UNIVERSITATEA TEHNICĂ CLUJ-NAPOCA

DEPARTAMENTUL ELECTROTEHNICĂ ŞI MĂSURĂRI

Cursul 13 REŢELE PRIVATE VIRTUALE

Introducere curs	În acest curs sunt analizate re□elele private virtuale.
Obiective curs	• Componentele unei conexiuni VPN. • Proprietăţile conexiunii VPN. • Conexiuni VPN prin Internet sau intranet. • Protocoale utilizate în tunelările VPN. • Criptarea datelor.
Durată medie de studiu individual	Durata medie de studiu individual: 100 minute. Acest interval de timp presupune parcurgerea continutului cursului şi rezolvarea testelor de autoevaluare

Cuprins:

13.1. Introducere.

Acest capitol descrie o familie de tehnologii care permit "transferul" informaţiilor între clienţi individuali, sau reţele locale private (LAN), de-a lungul unei reţele publice care foloseşte protocolul IP *(Internet Protocol)*. Clienţii individuali, sau reţelele locale interconectate, se consideră reţele private, iar noua structură distribuită în mai multe locaţii, dar considerată o singură entitate, se numeşte reţea privată virtuală *(Virtual Private Network - VPN)*. Această entitate utilizează pentru "transportul" reţelei private virtuale procedee de încapsulare multiplă de nivel OSI 3 *(PPTP- Point to Point Tunneling Protocol)*, sau OSI 2 *(L2TP - Layer Two Tunneling Protocol)*.

O reţea privată virtuală este o entitate formată din mai multe reţele locale, aparţinând unor domenii de coliziuni diferite, conectate între ele prin intermediul unor legături publice sau medii de transmisie comune altor reţele, spre exemplu Internet. Datorită acestor legături publice, este periclitată

"intimitatea" datelor transmise. O astfel de rețea privată virtuală permite transmiterea datelor între două mașini, utilizând mediul public, prin simularea (virtual) unei legături private de tip punct la punct. Crearea, configurarea și utilizarea unei astfel de legături sunt definite ca **"VPN"**.

Pentru a simula o legătură punct la punct de acest tip, datele sunt încapsulate sau împachetate, adăugându-li-se un antet care furnizează informațiile de rutare necesare pentru ca acestea să poată străbate rețeaua publică și să ajungă la destinație. Pentru a nu se periclita "confidențialitatea" conținutului, aceste date sunt criptate la un capăt al acestei legături, urmând să fie decriptate la celălalt (la sosire). Acest tip de legătură se numește "conexiune **VPN**" [2, 3].

În **figura 13.1** se poate vedea o reprezentare schematică a conceptului de rețea privată virtuală (**VPN**). În cazul interceptării datelor pe legătura publică acestea nu pot fi descifrate decât dacă se cunoaște cheia de criptare.

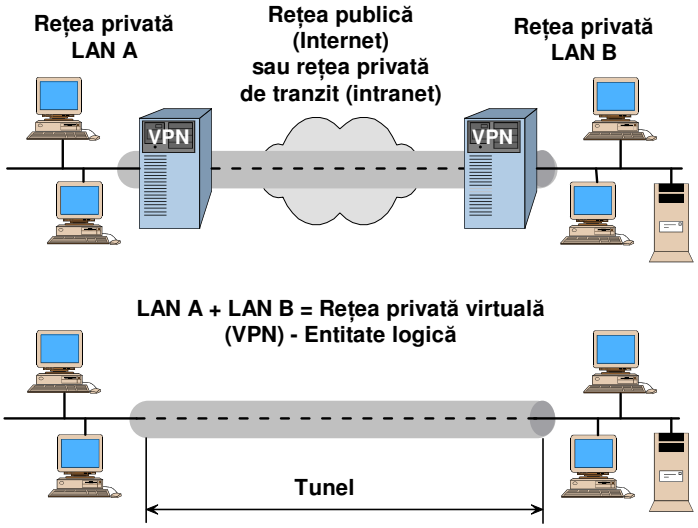

Fig. 13.1. Reprezentarea conceptului de rețea privată virtuală (**VPN**).

Conexiunile **VPN** permit utilizatorilor să lucreze de acasă, sau din altă locație, și să aibă acces la un server, sau o rețea locală, folosind infrastructura oferită de un furnizor public de servicii de rețea.

Din punctul de vedere al utilizatorului **VPN** este o conexiune punct la punct între două mașini, clientul **VPN** și serverul a căror resurse le solicită (**VPN** server). Configurația exactă a rețelei publice, sau tehnologiile de transmisie folosite, nu au nici o importanță atâta timp cât legătura apare ca o conexiune privată.

Conexiunile **VPN** permit rutarea pachetelor provenite de la diferite rețele locale, separate geografic, ale aceleiași instituții, prin intermediul unor "canale" care asigură confidențialitatea" datelor, ca și când aceasta ar dispune de propriile sale conexiuni de tip **WAN**.

Atât conexiunile directe la servere aflate la distanță (remote servers) cât și la rețele locale (rutate), conexiunile **VPN** permit unei organizații să facă tranzacții securizate prin rețele publice (dial-up, linii închiriate sau Internet).

13.2. Componentele unei conexiuni VPN.

O conexiune VPN include câteva componente prezentate în **figura 13.2.**

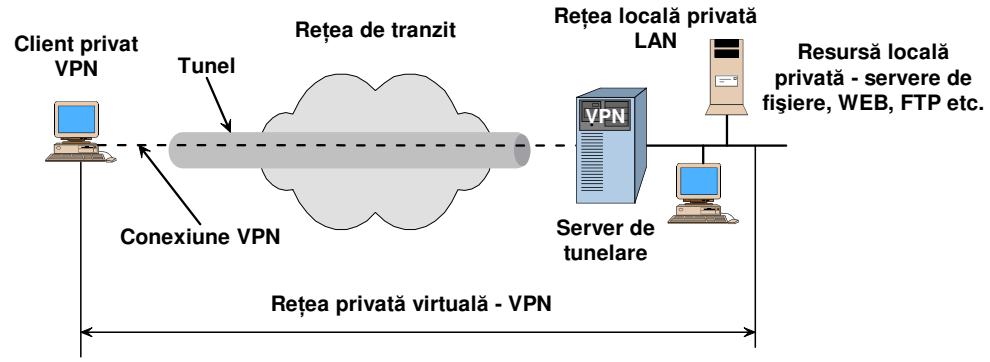

Fig. 13.2. Componentele conexiunii VPN.

1. **Serverul VPN** - este o maşină care asigură o legătură cu un client de **VPN** şi poate furniza accesul acestuia la resursele de rețea, sau o conexiune **VPN** între rutere. Sistemele de operare Microsoft Windows NT 4.0 şi 2000 (NT 5) sunt dotate cu componente care asigură accesul de la distanță *(**RAS** - Remote Access Server)* şi rutarea unei conexiuni **VPN** *(**RRAS** - Routing RAS)* ceea ce le permite realizarea de conexiuni **VPN** cu alte sisteme de operare produse de Microsoft.

2. **Clientul VPN** - este o maşină care inițiază o conexiune **VPN** (cerere adresată unui server **VPN**). Acesta poate să fie un calculator individual care face o cerere pentru a obține acces la un server de **VPN**, sau un ruter aparținând unei rețele locale (**LAN**) prin care se stabileşte o conexiune **VPN** (route-to-router **VPN** connection). Sistemele de operare Microsoft Windows sunt dotate cu componentele necesare stabilirii de conexiuni VPN. Pentru sistemele Windows 95/98 aceste componente se găsesc sub forma unor dispozitive virtuale *(virtual private networking adapter)* "instalate" înaintea adaptorului de rețea pentru linia telefonică (dial-up adapter). În cazul în care este necesară o conexiune **VPN** cu un alt sistem de operare, un sistem de operare Microsoft Windows-client poate utiliza şi soluțiile **PPTP** *(Point-to-Point Tunneling Protocol)* sau **L2TP** *(Layer Two Tunneling Protocol)* prin utilizarea **IPSec** *(Internet Protocol Security)*.

