IPsec

Sicurezza del livello Rete

Riservatezza a livello Rete

Includere la riservatezza al livello rete, si intende che tra due entità di rete (due router, un host e un router ecc):

- Il mittente cripta i dati contenuti nella parte payload del pacchetto. Il payload potrebbe contenere:
  - Un segmento TCP o UDP,
  - un messaggio ICMP,
  - un pacchetto di aggiornamento delle tabelle di instradamento (messaggi OSPF, …)
- Tutti i dati scambiati dovrebbero essere nascosti:
  - Pagine web, e-mail, trasferimenti di file P2P, pacchetti SYN …
- "si realizza una copertura completa"

Requisiti di sicurezza a livello Rete

Oltre alla riservatezza, un **protocollo di rete** sicuro potrebbe anche fornire altri servizi:

- L'autenticazione del mittente, per consentire al ricevitore di verificare la sorgente dei pacchetti criptati.
- L'integrità dei dati, in modo che l'entità destinataria possa controllare che non si tratti di pacchetti falsificati o modificati durante il percorso.
- Protezione contro l'attacco di ripetizione, e consentire al ricevitore di accorgersi se il pacchetto ricevuto è un duplicato.
- IPsec soddisfa tutti questi requisiti: riservatezza, autenticazione del mittente, integrità dei dati, e protezione contro l'attacco di ripetizione.

Virtual Private Network (VPN)

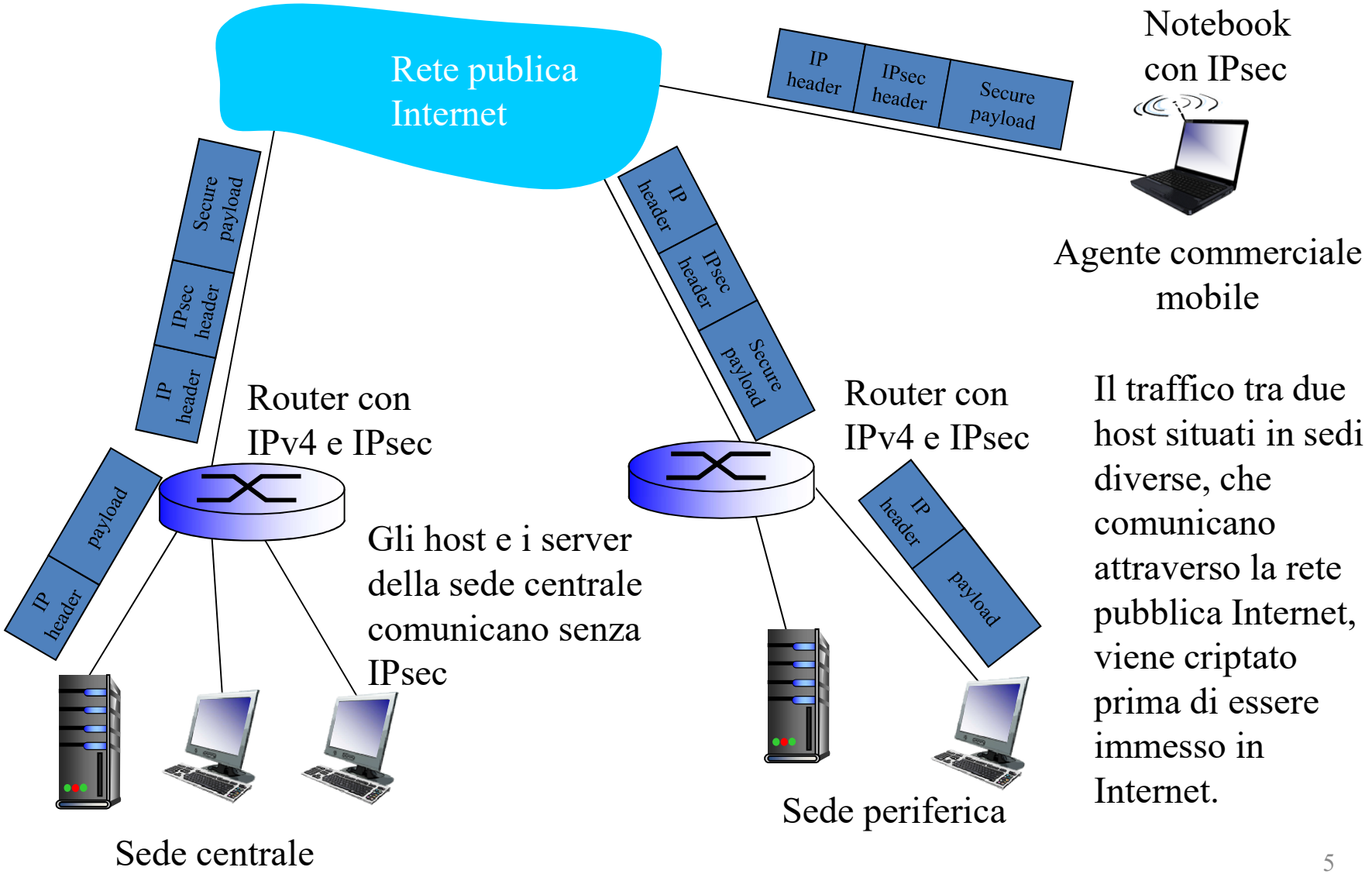
Per garantire la sicurezza, le organizzazioni preferirebbero disporre di una rete privata. I costi di questa soluzione sono:

- Amministrare i propri router,
- Acquistare canali,
- Configurare i servizi (DNS, DHCP, …).

