UNIVERSITATEA POLITEHNICĂ BUCUREŞTI
Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei

V P N - Virtual Private Network

Profesor coordonator:
Conf. Dr. Ing. Ştefan Stăncescu

Masterand:
Ing. Luca Adrian-Alexandru

- 2015 -

Cuprins

1. TIPURI DE VPN-URI 3

1.1. IMPLEMETATĂ PE INTRANET.....4

1.2. IMPLEMENTATĂ PE EXTRANET.....4

2. PROTOCOALE DE TUNELARE.....6

3. AVANTAJELE VPN-URILOR 13

CONCLUZII 20

BIBLIOGRAFIE.....21

1. Tipuri de VPN-uri

Reţelele private virtuale (VPN – Virtual Private Network) permit companiilor să stabilească conexiuni de reţea securizate, private, deseori prin Internet ori prin intermediul altor tipuri de reţele. VPN poate oferi scaderi de costuri semnificative prin comparaţie cu liniile închiriate private şi poate mari conectivitatea către locatiile din teritoriu, lucrul de la distanţă, clienţii, furnizorii şi partenerii.

Pe măsură ce indicii de conectivitate şi mobilitate se maresc, creşte şi nevoia ca reţelele să se adapteze şi să ofere noi servicii. Utilizatorii nu înţeleg problemele de securitate ale serviciilor de la distanţă, pe care le doresc productive, indiferent de locaţie. Utilizatorii care călătoresc în alte ţări, prin aeroporturi, la sediile clienţilor solicită să aibă capacitatea de a se conecta la resursele companiei pentru a-şi realiza lucrările. O dată cu nivelurile in crestere a conectivitatii, începând cu liniile din aeroporturi şi liniile T1, până la conexiunile din locaţii de concentrare Wi-Fi (Wireless Fidelity) şi clienţi cu conexiuni de mare viteză, cei care răspund de întreţinerea reţelelor se lovesc de câteva decizii dificile. Exista problema oferirii utilizatorilor serviciile solicitate, in orice locatie, într-un mod protejat şi rezonabil.[1]

VPN-urile (remote access) de tip acces de la distanţă, numite şi reţele virtuale private cu dial-up, este un tip de conexiune utilizator-LAN (fig. 1) folosită cel mai adesea de companii a caror angajaţi au necesităţi de conectare din diverse locatii la resursele reţelei companiei.

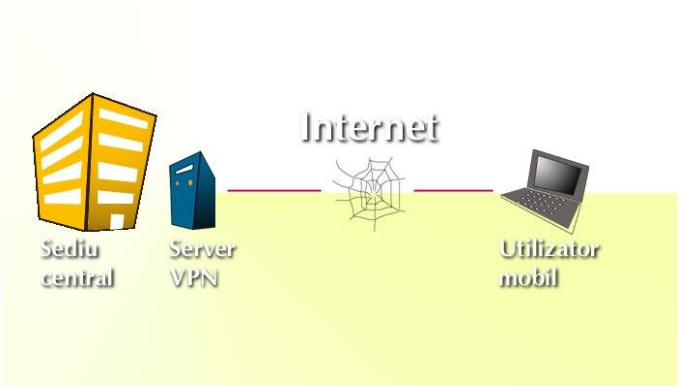


Figura 1: Remote-access VPN [8]

De regulă, în momentul când mai multi utilizatori doresc accesul la reţeaua locală, se angajeaza o companie de out-sourcing care utilizeaza un server pentru a acceSA reţeaua pentru acordarea de drepturi userilor şi computerelor acestora.

In general, atunci cand se implementeaza o tehnologie VPN între sediile companiei este preferat apelarea la acelaşi ISP pentru toate locaţiile. apropierea geografică de obicei nu are nici o legatura cu “distanta pe Internet”.

Prin folosirea de echipamente dedicate şi criptare pe scară largă, o firma poate interconecta multe sucursale printr-o reţea publică cum e si Internetul.

VPN-ul tip site-to-site poate fi de două tipuri dupa cum vom vedea.