3. **Tunel** (Tunnel), porțiunea dintr-o conexiune **VPN** prin care datele sunt încapsulate suplimentar pentru a fi transmise prin rețeaua publică.

4. **Conexiune VPN**, porțiunea din conexiune în care datele sunt criptate pentru securizare şi încapsulate.

Observație: Este posibilă realizarea de conexiuni care utilizează procese suplimentare de încapsulare (tunelare), fără criptarea datelor. Aceste conexiuni nu se consideră conexiuni VPN deoarece datele ne-criptate pot să fie interceptate.

5. **Protocolul de tunelare**, standardul de comunicație utilizat pentru crearea şi administrarea tunelului, încapsularea şi criptarea datelor private. Astfel de protocoale sunt **PPTP**, **L2TP** şi **IPSec**, prezentate în detaliu în acest capitol.

6. **Date tunelate**, datele trimise de-a lungul unei legături private punct la punct.

7. **Legătura de trecere publică** *(Transit Internetwork)*, porțiunea din rețeaua publică folosită pentru transferul datelor private încapsulate. Această porțiune este, de obicei, o rețea IP, publică sau chiar privată (Internet sau Intranet).

Crearea unei conexiuni **VPN** este foarte asemănătoare cu stabilirea unei conexiuni prin linia telefonică simplă (dial-up), sau de rutare suplimentară (demand-dial routing). Există două variante principale de conexiuni VPN, accesul de la distanță a unui server de conectare (remote access server), sau o conexiune securizată între două rutere aparținând unor rețele locale separate *(router-to-router VPN connection)*.

- **Conexiune VPN la distanță prin linie telefonică** *(Remote Access VPN Connection)* **comutată sau dedicată**.

Accesul de la distanță se face de către o maşină-client, sau un calculator personal care, pentru a se conecta la o rețea privată, inițiază o cerere de legătură adresată unui server de conectare (acces). Acesta furnizează resursele necesare unei conexiuni **VPN** şi accesul la o rețea, sau un alt serviciu privat (server de fişiere, date sau imprimare) la care este conectat.

Pentru un grad mai mare de securitate a conexiunii **VPN**, procesul de autentificare este reciproc şi are loc în faza de inițializare a legăturii. Clientul de la distanță, care face cererea de conectare (client **VPN**), se va "prezenta" serverului (autentifica), după care serverul se va autentifica şi el clientului. Este de remarcat că în cazul acestui tip de conexiune, pachetele de date au ca sursă chiar maşina client.

- **Conexiune VPN între rutere** *(Router-to-Router VPN Connection)***.**

O conexiune **VPN** între două rutere se stabileşte de către unul dintre acestea şi permite conectarea a două porțiuni ale unei rețele private (două rețele locale - **LAN** - distincte care aparțin administrativ aceleiaşi organizații). Serverul **VPN** furnizează o rută spre rețeaua la care acesta este conectat. Este de remarcat că în cazul acestui tip de conexiune, pachetele de date nu au ca sursă (decât în cazuri particulare) ruterul care serveşte unul dintre capetele conexiunii **VPN**, ci acestea provin de la alte maşini client. Ruterul care inițiază (cere) conexiunea **VPN** (client **VPN**) se autentifică ruterului care serveşte cererea (server **VPN**), iar acesta, pe bază de reciprocitate, va face la fel.

13.3. Proprietățile conexiunii VPN.

Conexiunile care folosesc PPTP şi L2TP alături de **IPSec**, sunt caracterizate de următoarele funcțiuni [2, 3]:

- Încapsulare,
- Autentificare,
- Criptarea datelor,
- Alocarea adresei, a numelui simbolic şi a serverului de nume.

Încapsularea

Tehnologiile folosite pentru realizarea conexiunilor **VPN** folosesc metode de încapsulare a datelor private, prin adăugarea unui antet (header) care să permită pachetelor să străbată porțiunea de rețea de tranzit şi să ajungă la destinația dorită (rețeaua privată destinație).

Autentificarea.

Autentificarea unei conexiuni VPN poate avea una dintre următoarele două variante:

- Autentificarea utilizatorului.

Pentru stabilirea unei conexiuni, serverul **VPN** cere clientului să se autentifice în faza de inițializare a conexiunii, pentru ca acesta să acesta să poată primi acces la resurse. Autentificarea reciprocă limitează posibilitatea unor servere false să intercepteze legătura şi să deturneze fluxul de date.

- Autentificarea datelor şi verificarea integrității acestora.

Pentru a verifica că datele trimise, de-a lungul unei conexiuni **VPN**, ajung acolo unde trebuie (la capătul corespunzător) şi nu suferă modificări pe parcurs, acestea conțin o secvență)sumă) de control criptată pe baza unei chei de criptare cunoscută doar de către maşina sursă şi destinație.

Criptarea datelor.

Pentru asigurarea confidențialității datelor private transmise de-a lungul unei conexiuni publice, acestea se criptează de către maşina sursă şi decriptate de către cea destinație. Acest proces poate avea loc doar dacă ambele maşini cunosc cheia de criptare corespunzătoare. Interceptarea pachetelor de date trimise de-a lungul unei conexiuni publice nu furnizează informați cu înțeles, fără cunoaşterea cheii de criptare. Lungimea acesteia este un parametru de securitate important deoarece durata decriptării, în cazul necunoaşterii cheii (proces posibil de altfel), este cu atât mai lungă cu cât lungimea cheii este mai mare. Decriptarea, în aceste condiții, necesită un volum semnificativ de resurse. De aceea se recomandă folosirea unei chei de criptare cu un număr de caractere cât mai mare posibil. Pe de altă parte, utilizarea unei chei de criptare un timp mai îndelungat (pentru o cantitate mare de date) creşte riscul descifrării acesteia. De aceea, tehnologia de criptare oferă posibilitatea schimbării cheii pe durata aceleiaşi conexiuni. Una dintre opțiunile de configurare a unei astfel de conexiuni este şi frecvența cu care trebuie schimbată cheia.

Alocarea adresei şi a serverului de nume.

La configurarea unui server **VPN**, se creează o interfață virtuală (de fapt o verigă suplimentară în lanțul de transmitere a datelor) care permite realizarea conexiunilor **VPN**. Când o maşină client face o cerere de stabilire a unei conexiuni **VPN**, se activează pe această maşină interfața virtuală care se conectează apoi la serverul **VPN**, stabilindu-se astfel conexiunea punct la punct securizată. Adresa **IP** a nodurilor de la capete poate fi furnizată dinamic de către serverul **VPN**, prin utilizarea unui serviciu **DHCP** (Dynamic Host Configuration Protocol) care operează pe această maşină, sau static prin utilizarea unei adrese de rețea şi a unei măşti. În cadrul aceluiaşi proces de inițializare a legăturii, are loc şi atribuirea adresei unui server de nume, **DNS** (Domain Name System, specific sistemelor de operare Unix) sau WINS (Windows Internet Name Service), aparținând rețelei la care este conectat serverul VPN.

13.4. Conexiuni VPN prin Internet sau intranet.

Conexiuni VPN prin Internet.

Aceste conexiuni se pot utiliza atunci când este nevoie de legături punct la punct securizate, între maşini singulare sau între rețele. De cele mai multe ori tronsoanele publice sunt parți din Internet sau Intranet-uri.

Conexiuni care traversează părți din Internet.

Utilizarea Internet-ului permite conectarea într-o rețea privată cu eliminarea legăturilor telefonice la distanțe mari, în cazul în care maşinile de la capetele conexiunii au legături directe la Internet.

Accesul de la distanță prin Internet.

Conectarea unui client individual.

Este de înțeles ca un client, care are nevoie de o legătură la o resursă aflată la distanță, să fie tentat să folosească o soluție cât mai ieftină cu putință. Legăturile telefonice la distanțe mari sunt scumpe, peste tot în lume. Se preferă, dacă este posibil, utilizarea unei legături locale la un server de conectare (NAS - Network Access Server) pus la dispoziție de un furnizor de servicii Internet (ISP). Deoarece acest furnizor oferă un mediu public de comunicare, clientul va avea nevoie de o conexiune **VPN**, până la serverul care oferă resursa necesară, care să-i protejeze datele împotriva interceptării.

