2 SERVICII DE SECURITATE ÎN REȚELELE FINANCIARE DESCHISE

2.1 Securitatea rețelelor financiare deschise (RFD)
2.2 Modelul OSI de securitate cifrografică
2.3 Servicii de securitate la nivel Legătură
2.4 Servicii de securitate la nivel Rețea
2.5 Servicii de securitate la nivel Aplicație

2 SERVICII DE SECURITATE RFD

Securitatea tranzacțiilor de i-comerț acoperă:

- **securitatea accesului la serviciu;**
- **identificarea corectă și autentificarea participanților;**
- **integritatea schimburilor;**
- **de obicei, confidențialitatea schimburilor;**
- **păstrarea probelor pentru soluționarea disputelor și litigiilor.**

Toate aceste măsuri de protecție pot face față așteptărilor utilizatorilor privind anonimatul și netrasabilitatea tranzacțiilor.

4.1 Obiectivele securității rețelelor financiare deschise

Obiectivele măsurilor de securitate în i-comerț sunt:

- **prevenirea faptului ca un intrus să citească sau să manipuleze conținutul sau secvențele mesajelor schimbate fără a fi detectat;**
- **împiedicarea falsificării instrucțiunilor de plată sau generării de mesaje false de către utilizatori cu intenții dubioase. De exemplu, comercianții și centrele de procesare nu trebuie să fie în stare să reutilizeze informațiile despre conturile bancare ale clienților lor pentru a genera comenzi frauduloase;**
- **respectarea cerințelor legale privind, de exemplu, revocarea plăților, soluționarea conflictelor, protecția consumatorilor, protecția vieții private și exploatarea datelor colectate privind clienții în scopuri comerciale;**
- **asigurarea accesului fiabil la serviciul de i-comerț, în conformitate cu termenii contractului;**
- **pentru un anumit serviciu, furnizarea aceluiași nivel de deservire tuturor clienților, indiferent de locația acestora și de variabilele de mediu. ♦**

4.2 Modelul OSI de securitate cifrografică

4.2.1 Modelul de referință OSI .....

4.2.2 Servicii de securitate: definiții și localizare

Securitatea constă în șase servicii (cerințe):

1. *Confidențialitatea*, adică mesajele (în unele cazuri și adresele) ce se transmit nu sunt divulgate unei terțe părți neautorizate.

2. *Integritatea datelor*, adică dovada faptului că mesajul nu a fost modificat după ce a fost expediat și înainte de primirea acestuia.

3. *Identificarea*, adică verificarea unei relații prestabilite între o caracteristică (parolă, cheie cifrografică, etc.) și o entitate.

4. *Autentificarea* participanților (utilizatori, entități de rețea și i-sisteme) constă în coroborarea identității pe care o entitate o revendică cu garanția unei terțe părți de încredere.

5. *Controlul accesului* pentru a se asigura că doar participanții autorizați a căror identitate a fost autentificată pot avea acces la resursele protejate.

6. *Nonrepudierea* (autentificarea originii datelor) – serviciul care oferă dovada integrității datelor și a originii acestora într-un mod care poate fi verificat de o terță parte, de exemplu, nonrepudierea că expeditorul a trimis mesajul sau că un destinatar a primit mesajul. ♦

4.2.2 Servicii de securitate: definiții și localizare

Implementarea serviciilor de securitate se poate face în cadrul unuia sau a mai multe straturi ale modelului OSI. Alegerea stratului depinde de mai mulți factori.

Dacă protecția trebuie să fie acordată întregului flux de date într-o manieră uniformă, intervenția trebuie să fie la stratul Fizic sau cel Legătură.

Singurul serviciu cifrografic disponibil în cadrul acestor straturi este *Confidențialitatea*, ce se realizează prin cifrarea datelor sau folosirea unor mijloace similare (salturi de frecvență, spectru extins, etc.).

Protecția traficului în cadrul stratului Fizic acoperă tot fluxul, nu doar datele utilizatorului, ci și informațiile legate de administrarea rețelei: alarme, sincronizare, actualizarea tabelului de rutare și așa mai departe.

Dezavantajul protecției în cadrul stratului Fizic – un atac de succes va destabiliza întreaga structură de securitate, deoarece aceeași cheie este utilizată pentru toate transmisiile.

În cadrul stratului Legătură, cifrarea poate fi capăt-la-capăt (sursă-destinație), cu condiția ca aceeași tehnologie să fie utilizată pe tot traseul.

4.2.2 Servicii de securitate: definiții și localizare

Cifrarea în cadrul stratului Rețea realizează o protecție selectivă în vrac; acoperă toate transferurile de date asociate cu o anumită subrețea de la un sistem final la alt sistem final.