Con una VPN il traffico delle organizzazioni sfrutta la rete pubblica:

- Viene criptato prima di accedere alla rete pubblica
- Risulta logicamente separato dal restante traffico

Virtual Private Network (VPN)



Il traffico tra due host situati in sedi diverse, che comunicano attraverso la rete pubblica Internet, viene criptato prima di essere immesso in Internet.

IPsec

Sommariamente, il funzionamento di IPsec può essere così riassunto:

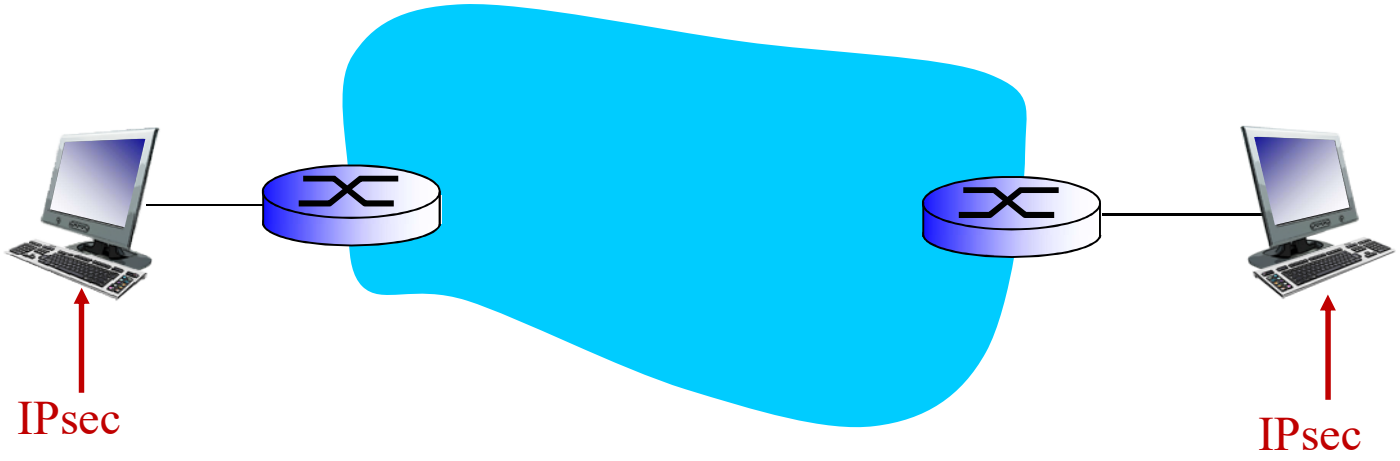
- Quando un host della sede centrale, invia un pacchetto IP a un collaboratore aziendale esterno, che si trova ad esempio presso un cliente, il router di frontiera converte il datagramma IPv4 in un datagramma IPsec e spedisce questo datagramma IPsec in Internet.
- Il datagramma in formato IPsec possiede la normale intestazione IPv4, affinché i router di Internet, che lo ricevono possano elaborarlo come se fosse un normale datagramma IPv4. Infatti i router non leggono la parte payload, dove è contenuta l'header IPsec;
- Inoltre la sezione payload del datagramma IPsec è criptata.
- Quando il datagramma IPsec arriva al notebook dell'agente commerciale estero, il sistema operativo del notebook decripta il payload (e fornisce i servizi di sicurezza quali la verifica dell'integrità dei dati) e consegna il payload decriptato al protocollo del livello superiore (TCP o UDP).

Servizi IPsec

- Integrità dei dati
- Autenticazione dell'origine
- Protezione contro l'attacco di ripetizione
- riservatezza

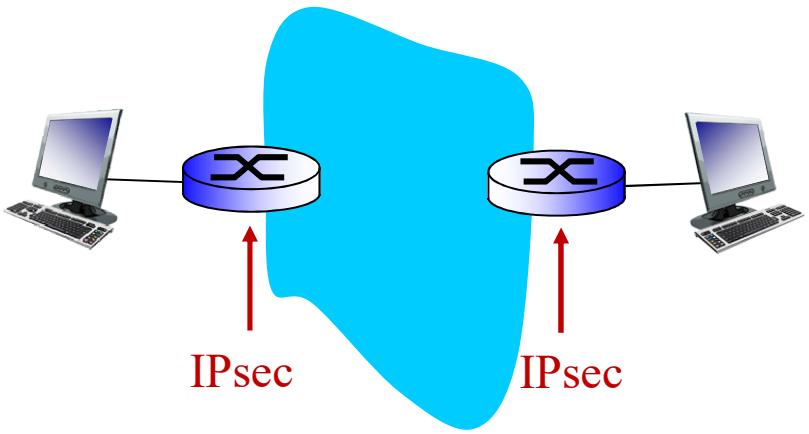
- Il protocollo fornisce due differenti modelli di servizio:
  - AH (Authentication Header)
  - ESP (Encapsulation Security Payload)