În acest caz, clientul va activa "interfața" **VPN**, care se conectează la componenta corespunzătoare care operează pe maşina destinație (serverul care oferă resursa), tunelul astfel creat va permite transferul datelor private prin Internet, spre o maşină singulară sau spre o rețea locală (**figura 13.3**).

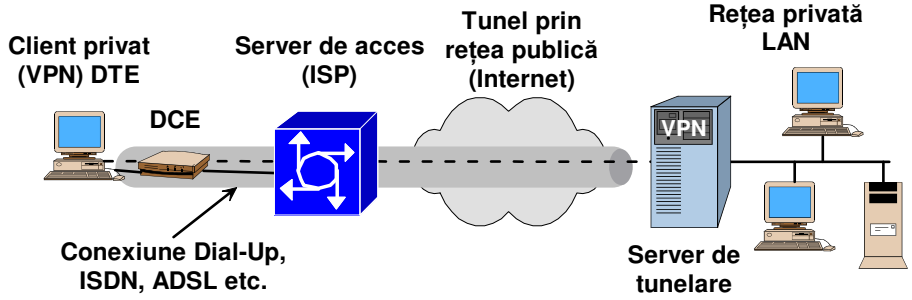

Fig. 13.3. Accesul prin Internet a unui client individual la o resursă privată.

Conectarea unor rețele, utilizând Internet.

Când se dorește interconectarea unor rețele locale prin Internet (aşa cum se poate vedea în **figura 13.4.**) se va folosi o poată de acces, un ruter ataşat la una dintre rețele, care să transmită pachetele unui alt ruter ataşat la cealaltă rețea. Între aceste două rutere se va stabili o conexiune **VPN**, care va opera aparent ca o legătură de nivel OSI 2 *(Data Link)*.

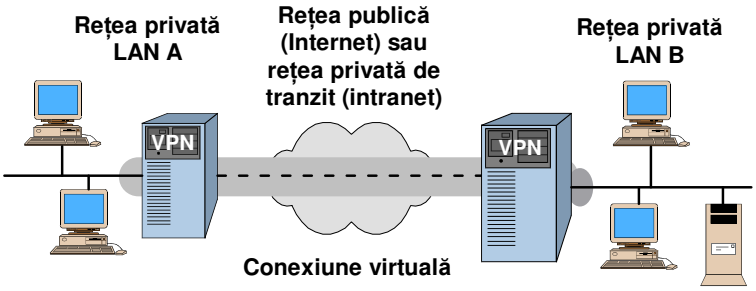

Fig. 13.4. Conectarea prin Internet a două rețele locale, despărțite geografic.

Conectarea unor rețele locale, despărțite geografic, utilizând linii telefonice dedicate (WAN).

În locul utilizării unor linii dedicate lungi (specifice tehnologiilor WAN), între două locații aflate la distanțe mari una de cealaltă, se pot folosi serviciile unor furnizori locali. O conexiune **VPN** poate fi inițiată de oricare dintre ruterele aflate la capetele traseului. Aceste pot expedia pachetele direct, pe baza unui protocol rutabil, sau pot iniția un tunel (conexiune **VPN**) între rețeaua sursă şi rețeaua destinație.

Conectarea unor rețele locale, separate geografic, utilizând linii telefonice comutate *(Dial-Up Links)*. În cazul unei rețele locale dotată cu un ruter, în locul utilizării unor conexiuni telefonice la distanță mare pe linie comutată, se pot folosi legături telefonice locale (tot pe linie comutată). Acesta poate folosi serviciile unui furnizor local, inițiind o conexiune **VPN** (ruter la ruter). Pentru aceasta, ruterul, care serveşte a doua rețea şi trebuie să opereze ca server **VPN**, trebuie să aibă o conexiune permanentă la Internet (poate fi o linie telefonică dedicată sau o altă legătură **WAN** permanentă).

Se poate ca nici unul dintre rutere să nu aibă o conexiune permanentă la un furnizor de servicii Internet. În acest caz, unul dintre aceştia trebuie să dispună de soluții care să permită inițierea unei conexiuni şi rutarea la cerere a pachetelor **DDR** *(Dial-on Demand Routing)*. Aceasta înseamnă că serverul de acces la rețea **NAS** *(Network Access Server)* va iniția legătura telefonică, prin linie comutată, cu ruterul clientului de la celălalt capăt al conexiunii.

Conexiuni VPN în cadrul aceleiaşi rețele *(Intranet-Based VPN Connections)***.**

O astfel de conexiune este mai avantajoasă în cazul în care este nevoie de legături securizate între părți ale aceleiaşi rețele locale.

Accesul la distanță în Intranet.

În unele rețele Intranet datele transmise între departamente trebuie să fie bine protejate împotriva interceptării. De aceea în multe situații, unele rețele sunt independente din punct de vedere fizic (neconectate la alte segmente de rețea). Aceasta face ca maşinile din aceste rețele să nu aibă acces la resurse importante aflate în alte segmente de rețea.

Pentru a elimina aceste neajunsuri, se pot folosi conexiuni **VPN** între departamentele cu pretenții speciale de securitate, în cadrul aceleiaşi rețele. Astfel, aceeaşi utilizatori pot transmite date secrete de-a lungul unei conexiuni **VPN**, separată de servere **VPN**, dar pot avea acces simultan şi la resurse publice.

Toate transmisiile făcute de-a lungul unei conexiuni **VPN** sunt criptate, ceea ce face ca acea parte din rețea să fie ascunsă utilizatorilor care nu au acces la aceasta. **Figura 13.5.** prezintă accesul la resurse prin **VPN** de-a lungul unei rețele locale (sau intranet).

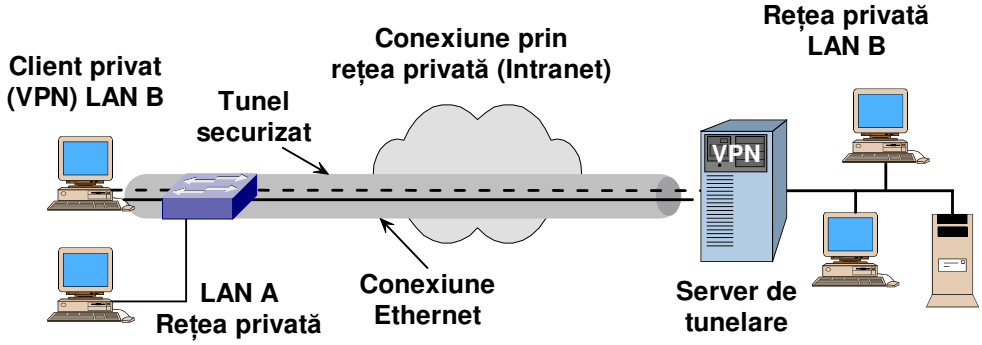

Fig. 13.5. Conexiune securizată care permite accesul la resurse aflate la distanță în Intranet.

Conectarea segmentelor de rețea folosind tronsoane intranet şi Internet.

Se pot conecta segmente de rețea într-un intranet utilizând conexiuni **VPN** ruter la ruter. Acest tip de conexiune poate să fie necesară pentru a conecta două departamente, a căror date sunt confidențiale, din locații diferite folosind simultan tronsoane ale unor rețele publice şi private. În acest caz pot sa existe două situații, diferite prin modul în care un client **VPN** (maşină individuală sau rețea locală) are acces la server-ul **VPN**.

