

Sicurezza a livello IP: IPsec e le reti private virtuali

Davide Cerri

Sommario

L'esigenza di proteggere l'informazione che viene trasmessa in rete porta all'utilizzo di diversi protocolli crittografici. Il presente articolo fornisce una breve introduzione ad uno di essi, IPsec, e a quella che attualmente ne è l'applicazione principale, ovvero la realizzazione di reti private virtuali.

Uno dei problemi più comuni a proposito della sicurezza su Internet riguarda la *riservatezza delle comunicazioni*: normalmente infatti l'informazione che viene trasmessa sulla rete viaggia in chiaro, ed è dunque accessibile a chiunque sia in grado di intercettare il traffico. Per risolvere questo problema si utilizzano opportuni protocolli che proteggono l'informazione in transito mediante tecniche crittografiche, così che chi non possiede la relativa chiave non sia in grado di comprenderle. Protocolli di questo tipo si possono trovare in posizioni diverse dello stack di rete; in particolare in questa sede ci occuperemo di IPsec (Internet Protocol Security), che si colloca al livello del protocollo IP.

IPsec non è in realtà un singolo protocollo, ma piuttosto un insieme di elementi che costituiscono un'architettura di sicurezza (di tipo peer-to-peer) a livello IP; è parte integrante di IPv6, ma è utilizzabile anche con IPv4. IPsec può essere utilizzato come soluzione end-to-end, proteggendo cioè lo scambio di informazioni direttamente tra il mittente e il destinatario della comunicazione, oppure può intervenire tra due sistemi intermedi che hanno la funzione di *security gateway*, come accade nella realizzazione di reti private virtuali. Trovandosi a livello rete, IPsec è una soluzione molto generale (può proteggere tutto il traffico IP) ed è trasparente rispetto alle applicazioni.

I servizi offerti nel complesso da IPsec sono l'*autenticazione* (cioè la garanzia dell'identità del mittente del pacchetto), l'*integrità* (cioè la garanzia che il pacchetto non sia stato alterato durante il transito) e la *riservatezza* (cioè la garanzia che le informazioni non siano leggibili da terzi, ottenuta mediante cifratura del pacchetto). I protocolli che costituiscono IPsec sono essenzialmente tre, ovvero:

- **AH** (Authentication Header);
- **ESP** (Encapsulating Security Payload);

- **IKE** (Internet Key Exchange).

AH ed ESP fanno parte del “nucleo” di IPsec: il primo fornisce solamente i servizi di autenticazione e integrità, mentre il secondo fornisce in più la riservatezza. Il fatto che esistano due protocolli con funzionalità sovrapposte (i servizi offerti da AH sono offerti anche da ESP, seppure in modo leggermente diverso) è dovuto a ragioni “storiche” connesse all’opportunità di avere un protocollo “esportabile” (AH non comprende funzioni di cifratura e dunque non rientra nelle restrizioni all’esportazione che riguardano il software crittografico), tuttavia alcuni ritengono che questa sia un’inutile complicazione e chiedono che AH venga eliminato o quantomeno reso opzionale.

AH ed ESP possono essere utilizzati secondo due modalità, ovvero *trasporto* e *tunnel*. Nella modalità trasporto (che è possibile solo tra due host e non tra due security gateway) gli header AH e/o ESP vengono inseriti tra l’header IP e l’header di trasporto, mentre nella modalità tunnel l’intero pacchetto IP originale viene incapsulato in un nuovo pacchetto (in figura 1 sono mostrate le posizioni degli header AH ed ESP all’interno del pacchetto nelle due modalità, e le porzioni del pacchetto coperte dalle funzioni di sicurezza).

Oltre ai protocolli, un concetto chiave nell’architettura di IPsec è quello di *Security Association* (SA): la SA è una sorta di “contratto” che le due parti devono stipulare prima di iniziare la comunicazione sicura, accordandosi su quali protocolli, algoritmi crittografici e chiavi utilizzare, ed è in sostanza l’elemento che specifica la “connessione” IPsec. Le SA sono dunque necessarie per poter comunicare tramite IPsec, tuttavia AH ed ESP non si preoccupano della loro gestione e presuppongono che le SA siano già state create con qualche altro meccanismo. In casi limitati si può pensare di creare manualmente le SA in fase di configurazione di IPsec (e questo è effettivamente possibile), ma è evidente che una soluzione di questo tipo non è applicabile in generale, e che vi è dunque la necessità di un meccanismo automatico di creazione delle SA; questo è appunto il compito del protocollo IKE.

