# Protocoale de tunelare folosite în rețele virtuale private

***Ing. Simona Livia CONSTANTIN****

***Rezumat.*** *Pentru a implementa o rețea VPN este necesară crearea unui tunel printr-o rețea publică pentru transferul datelor. Această lucrare prezintă protocolalele uzuale realizării unei rețele VPN. Tunelarea necesită trei tipuri diferite de protocoale şi anume: protocoale de transport, protocoale de încapsulare şi protocoale pasager. În general, protocolul IP este folosit ca protocol de transport deoarece cel mai des rețeaua publică de transport este internetul. Protocolul de încapsulare împachetează şi criptează datele originale cu un antet distinct (de ex. GRE, IPSec, L2F, PPTP, L2TP) iar protocolul pasager este folosit de către rețeaua sursă, transmite date în pachete prin tunel (de ex. IPX, NetBeui, IP etc.)*

***Cuvinte cheie:*** *VPN, IPSec, GRE, L2F, PPTP, L2TP, IPX, NetBeui.*

***Abstract.*** *In order to implement a VPN network is necessary to create a tunnel through a public network for transferring data. This paper highlights the most common protocols used to create a VPN. Tunnelling requires three types of protocols: transport protocols, encapsulation protocols and passenger protocols. Usually, IP is used as transport protocol because the internet is the most used as public network for the transport. The encapsulation protocol is responsible for packaging and encrypting the original data with a heading (for example: GRE, IPSec, L2F, PPTP, L2TP) and the passenger protocol that is used by the source network, transmits packet data through the tunnel (for ex. IPX, NetBeui, IP etc.).*

***Keywords:*** *VPN, IPSec, GRE, L2F, PPTP, L2TP, IPX, NetBeui*

## 1. Protocoale de tunelare

Implementarea unui VPN presupune crearea unui tunel printr-o rețea publică prin intermediul căruia să fie transferate datele. Ca o definiție, ***tunelarea (tunneling)*** este o metodă de folosire a infrastructurii unei inter-rețele pentru transferul datelor dintr-o rețea peste o altă rețea. În figura 1 este prezentat protocolul de ”tunelare” ce încapsulează cadrul de date inițial într-un antet adițional care poate traversa rețeaua intermediară.

Datele de transferat (încărcătura - *payload*) pot fi cadrele (sau pachetele) altui protocol. În loc de a transmite cadrul în forma în care a fost produs de nodul sursă, protocolul de tunelare încapsulează cadrul într-un antet adițional. Acesta conține informații de rutare astfel încât încărcătura încapsulată poate traversa inter-rețeaua intermediară. Pachetele încapsulate sunt apoi rutate între capetele tunelului prin inter-rețea.

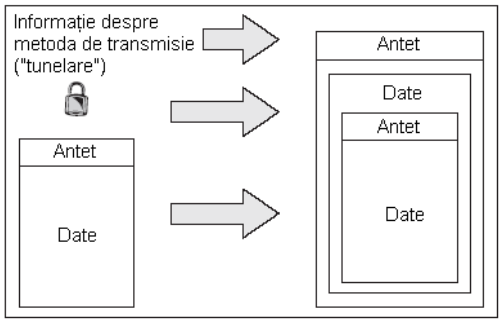


**Fig. 1**. Protocolul de ”tunelare” încapsulează cadrul de date inițial într-un antet adițional care poate traversa rețeaua intermediară.

* Institutul Național de Studii şi Cercetări pentru Comunicații.

Calea logică pe care pachetele încapsulate o urmează în inter-rețea se numeşte ***tunel***. Odată ce cadrele încapsulate ajung la destinație prin inter-rețea, cadrul este decapsulat şi trimis la destinația sa finală. De notat că tunelarea include întregul proces: încapsulare, transmitere şi decapsulare a pachetelor.

Pentru realizarea unui tunel, clientul şi serverul de tunel trebuie să folosească acelaşi *protocol de tunelare*.

Tehnologia de tunelare poate fi bazată pe un protocol de tunelare pe nivel 2 sau 3. Aceste nivele corespund modelului de referință OSI. Protocoalele de nivel 2 corespund nivelului *legătură de date*, şi folosesc *cadre* ca unitate de schimb. PPTP, L2TP şi L2F (expediere pe nivel 2) sunt protocoale de tunelare pe nivel 2; ele încapsulează încărcătura într-un cadru PPP pentru a fi transmis peste inter-rețea. Protocoalele de nivel 3 corespund nivelului *rețea*, şi folosesc *pachete*. IP peste IP şi Tunel IPSec sunt exemple de protocoale care încapsulează pachete IP într-un antet IP adițional înainte de a le transmite peste o inter-rețea IP[4].

Pentru tehnologiile de nivel 2, cum ar fi PPTP sau L2TP, un tunel este asemănător cu o sesiune; ambele capete ale tunelului trebuie să cadă de acord asupra tunelului şi să negocieze variabilele de configurare, cum ar fi atribuirea adreselor, criptarea, comprimarea. În cele mai multe cazuri, datele transferate prin tunel sunt trimise folosind un protocol bazat pe datagrame. Pentru gestionarea tunelului se foloseşte un protocol de menținere a tunelului.