În cazul în care accesul direct este permis, se poate utiliza un singur tunel între client şi resursa destinație. În cazul în care accesul spre un server **VPN**, care asigură tunelul spre resursa destinație, este accesibil doar prin utilizarea unui alt tunel **VPN**, se va adopta tunelare succesivă, aşa cum se poate vedea în **figura 13.6.**

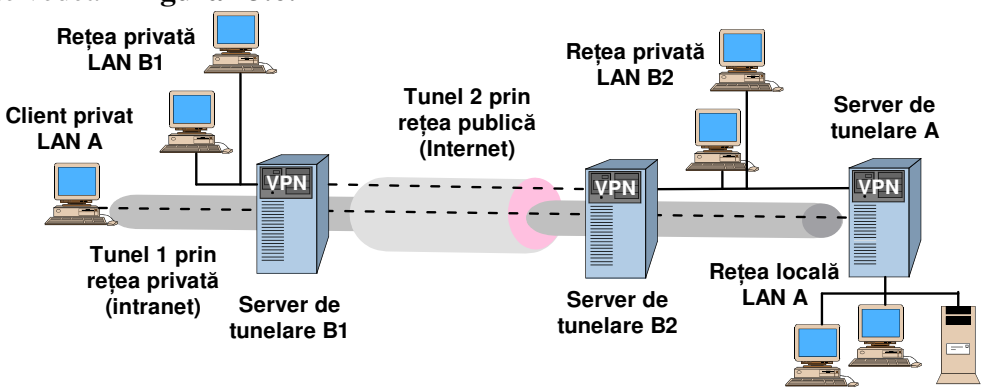

Fig. 13.6. Tunelarea multiplă prin tronsoane mixte private şi publice.

Pentru ca un client privat al rețelei locale **LAN A**, aparținând rețelei locale **LAN B1**, să aibă acces la rețeaua **LAN A** prin server-ul de tunelare **A**, este nevoie să fie utilizate două tunele.

Accesul clientului privat la propria rețea (**LAN A**) se poate face numai prin intermediul tunelului 1, format între acesta şi server-ul **VPN A**, dar pe care nu îl poate accesa direct, ci doar prin intermediul unui tunel de tranzit (tunel 2), format între server-ele. VPN B1 şi B2, aflate la capetele unui tronson de rețea publică.

Acest tunel suplimentar se numeşte "de tranzit" (Pass-Through) şi permite transferarea simultană a mai multor tunele de tip 1. Această soluție este des folosită în cazul conectării unor utilizatori domestici (home users), prin intermediul furnizorilor de servicii Internet (**ISP**), la resurse aflate la locul de muncă al acestora (enterprise network).

13.5. Protocoale utilizate în tunelările VPN.

13.5.1. Prezentare generală.

Pentru stabilirea conexiunilor virtuale tunelate se folosesc câteva protocoale specifice, dezvoltate pentru diferite platforme şi sisteme de operare. Cele mai des întâlnite sunt **SOCKS, SSL/TLS** dezvoltate pentru sistemele de operare **Unix** şi **PPTP, IPSec** şi **L2TP** dezvoltate pentru sistemele de operare din familia MS-**Windows**.

Dintre acestea, cele mai folosite pentru construirea tunelelor **VPN** de uz general sunt **PPTP**, **IPSec** şi **L2TP**, **SOCKS** fiind utilizat pentru „cortine" sau „ziduri de foc" în rețelele **Unix**, iar **SSL/TLS** pentru transferul securizat al datelor între clienți şi servere de web sau poştă electronică.

13.5.2. SOCKS

SOCKS este un protocol definit de **IETF** *(Internet Engineering Task Force)* care operează la nivelele superioare ale modelelor de referință, între nivelul transport şi aplicație (al modelului **TCP/IP**), potrivit pentru **UNIX** şi **Linux** dar mai puțin în cazul celorlalte sisteme de operare. Aceasta permite un control flexibil şi strict al traficului aplicațiilor prin tunelul rețelei private

virtuale (**VPN**). Dezavantajul major al acestui protocol este că el trebuie construit, compilat şi configurat în funcție de sistemul de operare şi aplicațiile pe care trebuie să le servească.

Protocolul are două variante **SOCKSv4** şi **SOCKv5**, cel din urmă permițând autentificarea accesului prin tunel pe baza unui nume de utilizator şi a unei parole. Implementarea acestuia se face pe baza unei perechi de componente client-server, prima operând ca o verigă intermediară între nivelul aplicație şi cel de transport, iar cea de a doua, ca aplicație de sine stătătoare.

Acest gen de arhitectură permite realizarea serverelor de comunicație (proxy) pentru transferul controlat al unor servicii dintr-o rețea spre alta. Aplicația client mandatează serverul SOCKS ca releu pentru a face cererea spre aplicația server corespunzătoare şi apoi să-i transmită înapoi răspunsul, aşa cum se poate vedea în **figura 13.7.**

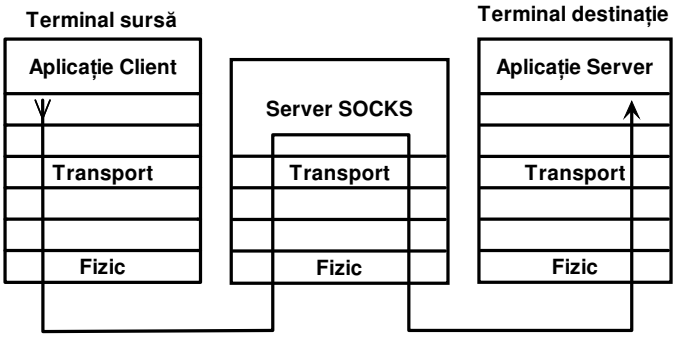

Fig. 13.7. Modul de implementarea SOCKS şi calea pe care o parcurg datele între sursă şi destinație.

Versiune **SOCKSv4** a protocolului, îndeplineşte trei funcții importante:

- asigură conexiune între sursă şi destinație,
- configurează circuitul virtual,
- asigură schimbul datelor între sursă şi destinație.

Varianta **SOCKSv5** adaugă, la cele de mai sus, funcția de autentificare.Datele sunt încapsulate, după adăugarea unui antet cu informații şi mesaje **SOCKS**, în segmente **TCP** şi pachete **IP** al căror format se poate vedea în **figura 13.8.**

Antet nivel Legătură	Antet IP	Antet TCP	Mesaj SOCKS	Date Utile	FCS

Fig. 13.8. Formatul unei datagrame într-o rețea cu implementare SOCKS.

13.5.3. SSL

SSL *(Secure Sockets Layer)* este un protocol dezvoltat de firma Netscape Communications Corporation pentru sisteme **UNIX,** folosit la transferul securizat al datelor între aplicații web şi poşta electronică, funcționând doar în rețele **TCP/IP**.

SSL, folosit uneori în conjuncție cu **TLS** *(Transport Layer Security)* foloseşte un mecanism de validare a conexiunii dintre sursă şi destinație bazat pe certificate de autorizare (CA). Protocolul asigură trei funcțiuni de bază [1]:

- **Criptarea datelor** transferate între aplicații,
- **Transferul cheilor** de criptare între aplicații,
- **Identificarea şi autentificarea sistemelor** de la capetele conexiunii virtuale.

Componenta **SSL** se introduce între nivelul "aplicație" şi "transport", conform modelului de referință **TCP/IP**, aşa cum se poate vedea în **figura 13.9.**

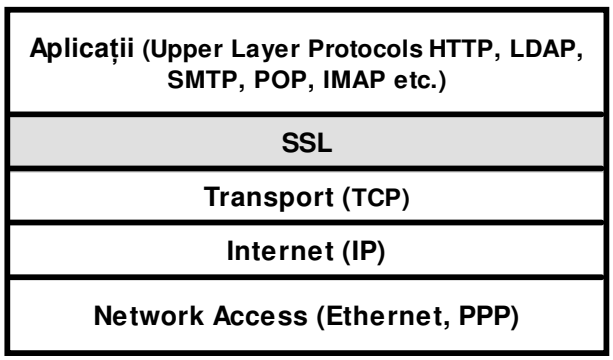

Fig.13.9. Poziționarea **SSL** între componentele modelului **TCP/IP**.

13.5.4. PPTP (Point-to-Point Tunneling Protocol)

PPTP este un protocol de tunelare care încapsulează **PPP** în segmente **TCP** şi apoi în pachete **IP**, în vederea transmiterii prin rețele bazate pe acesta din urmă. **PPTP** este documentat în **RFC 2637**. **PPTP** foloseşte o conexiune **TCP** pentru a iniția, întreține şi închide tunelul şi transmisia datelor. **PPP** permite comprimarea sau/şi criptarea datelor propriu-zise şi autentificarea terminalelor implicate în conexiune. Pentru încapsularea cadrelor se foloseşte o variantă modificată de GRE *(Generic Routing Encapsulation)* [2, 3].