IKE agisce nella fase di instaurazione della comunicazione IPsec, e permette di negoziare, creare, distruggere e in generale gestire le SA. La negoziazione avviene in due fasi: nella prima i due interlocutori creano una SA per IKE stesso, che protegge i messaggi del protocollo di scambio delle chiavi (questa è detta ISAKMP SA; ISAKMP - Internet Security Association and Key Management Protocol - è un framework per la gestione delle SA sulla base del quale è definito IKE), mentre nella seconda fase creano le SA per IPsec. La prima fase avviene con uno scambio di messaggi detto “main mode” (che consiste di sei messaggi) oppure con uno scambio più breve detto “aggressive mode” (tre messaggi), mentre lo scambio della seconda fase prende il nome di “quick mode” e consiste di altri tre messaggi. Durante la fase di negoziazione i due peer devono autenticarsi vicendevolmente: per farlo possono utilizzare la crittografia a chiave pubblica (chiavi asimmetriche, firme digitali e certificati) oppure una “pre-shared key”, cioè un’informazione segreta condivisa sulla quale si sono precedentemente accordati in altro modo (qualcosa di simile

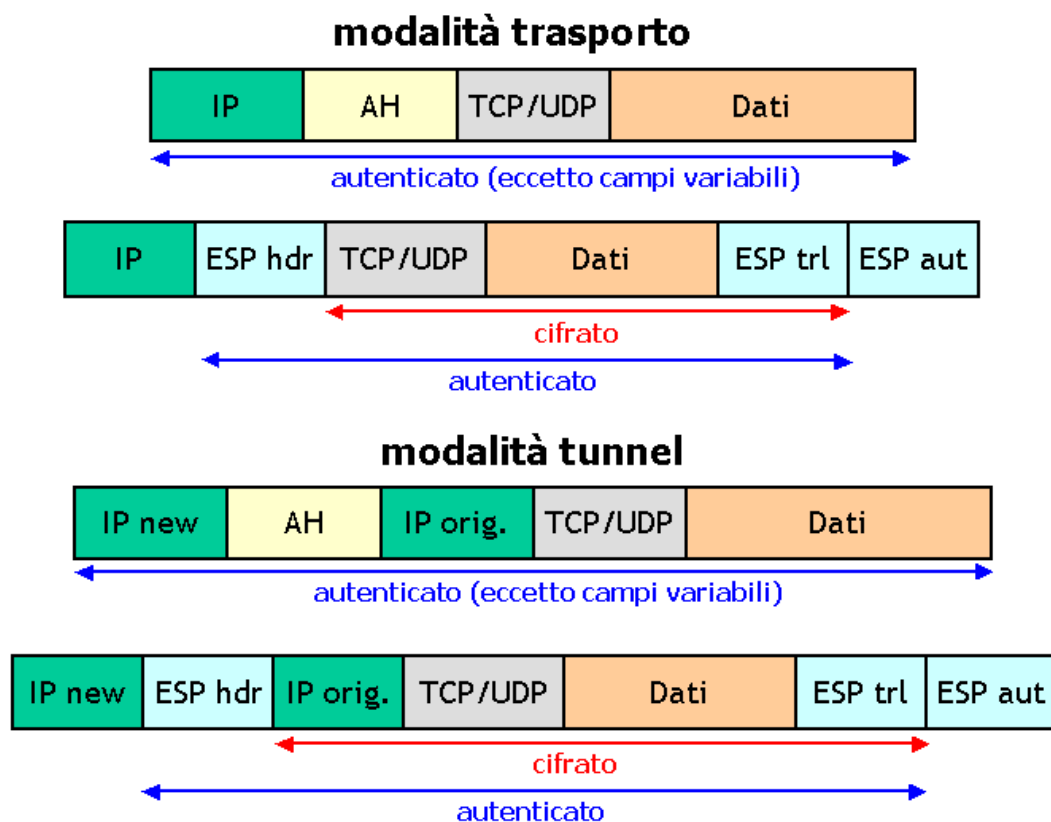


Figura 1: Formato dei pacchetti IPsec in modalità trasporto e tunnel.

ad una password, che viene però utilizzata per un'autenticazione mutua e non di una sola parte).

IPsec è una soluzione molto generale, e in teoria potrebbe essere utilizzato per proteggere qualunque tipo di traffico IP, tuttavia il suo uso attualmente più comune è connesso alla realizzazione di *reti private virtuali* (VPN – Virtual Private Network). Le reti private virtuali permettono di collegare tra loro delle reti locali tramite la rete Internet, garantendo però sicurezza (riservatezza, integrità...) al traffico che viaggia sulla rete esterna. Pensiamo di avere due reti locali geograficamente distanti (ad esempio due sedi di un'azienda), e di voler fare in modo che le macchine poste su queste due reti possano comunicare tra loro in maniera sicura, disponendo solo di un accesso ad Internet (figura 2). Posizioniamo allora in ciascuna delle due reti una macchina che faccia da security gateway e configuriamo un tunnel IPsec (utilizzando ESP) tra queste due macchine, configuriamo poi le tabelle di routing nelle due reti in modo che il traffico proveniente da una rete e destinato all'altra venga inviato al security gateway locale. A questo punto, un host sulla prima rete (ad