Securitatea în cadrul stratului Rețea este necesară și pentru a asigura comunicarea între componentele rețelei, în special pentru protocoalele stare-legături, în cazul cărora actualizările tabelelor de rutare sunt generate automat pe baza informațiilor primite, apoi sunt inundate în rețea.

Pentru protecție selectivă cu recuperare după o eroare sau dacă rețeaua nu este fiabilă, serviciile de securitate vor fi aplicate în cadrul stratului Transport. Serviciile acestui strat se aplică capăt-la-capăt. Aceste servicii sunt: Autentificarea, Controlul accesului, Confidențialitatea și Integritatea.

Dacă este necesară o protecție mai granulară sau dacă trebuie asigurat serviciul Nerepudiere, cifrarea se va efectua în cadrul stratului Aplicație. În cadrul acestui strat sunt disponibile toate serviciile de securitate, funcționează majoritatea protocoalelor de securitate pentru sistemele comerciale, ceea ce le eliberează de dependența de straturile inferioare.

4.2.2 Servicii de securitate: definiții și localizare

Nu există servicii de securitate la nivelul Sesiune.

Serviciile oferite la nivelul Prezentare sunt: Confidențialitate, care poate fi selectivă, de exemplu pentru un anumit domeniu de date; Autentificare, Integritate (integrală sau parțială) și Nerepudiere cu o dovadă a originii sau o dovadă a livrării.

De exemplu, protocoalele SSL/TLS sunt utilizate pe scară largă pentru a asigura conexiunea dintre un client și un server. În ceea ce privește modelul de referință TCP/IP, protocoalele SSL/TLS se aplică între stratul Transport și cel Aplicație.

În unele cazuri, poate fi suficient ca un atacator să descopere că are loc o comunicare între parteneri și apoi să încerce să identifice, de exemplu:

- caracteristicile bunurilor sau serviciilor comercializate;
- condițiile de achiziție, cum ar fi intervalele de livrare, condițiile și modalitățile de decontare;
- decontarea financiară.

Crearea unui canal sau a unui "tunel" între două puncte la nivelul Rețea poate constitui un scut împotriva unor atacuri de asemenea tip. ♦

4.3 Servicii de securitate la nivel Legătură

RFC 1661 (1994) al IETF definește protocolul PPP pentru traficul între două entități de rețea învecinate identificate cu adresele IP respective.

Protocolul de tunelare de nivel 2 L2TP, definit în IETF RFC 2661 (1999) și dezvoltat în RFC 3931 (2005), extinde operarea PPP prin separarea procesării pachetelor IP în cadrul cadrelor PPP de cea a fluxului de trafic dintre cele două entități de rețea.

Această distincție permite unui client de la distanță să se conecteze la un server de acces la rețea (NAS) al unei rețele private (corporative) prin Internetul public:

- clientul încapsulează cadrele PPP într-un tunel L2TP;
- prefixează antetul corespunzător L2TP;
- transportă noul pachet IP utilizând UDP.

Adresele IP din noul antet IP sunt atribuite de furnizorul local de servicii Internet (ISP) la punctul de acces local.

4.3 Servicii de securitate la nivel Legătură

Figura ilustrează aranjamentul în care dimensiunea antetului suplimentar variază de la 8 la 16 octeți (1 la 2 octeți pentru PPP, 8 la 16 octeți pentru L2TP).