Tehnologiile de tunelarea pe nivel 3 pleacă de la premiza că toate chestiunile de configurare au fost efectuate, de multe ori manual. Pentru aceste protocoale, poate să nu existe faza de menținere a tunelului. Pentru protocoalele de nivel 2, un tunel trebuie creat, menținut şi distrus. Implementarea unui VPN presupune crearea unui ”tunel” printr-o rețea publică prin intermediul căruia să fie transferate datele (fig. 2).

În esență, tunelarea este procesul prin care se introduce întreg pachetul IP în interiorul unui alt pachet, cu antete distincte, acesta fiind trimis ulterior prin rețea. Protocolul pachetului rezultat în urma tunelării este recunocut de către rețea şi de către ambele noduri sursă şi destinație, la nivelul inter-fețelor de tunelare, prin care pachetele intră şi ies din rețea.

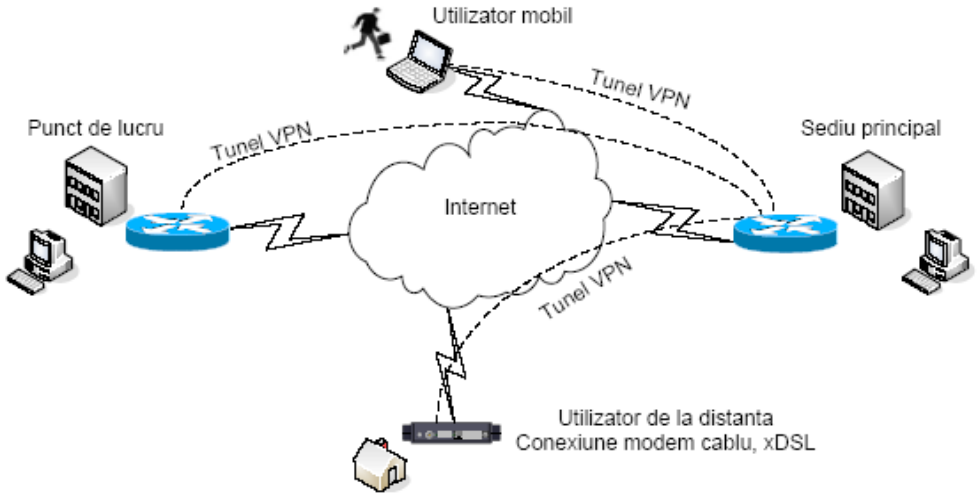


**Fig. 2.** Arhitectura unei rețele VPN cu tunele.

Tunelarea necesită trei protocoale diferite:

- **protocolul de transport** (uzual IP), protocolul utilizat de către rețeaua prin care se transferă informația (rețeaua publică de Internet sau orice rețea privată);
- **protocolul de încapsulare** care împachetează şi criptează datele originale cu un antet distinct (GRE, IPSec, *L2F, PPTP, L2TP*);
- **protocolul pasager** din rețeaua sursă care transmite date în pachetul trimis prin tunel (IPX, NetBeui, IP etc.).

## 2. Protocoale de transport

• **IP.** Internet Protocol (IP) este o metodă sau un protocol prin care datele sunt trimise de la un calculator la altul prin intermediul Internetului. Fiecare calculator (cunoscut ca HOST), are cel puțin o adresă IP unică pe Internet, care îl identifică între toate computerele de pe Internet. Când datele sunt trimise sau primite (de ex.: e-mail, pagini web) mesajul este împărțit în părți mai mici numite pachete. Fiecare pachet cuprinde adresa celui care trimite datele, dar şi a celui căruia îi sunt destinate. Fiecare pachet este trimis, prima oara la un "Gateway Computer" care interpretează o mică parte din adresă[1].

Computerul "Gateway" citeşte destinația pachetelor şi trimite pachetele la un alt "Gateway" şi tot aşa până ce pachetul ajunge la "Gateway"-ul la care are acces computerul destinatar.

Adresa IP este utilizată la nivelul programelor de prelucrare în rețea. În schimb, la nivelul utilizatorilor cu acces la Internet, identificarea calculatoarelor se face printr-un nume de calculator (host), gestionat de sistemul DNS.

Până în prezent au fost dezvoltate două versiuni ale protocolului Internet şi anume IPv4 şi IPv6.

***IP versiunea 4 – IPv4.*** Versiunea 4 a protocolului Internet are ca scop o arhitectura de adresare unică şi globală. IPv4 a început să fie folosit în Internet în anii 1970, iar în 1981 IP a fost standardizat în RFC 791 de către Grupul de lucru pentru Internet (IETF - Internet Engineering Task Force).

Adresele IPv4 au o lungime de 32 de biți (4 octeți). Fiecare adresă identifică o rețea (network) şi o stație de lucru (work station) din cadrul rețelei. Notația obişnuită este obținută prin scrierea fiecărui octet în formă zecimală, separați între ei prin puncte. De exemplu, 192.168.0.1 este notația folosită pentru adresa 11000000.10101000.00000000.00000001.

***IP versiunea 6 – IPv6.*** IPv6 este un protocol dezvoltat pentru a înlocui IPv4 în Internet. Adresele au o lungime de 128 biți (16 octeți), ceea ce este considerat suficient pentru o perioadă îndelungată. Teoretic există $2^{128}$, sau aproximativ $3{,}403 \times 10^{38}$ adrese unice. Lungimea mare a adresei permite împărțirea în blocuri de dimensiuni mari şi implicit devine posibilă introducerea unor informații suplimentare de rutare în adresă[5].