IPsec transport mode

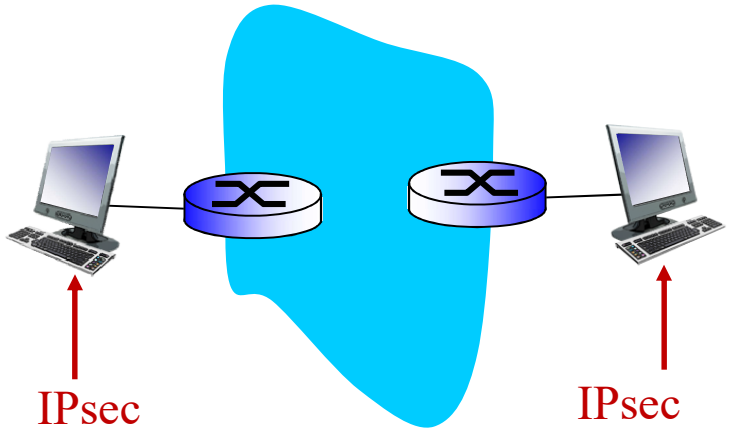


- I datagrammi IPsec sono trasmessi e ricevuti dai sistemi terminali
- IPsec protegge i protocolli dei livelli superiori

IPsec tunneling mode



- I router di frontiera riconoscono il formato IPsec



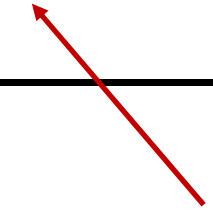
- Gli host riconoscono il formato IPsec

Protocolli IPsec

- Authentication Header (AH)
  - Fornisce l'autenticazione del mittente e l'integrità dei dati ma non la riservatezza
- Encapsulation Security Protocol (ESP)
  - Fornisce l'autenticazione del mittente, l'integrità dei dati e la riservatezza
  - È preferito ad AH

Ci sono quattro possibilità

Host mode con AH	Host mode con ESP
Tunnel mode con AH	Tunnel mode con ESP



Più importante e utilizzato

Security association (SA)

- Prima di trasmettere dati, è necessario stabilire una "security association (SA)" tra l'entità mittente e quella ricevente
  - le SA sono simplex: valgono in una sola direzione
- Le entità mantengono *l'informazione* di stato della SA
  - Anche i processi TCP mantengono informazioni di stato
  - Il protocollo IP non mantiene la connessione; IPsec è orientato alla connessione

Security association (SA)

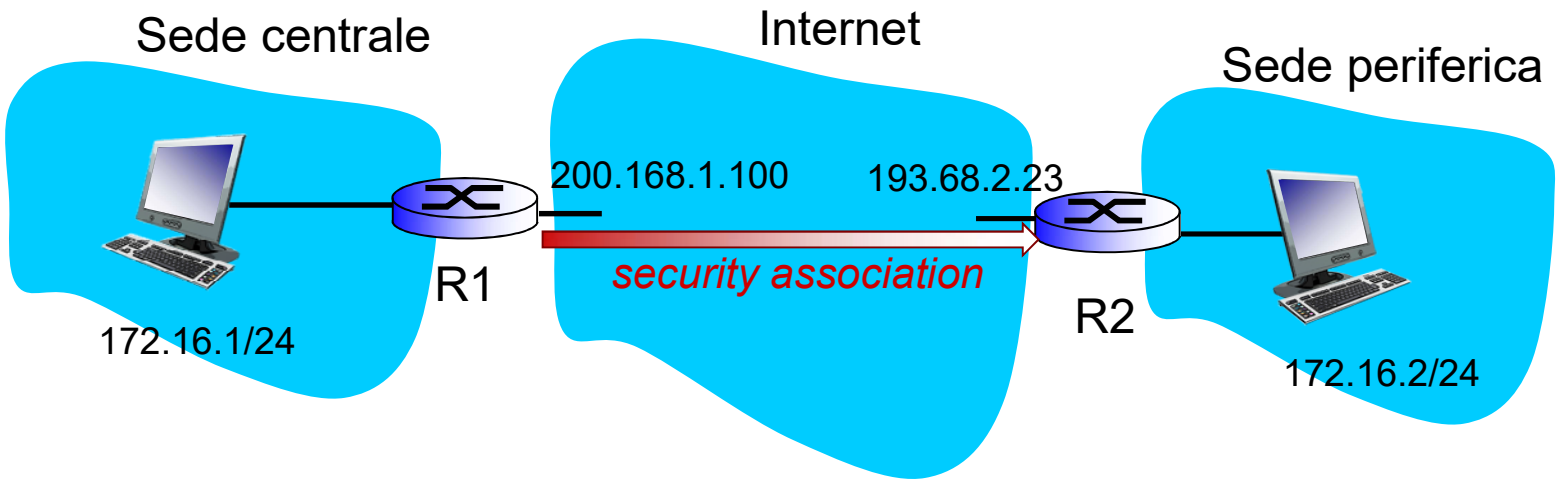
Si supponga che la rete aziendale abbia una sede centrale, una sede periferica e n agenti esterni mobili. Esiste un traffico IPsec bidirezionale tra la sede centrale e la periferica, ed altro traffico IPsec bidirezionale tra la sede centrale e gli agenti mobili.

Quante SA sono richieste nella VPN con sede centrale, sede periferica e agente esterno?