1.1. Implemetată pe Intranet

Reţeaua virtuală privată între sucursalele şi departamentele aceleiaşi companii. Intranet-ul este definit ca o conectare semi-permanentă folosind o reţea publică între un WAN şi o sucursala a companiei. aceste moduri de conectare LAN-LAN se considera că au cea mai mica expunere din punct de vedere al sigurantei deoarece companiile au încredere în sucursalele lor. În astfel de cazuri firma are gestiune asupra reţelei/nodurilor tinta cât şi asupra celei sursă. administratorii de sistem trebuie să decidă dacă aceasta situaţie este întâlnită şi în propria companie. [2]

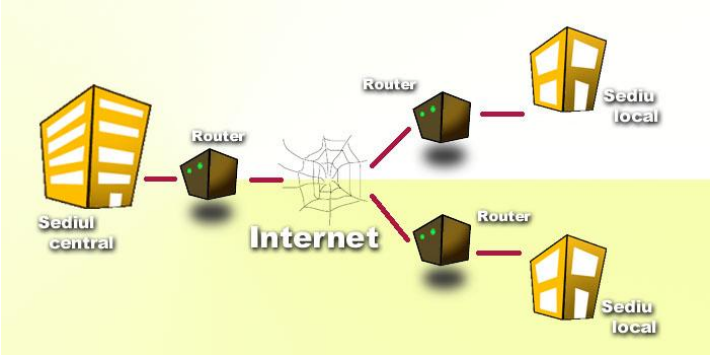


Figura 2: Intranet site-to-site VPN [8]

Cantităţi enorme de date sunt interschimbate frecvent între LAN-uri într-un VPN reţea privată, deci fundamentala este viteza de transfer şi interoperabilitatea. LAN-urile care sunt interconectate cu ajutorul unor baze de date centralizate sau prin alte resurse de calcul răspândite în reţeaua companiei ar trebui să fie apreciate ca făcând parte din aceeaşi reţea. Principalul motiv pentru care majoritatea comapniilor se indreapta către tehnologia VPN este costul redus al acestei implementari.

1.2. Implementată pe extranet

Reţeaua virtuală privată (VPN) care este oarecum ratacita faţă de intranet. Extranetul are scopul schimbului de mesaje cu partenerii, clienţii, furnizorii şi cu angajaţii la distanţă. Securizarea unei reţele de mari dimensiuni necesită ghidaje şi unelte adecvate. O retea externa VPN trebuie să faciliteze o ierarhie a securitatii şi accesarea datelor secrete să fie facuta sub cel mai strict control. Principala tinta al unei retele externe sau al VPN-ului între firme este să se asigure ca datele secrete ajung intacte şi exact cui îi sunt adresate fără a exista

riscul de a expune resursele protejate unor eventuale ameninţări, aşa ca firmele ar trebui să tina cont de cele mai avansate soluţii de VPN. [2]

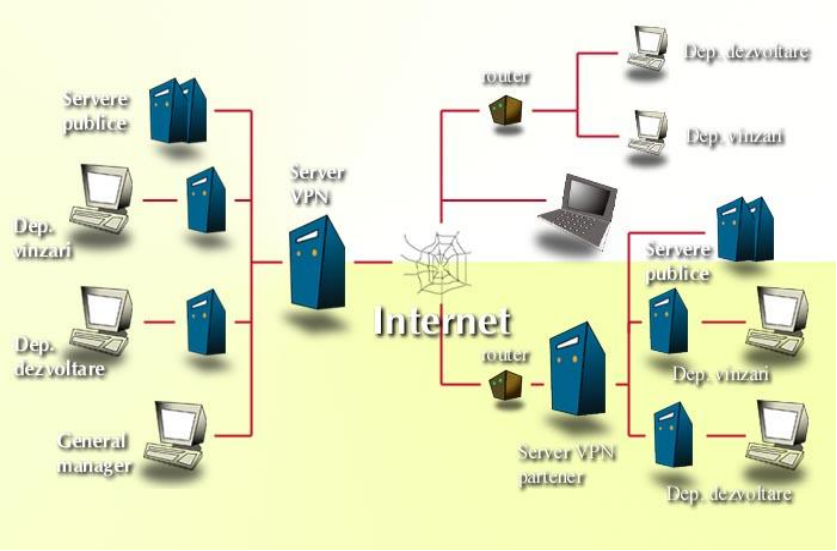


Figura 3: Extranet site-to-site VPN [8]