Windows Vista, Mac OS X, toate distribuțiile moderne de Linux, precum şi foarte multe alte sisteme de operare includ suport "nativ" pentru acest protocol. Cu toate acestea, IPv6 nu este încă folosit pe scară largă de către furnizorii de acces şi servicii Internet, numiți *Internet Service Providers* sau ISP.

Adresele IPv6 sunt scrise de obicei sub forma a 8 grupuri de câte 4 cifre hexazecimale, fiecare grup fiind separat de două puncte (:). De exemplu, 2001:0db8:85a3:08d3:1319:8a2e:0370:7334 este o adresă IPv6 corectă. Dacă unul sau mai multe din grupurile de 4 cifre este 0000, zerourile pot fi omise şi înlocuite cu două semne două puncte(::). De exemplu, 2001:0db8:0000:0000:0000:0000:1428:57ab se prescurtează 2001:0db8::1428:57ab. Această prescurtare poate fi făcută o singură dată, altfel ar putea apărea confuzii cu privire la numărul de câmpuri omise.

• **TCP.** Modelul TCP/IP (Transmission Control Protocol/Internet Protocol) a fost creat de US DoD (US Department of Defence - Ministerul Apărării Naționale al Statelor Unite) din necesitatea unei rețele care ar putea supraviețui în orice condiții. DoD dorea ca, atâta timp cât funcționau maşina sursă şi maşina destinație, conexiunile să rămână intacte, chiar dacă o parte din maşini sau din liniile de transmisie erau brusc scoase din funcțiune. Era nevoie de o arhitectură flexibilă, deoarece se aveau în vedere aplicații cu cerințe divergente, mergând de la transferul de fişiere până la transmiterea vorbirii în timp real.

Aceste cerințe au condus la alegerea a patru niveluri pentru modelul TCP/IP: Aplicație, Transport, Rețea (sau Internet) şi Acces la Rețea.

***Nivelul Aplicație.*** Nivelul aplicație se referă la protocoalele de nivel înalt folosite de majoritatea aplicațiilor, precum terminalul virtual (TELNET), transfer de fişiere (FTP) şi poşta electronică (SMTP). Alte protocoale de nivel aplicație sunt DNS (Domain Name Service), NNTP sau HTTP.

În majoritate implementărilor, nivelul aplicație tratează nivelurile inferioare ca o "cutie neagră" care oferă o infrastructură sigură de comunicații, deşi majoritatea aplicațiilor cunosc adresa IPsau portul folosit. Majoritatea protocoalelor de la nivelul aplicație sunt asociate cu modelul client-server. Serverele au de obicei asociate porturi fixe, atribuite de IANA: HTTP are portul 80, FTP portul 21, etc. În schimb, clienții folosesc porturi temporare[3].

***Nivelul Transport.*** Este identic cu cel din modelul OSI, ocupându-se cu probleme legate de siguranță, control al fluxului şi corecție de erori. El este proiectat astfel încât să permită conversații între entitățile pereche din gazdele sursă, respectiv, destinație. În acest sens au fost definite două protocoale capăt-la-capăt.

Primul din ele, TCP (Trasmission Control Protocol). El este un protocol sigur orientat pe conexiune care permite ca un flux de octeți trimişi de pe o maşină să ajungă fără erori pe orice altă maşină din inter-rețea. Acest protocol fragmentează fluxul de octeți în mesaje discrete şi pasează fiecare mesaj nivelului internet. TCP tratează totodată controlul fluxului pentru a se asigura că un emițător rapid nu inundă un receptor lent cu mai multe mesaje decât poate acesta să prelucreze.

Al doilea protocol din acest nivel, UDP (User Datagram Protocol), este un protocol nesigur, fără conexiuni, destinat aplicațiilor care doresc să utilizeze propria lor secvențiere şi control al fluxului. Protocolul UDP este de asemenea mult folosit pentru interogări rapide întrebare-răspuns, client-server şi pentru aplicații în care comunicarea promptă este mai importantă decât comunicarea cu acuratețe, aşa cum sunt aplicațiile de transmisie a vorbirii şi a imaginilor video.

***Nivelul Rețea (Internet).*** Scopul inițial al nivelului rețea era să asigure rutarea pachetelor în interiorul unei singure rețele. Odată cu apariția interconexiunii între rețele, acestui nivel i-au fost adăugate funcționalități de comunicare între o rețea sursă şi o rețea destinație.

În stiva TCP/IP, protocolul IP asigură rutarea pachetelor de la o adresă sursă la o adresă destinație, folosind şi unele protocoale adiționale, precum ICMP sau IGMP. Determinarea drumului optim între cele două rețele se face la acest nivel.

Comunicarea la nivelul IP este nesigură, sarcina de corecție a erorilor fiind plasată la nivelurile superioare (de exemplu prin protocolul TCP). În IPv4 (nu şi IPv6), integritatea pachetelor este asigurată de sume de control.

***Nivelul Acces la rețea.*** Se ocupă cu toate problemele legate de transmiterea efectivă a ZU-ului pe o legătură fizică, incluzând şi aspectele legate de tehnologii şi de medii de transmisie, adică nivelurile OSI Legătură de date şi Fizic.