- Ci sono due SA tra il router di frontiera della sede centrale e il router di frontiera della sede periferica (una in ogni direzione);
- Ci sono due SA tra il router di frontiera della sede centrale e il notebook di un agente esterno.
- Quindi in totale ci sono $(2 + 2n)$ *SA*.

Non tutto il traffico inviato su Internet da un router di frontiera o dai notebook è IPsec. Ad esempio quando si chiede una pagina web.

Esempio SA da R1 a R2



R1 mantiene le informazioni di stato nella SA:

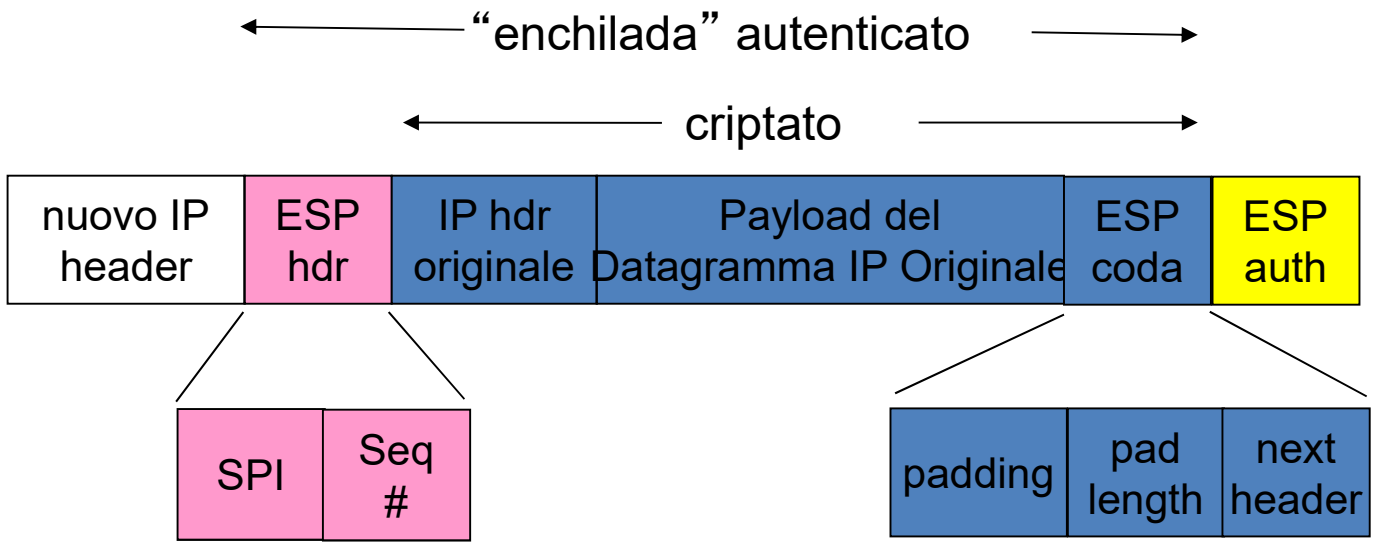
- Un identificatore di SA di 32 bit: *Security Parameter Index (SPI)*
- L'interfaccia di origine della SA (200.168.1.100)
- L'interfaccia di destinazione della SA (193.68.2.23)
- Il tipo di criptografia usata (esempio: 3DES con CBC)
- Chiave di criptografia
- Tipo di calcolo dell'integrità dei dati usato (es. HMAC con MD5)
- Chiave di autenticazione

Security Association Database (SAD)

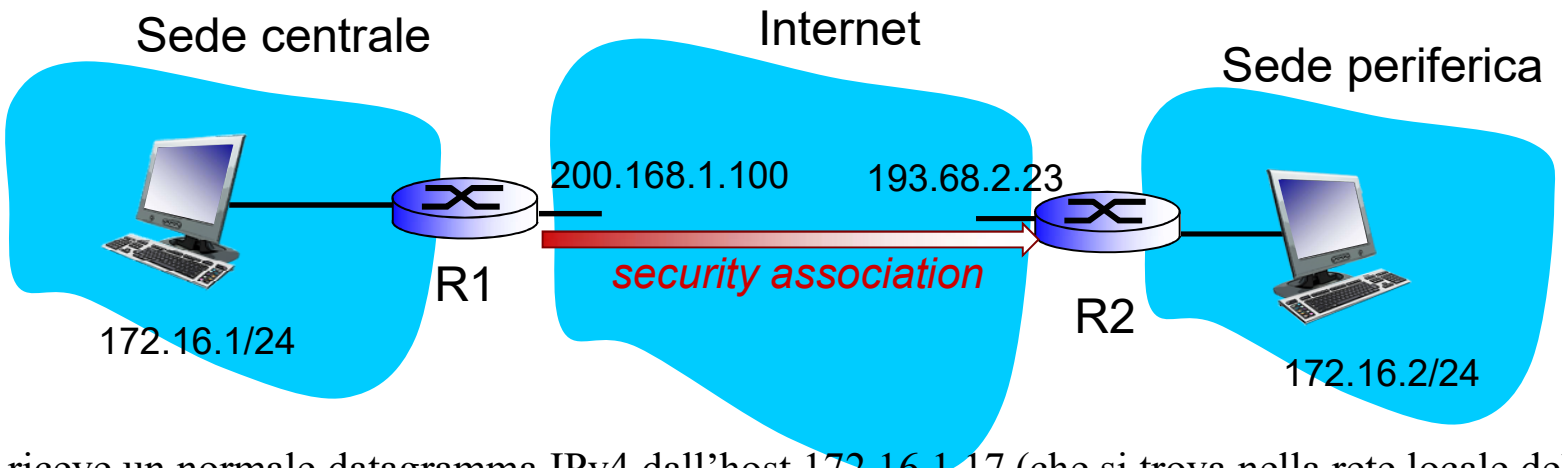
- Le informazioni di stato delle SA, in un lato della connessione, sono tenute nel *security association database (SAD)*, dal quale sono lette per essere elaborate.
- con n agenti mobili, ci sono 2+2n SA nel SAD di R1
- quando deve trasmettere un datagramma IPsec, R1 accede al SAD per determinare come elaborare il datagramma.
- quando il datagramma Ipsec arriva a R2, R2 esamina l'SPI contenuto nel datagramma IPsec, e lo usa come chiave di accesso al SAD, ed elabora il datagramma.