Utilizarea tunelării **PPTP** permite îmbinarea avantajelor de accesibilitate şi rată mare de transfer prin utilizarea unei rețele IP cablate, cu cele ale de securitate, prin autentificare, compresie şi criptare, a conexiunilor *Dial-Up* prin server de acces (*NAS – Network Access Server*, sau *RAS – Remote Access Server*).

Autentificarea utilizată este similară cu cea folosită de **PPP** în cazul conexiunilor *Dial-Up* şi anume:

- **PAP** (*Password Authentication Protocol*) , metodă de autentificare prin parolă transmisă în clar;
- **CHAP, MS CHAP** *(Microsoft Challenge-Handshake Authentication Protocol)* metodă de autentificare prin trimiterea periodică, de către serverul de acces, a unei chei de control *(Challange).* Clientul foloseşte această cheie şi aplică asupra parolei un algoritm ciclic de criptare *(MD5 - Message Digest-5)*, după care trimite serverului de acces rezultatul obținut *(hash).*Serverul face acelaşi lucru cu parola înscrisă în baza sa de date şi compară rezultatele;
- **SPAP** *(Shiva Password Authentication Protocol)* metodă de autentificare prin transmiterea de către client, serverului de autentificare, a unei parole criptate. **SPAP** foloseşte un algoritm bi-direcțional de criptare, prin trimiterea cheii de criptare, criptarea parolei şi decriptarea ei. Serverul de acces verifică apoi parola, obținută prin decriptare, cu cea înscrisă în baza de date;
- **EAP-TLS** *(Extensible Authentication Protocol -Transport Level Security)* permite adăugarea de modalități suplimentare de autentificare prin *smart card*, transfer de chei publice, protocol *Kerberos* etc., în conjuncție cu un server extern de autentificare **RADIUS** *(Remote Authentication Dial In User Service)*. Mesajele necesare pentru autentificare sunt criptate şi încapsulate în pachete speciale, fiind apoi transferate între serverul de acces (NAS) şi cel de autentificare (RADIUS).

Pentru criptarea şi compresia conținutului câmpului de date, PPTP foloseşte algoritmi de compresie, ca **LZS** sau **MPPC/MPPE** *(Microsoft Point to Point Compression / Encription)*, pentru compresia şi criptarea datelor. **MPPE** oferă suport doar pentru criptarea legăturii (transferul datelor) nu şi pentru criptarea conexiunii dintre cele două terminale. Când se impune acest lucru, trebuie folosit suportul de criptare la un nivel superior, prin utilizarea **IPSec**, pentru criptarea pachetelor care parcurg tunelul creat de **PPTP**.

PPTP se prezintă ca un serviciu introdus între nivelul standard de transport şi cel de aplicație, reprezentat printr-o pereche "client-server", acesta din urmă utilizând o conexiune **TCP** pe potul 1723.

Tunelul **PPTP** este inițiat şi administrat prin mesaje de control transmise periodic, separat de pachetele cu date utile, între aplicația client şi cea server. Formatul unui astfel de pachet de control se poate vedea în **figura 13.10**.

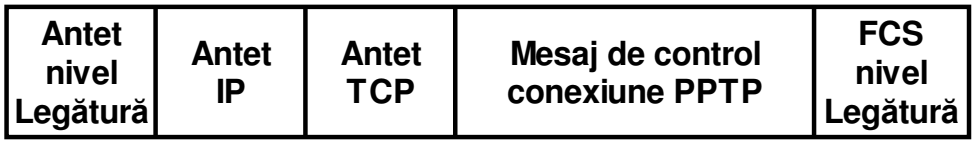

Fig. 13.10. Formatul unei datagrame cu informații de control **PPTP**.

Transferul datelor prin tunel presupune mai multe nivele de încapsulare, aşa cum se poate vedea în **figura 13.11**.

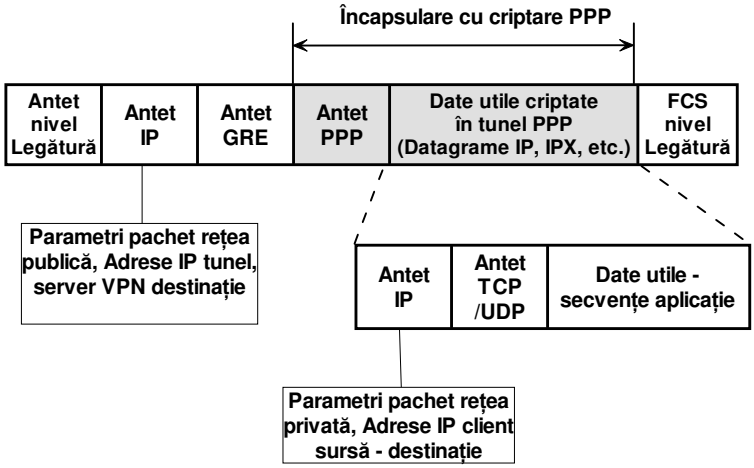

Fig. 13.11. Încapsularea datelor în tunel PPTP cu criptare.

Încapsularea în cadrele PPP.

Datele care trebuie transferate sunt criptate şi încapsulate într-un cadru **PPP**, căruia I se adaugă un antet **GRE** (*Generic Routing Encapsulation,* descris în RFC 1701 şi RFC 1702). Acesta este folosit pentru scopuri generale de transfer ale diferitelor protocoale prin rețele IP şi are codul 47 (vezi fişierul `protocol`).

Încapsularea pachetelor GRE.

Cadrele **PPP**, împreună cu antetul **GRE**, sunt apoi încapsulate în pachete **IP** şi transferate în rețea. La destinație, datele suferă un proces de decapsulare succesivă cu decriptare şi decompresie.

13.5.5. L2TP (*Layer Two Tunneling Protocol*) şi IPSec (*Internet Protocol Security*).

L2TP *(Layer Two Tunneling Protocol)* este o combinație între **PPTP** şi **L2F** *(Layer 2 Forwarding)* o tehnologie propusă de CISCO Systems Inc., în vederea obținerii unui protocol de tunelare care să combine avantajele celor două şi este documentat de RFC 2661. **L2TP** încapsulează cadrele **PPP** care pot apoi să fie trimise de-a lungul unor rețele **IP**, **X25**, **Frame Relay** sau **ATM**.

În continuare se va prezenta doar varianta de încapsulare în rețele **IP**, în care cadrele **L2TP** sunt încapsulate în datagrame **UDP** care pot fi trimise apoi în Internet sau în rețele locale, intranet. Soluția presupune existența a două tipuri separate de mesaje, de control şi date tunelate.

Acestea din urmă, transferate prin cadrele **PPP**, pot fi criptate şi/sau comprimate. Criptarea se poate face utilizând **MPPE**, sau **IPSec ESP** *(Encapsulating Security Payload)*, sistemele de operare din familia Microsoft Windows folosind a doua variantă. Pachetele transmise de un client printr-un

tunel **L2TP-IPSec**, într-o rețea **IP**, trebuie să fie livrate direct unui server corespunzător. Autentificarea folosită de **L2TP** trebuie să fie aceeaşi cu cea **PPP**, adică **EAP**, **MS CHAP**, **CHAP**, **SPAP**, sau **PAP**.

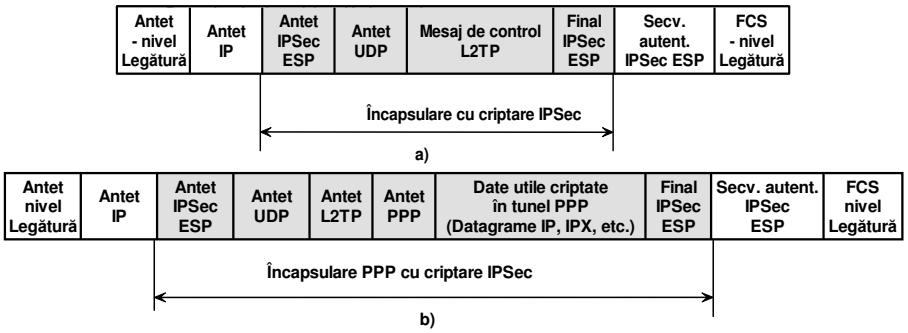

Fig. 13.12. Structura datagramelor cu încapsulare L2TP-IPSec.

