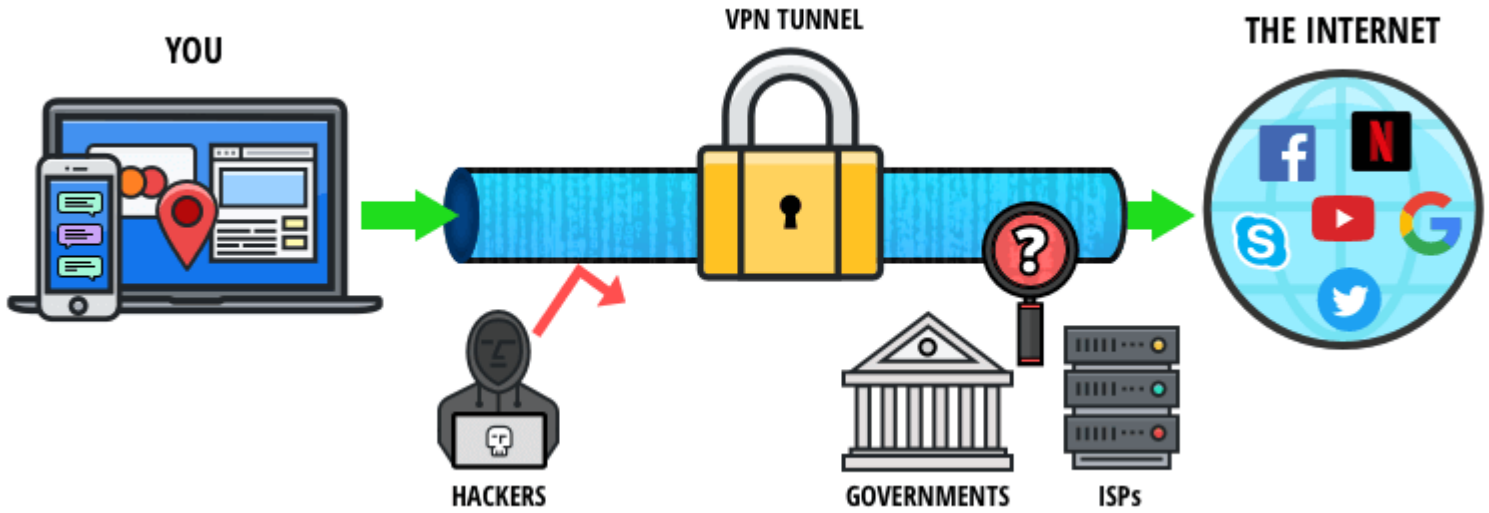
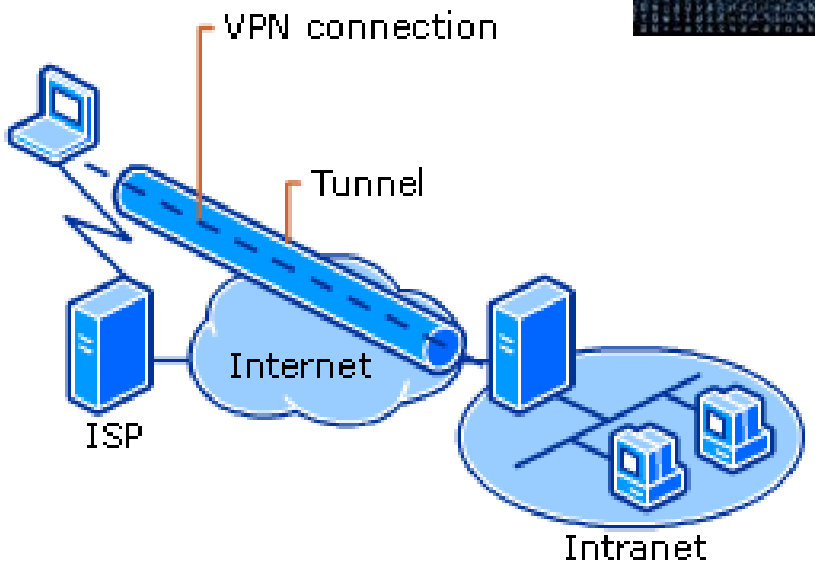
SICUREZZA E PROTOCOLLI DI SICUREZZA NELLE VPN



LA SICUREZZA NELLE VPN

- **Autenticazione**
- **Cifratura**
- **Tunneling**



LA SICUREZZA NELLE VPN: Autenticazione dell'identità

Autenticazione dell'identità: processo con cui un sistema informatico o un utente verifica la corretta identità di un altro sistema informatico, applicativo o utente che vuole comunicare attraverso una connessione, per poi concedergli l'autorizzazione a usufruire dei relativi servizi associati.

LA SICUREZZA NELLE VPN: Autenticazione dell'identità

La porta di accesso di un client alla sua VPN risulta essere un **server NAS** dotato di processo di autenticazione o server dedicato all'autenticazione come il **server AAA**.

LA SICUREZZA NELLE VPN: Autenticazione dell'identità

Al fine di connettersi alla VPN desiderata occorre dunque prima autenticarsi. Questa procedura è nota come **MultiFactor Authentication** (MFA). Per esempio, dopo aver effettuato il login con username e password, viene chiesto di immettere un codice generato tramite una chiave elettronica (**key fob**) che cambia ogni volta. Questa modalità attualmente è superata dall'uso di applicazioni per smartphone che alla generazione di sequenze di caratteri da usare una volta sola (**one-time password**) associano altri fattori quali: l'impronta di un dito (**fingerprint**) oppure la lettura di un **QR code** che compare nella pagina web di autenticazione.

Solo dopo aver superato la fase di autenticazione si viene autorizzati ad accedere ai servizi della rete. Affinchè la VPN funzioni come la LAN aziendale, l'amministratore dovrà definire, per ciascun utente, le opportune autorizzazioni per l'accesso ai servizi della rete (policy di servizio). Per esempio, la condivisione di risorse (dischi, stampanti, ecc.) può essere autorizzata solo per il personale dell'azienda, mentre ai client VPN esterni si consente di accedere a servizi di navigazione Internet o posta elettronica.

LA SICUREZZA NELLE VPN: Autenticazione dell'identità

I protocolli per la sicurezza nelle VPN garantiscono anche **integrità** e **autenticità** dei dati, cioè che i pacchetti ricevuti non siano stati modificati e che provengano da fonte certa.

Per controllare che non siano state effettuate azioni indesiderate e non autorizzate, occorre prevedere meccanismi di accounting.

LA SICUREZZA NELLE VPN: Autenticazione dell'identità

Con il termine **accounting** si intendono tutte le azioni volte a misurare e documentare le risorse concesse a un utente durante un accesso.

Ciò può includere la durata della sessione di lavoro, il quantitativo dei dati (inviati e ricevuti) in una sessione di lavoro, ecc…

LA SICUREZZA NELLE VPN: Cifratura

Le VPN per cifrare il traffico in rete utilizzano un'ampia gamma di algoritmi di crittografia (3-DES, CAST, IDEA, ecc.). Sia l'algoritmo da usare sia le chiavi segrete devono essere concordate e scambiate tra mittente e destinatario attraverso protocolli di sicurezza.

LA SICUREZZA NELLE VPN: Cifratura

Nello specifico caso delle reti VPN, viene soprattutto utilizzato il protocollo **Internet Key Exchange** (**IKE**), il cui compito principale è proprio implementare lo scambio delle chiavi per cifrare i pacchetti.

LA SICUREZZA NELLE VPN: Tunneling

Lo scopo dei **protocolli di tunneling** è aggiungere un livello di sicurezza con l'**incapsulamento** al fine di proteggere ogni pacchetto nel suo viaggio su Internet.