Modelul de referință TCP/IP nu spune mare lucru despre ce se întâmplă acolo, însă menționează că gazda trebuie să se lege la rețea, pentru a putea trimite pachete IP, folosind un anumit protocol. Acest protocol nu este definit şi variază de la gazdă la gazdă şi de la rețea la rețea.

## Protocoale de încapsulare

• **Mecanismul GRE.** Pentru rutarea cu adrese private, se încapsulează pachetele IP transmise în Internet cu antete suplimentare prin aşa-numitul mecanism GRE (*Generic Routing Encapsulation*), descris în RFC 1701. Pachetului inițial (*payload packet /original packet*) i se adaugă un antet GRE (*GRE Header*) şi un antet de expediere privind modul de transfer specificat conform protocolului de rețea (*delivery header*).

În antetul GRE se specifică ruta pe care se va trimite forțat pachetul la destinație, fără a se lua alte decizii de rutare în routerele intermediare.

GRE asigură transparența adreselor intermediare şi securitatea transmisiei, prin realizarea unui aşa-numit "tunel de transmisie" (*tunnelling*) .

Uzual este cazul încapsulării pachetelor IP pentru transmisii cu IP (*IP over IP*) conform RFC 1702, standard definit pentru GRE.

Adresele IP private pot fi utilizate în încapsularea GRE astfel încât cadrul să fie interpretat ca fiind încapsulat GRE şi routerele 'de la distanță' să extragă adresa de destinație privată din pachetul original.

*Exemplu[3].* Să presupunem existența a două rețele locale de calculatoare A şi B având alocate adresele IP private 192.168.3.0 şi 192.168.4.0.

Aceste rețele sunt conectate în WAN prin intermediul a două routere cu adresele IP publice alocate interfețelor: 193.162.35.110 şi 195.16.23.12.

Cele două routere comunică prin intermediul unui al treilea router cu adresa 194.225.140.1.

Un pachet trimis de la adresa 192.168.3.2 către 192.168.4.5 va fi încapsulat prin procedeul GRE specificându-se în antetul de transmisie numai adresele IP private ale routerului-sursă şi respectiv routerului-destinație fără a se menționa adresa routerului intermediar. Adresa acestuia este inclusă doar în tabelele de rutare nefiind vizibilă din exterior. Urmează ca în LAN-ul B să se extragă datele şi să se citească adresa IP alocată local destinației .

Tunelarea are implicații uimitoare pentru VPN-uri. Se pot astfel transmite pachete care utilizează adrese IP private în interiorul unui pachet care utilizează adrese IP reale, în acest fel se poate extinde rețeaua privată prin Internet. Dar se poate transmite şi un pachet care nu este suportat de protocolul Internet (precum NetBeui) în interiorul unui pachet IP iar acesta poate fi apoi transmis cu uşurință prin Internet.

• **IPSec.** Internet Protocol Security sau IPSec, este o suită de protocoale care asigură securitatea unei rețele virtuale private prin Internet. IPSec este o funcție de layer 3 şi de aceea nu poate interacționa cu alte protocoale de layer 3, cum ar fi IPX şi SNA.

Însă IPSec este poate cel mai autorizat protocol pentru păstrarea confidențialității şi autenticității pachetelor trimise prin IP. Protocolul funcționează cu o largă varietate de scheme de criptare standard şi negocieri ale proceselor, ca şi pentru diverse sisteme de securitate, incluzând semnături digitale, certificate digitale, chei publice sau autorizații. Încapsulând pachetul original de date într-un pachet de tip IP, protocolul IPSec scrie în header toată informația cerută de terminalul de destinație. Deoarece nu există modalități de autentificare sau criptare licențiate, IPSec se detaşează de celelalte protocoale prin interoperabilitate. El va lucra cu majoritatea sistemelor şi standardelor, chiar şi în

paralel cu alte protocoale VPN. De exemplu, IPSec poate realiza negocierea şi autentificarea criptării în timp ce o rețea virtuală de tip L2TP primeşte un pachet, inițiază tunelul şi trimite pachetul încapsulat către celălalt terminal VPN.

IPSec foloseşte un algoritm pentru schimbarea cheilor între părți, numit Internet Key Exchange (IKE), care permite calculatoarelor să negocieze o cheie de sesiune în mod securizat, folosind protocoalele ISAKMP pentru crearea de Security Associations şi OAKLEY bazat pe algoritmul Diffie-Hellman pentru schimbarea cheilor între cele două părți. IKE se poate folosi în conjuncție cu Kerberos, certificate X.509v3 sau chei preshared.

Authentication Header (AH) este ataşat fiecărei datagrame şi conține semnătura sub formă de hash HMAC cu MD5 sau HMAC cu SHA-1.

Encapsulated Security Payload (ESP) criptează conținutul pachetelor în două moduri: transport (protejează doar conținutul pachetului, nu şi header-ul) sau tunel (întreg pachetul este criptat). ESP foloseşte de asemenea hash-uri HMAC cu MD5 sau HMAC cu SHA-1 pentru autentificare şi DES-CBC pentru criptare [2].

Pentru a securiza comunicația în rețea cu IPSec între calculatoarele Windows folosim o colecție de reguli, politici şi filtre pentru a permite în mod selectiv doar comunicația pentru anumite protocoale.