Pentru inițierea şi administrarea tunelului, **L2TP** foloseşte pachete de acelaşi tip, cu cele pentru transferul datelor tunelate, aşa cum se poate vedea în **figura 13.12**. Mesajele de control sunt transmise direct, în câmpul de date a datagramei, (**figura 13.12 a**), iar datele tunelate sunt încapsulate, mai întâi, în cadre **PPP**, (**figura13.12 b**).

Informația, sub formă de mesaje de control sau date tunelate, se transmit prin datagrame **UDP**, prin acelaşi circuit, identificat prin portul fix 1701. Deoarece pentru încapsulare se folosesc datagrame **UDP**, care este un protocol fără mecanisme de control a transmisiei, **L2TP** foloseşte mesaje de control pentru confirmarea livrării la destinație a datelor tunelate. În corpul antetului **L2TP** există câmpuri cu funcție asemănătoare cu cele folosite de **TCP** pentru confirmarea segmentelor *(Next Receive ~ Acknoledgement Number, Next Sent ~ Sequence Number)*. **L2TP** acceptă mai multe "canale", numite **sesiuni** *(sessions)* pentru fiecare tunel folosit. În antetul protocolului **L2TP** există elemente de identificare atât pentru tunel *(Tunnel ID* cât şi pentru identificarea sesiunilor *(Session ID)* din cadrul unui tunel. Formatul antetului **L2TP** se poate vedea în **figura 13.13.**

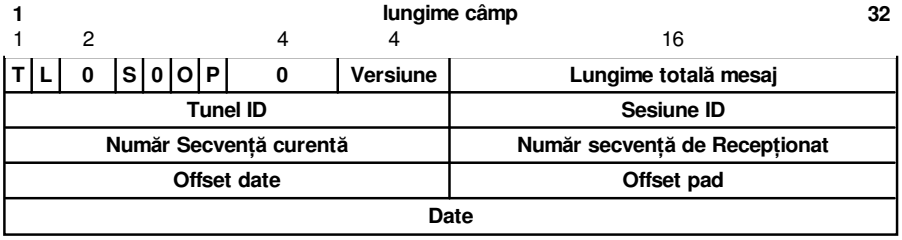

Fig. 13.13. Formatul antetului L2TP.

Semnificația câmpurilor din antetul L2TP este următoarea:

- **T** (1 bit), tip mesaj. Are valoarea 0 pentru cazul transmiterii datelor tunelate şi 0 pentru mesajele de control;
- **L** (1 bit), activează utilizarea câmpului Lungime totală mesaj. Pentru mesajele de control, acest bit trebuie să fie egal cu 1;
- **S** (1bit), activează utilizarea câmpurilor **NS** (Număr Secvență curentă) şi **NR** (Număr secvență de Recepționat). Pentru mesajele de control acest bit trebuie să fie egal cu 1;
- **O** (1 bit), indică prezența câmpului **Offset date**. Pentru mesajele de control acest bit trebuie să fie egal cu 0;
- **P**, bit de prioritate prin care se impune pentru mesajul curent, un tratament preferențial la transmisie şi adăugarea lui în cozi. Este utilizat doar în cazul transmisiei de date, pentru mesajele de control, acest bit trebuie să fie 0;
- **Versiune** (4 biți), indică versiunea protocolului L2TP folosit. Valoarea egală cu 1 este rezervată pentru pachete **L2F**, care pot fi transmise amestecat cu cele **L2TP**.Pachetele sosite cu altă valoare decât una cunoscută trebuie abandonate;

- **Lungimea totală a mesajului** (16 biţi) este un câmp opţional, folosit doar dacă bitul **L** este 1, care indică lungimea totală a mesajului:
- **Tunel ID** (16 biţi), reprezintă numărul de identificare a tunelului pentru o anumită conexiune şi are doar semnificaţie locală, indicând "destinatarul" mesajului. Acelaşi tunel poate să aibă numere de identificare diferite la cele două capete;
- **Sesiune ID** (16 biţi), reprezintă numărul de identificare a sesiunii dintr-un tunel şi are doar semnificaţie locală, indicând "destinatarul" mesajului. Aceeaşi sesiune poate să fie identificată diferit la cele două capete ale tunelului;
- **Numărul secvenţei curente** (16 biţi) este un câmp opţional care indică numărul de ordine al secvenţei de date sau al mesajului de control. Numărul secvenţei începe cu 0 şi este apoi incrementat cu 1 (modulo 2^{16}), după fiecare mesaj transmis;
- **Numărul secvenţei de recepţionat** (16 biţi) este un câmp, folosit pentru confirmare, care indică numărul de ordine al secvenţei care trebuie transmisă. Valoarea sa este egală cu numărul ultimei secvenţe recepţionate plus 1 (modulo 2^{16});
- **Offset date** (16 biţi) este un câmp opţional care indică numărul de octeţi, faţă de începutul antetului L2TP, de unde începe câmpul **Date** . Se foloseşte în conjuncţie cu bitul **O** care indică utilizarea opţională a câmpului **Offset pad**;
- **Offset Pad** (variabil) este un câmp de completare cu 0 pentru a obţine datagrame de lungime multiplu de 32 biţi;
- **Date** (variabil) câmp care conţine datele utile sau mesajele de control.

13.5.6. IPsec (Internet Protocol Security)

Noţiuni generale.

IPsec este o extensie a suitei de protocoale **TCP/IP** care permite securizarea comunicaţiei, în mod transparent faţă de aplicaţii, furnizând servicii de autentificare a sursei, controlul accesului, verificare a integrităţii şi criptare a datelor. Acest protocol a fost descris iniţial în documentele IETF RFC 1825-1829, înlocuite mai târziu de RFC 2401-2412 şi RFC 4301-4309.

IPsec operează la nivelul **OSI 3** reţea, aşa cum se poate vedea în **figura 13.14**, spre deosebire de alte protocoale, cum sunt **SSL/TLS** sau **SSH**, care operează de la nivelul OSI 4 până la 7.

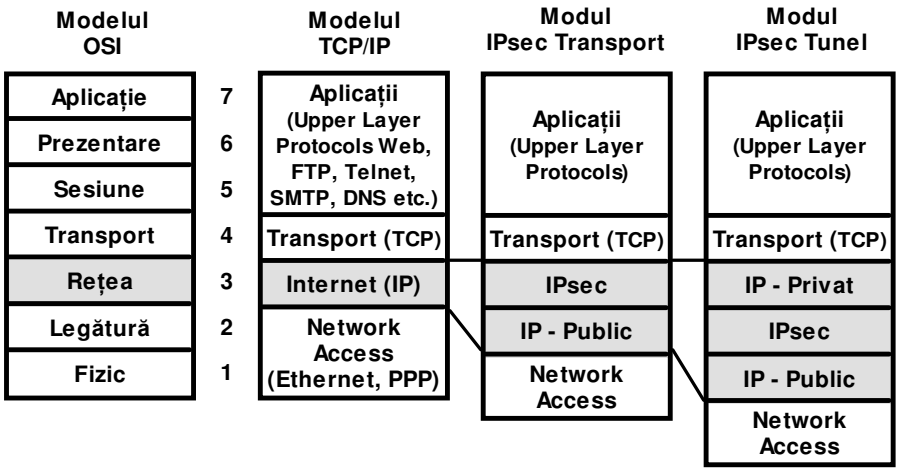

Fig. 13.14. Implementarea IPsec în raport cu modelele de referinţă OSI şi TCP/IP.

Aceasta face ca **IPsec** să fie un protocol flexibil, permiţând protejarea informaţiei conţinută de unitatea de date de la nivelul OSI 4 transport, **TCP** şi **UDP**. Avantajul utilizării protocolului **IPsec** este că aplicaţiile, operând la nivelul OSI 7, nu trebuie configurate să folosească un anumit protocol de criptare, aflat la un nivel imediat inferior.