Le VPN possono essere protette in **modalità trasporto** o in **modalità tunnel** (tunneling).

LA SICUREZZA NELLE VPN: Tunneling

Nel caso di modalità trasporto hanno un ruolo fondamentale i **software** impiegati. Immaginiamo un lavoratore mobile (teleworker) che deve collegarsi alla sede centrale attraverso l'unico carrier disponibile in qualsiasi punto del mondo, ovvero Internet. Il suo dispositivo (notebook, tablet, ecc.) dovrà dotarsi di software per VPN. Il collegamento potrà essere effettuato con qualsiasi ISP in quanto cifratura e decifratura dei dati verranno garantite dal software installato sul dispositivo e dagli apparati riceventi presso la sede centrale. Internet lascerà in chiaro solamente le informazioni di instradamento IP (header e trailers dei pacchetti).

LA SICUREZZA NELLE VPN: Tunneling

Nel caso di modalità tunneling hanno un ruolo fondamentale gli **apparati** e, in particolar modo, router e firewall. È la tecnologia tipica di un collegamento tra una filiale e la sede centrale (Site-to-site VPN). Gli apparati sono preposti a trasformare e codificare tutto il traffico tra gli end-point. Per gli utenti finali non vi è alcuna percezione della protezione applicata.

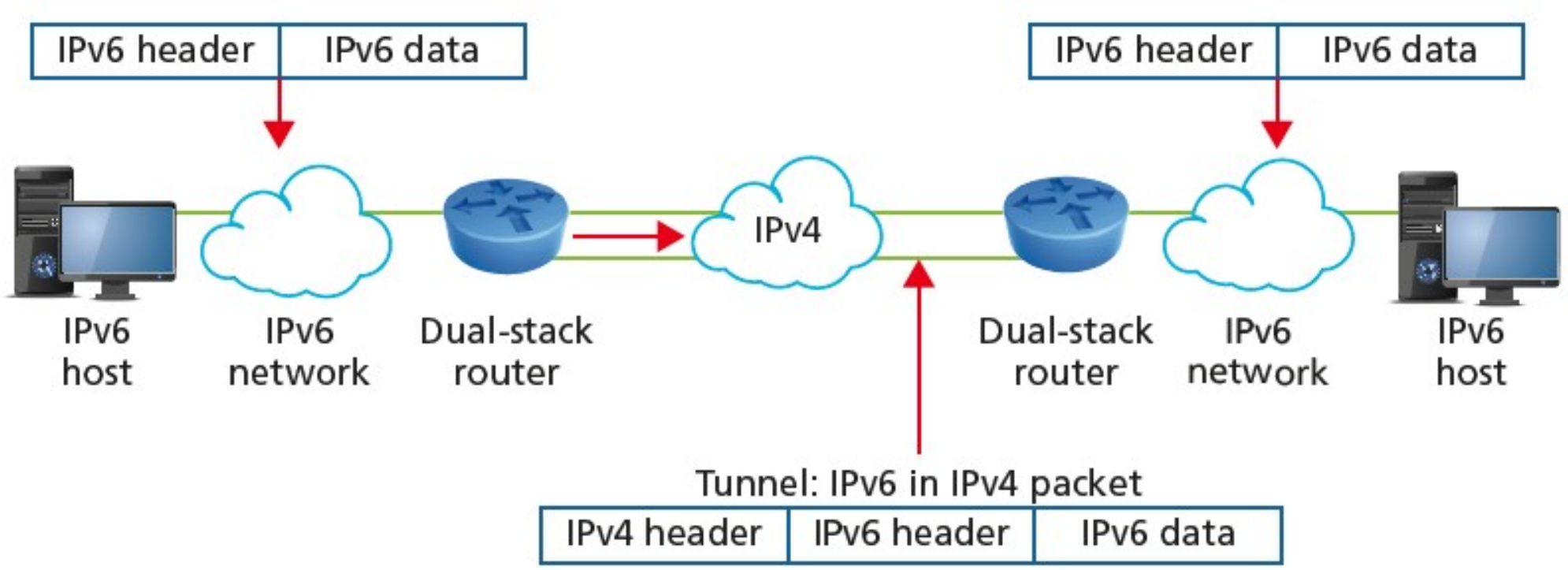
In questa modalità un intero pacchetto viene posto all'interno di un altro pacchetto prima di essere trasportato su Internet. Il pacchetto esterno protegge il contenuto dalla vista del pubblico e assicura che il pacchetto passeggero si muova all'interno di un tunnel virtuale.

LA SICUREZZA NELLE VPN: Tunneling

Tale stratificazione di pacchetti viene chiamata **incapsulamento**. Gli host o i dispositivi di rete su entrambe le estremità del tunnel (**tunnel interface**) possono incapsulare i pacchetti in uscita e riaprire i pacchetti in entrata. Gli utenti (a una estremità del tunnel) e il personale IT (a una o entrambe le estremità del tunnel) dovranno configurare le interfacce di cui sono responsabili per utilizzare il protocollo di tunneling, chiamato anche protocollo di incapsulamento.

LA SICUREZZA NELLE VPN: Tunneling

Esempio di tunneling: pacchetto IPv6 incapsulato in IPv4.

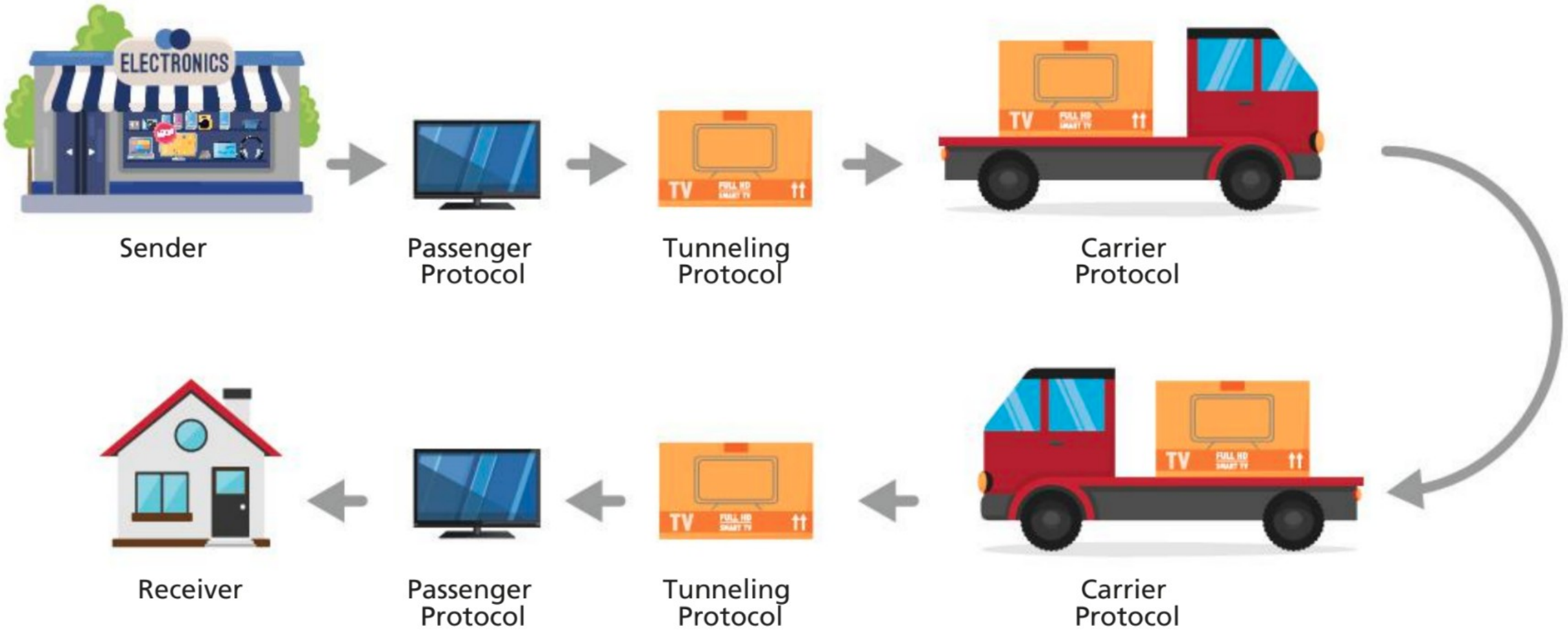


Il pacchetto è in viaggio con lo stesso protocollo di trasporto (**carrier protocol**) che avrebbe utilizzato senza il tunnel VPN.