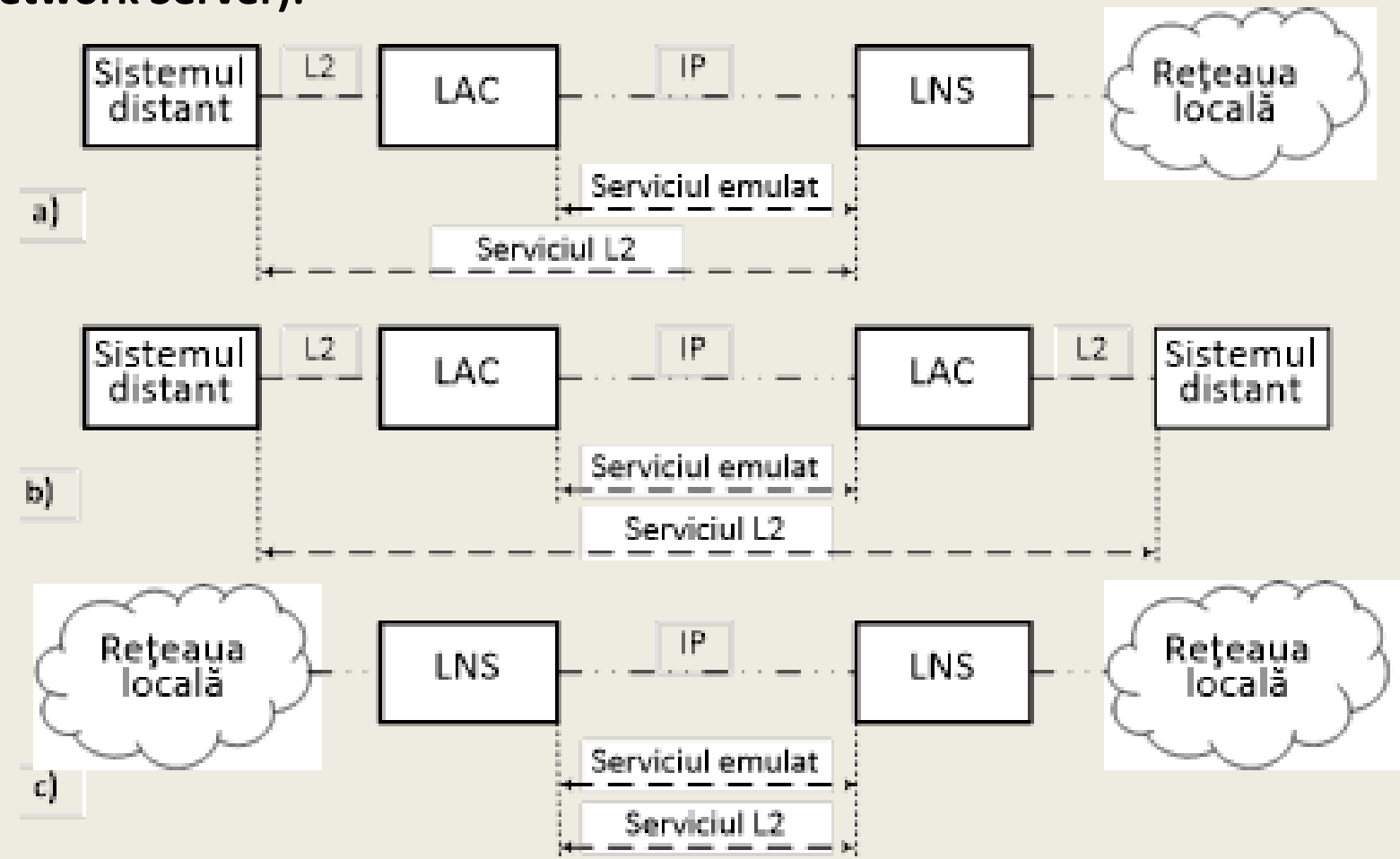
Având în vedere că câmpul pentru UDP este de 8 octeți și că antetul IP este de 20 de octeți, volumul total suplimentar este între 37 și 46 octeți.

Antet IP (nou)	Antet UDP (nou)	Antet L2TP	Antet PPP	Antet IP (original)	Antet TCP/UDP	Date

L2TP nu oferă servicii de securitate, dar este posibil să se utilizeze IPSec pentru a securiza tunelul de nivel 2, deoarece L2TP rulează pe IP (a se vedea s. 4.4). ♦

4.3 Servicii de securitate la nivel Legătură

Schemele de tunelare L2TP (LAC – L2TP Access Concentrator, LNS – L2TP Network Server):



L2TP nu oferă servicii de securitate, dar este posibil să se utilizeze IPSec pentru a securiza tunelul de nivel 2, deoarece L2TP rulează pe IP (a se vedea s. 4.4). ♦

4.4 Servicii de securitate la nivel Rețea

Serviciile de securitate de la nivel Rețea sunt oferite capăt-la-capăt și includ: Controlul accesului la rețea, Autentificarea utilizatorilor și/sau a gazdelor, Autentificarea și Integritatea transferurilor de date.

Aceste servicii sunt transparente pentru aplicații și utilizatorii finali, iar responsabilitățile lor revin administratorilor entităților de rețea.

Autentificarea la nivel Rețea poate fi simplă sau puternică. Autentificarea simpla utilizează perechea nume și parolă (parola poate fi una de unică folosință), în timp ce autentificarea puternică utilizează semnăturile numerice sau schimbul de certificate emise de o autoritate de certificare recunoscută (CA).

Utilizarea autentificării puternice necesită prezența cheilor de cifrare la toate nodurile de rețea, ceea ce impune protecția fizică a tuturor acestor noduri.