O retea VPN externa sigura, în care o firma distribuie informaţii cu clienţii, furnizorii, partenerii şi angajaţii situati la distanţă cu ajutorul reţelei publice stabilind legături unidirecţionale de la un end to end printr-un server VPN. Acest tip de sistem da voie unui administrator de reţea să defineasca drepturi specifice, cum ar fi cele ce ar permite unui membru din conducerea unei firme partenere să acceseze diferite/anumite rapoarte de vânzări de pe un server protejat. acest tip de acces nu este posibil cu orice tip de soluţie VPN.

Într-o situaţie reală de interconectare între parteneri de afaceri, administratorii trebuie să caute o soluţie de VPN care să filtreze accesul la resurse în funcţie de cât mai multe parametrii posibili, inclusiv sursa, destinaţia, utilizarea aplicaţiei, tipul de criptare şi autentificare folosit, şi identităţile individuale şi de grup. Managerii de sistem trebuie să identifice utilizatorii individual, nu numai adresele IP, fie prin parole, token card, smart card, sau orice alta metode de autentificare. Parolele sunt de obicei suficiente pentru o aplicaţie obişnuită de birou, dar nu sunt la fel de sigure precum token-urile sau smart card-urile. [1]

Reţelele private virtuale folosesc Internetul pentru a interconecta mai multe reţele LAN, printr-o conexiune garantata. Conectarile VPN fac posibil acest lucru cu două procese esentiale: ***crearea de tunele*** şi ***securizarea***. In primul rand, o reţea VPN creează un circuit ,,virtual" între cele două puncte interconectate, prin intermediul Internetului. Mai apoi, utilizeaza tehnica creării de tunele pentru a impacheta datele în limbajul Internetului - TCP/IP - astfel încât să poată fi transportate facil. Prin securizare se înţelege criptarea şi împachetarea pachetelor trimise, astfel încât numai adresantul căreia ii sunt destinate să le poată decodifica şi citi.

2. Protocoale de tunelare

VPN-urile securizate utilizeaza protocoale de tunelare, acele protocoale care garanteaza confidenţialitatea, blocând intruşii şi accesul la date, autentificarea trimitatorului şi integritatea mesajelor. Dacă sunt selectate, introduse şi folosite în mod corespunzător, astfel de tehnici pot garanta comunicaţii securizate în cadrul unei reţele nefiabile.

În principiu***, tunelarea este tehnicade plasare a unui pachet întreg într-un alt pachet expediat apoi în reţea***. Protocolul pachetului exterior este perceput de reţea la ambele capete, intitulate interfeţe tunel. La aceste capete pachetele intră şi ies din reţea. [3]

Datele care trebuiesc transferate (sau payload-ul) pot fi cadrele (sau pachetele) ale altui protocol. În loc să trimită un cadru care este produs în nodul de origine, protocolul de tunelare încapsulează cadrul într-un antet suplimentar. Pachetele împachetate sunt apoi dirijate între terminaţiile tunelului construit peste reţeaua de internet. Calea logică prin care pachetele încapsulate strabat reţeaua de internet se numeşte tunel.[3]