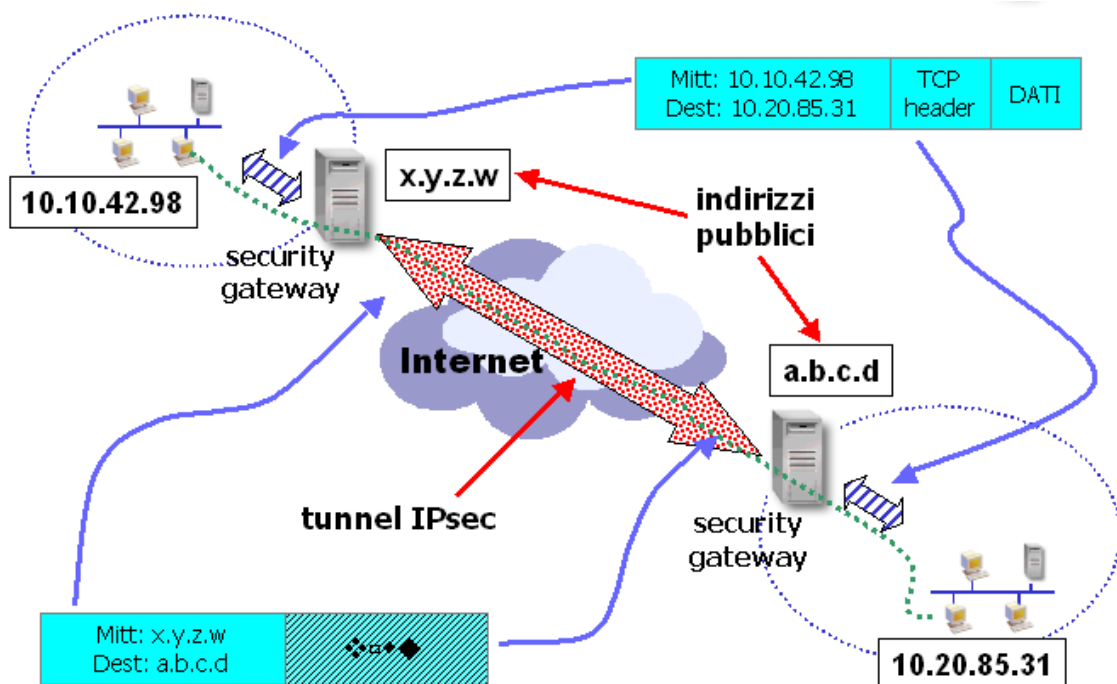


Figura 2: Rete privata virtuale (VPN).

esempio con l'indirizzo 10.10.42.98) che vuole comunicare con un host sulla seconda (ad esempio 10.20.85.31) si limiterà ad inviare il relativo pacchetto IP senza alcun particolare accorgimento. Tale pacchetto arriverà al security gateway della prima rete, che si accorgerà che è destinato alla seconda: il gateway *cifrerà* quindi il pacchetto e lo *incapsulerà* in nuovo pacchetto IP, che avrà come mittente il suo indirizzo pubblico (x.y.z.w in figura) e come destinazione l'indirizzo pubblico del secondo gateway (a.b.c.d). Tale pacchetto viaggerà normalmente su Internet, ma chi lo intercettasse vedrebbe solamente che è in corso una comunicazione IPsec tra i due gateway, mentre non conoscerebbe né i contenuti della comunicazione, né il protocollo utilizzato (a livello trasporto e applicazione), né il mittente e il destinatario reali della comunicazione (l'intero pacchetto IP originale è inviato cifrato). Quando il pacchetto arriverà al secondo gateway, questo ne controllerà l'autenticità e l'integrità e decifrerà la porzione cifrata ricostruendo così il pacchetto originale, che inoltrerà poi verso la destinazione. L'host sulla seconda rete riceverà quindi il pacchetto così come è stato inviato dal mittente originale: gli host sulle due reti possono dunque comunicare tra loro senza conoscere alcun dettaglio riguardo al tunnel IPsec (di cui possono anche ignorare l'esistenza). Si ha così, virtualmente, un'unica rete privata che sfrutta l'infrastruttura della rete pubblica, dato che il tunnel IPsec appare alle macchine sulle due reti locali come un unico link virtuale.

Pur essendo stato definito ormai alcuni anni fa (gli RFC di AH, ESP e IKE risalgono

al novembre 1998), IPsec è utilizzato al momento in casi abbastanza limitati. I maggiori problemi sono probabilmente quelli che riguardano la fase di instaurazione della connessione, ovvero il protocollo IKE. IKE offre infatti parecchie opzioni ed è molto complesso; trattandosi di protocolli di sicurezza la complessità è particolarmente negativa, inoltre dà facilmente luogo a problemi di interoperabilità tra diverse implementazioni. Per migliorare e semplificare l'attuale protocollo IKE, e per risolverne alcuni problemi (ad esempio in presenza di NAT), è attualmente in corso presso il working group "ipsec" dell'IETF la discussione sulla futura versione del protocollo. La soluzione dei problemi di interoperabilità tra diverse implementazioni di IPsec è anche uno degli scopi primari del Virtual Private Network Consortium (VPNC, <http://www.vpnc.org>), sul cui sito web è possibile trovare informazioni su alcuni test di conformità (a diversi livelli) e di interoperabilità dei prodotti di diversi membri del consorzio.