4.4 Servicii de securitate la nivel Rețea

IPSec este o suită de protocoale definită pentru securizarea transferurilor de date la nivel Rețea (IP) între două entități. Documentația IPSec este disponibilă în IETF RFC 6071 (2011). Arhitectura generală de securitate a IPSec-v2 este descrisă în IETF RFC 2401; arhitectura IPSec-v3 este descrisă în RFC 4301 (2005).

IPSec oferă autentificare, confidențialitate și gestionarea cheilor, nefiind legat de algoritmi cifrografici specifici.

IPsec foloseşte autentificarea şi cifrarea fiecărui pachet de date. El permite autentificarea reciprocă a respondenţilor la începutul sesiunii de lucru şi, de asemenea, negocierea cheilor criptografice de folosit în cadrul acesteia.

Pentru a folosi IPsec, nu se cer careva modificări speciale în cadrul aplicaţiei. IPsec asigură protecţia traficului de date într-o reţea IP pentru orice aplicaţie.

Serviciile IPsec necesare sunt oferite prin selectarea adecvată a protocoalelor de securitate, a algoritmilor cifrografici şi a cheilor cifrografice. IPsec este de tip terminal-terminal şi poate fi folosit pentru protecţia unuia sau a mai multor fluxuri de date între:

a) o pereche de staţii;

b) o pereche de porţi de securitate;

c) o poartă de securitate şi o staţie.

Poartă de securitate se numeşte un sistem intermediar care are implementat IPsec, de exemplu o i-barieră (firewall) sau un ruter IPsec activat.

4.4 Servicii de securitate la nivel Rețea

Pentru asigurarea serviciilor de securitate a traficului de date, IPsec foloseşte două protocoale: Antetul de autentificare (*Authentication Header* – AH) şi Încapsularea securizată a sarcinii utile (*Encapsulating Security Payload* – ESP). Implementările IPsec trebuie să suporte ESP şi pot să suporte AH. Există foarte puţine cazuri, când ESP nu poate, iar AH poate îndeplini funcţionalităţile necesare de securitate. Atât AH, cât şi ESP oferă controlul accesului, fortificat prin distribuirea cheilor criptografice şi gestiunea fluxurilor de trafic.

Ambele protocoale, AH şi ESP, pot fi folosite aparte sau împreună. Fiecare din ele poate opera atât în modul Transport, cât şi în cel Tunel. În modul Transport, AH şi ESP oferă protecţia în primul rând pentru protocoalele de nivel superior, pe când în modul Tunel – pentru pachetele IP tunelate.

În modul Transport, doar sarcina utilă a pachetelor IP este, de obicei, securizată. Nivelele Transport şi Aplicaţie întotdeauna sunt securizate prin haşare, de aceea acestea nu pot fi nicicum modificate. Operaţiile ce ţin de rutare rămân intacte, deoarece acestea necesită modificări în antetul IP.

În modul Tunel, este securizat întregul pachet IP, acesta fiind încapsulat într-un nou pachet IP, inclusiv un nou antet IP.

Pentru funcţionare, atât AH, cât şi ESP folosesc Asociaţii de securitate (*Security Associations* – SA).

4.4 Servicii de securitate la nivel Rețea

Protocolul *Authentication Header* – AH, definit în RFC 4302 (2005) și RFC 7321 (2014), furnizează servicii de autentificare și integritate pentru sarcina utilă și informațiile de rutare din antetul IP original şi, opţional, protecţia contra atacurilor de replicare a pachetelor IP.

AH operează deasupra IP, folosind protocolul 51 (RFC 5237). El protejează toate câmpurile pachetelor IPv4, cu excepţia câmpurilor antetului ce se modifică pe parcursul transmisiei (DSCP/TOS, ECN, *etc.*).

Protocolul *Encapsulating Security Payload* – ESP, descris în RFC 4303 (2005) și RFC 7321 (2014) și asigură protecţia autenticităţii originii, integrităţii, confidenţialităţii şi, opţional, protecţia contra atacurilor de replicare a pachetelor IP. Astfel, ESP, pe lângă funcţionalităţile AH, asigură şi confidenţialitatea.

ESP poate suporta, la necesitate, doar funcţiile de cifrare sau doar de autentificare, deşi folosirea cifrării fără autentificare nu este sigură.

ESP operează deasupra IP, folosind numărul de protocol 50. Spre deosebire de AH, ESP în modul Transport nu asigură integritatea și autentificarea pentru întregul pachet IP. Însă, în modul Tunel, în care întregul pachet IP iniţial este încapsulat într-un pachet ESP, acesta asigură protecţia întregului pachet IP intern, dar nu asigură o asemenea protecţie pentru antetul extern al pachetului (opţiunile externe ale IPv4 sau antetele de extensie IPv6).