Arhitectura de securitate a protocolului. Componente de bază.

IPsec este implementat sub forma unui set de componente de criptare a pachetelor, autentificarea mutuală a terminalelor şi stabilire a parametrilor de securizare. Aceste componente asigură o arhitectură de securitate, în interiorul protocolului **IP**, prin care se deschide câte o conexiune securizată unidirecțională. Transferul bidirecțional este posibil prin deschiderea, în paralel, a unei perechi de conexiuni securizate prin criptare şi autentificare reciprocă.

Pentru identificarea, autorizarea şi verificarea integrității pachetelor transmise, **IPsec** adaugă în structura pachetului **IP** o colecție de informații, denumită generic **SA** *(Security Associations)*. Acestea sunt gestionate şi controlate cu ajutorul componentelor **SPI** *(Security Parameter Index)* şi **SADB** *(Security Association Database)*, baze de date în care sunt păstrați parametri de securizare (autentificare şi criptare) asociați cu adresele terminalelor, între care are loc transmisia.

În cazul transmisiilor multicast, asocierea parametrilor de securitate se poate face pe grupuri de terminalele, fiecare terminal putând fi asociat cu mai multe criterii de securizare.

Moduri de implementare.

IPsec permite două moduri de implementare:

- **Transport**, este un mod de încapsulare suplimentară, în care se protejează prin criptare doar conținutul pachetului, nu şi antetul acestuia. În modul transport se adaugă un antet suplimentar, între antetul de transport (**TCP** sau **UDP**) şi cel de rețea (**IP**), dar nu se modifică structura acestuia din urmă. Aceasta permite transferul pachetului prin rețea, ca şi al celorlalte pachete care nu folosesc **IPsec**;
- **Tunel**, este un mod de încapsulare care poate proteja prin criptare întregul pachet. **IPsec** preia un pachet **IP**, gata format, îl criptează şi îl încapsulează în alt pachet pe care îl trimite apoi prin rețeaua publică (tunel).

Protocoale de autentificare şi criptare.

Protocoalele utilizate pentru transferul acestor informații sunt: **AH** *(Authentication Header)*, care permite criptarea şi/sau autentificarea pachetelor şi **ESP** *(Encapsulating Security Payload* – încapsularea cu securizare a datelor utile). Acestea folosesc, pentru stabilirea şi transferul parametrilor **SA** *(Security Associations),* un mecanism de schimb al cheilor de criptare numit **IKE** *(Internet Key Exchange).*

IKE.

IKE *(Internet Key Exchange)* este un protocol, definit în documentul RFC 2409, care operează alături de **ISAKMP**, folosit pentru transferul cheilor de criptare, în funcție de informațiile furnizate de SA.

IKE permite terminalelor să negocieze, în mod securizat, o cheie de sesiune, folosind protocoalele **ISAKMP** *(Internet Security Association and Key Management Protocol)* pentru crearea de „asocieri de securitate" SA şi OAKLEY, bazat pe algoritmul Diffie-Hellman (conceput de Whitfield Diffie şi Martin Hellman), pentru schimbarea cheilor între cele două părți. **IKE** se poate folosi alături de protocolul de autentificare Kerberos, certificate X.509v3 sau chei distribuite anterior.

AH.

AH *(Authentication Header)* a fost conceput pentru a furniza informațiile necesare verificării integrității datelor şi autentificării originii acestora. Antetul de autentificare **AH** are o singură parte, care este ataşată fiecărei datagrame (aşa cum se poate vedea în **figura 13.15**) şi conține semnătura, sub forma unui cuvânt criptat **HMAC** *(Hash Message Authentication Code),* obținută cu ajutorul algoritmilor de criptare MD5 (Message Digest versiunea 5), sau **SHA-1** *(Secure Hash Algorithm)*.

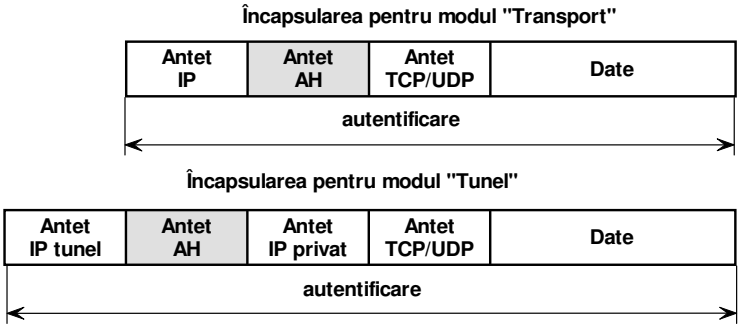

Fig. 13.15. Formatul pachetului cu autentificare AH.

În cazul utilizării protocolului AH, informaţiile din antetul **IP** nu se modifică. Deoarece, informaţiile de autentificare a pachetului se calculează ţinând seama şi de conţinutul antetului, nu este permisă modificarea sa, de-a lungul traseului spre destinaţie.

ESP.

ESP *(Encapsulated Security Payload)* a fost conceput pentru a furniza servicii de verificare a integrităţii, autentificarea originii şi confidenţialitate a datelor. **ESP** are două părţi, un antet şi o coadă, conţinând informaţiile necesare securizării transferului, prin criptarea conţinutului pachetelor. Ca şi în cazul **AH**, **ESP** foloseşte pentru autentificare coduri criptate **HMAC,** bazate pe algoritmii de criptare **MD5** sau **SHA-1,** iar pentru criptarea conţinutului, algoritmul **DES-CBC** *(Data Encryption Standard* cu *Cipher Block Chaining* mod de criptare succesivă).

Formatul pachetelor, după încapsulare, se poate vedea în **figura 13.16**.

ISAKMP.

ISAKMP *(Internet Security Association and Key Management Protocol)* este un protocol care furnizează următoarele servicii:

- gestionarea asocierilor la criteriile de securitate,
- stabilirea algoritmilor de autentificare şi criptare,
- stabilirea protocoalelor de securizare;
- transferul cheilor de autentificare şi criptare
- autentificarea iniţială a părţilor.

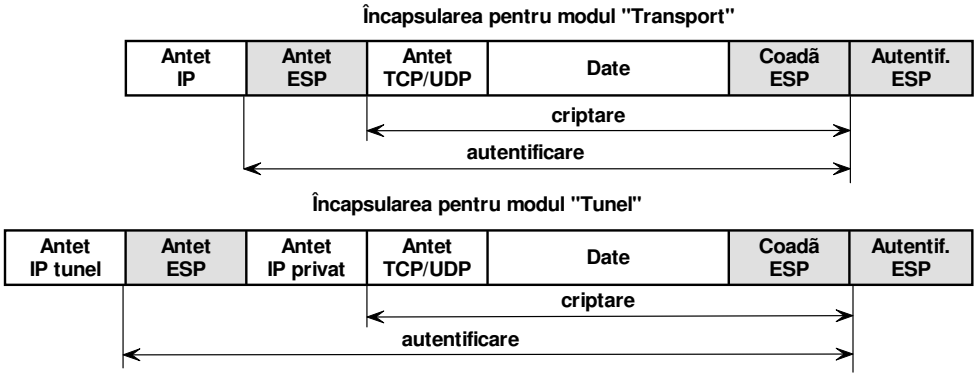

Fig. 13.16. Formatul pachetului cu încapsulare ESP.

13.6. Criptarea datelor

Criptarea datelor are ca scop principal eliminarea riscului ca datele transferate printr-o reţea publică să nu poată fi interceptate de către alţi utilizatori, ai mediului comun de transmisie, decât cei care se află la capetele circuitului virtual. Pentru criptare se folosesc, de obicei, algoritmi de criptare care se pot împărţi în două clase, şi anume:

- **Algoritmi simetrici**, în care este folosită aceeaşi cheie de criptare atât pentru criptare cât şi pentru decriptarea datelor. Din această categorie face parte algoritmul **DES** *(Data Encryption Standard)* care foloseşte schimbul, între parteneri, a unei chei publice. Avantajul principal al acestei

metode este simplitatea şi uşurinţa implementării. Principalul dezavantaj este nivelul scăzut de securitate, ceea ce impune utilizarea ulterioară a altei chei secrete de criptare.