IPsec datagram

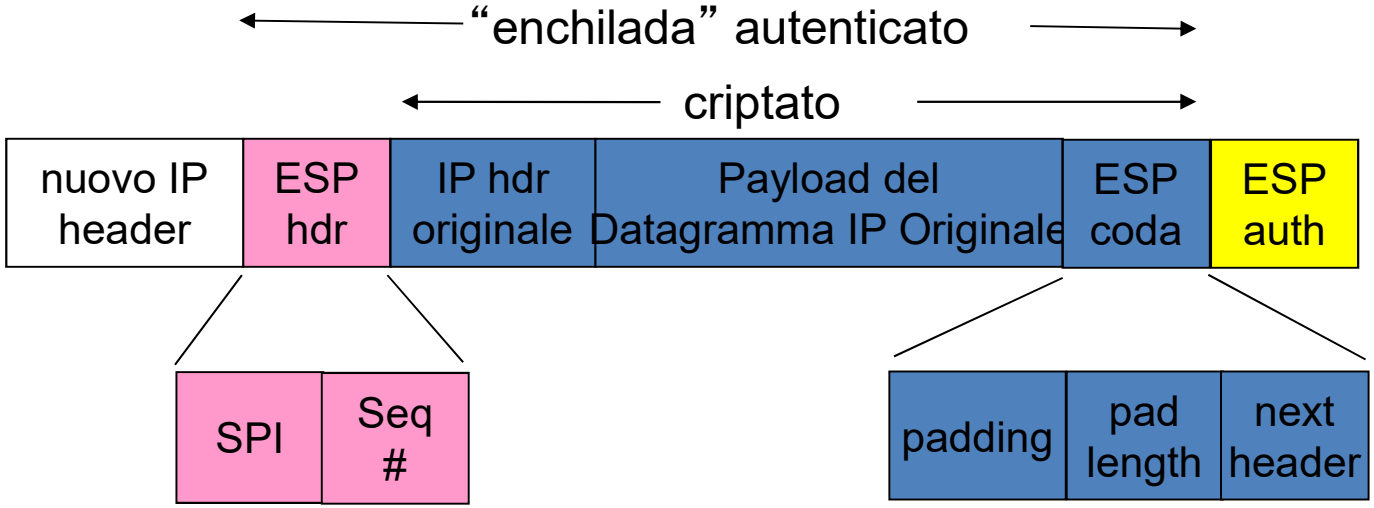
modo tunnel con ESP



Processo di creazione pacchetto IPsec



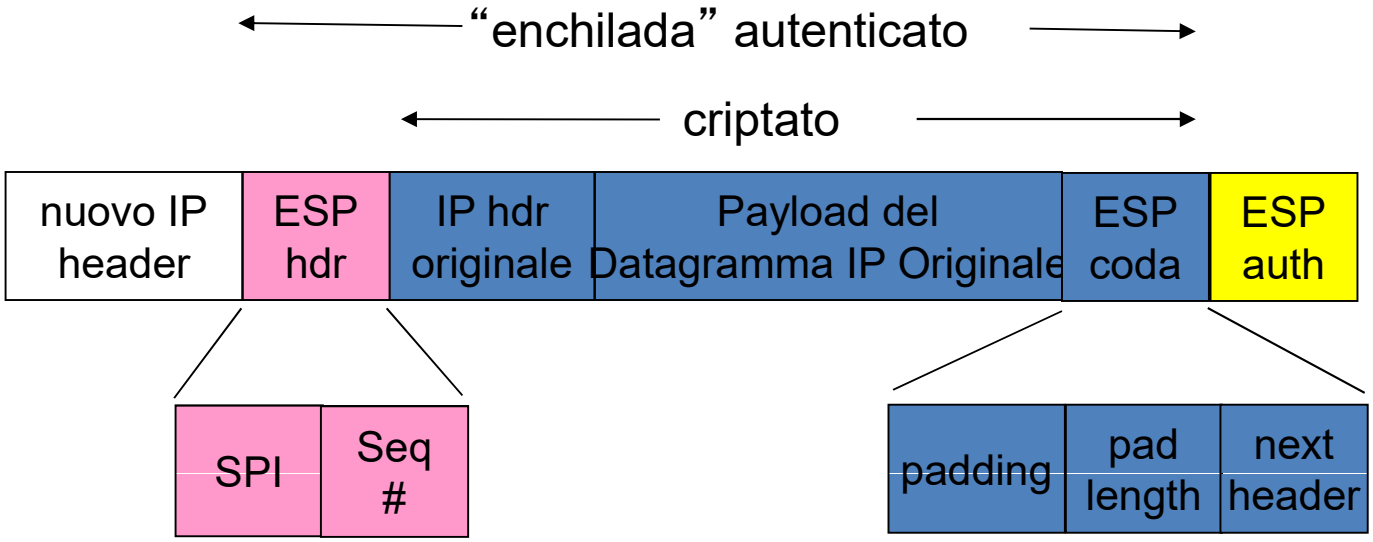
R1 riceve un normale datagramma IPv4 dall'host 172.16.1.17 (che si trova nella rete locale della sede centrale) e lo deve consegnare all'host 172.16.2.48 (nella rete locale della sede periferica). Il Router R1 deve convertire il datagramma IPv4 in un datagramma Ipsec.