LA SICUREZZA NELLE VPN: Tunneling

Per capire meglio le relazioni tra protocolli incapsulati facciamo un esempio :
Supponiamo che un cliente abbia ordinato un televisore da un rivenditore e che gli verrà consegnato tramite corriere.
Il rivenditore predispone il televisore (passenger protocol) in una scatola d'imballaggio (tunneling protocol).
Gli addetti al magazzino del venditore quindi caricano l'imballo sul camion del corriere (carrier protocol).
Il corriere viaggia sulle autostrade (Internet) fino a casa del cliente e consegna l'imballo.
Il cliente apre l'imballo (tunneling protocol) e prende il televisore (passenger protocol).
Senza il tunnel, il televisore sarebbe stato ugualmente inviato col corriere, ma senza scatola d'imballaggio!

LA SICUREZZA NELLE VPN: Tunneling



LA SICUREZZA NELLE VPN

I protocolli usati per il tunneling sono diversi:

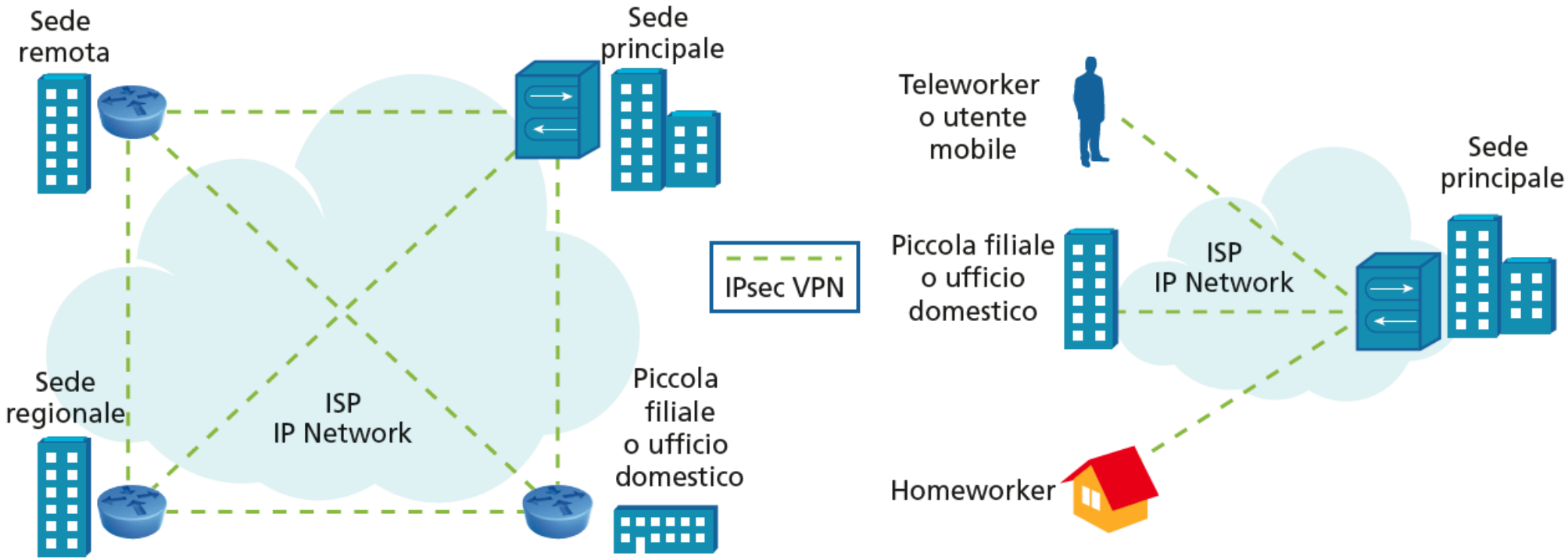
- IPsec (IP security);
- SSL/TLS (Secure Sockets Layer/Transport Layer Security);
- BGP/MPLS (Border Gateway Protocol/Multiprotocol Label Switching);
- PPTP (Point-to-Point Tunneling Protocol);
- IEEE 802.1Q (Ethernet VLANs);
- SSH (Secure SHell);
- GRE (Generic Routing Encapsulation);
- L2TP (Layer 2 Tunneling Protocol).

PROTOCOLLI PER LA SICUREZZA NELLE VPN

- IPsec
- SSL/TLS

PROTOCOLLI PER LA SICUREZZA NELLE VPN: IPsec

IPsec VPN: due scenari



PROTOCOLLI PER LA SICUREZZA NELLE VPN: IPsec

Ipsec non è un singolo protocollo, ma piuttosto una architettura di sicurezza a livello network, composta da vari protocolli e da altri elementi. I protocolli principali che costituiscono IPsec sono:

- **Authentication Header** (AH): garantisce autenticazione e integrità del messaggio ma non offre confidenzialità;
- **Encapsulating Security Payload** (ESP): fornisce autenticazione, confidenzialità e integrità del messaggio;
- **Internet Key Exchange** (IKE): implementa lo scambio delle chiavi per realizzare il flusso crittografato.

PROTOCOLLI PER LA SICUREZZA NELLE VPN: IPsec

Nel momento in cui due host devono inviarsi dei dati tramite la VPN, usando AH o ESP, è necessario instaurare prima una connessione logica tra loro, detta **Security Association** (SA) e per stabilirla viene usato IKE.

PROTOCOLLI PER LA SICUREZZA NELLE VPN: IPsec

IKE sia in ambito IPv4 sia IPv6 è un protocollo a livello application che usa UDP ma implementa un servizio affidabile; infatti, quando invia una richiesta per attivare una SA, la ritrasmette se non riceve risposta.

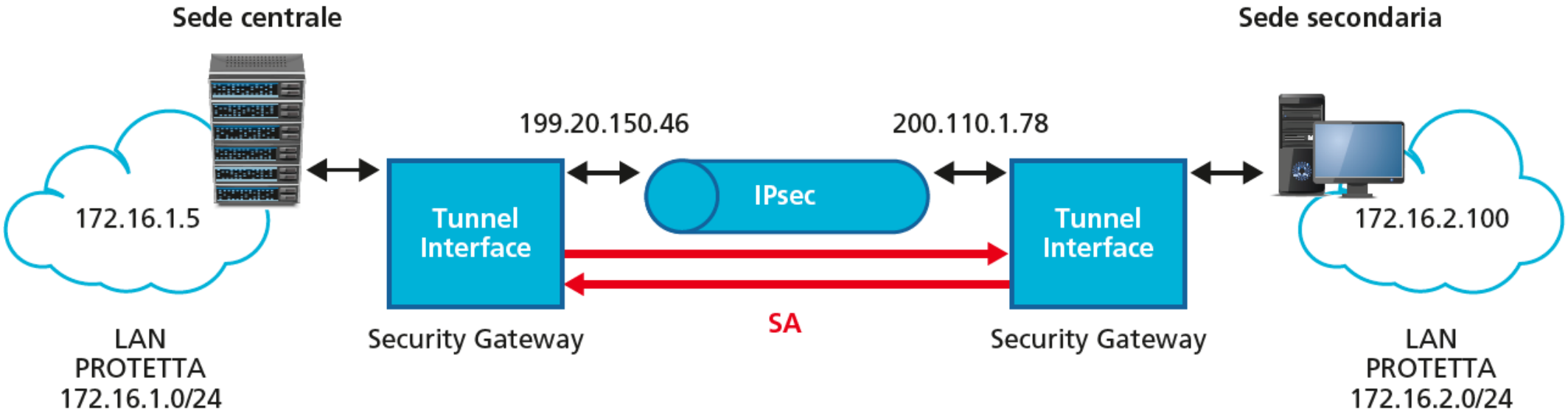
In generale, le chiavi associate alle SA devono essere usate per un tempo limitato e per proteggere una quantità limitata di dati. Nel caso servisse trasferire altri dati, si instaura una nuova SA.

