessioni di Phase II possono essere attivate (ottimizzazione)
  - è impiegata di frequente (ogni due/tre minuti) per effettuare il refresh delle chiavi crittografiche

46

### IKE Fase 1

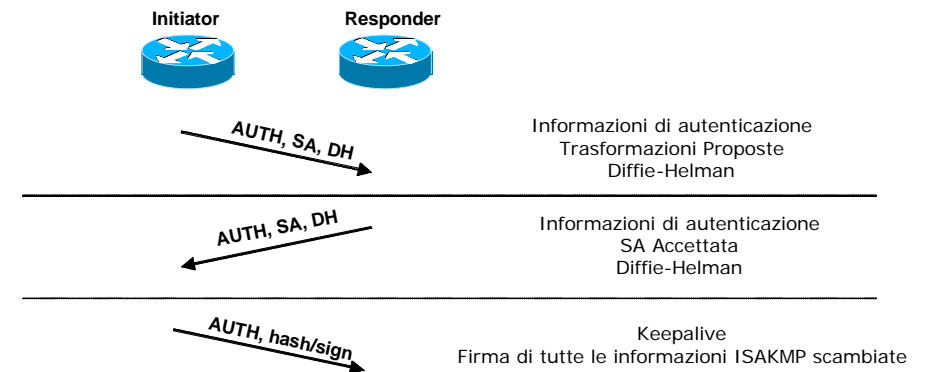
- Lo scopo della Fase 1 è creare una ISAKMP SA che protegga i messaggi ISAKMP della successiva fase 2



47

### IKE Fase 2

- Lo scopo della Fase 2 è creare una IPSEC SA che protegga il flusso dei dati



48