Politicile de IPSec pot fi create şi aplicate cu Group Policy pentru calculatoarele din domeniu. Pentru calculatoare care nu sunt în domeniu, de exemplu serverele bastion, politicile pot fi aplicate cu script-uri linie de comandă.

Implementarea unei soluții VPN de comunicație reliefează unele probleme specifice, probleme ce apar din cauza absenței standardelor. Internet Engineering Task Force (IETF) a stabilit un grup de lucru dedicat definirii standardelor şi protocoalelor legate de securitatea Internetului. Unul dintre cele mai importante scopuri ale acestui grup de lucru este finalizarea standardului IPSec, care defineşte structura pachetelor IP şi considerentele legate de securitatea în cazul soluțiilor VPN.

De-a lungul ultimilor ani, grupul de lucru IPSec din cadrul IETF a înregistrat mari progrese în adăugarea de tehnici de securitate criptografice la standardele pentru infrastructura Internet. Arhitectura de securitate specificată pentru IP (fig. 3) furnizează servicii de securitate ce suportă combinații de autentificare, integritate, controlul accesului şi confidențialitate.

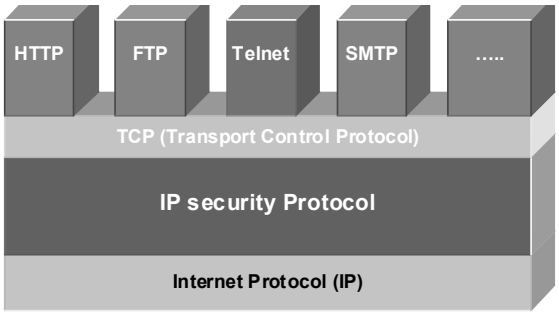


**Fig. 3.** Protcolul de securitate Internet (IP).

**IPSec** a apărut în cadrul efortului de standardizare pentru IPv6 şi reprezintă singura soluție deschisă pentru securizarea conexiunilor pe Internet. IPSec poate fi configurat pentru două moduri distincte: modul tunel şi modul transport. În modul tunel, IPSec încapsulează pachetele IPv4 în cadre IP securizate, pentru transferul informației între două sisteme firewall, de exemplu. În modul transport, informația este încapsulată într-un altfel de mod, încît ea poate fi securizată între punctele terminale ale conexiunii, deci „ambalajul" nu ascunde informația de rutare cap-la-cap. Modul tunel este cea mai sigură metodă de securizare, însă creşte gradul de încărcare a sesiunii de comunicație, prin mărirea dimensiunilor pachetelor.

Standardul pentru Arhitectura de Securitate IP, descris în RFC 2401, prezintă mecanismele de securitate pentru IP versiunea 4 (IPv4) şi pentru IP versiunea 6 (IPv6).

La ora actuală există două tipuri de antete (headere) ce pot fi ataşate la un pachet IP pentru realizarea securității. Acestea sunt:

- ***Authentification Header*** (AH) - *antetul de autentificare* – care furnizează serviciile de integritate şi autentificare.
- ***Encapsulated Security Payload*** (ESP) - *învelişul de securitate* - care furnizează confidențialitate şi, în funcție de algoritmii şi de modurile folosite, poate furniza, de asemenea, integritate şi autentificare.

Pe lângă autentificarea sursei, AH asigură numai integritatea datelor, în timp ce ESP, care asigura până acum doar criptarea, acum asigură atât criptarea, cât şi integritatea datelor. Diferența dintre integritatea datelor prin AH şi cea dată de ESP stă în scopul datelor care sunt autentificate. AH autetifică întregul pachet, în timp ce ESP nu autentifică antetul IP exterior. În autentificarea ESP, sumarul de mesaj se află în finalul pachetului, în timp ce în AH, sumarul se găseşte înăuntrul antetului de autentificare.

Cele două antete, respectiv mecanisme de securitate, pot fi folosite independent unul de celălalt, combinate sau într-un mod imbricat. Ele sunt definite în mod independent de algoritm astfel încât algoritmii criptografici pot fi înlocuiți fără ca alte părți din implementare să fie afectate. În mod implicit sunt specificați algoritmi standard, pentru asigurarea interoperabilității.

Ambele mecanisme de securitate IP pot furniza servicii de securitate între:

– două calculatoare gazdă ce comunică între ele;

– două gateway-uri de securitate comunicante;

– un calculator gazdă şi un gateway.

Sunt în curs de dezvoltare protocoale şi tehnici criptografice care să asigure gestiunea cheilor la nivelul de securitate din IP printr-un mecanism standardizat de administrare a cheilor care să permită o negociere, distribuție şi stocare a cheilor de criptare şi autentificare în condiții de completă corectitudine şi siguranță. Un exemplu îl constituie *Protocolul de Gestiune a Cheilor pentru Internet* (**ISAKMP**– *Internet Security Association and Key Management Protocol*) care este un protocol de nivel aplicație, independent de protocoalele de securitate de la nivelele inferioare. ISAKMP are la bază tehnici derivate din mecanismul Diffie-Hellman pentru schimbarea cheilor. O standardizare în structura de pachete şi în mecanismul de administrare a cheilor va duce la completa interoperabilitate a diferitelor soluții VPN.