4.4 Servicii de securitate la nivel Rețea

Ambele protocoale AH și ESP protecția împotriva atacurilor de repetare (replay) o oferă cu ajutorul unui număr de secvență care crește în mod monoton și care are lungimea de 64 de biți.

Schimbul de chei se efectuează cu versiunea 2 a protocolului Internet Key Exchange (IKE), definit în RFC 7296 (2014) și RFC 7427 (2015).

***Asociaţia de securitate* (SA) este o „conexiune" unidirecţională, care oferă servicii de securitate pentru traficul respectiv de date. Ea este reprezentată de un set de algoritmi și parametri, de exemplu chei, care se folosesc pentru cifrarea şi autentificarea unui flux unidirecţional de date. În cazul de fluxuri bidirecţionale, securizarea în cauză se efectuează de către o pereche de SA. Serviciile de securitate sunt oferite unei SA prin folosirea AH sau ESP, dar nu a ambelor protocoale împreună. Dacă pentru un flux de date se aplică ambele protocoale AH şi ESP, atunci este necesară crearea a două SA.**

IPsec foloseşte, în funcţie de implementare, aşa standarde, algoritmi şi modele de securitate ca: Algoritmul DES, Algoritmul DES triplu, Modelul Diffie-Hellman, Message Digest 5 (MD5), Algoritmul de haşare securizată (SHA-1), Semnătura RSA, Internet Key Exchange (IKE), Autorităţi de certificare ş.a. Implicit, pentru cifrare/descifrare, IPsec foloseşte algoritmul DES cu chei de 56 biţi.

4.4 Servicii de securitate la nivel Rețea

Ambele protocoale AH și ESP protecția împotriva atacurilor de repetare (replay) o oferă cu ajutorul unui număr de secvență care crește în mod monoton și care are lungimea de 64 de biți.

Modul Tunel de funcţionare a IPsec este modul implicit de folosire a IPsec. În acest mod, întregul pachet original IP este protejat de IPsec. În acest scop, IPsec împachetează pachetul original IP, îl cifrează, adaugă la acesta un nou antet IP şi apoi îl transmite către celălalt capăt al tunelului IPsec. Pentru securizare în modul Tunel, IPsec poate folosi ESP – IPsec(ESP), AH – IPsec(AH) sau ambele facilităţi împreună. Totuşi, mai frecvent în acest scop se foloseşte ESP.

AH protejează întregul pachet original, dar nu şi toate câmpurile noului antet IP, deoarece conţinutul unora din acestea se modifică la tranzitarea nodurilor de reţea. AH protejează toate acele câmpuri ale noului antet IP, care nu se modifică la tranzitarea nodurilor de reţea.

Modul Tunel al IPsec este folosit, de obicei, pentru securizarea transferurilor de date între o pereche de porţi de reţea sau de la o staţie către o poartă, în ultimul caz poarta operând ca un proxy pentru staţiile din aria lui.

4.4 Servicii de securitate la nivel Rețea

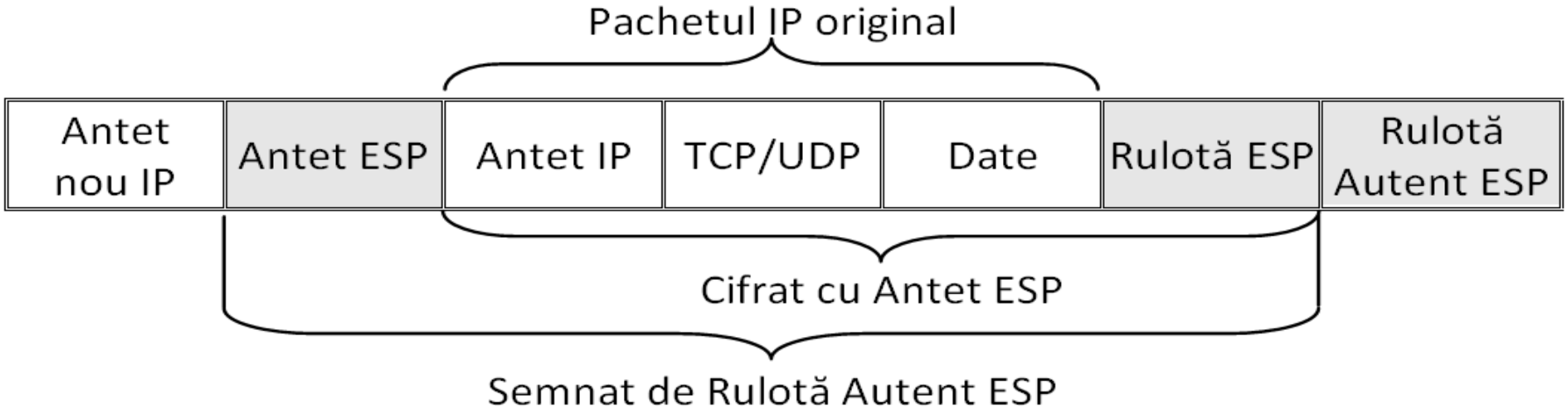


Figura 1 – Schema modului Tunel IPsec(ESP)