R1 converte il datagramma originale in un datagramma IPsec

- Aggiunge alla fine del datagramma originale (nel quale c'è anche l'header originale) un campo "ESP trailer".
- Cripta il resultato usando l'algoritmo e la chiave specificati nella SA.
- Antepone a questa parte criptata l'"ESP header", creando così l'"enchilada".
- Crea il MAC per l'autenticazione dell'intero *enchilada*, usando usando l'algoritmo e la chiave specificati nella SA
- Aggiunge il MAC subito dopo l'enchilada, formando il *payload*;
- crea un nuovo header, con i campi dell'header IPv4 e lo inserisce prima del payload.

Formato dell'enchilada:



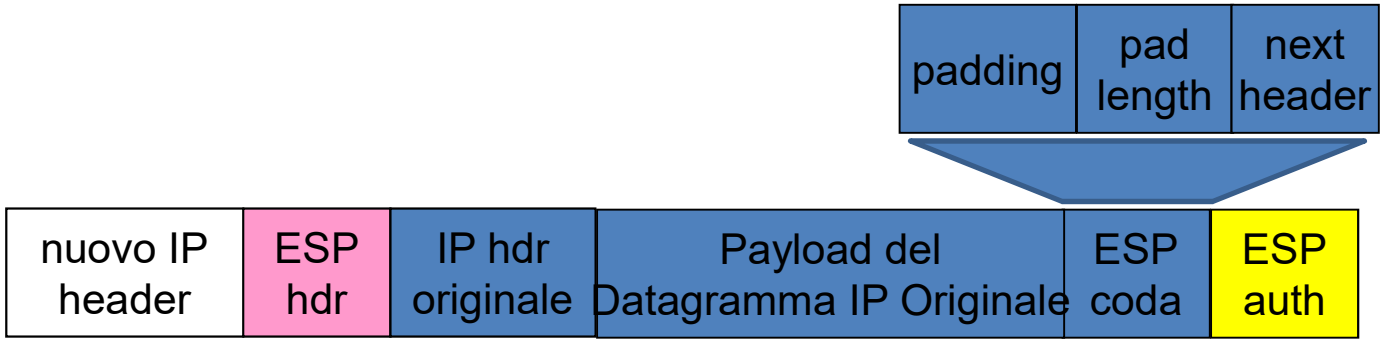
- ESP trailer: riempimento per il cifrario a blocchi
- ESP header:
  - SPI, serve al ricevitore per elaborare i dati
  - Numero di sequenza, per contrastare l'attacco di ripetizione
- MAC nel campo "ESP auth" viene creato con la chiave segreta condivisa

Consegna del pacchetto IPsec

- Dopo che R1 ha immesso il datagramma IPsec nella rete pubblica Internet, il pacchetto attraversa molti router prima di raggiungere R2.
- Ognuno di questi router elabora il datagramma come se fosse un datagramma in formato IPv4. I router ignorano il campo payload, non si accorgono che trasporta dati criptati nel formato IPsec.
- Per i router della rete pubblica l'indirizzo IP di destinazione, specificato nell'header, è R2.