IPSec va avea un succes major în mediile LAN-LAN, însă în cazul considerațiilor client/server va fi de o utilitate limitată la câțiva ani. Cauzele acestei disfuncții stau în penetrarea relativ limitată a PKI şi în problemele de scalabilitate. Implementarea sa pretinde cunoaşterea domeniului de adrese IP pentru a stabili indentitatea utilizatorilor, cerință care face acest protocol impracticabil în mediile cu alocare dinamică a adreselor, cum este cazul ISP.

IPSec nu suportă alte protocoale de rețea în afară de TCP/IP şi nu specifică o metodologie de control al accesului în afară de filtrarea pachetelor. Din moment ce foloseşte adresarea IP ca parte a algoritmului de autentificare, se pare că este mai puțin sigur de cât alte protocoale de nivel înalt la capitolul identificarea utilizatorilor.

Poate cel mai important dezavantaj al IPSec îl constituie absența unui sprijin ferm din partea Microsoft. Compania din Redmond nu a pomenit nimic despre suportul IPSec în sistemele sale de operare client. Se poate spune că IPSec se află în competiție cu PPTP şi L2TP în ceea ce priveşte construirea de conexiuni tunel, de aceea nu este clar dacă Microsoft va face schimbări radicale în

stiva IPv4 pentru a suporta IPSec la niveluri superioare.

O parte a standardului IETF IPSec constă în definirea unei scheme de administrare automată a cheilor, care include conceptul de PKI (Public Key Infrastructure). Aceasta este o comunitate deschisă de CA (Certificate Authorities - Autorități de certificare) care, în cele mai multe cazuri, utilizează un model ierarhic pentru a construi asocieri de încredere acolo unde nu au existat. Existența PKI este importantă la stabilirea unei rețele VPN între o rețea de corporație şi o rețea a unui partener sau furnizor, deoarece necesită un schimb securizat de chei între ele, prin intermediul unei a treia părți (CA), în care ambele noduri VPN au încredere[3]. În figura 4 este ilustrat mecanismul de criptarea a datelor IPSec utilizând chei publice şi chei private.

Schema obligatorie de administare automată a cheilor, definită de IETF IPSec pentru IPv6 este ISAKMP/Oakley (Internet Security Association and Key Management Protocol) cu opțiunea SKIP (Simple Key management for IP). Spre deosebire de soluțiile VPN care nu oferă nici o formă de administrare automată a cheilor, o soluție VPN care suportă această caracteristică prin utilizarea uneia dintre tehnologiile de instalare VPN permite administratorilor de securitate să creeze, să distribuie şi să revoce cheile de criptare VPN în mod simplu şi sigur, prin intermediul sistemului **PICI.**

**ISAKMP/Oakley** este răspunsul grupului IPSec la modul de negociere al algoritmilor criptografici şi schimbul de chei prin Internet. El este de fapt un protocol hibrid ce integrează protocolul de administrare a cheilor şi asociații de securitate pentru Internet (*Internet Security Association and Key Management Protocol,* sau ISAKMP) împreună cu un subset al schemei Oakley de schimb de chei.

ISAKMP/Oakley furnizează următoarele:

- servicii de negociere a protocoalelor, algoritmilor şi cheilor criptografice;
- servicii de autentificare primară a entităților comunicante;
- administrarea cheilor criptografice;
- schimbul protejat de chei.

Schimbul de chei este un serviciu strâns legat de administrare a asocierilor de securitate, AS. Când este necesară crearea unei AS, trebuie să se schimbe chei. Prin urmare ISAKMP/Oakley le împachetează împreună şi le trimite ca pachet integrat.

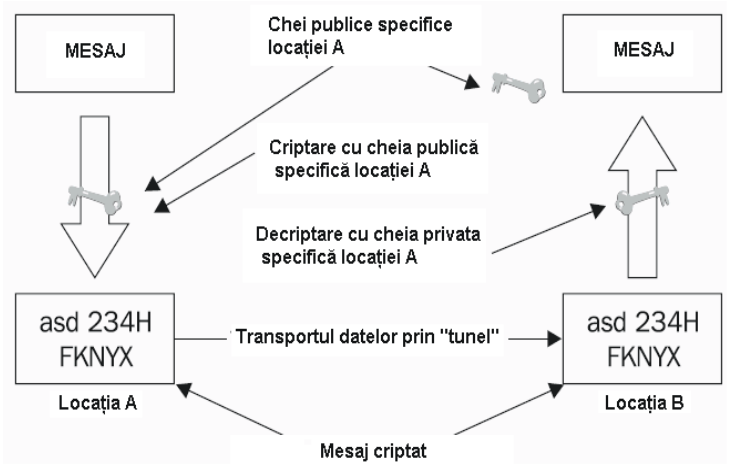


**Fig. 4.** Mecanismul de criptarea a datelor IPSec utilizând chei publice şi chei private.

În plus față de protocolul ISAKMP/Oakley, standardul IPSec specifică faptul că sistemele trebuie să suporte şi schimbul manual de chei. În majoritatea situațiilor însă, acest lucru este ineficace. Deci ISAKMP/Oakley rămâne singurul modul eficient şi sigur de negociere a AS-urilor şi de schimb al cheilor printr-o rețeaua publică.

ISAKMP/Oakley funcționează în două faze. În prima fază, entitățile ISAKMP stabilesc un canal protejat (denumit ISAKMP-SA) pentru desfăşurarea protocolului ISAKMP. În faza a doua, cele două entități negociază asocieri de securitate (AS-uri) generale. O entitate ISAKMP este un nod compatibil IPSec, capabil să stabilească canale ISAKMP şi să negocieze AS-uri. Poate fi un calculator de birou sau un echipament numit *gateway* de securitate care negociază servicii de securitate pentru abonați.