PROTOCOLLI PER LA SICUREZZA NELLE VPN: IPsec

LESSICO

La presenza di un gateway a gestire le SA permette di lavorare in modalità tunnel. Tale gateway prende il nome di **security gateway**.

VPN Site-to-site con tunneling Ipsec.



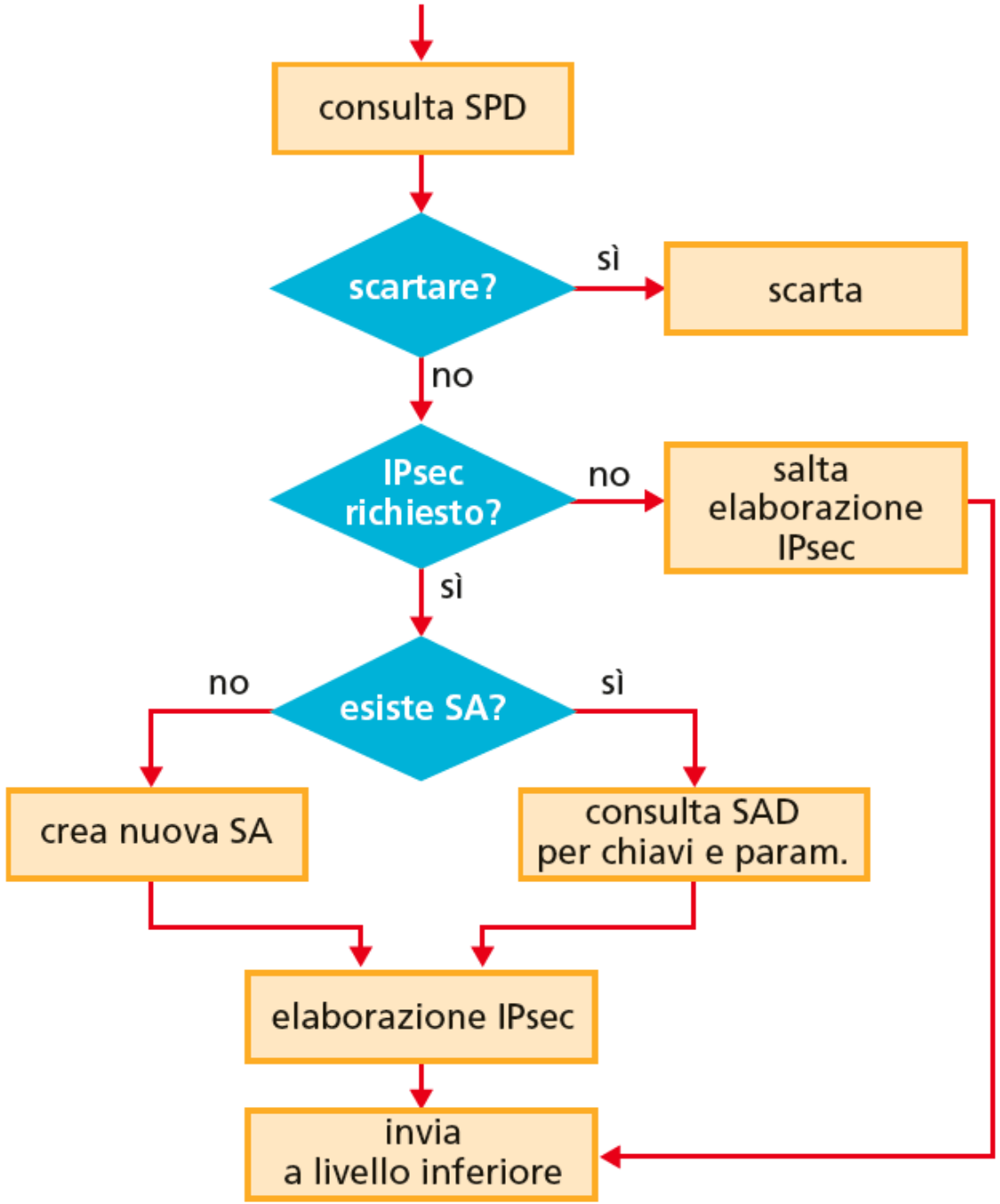
PROTOCOLLI PER LA SICUREZZA NELLE VPN: IPsec

Le SA sono **unidirezionali**, per cui sono necessarie due SA per permettere a due host di comunicare tra di loro.

Tutte le Security Association attive su un host (o su un security gateway) sono contenute in un database detto **SAD** (Security Association Database), mentre esiste un altro database detto **SPD** (Security Policy Database) che contiene le politiche di sicurezza: è tramite queste che il sistema decide se un pacchetto debba essere scartato, lasciato passare in chiaro oppure elaborato tramite IPsec.

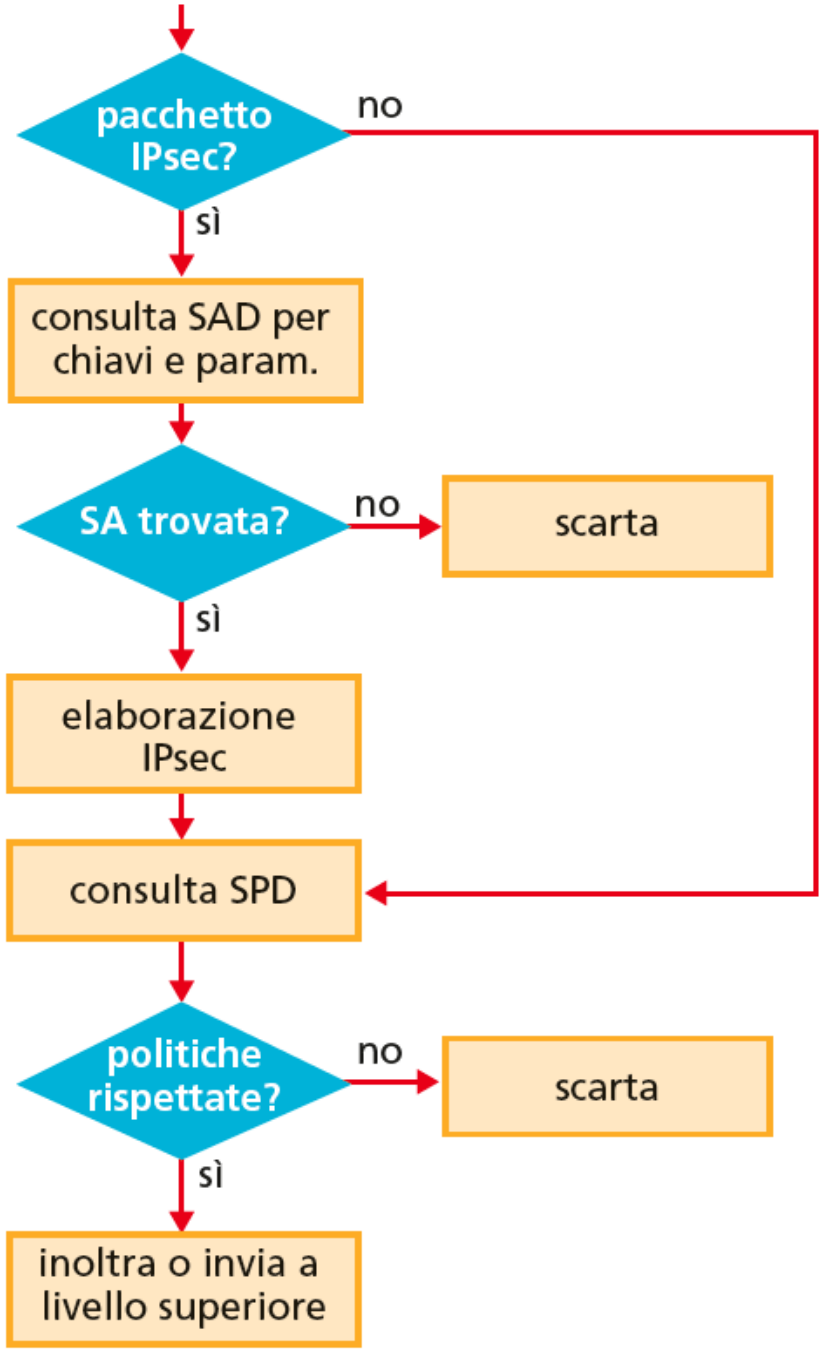
PROTOCOLLI PER LA SICUREZZA NELLE VPN: IPsec