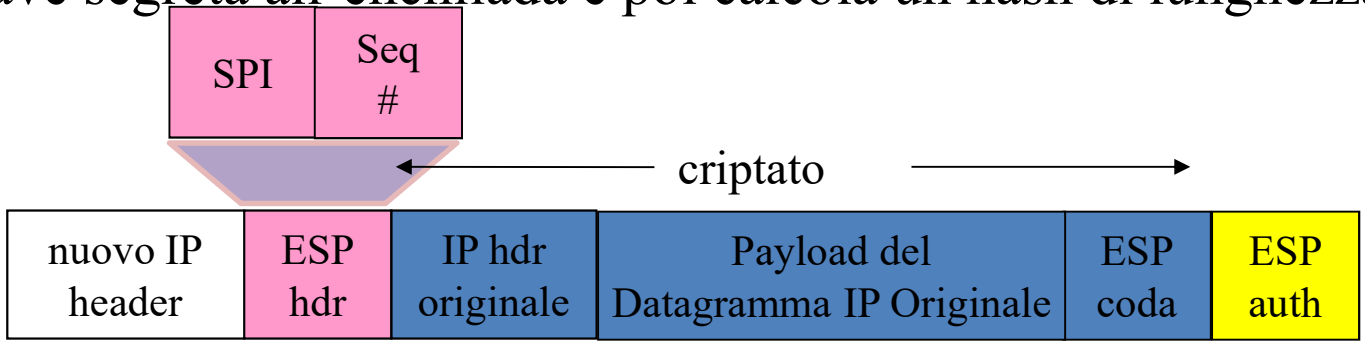
Formato del pacchetto

- L'ESP trailer è formato da tre campi: padding; pad length; e next header.
- I cifrari a blocchi richiedono che il messaggio da criptare abbia una lunghezza multipla intera di un blocco.
- Il campo Padding (consistente di byte privi di significato) serve a far raggiungere la lunghezza desiderata al datagramma originale (compreso i campi pad length e next header), ne risulta quindi un "messaggio" formato da un numero intero di blocchi.
- Il campo pad-length indica al ricevitore quanto padding è stato inserito dal mittente (e che quindi deve rimuovere).
- Il campo next header identifica il protocollo (es. UDP) dei dati contenuti nel campo payload.
- Il payload (quello del datagramma IP originale) e l'ESP trailer vengono concatenati e poi criptati.



Formato del pacchetto

- Davanti all'unità criptata c'è l'ESP header, che viene trasmessa in chiaro e contiene due campi: SPI e il numero di sequenza.
- SPI indica al ricevitore la SA a cui appartiene il datagramma; il ricevitore usa SPI come chiave di accesso al SAD per determinare gli appropriati algoritmi e le corrispondenti chiavi per autenticare e decriptare.
- Il campo numero di sequenza è usato per proteggere la trasmissione dall'attacco di ripetizione.
- Il mittente aggiunge in fondo al pacchetto l'authentication MAC.
- Il mittente calcola il MAC sull'intero enchilada (formato da ESP
- header, datagramma IP originale, e l'ESP trailer – datagramma e trailer sono criptati). Nel calcolo del MAC, il mittente aggiunge una chiave segreta all'enchilada e poi calcola un hash di lunghezza fissa.



Elaborazione del datagramma IPsec

- Quando R2 riceve il datagramma IPsec, R2 osserva che l'indirizzo IP destinazione del datagramma corrisponde all'indirizzo della sua interfaccia. R2 quindi elabora il datagramma. Poiché il campo protocollo (nell'header IP di sinistra) è 50, R2 applica l'elaborazione IPsec ESP al datagramma.
- Primo, R2 estrae dall'enchilada, l'SPI per determinare a quale SA appartiene il datagramma.
- Secondo, R2 calcola il MAC dell'enchilada e verifica che corrisponde a quello contenuto nel campo ESP. In questo modo, se il confronto da esito positivo, R2 è sicuro che il datagramma proviene da R1 e non ha subito manomissioni.
- Terzo, controlla il campo numero di sequenza per verificare che il datagramma è nuovo (non è una replica di un datagramma precedente).
- Quarto, R2 decripta la parte criptata usando l'algoritmo e la chiave specificati nella SA.
- Quinto, rimuove il padding ed estrae il datagramma IP originale.
- Infine, sesto, introduce il datagramma originale nella rete locale della sede periferica, per raggiungere la destinazione finale.

Numeri di Sequenza IPsec

- Quando viene creata una nuova SA, il mittente crea una variabile e la inizializza a 0
- Ogni volta che un datagramma viene inserito nella SA:
  - Il mittente incrementa il contatore dei numeri di sequenza
  - Copia il valore della variabile nel campo “numero di sequenza” del pacchetto
- Scopo dei numeri di sequenza:
  - Impedire a un intruso che intercetta i pacchetti di registrarli e ripeterli
  - I pacchetti duplicati vengono scartati dal ricevitore
- metodo:
  - Il destinatario verifica che non si tratti di un pacchetto duplicato
  - Non memorizza i pacchetti ricevuti ma si serve di una finestra con i numeri sequenza attesi

Security Policy Database (SPD)

- Resta da risolvere ancora un problema.
- Quando R1 riceve un datagramma (non ancora sicuro) da un host nella rete sorgente, che è destinato a un indirizzo IP esterno, R1 deve riconoscere la necessità di convertire il datagramma nel formato IPsec. In tal caso R1 deve anche sapere quale SA (tra tutte quelle presenti nel suo SAD) deve usare per costruire il datagramma IPsec.
- Il problema è risolto come segue. Insieme al SAD, l'entità Ipsec mantiene un'altra struttura dati chiamata la **Security Policy Database (SPD).**
- **L'SPD indica quali tipi di datagrammi (legati a: indirizzo IP sorgente, indirizzo IP** destinazione, e protocollo) devono essere convertiti in IPsec; e, per quelli che devono essere convertiti, quale SA deve essere riferitas.
- L'informazione in un SPD indica "che cosa" fare con un datagramma entrante. L'informazione nel SAD indica "come" farlo.

Security Policy Database (SPD)

- policy: per un dato datagramma, il mittente deve sapere se convertirlo in IPsec
- Deve anche sapere quale SA usare
  - Lo deduce da: indirizzo IP sorgente, destinazione o protocollo.
- Le informazioni nell'SPD indicano "cosa" fare con i datagrammi entranti
- Le informazioni nel SAD indicano "come" farlo

Riepilogo dei servizi IPsec

(Esempio) un intruso intercetta i pacchetti in transito tra R1 ed R2. Non conosce le chiavi di criptografia e di autenticazione.