Oakley furnizează trei moduri de schimb al cheilor şi de stabilire a AS-urilor – două pentru schimburile din faza întâi ISAKMP şi unul pentru schimburile din faza a doua.

- ***modul principal*** este folosit în prima fază a protocolului ISAKMP pentru stabilirea unui canal protejat.
- ***modul agresiv*** este o altă cale de realizare a schimburilor din prima fază a protocolului ISAKMP/ Oakley – el este ceva mai simplu şi mai rapid decât modul principal şi nu asigură protecția identității pentru nodurile care negociază, pentru că ele trebuie să-şi transmită identitățile înainte de a fi negociat un canal protejat.
- ***modul rapid*** este folosit în faza a doua a protocolului ISAKMP la negocierea unui AS general pentru cumunicație.

De fapt, ISAKMP/Oakley mai are încă un mod de lucru, denumit **modul grupului nou** (new group mode), care nu se integrează în nici una din cele două faze şi care este folosit în negocierea parametrilor pentru schema Diffie-Hellman.

Cel mai semnificativ aspect referitor la IPSec nu constă în robustețea cu care a fost proiectat, ci în simplul fapt că IPSec este un standard Internet acceptat şi că în momentul de față un număr mare de utilizatori şi furnizori de servicii cooperează pentru a furniza o gamă completă de soluții IPSec. Folosind capacitatea de tunelare a IPSec, se pot implementa ***rețele virtuale private*** (**Virtual Private Network - VPN**).

- **L2F.** Layer 2 forwarding (L2F) este un protocol de tip forwarding, folosit pentru tunelarea protocoalelor de nivel înalt într-un protocol de nivel 2 (legătură de date - Data Link). De exemplu, se folosesc ca protocoale L2: HDLC, HDLC asincron sau cadre SLIP. Deşi această soluție facilitează conectivitatea pe linii de acces în rețele cu comutație de circuite, informația din fluxul L2F *nu este criptată*. Acest protocol a fost creat de Cisco. Combinat cu PPTP, constituie componentă a L2TP.

- **PPTP.** Point to point tunneling protocol (PPTP), reprezintă o extensie a Point-to-Point Protocol (PPP), care încapsulează datele, IPX sau NetBEUT în pachetele IP (fig. 5). Acest protocol este folosit în mod fundamental de echipamentele ISP, deoarece duce la un numitor comun participanții la sesiuni de comunicații. Este cea mai cunoscută dintre opțiunile pentru securitatea transferului de date în rețeaua VPN. Dezvoltat de Microsoft şi inclus în Windows NT v 4.0 pentru a fi folosit cu serviciul de rutare şi acces de la distanță (Routing & Remote Access Service). Este plasat la nivelul 2 OSI. Acesta permite traficului IP, IPX şi NetBEUI să fie criptat şi încapsulat într-un antet IP pentru a fi transmis peste o inter-rețea IP de corporație sau publică (Internet).

- **L2TP.** Layer 2 Tunneling Protocol, sau L2TP, este o combinație dintre un protocol al firmei Cisco Systems (L2F) şi cel al firmei Microsoft denumit Point-to-Point Tunneling Protocol (PPTP).

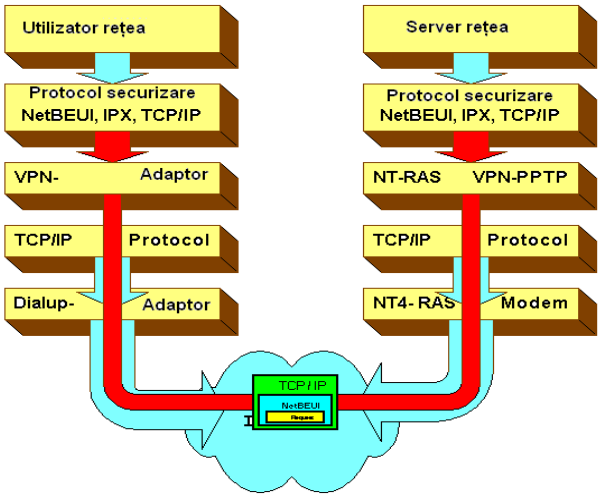


**Fig. 5.** Încapsularea datelor IPX sau NetBEUT în pachetele IP în cazul utilizării protocolului PPTP (Point to point tunneling protocol) pentru implementarea VPN.

Fiind conceput pentru a suporta orice alt protocol de rutare, incluzând IP, IPX şi AppleTalk, acest L2TP poate fi rulat pe orice tip de rețea WAN, inclusiv ATM, X.25 sau SONET. Cea mai importantă trăsătură a L2TP este folosirea protocolului Point-to-Point, inclus de Microsoft ca o componentă a sistemelor de operare Windows 95, Windows 98 şi Windows NT. Astfel că orice client PC care rulează Windows este echipat implicit cu o funcție de tunneling, iar Microsoft furnizează şi o schemă de criptare denumită Point-to-Point Encryption. În afara capacității de creare a unei VPN, protocolul L2TP poate realiza mai multe tunele simultan, pornind de la acelaşi client, de exemplu spre o bază de date a firmei şi spre intranetul aceleiaşi firme. Schema bloc principială privind utilizarea protocolului L2TP (Layer 2 Tunneling Protocol) într-o rețea VPN este ilustrată în figura 6.