Elaborazione dei pacchetti IPsec: traffico in uscita (outbound)



PROTOCOLLI PER LA SICUREZZA NELLE VPN: IPsec

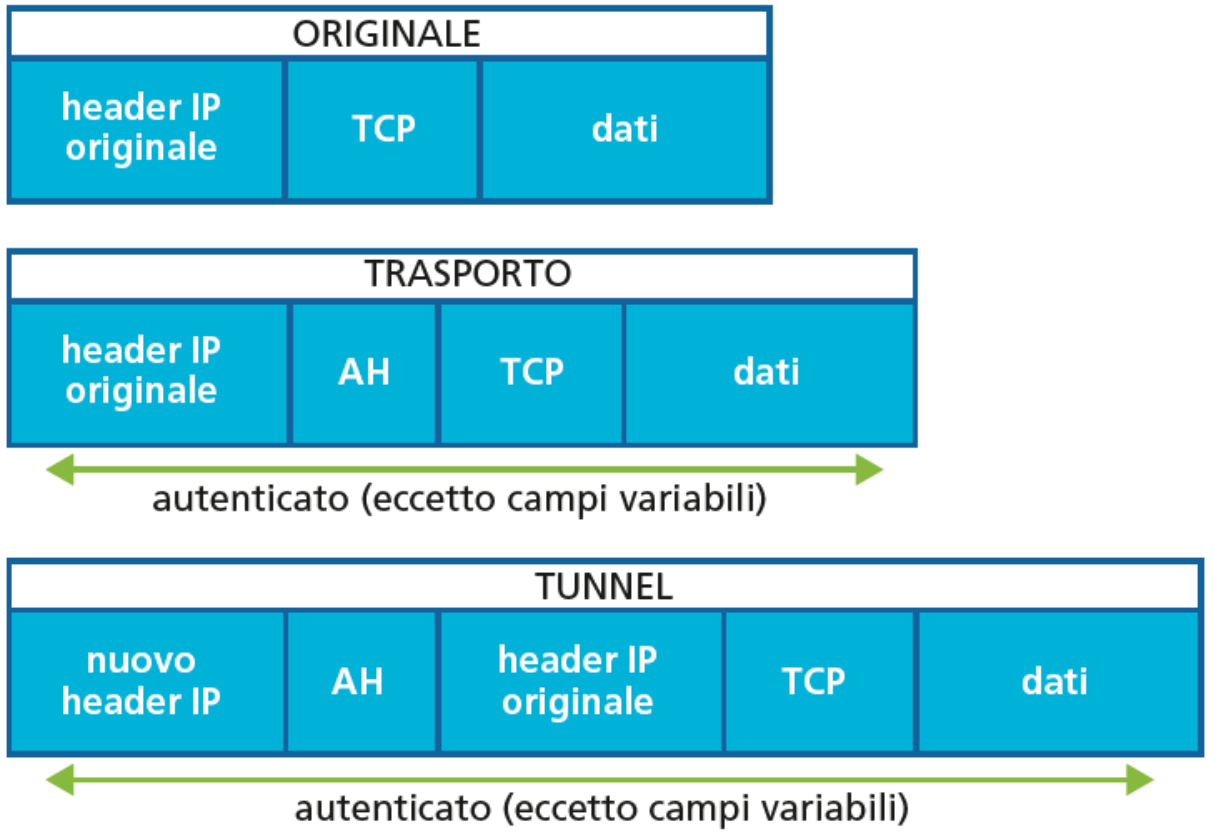
Elaborazione dei pacchetti IPsec: traffico in ingresso (inbound)



PROTOCOLLI PER LA SICUREZZA NELLE VPN: Authentication Header

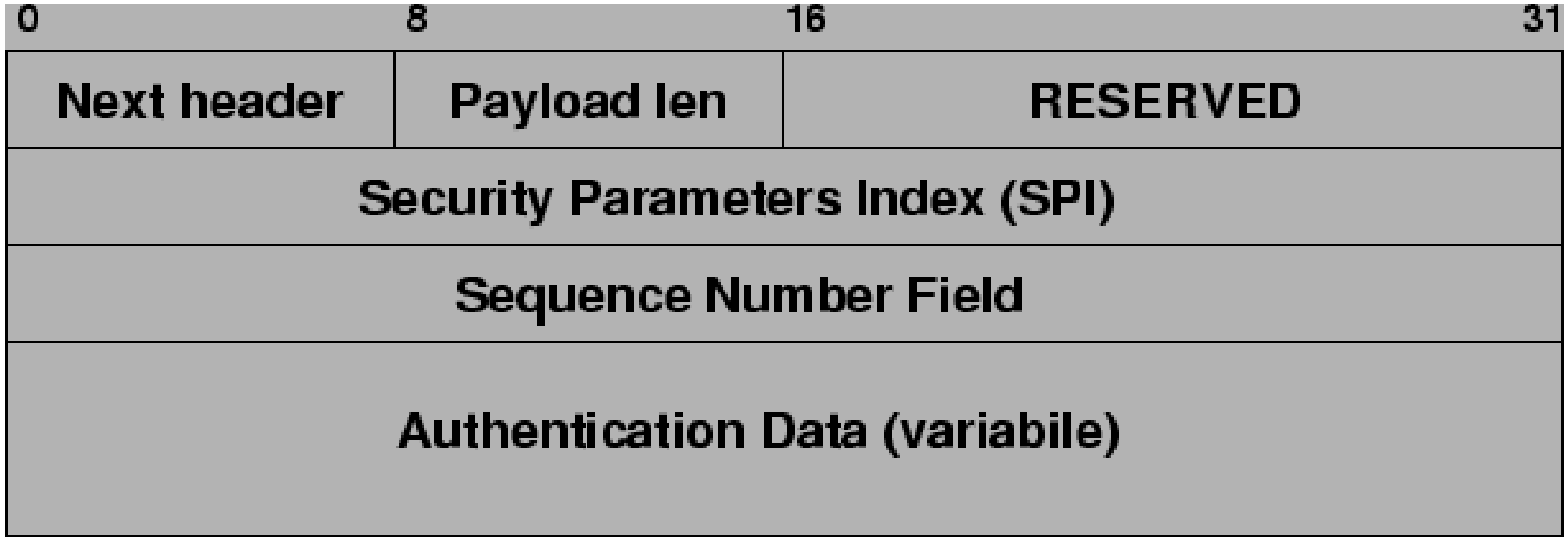
Il **protocollo AH** fornisce servizi di autenticazione, integrità e protezione da attacchi di tipo **replay,** in cui un intruso immette nella rete un pacchetto autentico precedentemente intercettato.