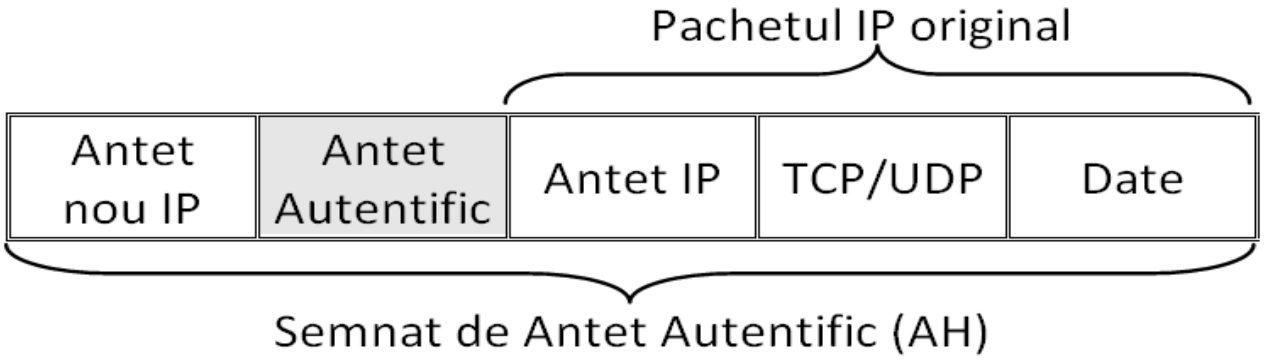


Figura 2 – Schema modului Tunel IPsec(AH)

4.4 Servicii de securitate la nivel Rețea

Modul Transport de funcţionare a IPsec serveşte pentru comunicări punct terminal-punct terminal, protejând întregul pachet original IP. În acest scop, IPsec împachetează pachetul original IP, îl cifrează, adaugă la acesta antetul original IP şi apoi îl transmite către celălalt capăt al tunelului IPsec. Pentru securizare în modul Transport, IPsec poate folosi ESP – IPsec(ESP), AH – IPsec(AH) sau ambele facilităţi împreună. Totuşi, mai frecvent în acest scop se foloseşte ESP.

Spre deosebire de modul Tunel, în modul Transport ESP (și cel Transport AH) în calitate de antet IP nou se foloseşte o copie a celui IP original cu modificări minore, inclusiv identificarea ESP (AH) în cadrul acestuia cu numărul de protocol Internet 50 (51). Astfel, noul antet IP nu este protejat.

Modul Transport al IPsec este folosit, de obicei, pentru securizarea transferurilor de date între două staţii, din care una este client, iar cealaltă este server, sau între o stație şi o poartă, ultima fiind tratată ca o staţie-gazdă. Ca exemplu ap putea servi o sesiune Telnet de la o staţie către un server.