- Non può leggere i dati nel datagramma originale.
- Non può leggere nemmeno l'header del datagramma originale, in cui c'è
  - codificato il protocollo del segmento contenuto nell'header del datagramma originale,
  - l'indirizzo IP sorgente,
  - l'indirizzo IP destinatario.
- Per i datagrammi inviati sulla SA, l'intruso vede solo che il datagramma è partito da un host nella sottorete 172.16.1.0/24 ed è destinato ad un host contenuto nella sottorete 172.16.2.0/24. L'intruso non sa se trasporta un segmento TCP, UDP, o dati ICMP; l'intruso non capisce nemmeno se ci sono dati del livello applicazione (HTTP, SMTP, o altro).
- Questa riservatezza, quindi, estende la protezione di SSL.

Riepilogo dei servizi IPsec

(Esempio) un intruso intercetta i pacchetti in transito tra R1 ed R2. Non conosce le chiavi di criptografia e di autenticazione.

Se l'intruso cerca di manomettere un datagramma intercettato sulla SA alterando alcuni bit, quando questo datagramma manomesso arriva a R2, fallirà il controllo di integrità (utilizzando il MAC), vanificando i tentativi dell'intruso.

Se l'intruso cerca di mascherarsi da R1, la creazione di un datagramma IPsec con indirizzo di origine 200.168.1.100 e indirizzo destinazione 193.68.2.23 sarà inutile, in quanto questo datagramma sarà scartato quando R2 applica la verifica dell'integrità.

Infine, poiché IPsec include i numeri di sequenza, l'intruso non sarà in grado di creare un attacco di ripetizione.

Riepilogando:
IPsec fornisce, a una qualsiasi coppia di dispositivi che elaborano pacchetti a livello rete, la riservatezza, l'autenticazione dell'origine, l'integrità dei dati e la prevenzione contro l'attacco di ripetizione.

IKE: Internet Key Exchange

Quando una VPN ha pochi tra cui stabilire la connessione privata (ad esempio, due router), l'amministratore di rete può introdurre manualmente le informazioni della SA (algoritmi di criptografia/autenticazione, le chiavi e gli SPI) nei SAD dei dispositivi che si trovano agli estremi della VPN:

Esempio di SA

```
SPI: 12345
Source IP: 200.168.1.100
Dest IP: 193.68.2.23
Protocol: ESP
Encryption algorithm: 3DES-cbc
HMAC algorithm: MD5
Encryption key: 0x7aeaca…
HMAC key:0xc0291f…
```

- L'impostazione manuale risulta improponibile per le VPN con centinaia di coppie di dispositivi terminali, come in una rete estesa geograficamente. Si richiede un meccanismo automatico per creare le SA.
- IPsec ricorre al protocollo IKE (Internet Key Exchange)

IKE: PSK e PKI

- PSK: pre-shared secret key (PSK)
- PKI: public/private keys Infrastructure

L'autenticazione (provare l'identità) avviene con

- pre-shared secret (PSK) o
  - Entrambi i dispositivi terminali iniziano con una chiave segreta condivisa, tramite il protocollo IKE si autenticano reciprocamente eggenerano le SA per entrambe le direzioni, dopo aver deciso gli algoritmi di criptografia e di autenticazione, con le relative chiavi
- PKI (public/private keys e certificati).
  - Entrambi i dispositivi terminali iniziano scambiandosi i certificati, tramite il protocollo IKE si autenticano, creano le IPsec SA (una per ogni direzione).

Fasi IKE

- IKE ha due fasi
  - *fase 1:* stabilisca una connessione IKE-SA bidirezionale
    - nota: IKE SA è differente da IPsec SA
    - Viene denominata ISAKMP security association
  - *fase 2:* entrambi i router rivelano la loro identità firmando i messaggi. Un intruso non legge queste informazioni perchè viaggiano sulla connessione protetta IKE SA. durante questa fase, i due router negoziano gli algoritmi IPsec di criptografia e autenticazione che saranno usati sulla connessione SA IPsec.
- La fase 1 ha due modi:
  - Modo aggressivo usa pochi messaggi
  - Modo main protegge l'identità ed è più flessibile

Fase 2 IKE

- Nella fase 2 di IKE, i due router creano una SA in ciascuna direzione. Al termine della fase 2, sono stati scelti gli algoritmi e le chiavi per I due lati della SA.
- I due router possono usare le SA per proteggere i datagrammi trasmessi.
- Lo scopo principale di avere due fasi in IKE è il costo del calcolo: la seconda fase non coinvolge la criptografia con chiavi pubbliche e private, quindi IKE può generare un elevato numero di SA tra le due entità IPsec senza calcoli complessi e lunghi.

Riepilogo IPsec

- Lo scambio dei messaggi IKE consente di scegliere algoritmi, chiavi segrete, numeri SPI.
- Esiste la versione AH o ESP (o entrambi)
  - AH fornisce controllo dell'integrità e l'autenticazione della sorgente
  - ESP (con AH) fornisce anche la riservatezza
  - Le coppie IPsec possono essere due sistemi terminali, due routers/firewall, o un router/firewall ed un sistema terminale