NB: AH autentica l'intero pacchetto IP ad eccezione dei campi variabili dell'header IP originale.



PROTOCOLLI PER LA SICUREZZA NELLE VPN: Authentication Header

Formato dell'header AH:



PROTOCOLLI PER LA SICUREZZA NELLE VPN: Authentication Header

- **Next header**: contiene il codice identificativo del protocollo dell'header successivo (TCP, UDP, ICMP, ecc...)
- **Payload length**: contiene la lunghezza dell'header AH.
- **Reserved**: riservato per usi futuri, deve essere posto a zero.
- **Security Parameters Index (SPI)**: contiene un valore numerico che, insieme con l'indirizzo IP di destinazione ed il protocollo (ovvero AH, in questo caso) identifica la security association utilizzata. Viene stabilito dal destinatario quando la SA viene negoziata.

PROTOCOLLI PER LA SICUREZZA NELLE VPN: Authentication Header

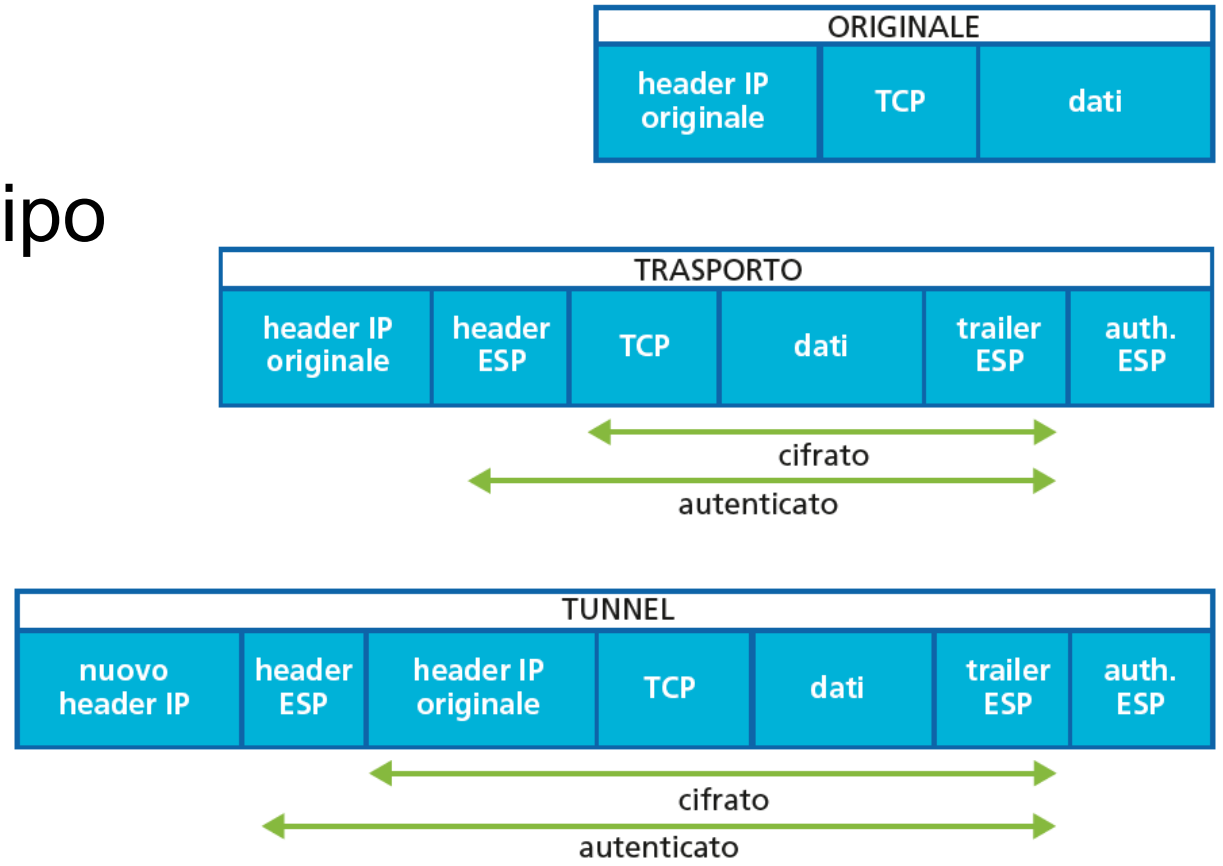
- **Sequence number**: specifica il numero di sequenza del pacchetto all'interno della SA, per prevenire i replay attack. Il destinatario gestisce i numeri di sequenza (se il servizio anti-replay è abilitato) tramite un meccanismo a finestra.
- **Authentication data**: contiene il valore per il controllo dell'integrità (Integrity Check Value -- ICV) del pacchetto. La lunghezza di questo campo è variabile ma deve essere un multiplo di 32 bit, per cui è possibile inserire un padding.

NB: AH presuppone che esista già una security association tra i due nodi, e non si preoccupa quindi di negoziarne i parametri.

PROTOCOLLI PER LA SICUREZZA NELLE VPN: ESP

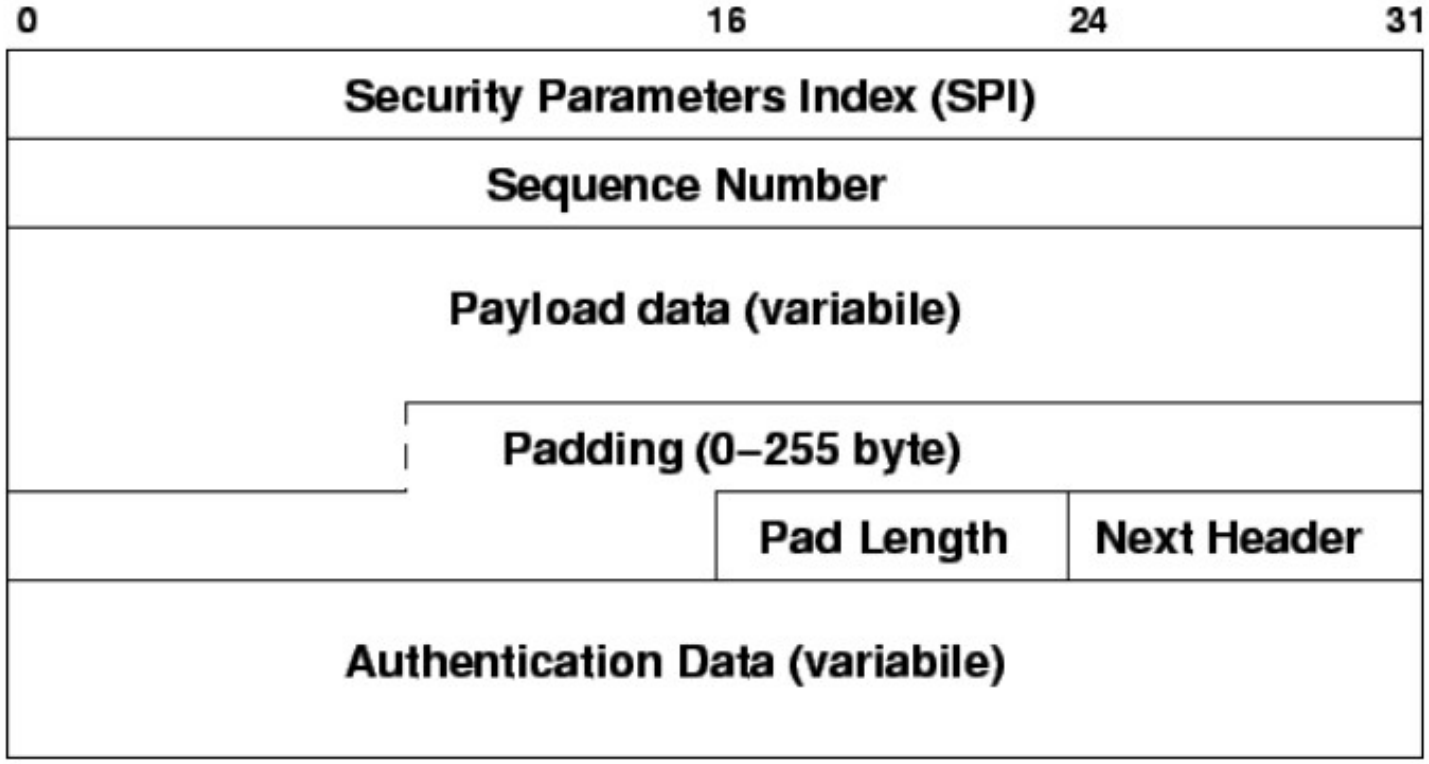
Il **protocollo ESP** fornisce servizi di confidenzialità autenticazione, integrità e protezione da attacchi di tipo **replay**.