## Protocoale pasager

- **IPX.** Tunelare IPX (Internetwork Packet Exchange) pentru Novell NetWare peste IP. Când un pachet IPX este trimis unui server NetWare sau unui ruter IPX, serverul sau ruterul anvelopează pachetul IPX într-un UDP cu antet IP, şi îl trimite apoi peste inter-rețeaua IP. Ruterul IP-IPX destinație dă la o parte UDP-ul şi antetul IP, şi trimite pachetul către destinația IPX[3].

Protocolul IPX este un protocol bazat pe datagrame (fără conexiune). Termenul fără conexiune înseamnă că atunci când o aplicație foloseşte IPX pentru a comunica cu alte aplicații din cadrul rețelei, nu este stabilită nici o conexiune sau cale de date între cele două aplicații. Deci, pachetele IPX sunt trimise către destinațiile lor, dar nu se garantează şi nici nu se verifică faptul că acestea ajung sau nu la destinație. Termenul datagramă (datagram) desemnează faptul că un pachet este tratat ca o entitate individuală, care nu are nici o legătură sau relație secvențială cu alte pachete. IPX execută funcții echivelente nivelului rețea din modelul OSI.

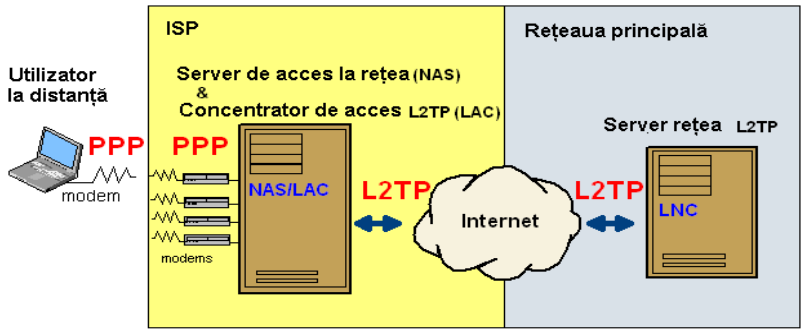


**Fig. 6.** Schemă bloc principială privind utilizarea protocolului L2TP (Layer 2 Tunneling Protocol) într-o rețea VPN.

Aceste funcții includ adresare, rutare şi transfer de pachete pentru schimburi de informație, funcțiile IPX fiind dedicate transmisiei de pachete în cadrul rețelei

- **NetBeui.** Interfața utilizator extinsă NetBIOS (NetBEUI) este un protocol de rețea utilizat de obicei în rețele locale (LAN) mici care au între 1 şi 200 de computere. NetBEUI este rapid şi de dimensiuni reduse şi funcționează bine în cadrul unei rețele locale (LAN), dar nu este rutabil, aşadar computerele care nu sunt în aceeaşi rețea sau subrețea locală nu pot să îl utilizeze pentru a comunica. NetBEUI a fost în mare parte înlocuit cu TCP/IP.

**Abrevieri folosite în lucrare**

| | | |
|---|---|---|
| AH | Autentication Header | Antet de autentificare |
| DNS | Domain Name System | Sistemul Numelor Domeniilor |
| ETSI | European Telecommunications Standards Institute | Institutul european pentru standarde de telecomunicații |
| GRE | Generic Routing Encapsulation | Mecanism de încapsulare |
| IETF | Internet Engineering Task Force | |
| IKE | Internet Key Exchange | Interschimbarea cheilor de internet |
| IP | Internet Protocol | Protocol Internet |
| IPX | Internetwork Protocol Exchange | Schimb de protocoale între rețele |
| IPSEC | Internet Protocol SECurity | Securitate IP |
| ISAKMP | Internet Security Association and Key Management Protocol | Protocolul de management al cheilor şi asociația securității Internetului |
| L2F | Layer 2 Forwarding | Transmitere către nivelul 2 |
| L2TP | Layer 2 Tunneling Protocol | Protocol de tunelare de nivel 2 |
| OSI | Open Systems Interconnection | Interconectarea sistemelor deschise |
| PPP | Point-to-Point Protocol | Protocol punct la punct |
| PPTP | Point-to-Point Tunneling Protocol | Protocol de tunelare punct-la-punct |
| TCP | Transmission Control Protocol | Protocol de control al transmisiei |
| UDP | User Datagram Protocol | Protocolul Datagramelor utilizatorilor |
| VPN | Virtual Private Network | Rețea Virtuala Privată |
| WAN | Wide Area Network | Rețele de zonă mare |

## Bibliografie


[1] **Robert WOOD** - *Next-Generation Network Services*, Cisco Press, 2005

[2] *Rețea virtuală IT-C pentru unități de învățământ şi cercetare dispersate geografic CERVIT*, Proiect coordonat de I.N.S.C.C, 2009.

[3] **Simona Livia Constantin** - *Metodologie de evaluare a QoS în rețele complexe de tip „ALL-IP”*, 2009.

[4] http://www.chip.ro/revista/iunie_2000/46/retele_virtuale_private/8232

[5] **Iljitsch van Beijnum** - *Running IPv6*.