- **Algoritmi asimetrici,** în care se folosesc două chei, una publică şi una privată care este ţinută secretă. Algoritmii folosiţi sunt de tip ireversibil, adică o criptare o dată făcută nu mai poate fi descifrată, chiar în cazul cunoaşterii cheii de criptare, fără a avea alte informaţii suplimentare. Aplicaţia server care utilizează **SSL** foloseşte o cheie privară pentru criptarea datelor şi trimite cheia publică aplicaţiei client. Cheile de criptare sunt construite în aşa fel încât un mesaj criptat cu una dintre chei nu poate fi decriptat decât utilizând cheia pereche. Astfel, cheia publică nu poate fi folosită la criptarea şi decriptarea aceluiaşi mesaj.

Cel mai des folosit algoritm de criptare cu cheie publică este **RSA** (denumire derivată din prenumele autorilor săi Ron **R**ivest, Adi **S**hamir şi Leonard **A**dleman). Complexitatea algoritmului face criptarea mult mai sigură decât în cazul algoritmilor simetrici, utilizarea sa la criptarea datelor utile pare o soluţie tentantă. Numărul mare de calcule necesare pentru determinarea cheilor îl fac foarte lent şi de aceea acest algoritm este folosit doar pentru criptarea cheii unui algoritm simetric (de exemplu **DES**), care este folosit apoi la criptarea datelor utile. Acesta din urmă (**DES**) poate să fie de 10.000 de ori mai rapid decât **RSA**, iar gradul de securitate al metodei depinde de securitate al transferului cheii algoritmului simetric.

Iniţierea unei conexiuni **SSL** presupune parcurgerea următoarelor faze:

- Aplicaţia client face cererea pe portul securizat,
- Aplicaţia server răspunde cu un certificat digital care conţine cheia publică,
- Clientul verifică data de expirare a certificatului,
- Clientul verifică dacă Certificatul de Autenticitate (**CA**) apare în lista sa cu adresele de încredere, dacă apare se trece la faza următoare iar dacă nu este cerută confirmarea acceptării sau nu a conexiunii. Certificatul de autorizare se poate obţine şi instala şi separat sub forma unui fişier sau şir de caractere.
- Clientul verifică apoi dacă numele simbolic al maşinii şi cel al domeniului **FQDN** *(Fully Qualified Domain Name)*, care găzduieşte aplicaţia server, corespunde cu cel trecut în certificat (CN Common Name).
- Iniţierea conexiunii **SSL**, în cazul în care sunt îndeplinite toate condiţiile de mai sus.

Asigurarea autenticităţii şi integrităţii datelor

Integritatea datelor transferate se verifică cu ajutorul unor algoritmi, cum este **HMAC** *(Hash Message Authentication Code)* bazat pe **SHA**-1 (Secure Hash Algorithm versiunea 1) sau MD5 (Message Digest Algorithm versiunea 5) bazaţi pe sume rezumative succesive (Message Digest) ale mesajelor transferate. Procesul schimbării cheilor de criptare, criptarea, transferul şi decriptarea datelor parcurg următoarele etape.

Criptarea

- 1. La această etapă, mesajul original "Text clar" este criptat pe baza cheii private a sursei, rezultând "Textul cifrat 1" care foloseşte la autentificarea sursei (aplicaţie sau maşină);
- 2. "Textul cifrat 1" este criptat cu ajutorul cheii publice a destinaţiei, rezultând "Textul cifrat 2", care va asigura verificarea autenticităţii destinaţiei, deoarece doar destinaţia este capabilă să descifreze mesajul utilizând propria cheie privată;
- 3. Se crează "SHA-1 MsgDigest 1" suma rezumativă succesivă, bazată pe algoritmul SHA-1, a mesajului "Text clar"
- 4. Suma rezumativă, obţinută în etapa 3, este criptată pe baza cheii private a sursei şi se foloseşte ca "Semnătură digitală" a mesajului iniţial "Text clar". Rolul acesteia este de a se putea verifica la recepţie integritatea mesajului iniţial şi autenticitatea sursei;
- 5. Se transmit spre destinaţie "Semnătura digitală" şi "Textul cifrat 2".

Decriptarea datelor

- 1. În prima etapă mesajul "Text cifrat 2" este decriptat cu ajutorul cheii private a destinaţiei, rezultând mesajul "Text cifrat 1";

- 2. Mesajul "Text cifrat 1" este decriptat cu ajutorul cheii publice a sursei, rezultând "Text clar"
- 3. Se creează suma rezumativă de control "SHA-1 Msg Digest 2", bazată pe SHA-1, a mesajului "Text clar";
- 4. Se decriptează "Semnătura digitală" folosind cheia publică a sursei rezultând "SHA-1 Msg Digest 1"
- 5. Se compară "SHA-1 MsgDigest 1" cu "SHA-1 MsgDigest 2", iar dacă acestea sunt egale se confirmă valabilitatea mesajului "Text clar".

TESTE DE AUTOEVALUARE

I. Alegeți răspunsul corect:

1. Componentele unei conexiuni VPN sunt:

   a) Server VPN, client VPN, tunel, protocol de tunelare, rețea de tranzit, algoritm de criptare;
   b) Server VPN, client VPN, tunel, protocol de tunelare, rețea de tranzit, date tunelate;
   c) Server WEB, client WEB, tunel, protocol de tunelare, rețea de tranzit, algoritm de autentificare;
   d) Server VPN, client VPN, tunel, protocol de tunelare, rețea de tranzit, algoritm de autentificare;
   e) Server VPN, client VPN, tunel, protocol de criptare, rețea de tranzit, algoritm de conectare.

2. Conexiunile care folosesc PPTP şi L2TP alături de IPSec, îndeplinesc următoarele funcțiuni:
   a) rutare, autentificare, criptarea datelor, alocarea adresei, a numelui simbolic şi a serverului de nume (DNS);
   b) încapsulare, autentificare, criptarea datelor, alocarea adresei, verificarea erorilor şi a serverului de nume (DNS);
   c) încapsulare, autentificare, criptarea (eventual compresie) datelor, alocarea adresei, a numelui simbolic şi a serverului de nume (DNS);
   d) încapsulare, autentificare, criptarea datelor, transport, a numelui simbolic şi a serverului de nume (DNS);
   e) încapsulare, criptarea datelor, alocarea adresei, a numelui simbolic şi a serverului de nume (DNS).

3. Metodele de autentificare, utilizate în cazul conexiunilor VPN, sunt:
   a) PAP, CHAP, SSL, SPAP, EAP;
   b) PAP, CHAP, MS-CHAP, SPAP, EAP;
   c) PPTP, CHAP, MS-CHAP, SOCKS, EAP;
   d) PAP, CHAP, MD5, SPAP, EAP;
   e) PAP, CHAP, IPSec, L2TP, EAP.

I. Alege□i răspunsul corect:

1. Conexiunile VPN permit utilizatorilor să lucreze de acasă, sau din altă locație şi să aibă acces la resursele unei rețele locale private, folosind infrastructura oferită de un furnizor public de servicii de rețea.
   □ adevărat □ fals

2. Arhitectura unei conexiuni VPN este de tip „Punct-la Punct”.
   □ adevărat □ fals

3. Cadrele protocolului de tunelate PPTP se încapsulează direct în pachetele IP, transferate prin rețeaua de tranzit.
   □ adevărat □ fals

RĂSPUNSURI

I. Varianta de răspuns corectă:

1. b
2. c
3. B

II. Alege□i răspunsul corect:
1. adevărat
2. adevărat
3. fals

Bibliografie

1. **Martin, F**., „*SSL Certificates HOWTO*”, v0.5, Distribuție Linux, 2002
2. Microsoft Windows 2000 Resource Kit, Cap. 9, Virtual Private Networking
3. http://www.securitytechnet.com/resource/security/vpn/INBE_VPN.doc