4.4 Servicii de securitate la nivel Rețea

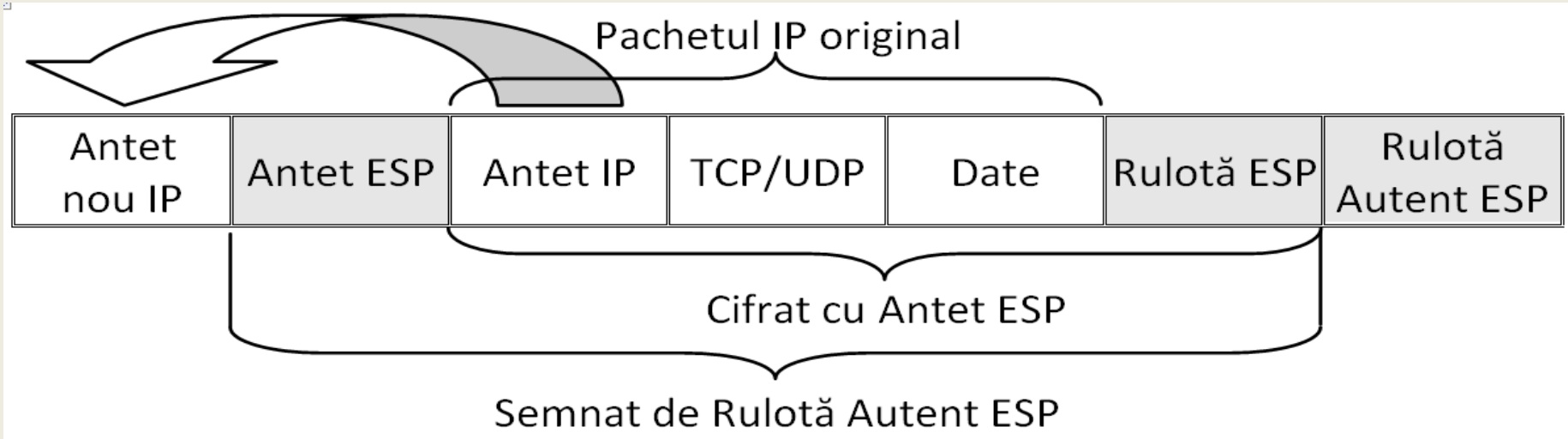


Figura 3 – Schema modului Transport IPsec (ESP)

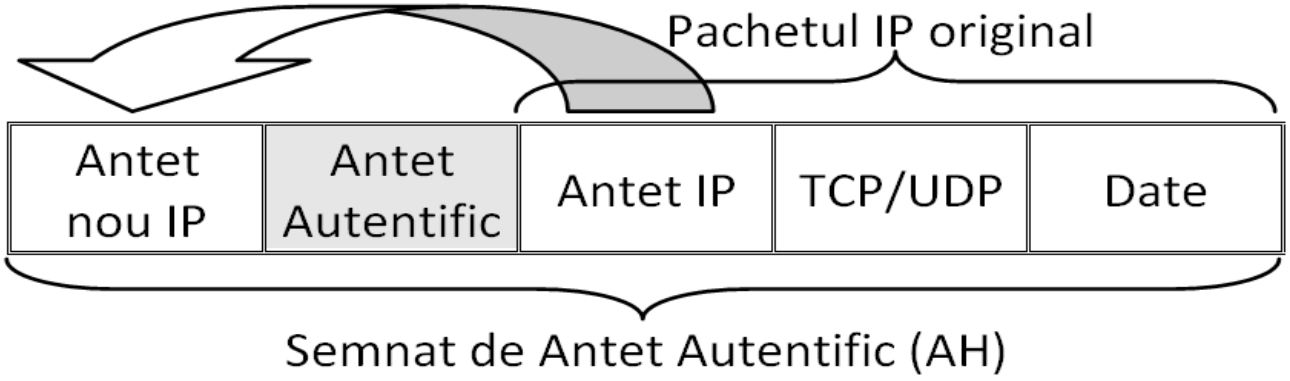
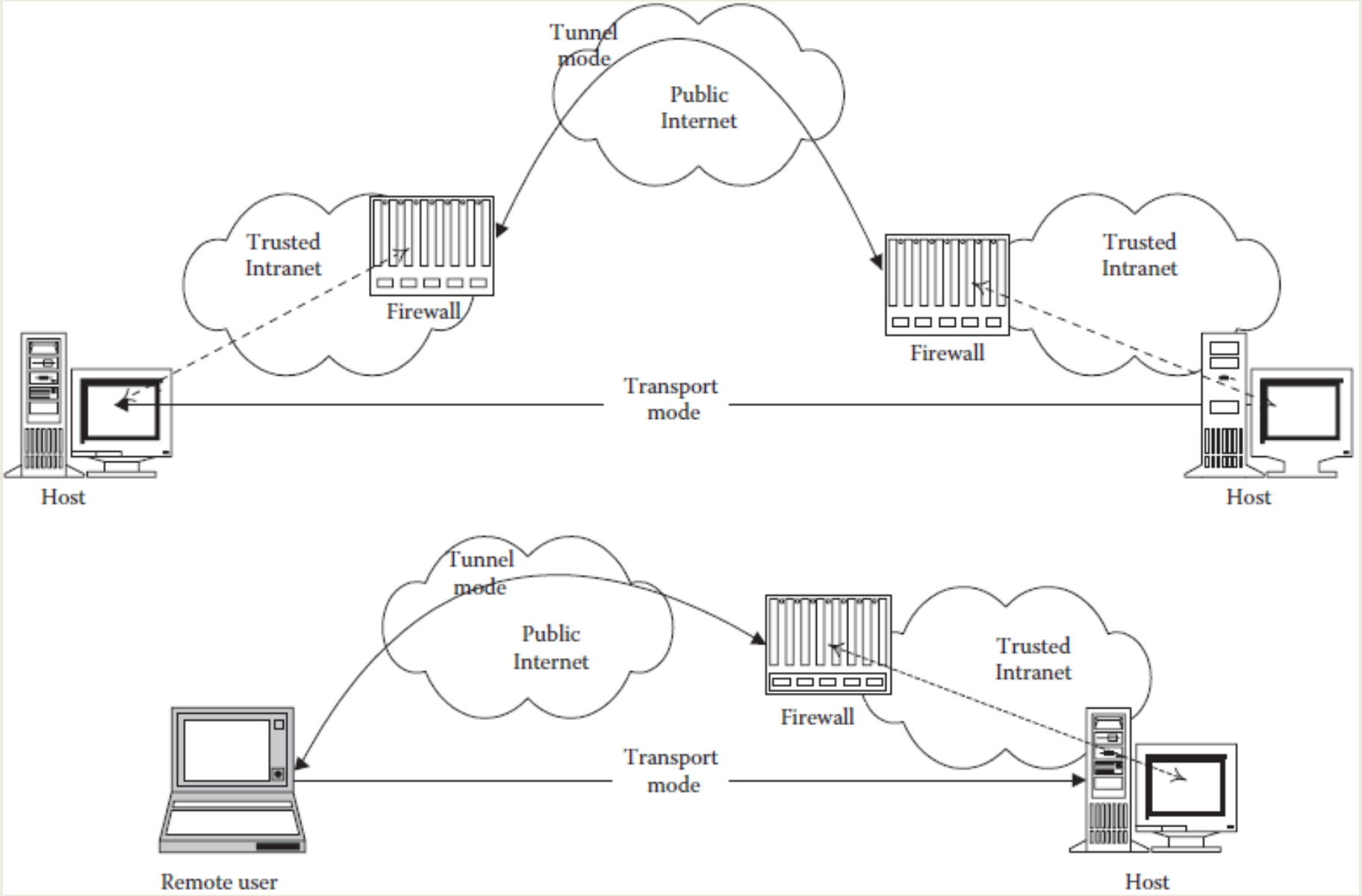