NB: a differenza di AH, l'autenticazione non copre l'header IP esterno



PROTOCOLLI PER LA SICUREZZA NELLE VPN: ESP

Formato dell'header ESP:



Anche ESP, come AH, presuppone che esista già una SA tra i due nodi e non si preoccupa di negoziarne i parametri

PROTOCOLLI PER LA SICUREZZA NELLE VPN: ESP

- **Security Parameters Index (SPI) :** contiene un valore numerico che, insieme con l'indirizzo IP di destinazione e il protocollo (in questo caso ESP), permette di identificare la security association utilizzata.
- **Sequence number**: contiene il numero di sequenza del pacchetto nell'ambito della security association.
- **Payload data:** contiene il payload del pacchetto IP originale (se in modalità trasporto) oppure l'intero pacchetto IP originale (se in modalità tunnel), cifrato se si utilizza il servizio di riservatezza. Nel caso l'algoritmo di cifratura utilizzato necessiti di un vettore di inizializzazione (Initialization Vector -- IV), questo viene inserito all'inizio del payload.

PROTOCOLLI PER LA SICUREZZA NELLE VPN: ESP

- **Padding**: può essere necessario sia perché l'algoritmo di cifratura può richiedere che il testo in chiaro abbia una dimensione multipla di un certo valore, sia per assicurare il corretto allineamento dei campi successivi. È anche possibile aggiungere un padding per limitare gli effetti di un'analisi del traffico basata sulla dimensione dei pacchetti.
- **Pad length**: contiene la lunghezza del padding.
- **Next header**: contiene il codice identificativo del protocollo per i dati contenuti nel payload, per esempio TCP o UDP. Si noti che, se si utilizza il servizio di riservatezza, questo campo è cifrato.
- **Authentication data**: contiene il valore di controllo integrità (ICV), calcolato sull'intero pacchetto ESP escluso questo campo. È presente solo se si utilizza il servizio di autenticazione/integrità.

PROTOCOLLI PER LA SICUREZZA NELLE VPN: IKE

Nell'architettura IPsec è centrale la Security Association, ma né AH né ESP si preoccupano della sua gestione. Il protocollo IKE risolve questo problema.

Il protocollo ISAKMP (Internet Security Association and Key Management Protocol) è parte di IKE e definisce le procedure e il formato dei pacchetti per la gestione (creazione, modifica, cancellazione) delle SA e per lo scambio e l'autenticazione delle chiavi, indipendentemente dalla tecnica di generazione delle chiavi stesse, dagli algoritmi di cifratura e dai meccanismi di autenticazione.

PROTOCOLLI PER LA SICUREZZA NELLE VPN: IKE

Il **protocollo IKE** realizza un collegamento peer-to-peer in **due fasi**: nella prima i due host creano una Security Association per IKE stesso (**IKE SA**), ovvero un canale sicuro da utilizzare per i messaggi di IKE; nella seconda fase utilizzano la SA appena creata per negoziare Security Association per altri protocolli (**IPsec SA**).

LO SAI CHE

IKE si occupa dell'autenticazione dell'identità dell'interlocutore, mentre AH e ESP dell'autenticazione della provenienza dei dati. La prima è volta a garantire che l'interlocutore è chi effettivamente sostiene di essere, mentre la seconda è volta a garantire che i dati ricevuti provengano effettivamente dall'interlocutore identificato dalla prima.

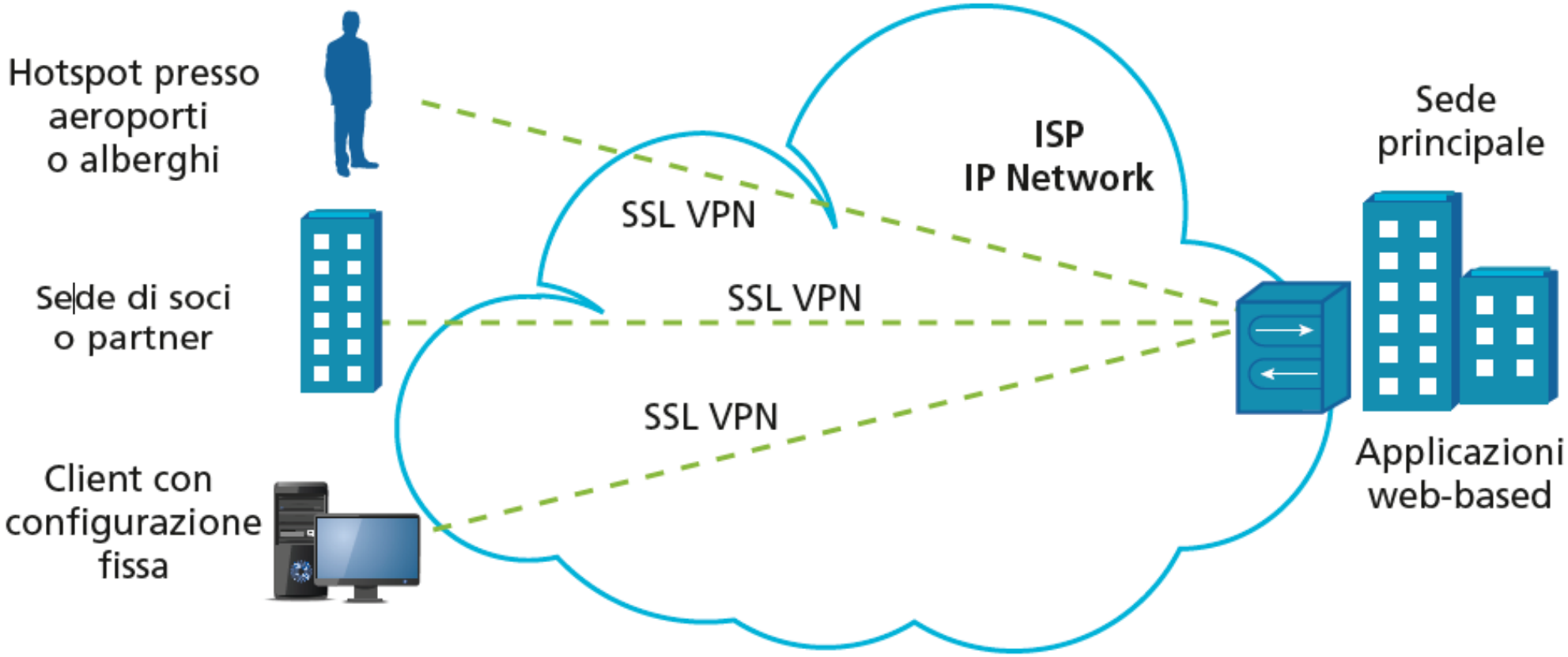
PROTOCOLLI PER LA SICUREZZA NELLE VPN: SSL/TLS

Una valida alternativa a IPsec è rappresentata dall'utilizzo dei protocolli **SSL/TLS** (*Secure Sockets Layer/Transport Layer Security*).