Figura 4 – Schema modului Transport IPsec (ESP)

VPN cu IPSec [3]



4.5 Servicii de securitate la nivel Aplicație

Majoritatea protocoalelor de securitate pentru i-comerț funcționează la nivelul Aplicație, ceea ce le face independente de straturile inferioare. La acest nivel, întreaga gamă de servicii de securitate este disponibilă:

1. **Confidențialitate, totală sau selectivă pe câmp sau pe fluxul de trafic.**
2. **Integritatea datelor.**
3. **Autentificare entităților perechii.**
4. **Autentificare sursei entităților perechii.**
5. **Controlul accesului.**
6. **Nerepudierea transmiterii cu dovada sursei.**
7. **Nerepudierea recepției cu dovada recepției.**

Secure shell (SSH), de exemplu, oferă securitate la nivel Aplicație și permite utilizatorului conectarea, execuția de comenzi și transferul de fișiere în siguranță.

Drepturile de proprietate intelectuală asupra articolelor dematerializate vândute online reprezintă o provocare intelectuală și tehnică. Scopul este de a preveni reproducerea ilegală a ceea ce este ușor de reprodus prin utilizarea "filigranelor" încorporate în produs. Mijloacele utilizate diferă în funcție de faptul că produsele protejate sunt efemere (cum ar fi știrile), orientate către consumatori (cum ar fi filme, muzică, cărți, articole sau imagini) sau pentru producție (cum ar fi i-aplicațiile întreprinderii).

4.5 Servicii de securitate la nivel Aplicație

Mecanismele suplimentare de securitate sunt specifice unei anumite utilizări sau aplicației utilizatorului final la îndemână. De exemplu, sunt considerați câțiva parametri suplimentari pentru a asigura plățile electronice, cum ar fi plafonul cheltuielilor permise sau retragerile într-un interval de timp predefinit.

Detectarea și gestionarea fraudelor depind de supravegherea:

- **activități la punctele de vânzare (terminale de comerț, automate, etc.);**
- **evenimente pe termen scurt;**
- **tendințe pe termen lung, cum ar fi comportamentul unei subpopulații, într-o zonă geografică și într-un anumit interval de timp.**

În asemenea cazuri, gestionarea auditului ia în considerare alegerea evenimentelor de colectare și/sau înregistrare, validarea unei piste de audit, definirea pragurilor de alarmă pentru încălcările de securitate suspectate și așa mai departe. ♦

.