Le differenze tra i due protocolli sono poche e marginali, tuttavia sono non compatibili. In generale, vengono implementati entrambi e viene garantita l'**interoperabilità**.

PROTOCOLLI PER LA SICUREZZA NELLE VPN: SSL/TLS

VPN SSL/TLS-based: possibile scenario



PROTOCOLLI PER LA SICUREZZA NELLE VPN: SSL/TLS

TLS è un protocollo di livello Session dello stack ISO/OSI. Opera quindi al di sopra del protocollo di livello Transport. È uno standard IETF e deriva dal protocollo SSL.

SSL è stato originariamente proposto da Netscape Communications, ma è un protocollo open.

PROTOCOLLI PER LA SICUREZZA NELLE VPN: SSL/TLS

Il protocollo SSL/TLS è composto da due livelli: **Record Protocol** e **Handshake Protocol**.

HTTP/HTTPS	Application
SSL/TLS Handshake Protocol	Session
SSL/TLS Record Protocol	
TCP	Transport
IP	Network

PROTOCOLLI PER LA SICUREZZA NELLE VPN: SSL/TLS

Il **Record Protocol** opera subito sopra un protocollo di livello Trasporto affidabile (come TCP) ed è utilizzato per incapsulare protocolli di livello superiore.

L'**Handshake Protocol** si occupa della fase di negoziazione in cui si autentica l'interlocutore e si stabilisce la crittografia comune.

La realizzazione di una **VPN SSL/TLS-based** passa innanzitutto attraverso l'uso di **SSL/TLS**, al posto di IKE dell'IPsec, per la fase di **autenticazione** degli estremi del tunnel e la creazione delle **chiavi**.

PROTOCOLLI PER LA SICUREZZA NELLE VPN: SSL/TLS

SSL/TSL è un semplice protocollo Client/Server che ha lo scopo di autenticare il server da parte del client e, opzionalmente, anche il client da parte del server, e di creare un canale cifrato, sicuro, di comunicazione tra i due.

LO SAI CHE

Diverse versioni del protocollo SSL/TLS sono ampiamente utilizzate in applicazioni come i browser, le e-mail, la messaggistica istantanea e il voice over IP (VoIP). Un esempio di applicazione è nel protocollo HTTPS.

PROTOCOLLI PER LA SICUREZZA NELLE VPN: SSL/TLS

L'autenticazione è basata sui **certificati digitali** riconosciuti da una Certification Authority.

Il server invia il proprio certificato firmato dalla CA al client che ne verifica la validità confrontandone la **firma digitale** con quella della CA a lui nota. Se la firma digitale è valida, accetta il certificato e autentica il Server.

Analogamente il server può chiedere il certificato al client per verificarne la validità e procedere con l'autenticazione, a quel punto reciproca.

PROTOCOLLI PER LA SICUREZZA NELLE VPN: SSL/TLS

Passi necessari per stabilire una connessione sicura:

1) **Client** → **Server**: il client invia al server la richiesta di connessione includendo la lista degli algoritmi di crittografia supportati e un valore random necessario a creare la **pre-master-key**, che a sua volta servirà a generare la chiave privata di crittografia comune a entrambi.

PROTOCOLLI PER LA SICUREZZA NELLE VPN: SSL/TLS

2) **Server** → **Client**: il server invia al client il proprio certificato digitale, la scelta dell'algoritmo di crittografia, il proprio valore casuale per la pre-master-key e la richiesta del certificato del client.

3) **Client** → **Server**: il client verifica il certificato del server e, se la verifica risulta negativa, il protocollo fallisce; altrimenti invia al server il proprio certificato digitale e la pre-master-key cifrata con la chiave pubblica del server. Infine il client accoda la richiesta di passare a comunicazioni cifrate a partire dai pacchetti seguenti.

PROTOCOLLI PER LA SICUREZZA NELLE VPN: SSL/TLS

4) **Server** → **Client**: il server conferma al client di aver accettato il suo certificato digitale e passa alla fase di comunicazioni cifrate.

NB: Dopo il punto 3 sia il client che il server hanno tutte le informazioni necessarie per calcolare la chiave, comune ad entrambi, e gli algoritmi a cui applicarla.

PROTOCOLLI PER LA SICUREZZA NELLE VPN: IPsec vs SSL/TLS

SSL/TLS è adatto a proteggere la comunicazione tra due applicazioni (autentica l'applicazione o l'utente), **IPsec** può facilmente rendere sicuro il traffico tra host o tra intere sottoreti (autentica la macchina).

Principali differenze tra i due protocolli.

IPsec	SSL/TLS
Architettura complessa.	Singoli protocolli.
Peer-to-peer (IKE).	Client/Server.
Livello Network.	Livello Session.
Canale tra due macchine.	Canale tra due applicazioni.
Protezione di tutto il traffico IP.	Protezione solo del traffico TCP.
Protezione di tutto ciò che segue l'header IP.	Protezione dei dati del livello Application.
Impatto maggiore sul sistema operativo.	Impatto maggiore sulle applicazioni.

VPN DI FIDUCIA E VPN SICURE

Le reti VPN possono essere classificate in base ai protocolli che utilizzano e al grado di sicurezza che garantiscono, in tre categorie:

- **Trusted** VPN
- **Secure** VPN
- **Hybrid** VPN

VPN DI FIDUCIA E VPN SICURE

Nelle **Trusted VPN** la riservatezza dei dati trasmessi attraverso Internet è controllata da un Internet Service Provider (ISP).
Queste non utilizzano i protocolli che permettono la cifratura ed il conseguente tunneling dei dati trasmessi. L'ISP assicura una qualità del servizio (QoS) attraverso l'utilizzo ed il controllo di percorsi dedicati, garantendo che nessun altro possa usufruire del canale assegnato ad una determinata VPN in un determinato momento. L'azienda che si rivolge all'ISP ha fiducia che i percorsi attraverso cui i suoi dati si muovono siano mantenuti sicuri.

VPN DI FIDUCIA E VPN SICURE

Le **Secure VPN** utilizzano protocolli che consentono la cifratura e il tunneling.

Per essere definita tale, una VPN deve garantire:

- La presenza di un sistema di autenticazione;
- Che i dati viaggino criptati;
- Che il livello di cifratura dei dati sia elevato e modificabile nel tempo.

VPN DI FIDUCIA E VPN SICURE

Le **Hybrid VPN** rappresentano il tentativo di unire le caratteristiche delle Trusted VPN e delle Secure VPN, infatti le **Secure VPN** assicurano la cifratura dei dati ma non assicurano i percorsi; le **Trusted VPN** assicurano le proprietà dei percorsi ma non garantiscono un alto livello di sicurezza.