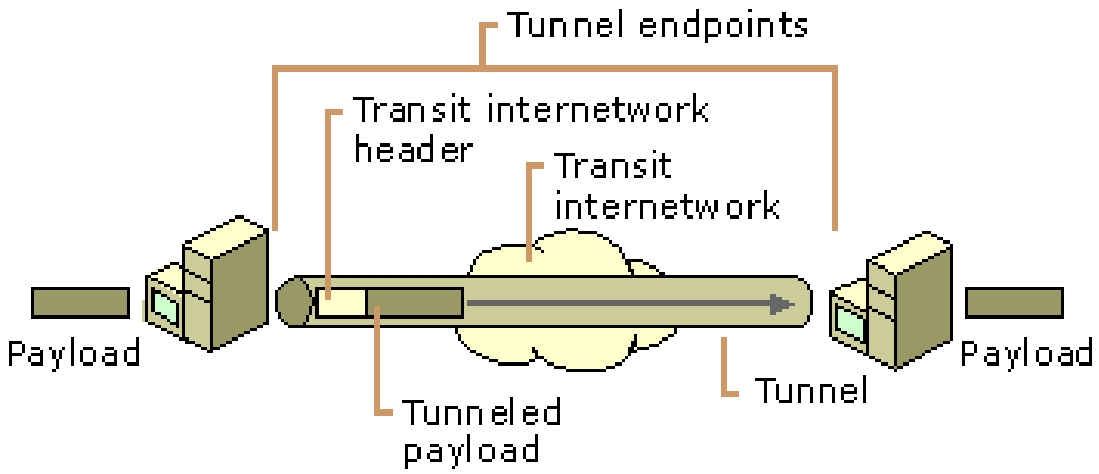


Figura 4: Principiul tunelării [9]

Tunelarea implică trei feluri de protocoale diferite:

- **protocolul de transport**: utilizat de reţeaua pe unde circulă informaţia;
- **protocolul de încapsulare**: (GRE, PPTP, L2TP, L2F, IPSec) care înfăşoară datele originale;
- **protocolul de călătorie**: protocolul original cu care sunt transportate datele (IPX, NetBeui, IP).

Tunelarea are implicaţii surprinzatoare în VPN-uri . De exemplu, se poate pune un pachet care utilizeaza un protocol nesuportat de Internet (NetBeui) într-

un pachet IP şi să fie expediat în mod securizat prin Internet. Sau să se pună un pachet cu o adresă IP nedirijabila într-un pachet IP pentru a mari reţeaua privată prin Internet.

Într-un VPN *locaţie la locaţie*, GRE (Generic Routing Encapsulation) este protocolul de încapsulare care asigură cadrul de lucru pentru protocolul de călătorie şi de transport, bazate pe IP, fiind definit în RFC 1701 şi RFC 2784 cu completările în RFC 1702. Dezvoltat la inceput de compania CISCO, GRE cuprinde informaţii despre ce tip de pachet se încapsulezi, despre conexiunea dintre client şi server, reprezentând o metodă de dirijare a pachetelor IP care sunt nedirijabile. [3]

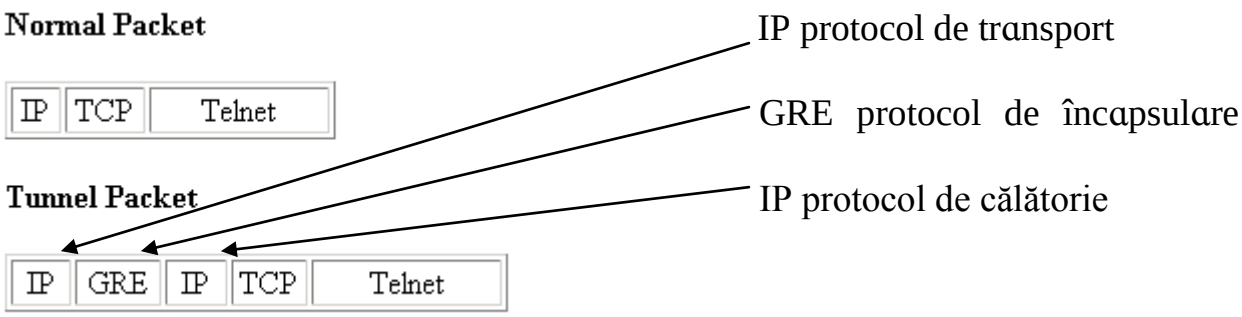


Figura 5: Pachet tunelat [7]

De asemenea poate fi utilizat şi pentru rutarea pachetelor multicast in cadrul reţelelor incompatibile. Protocolul GRE poate ruta pachete non-IP (cum ar fi appleTalk, Internetwork Packet Exchange sau IPX) in cadrul reţelelor IP.

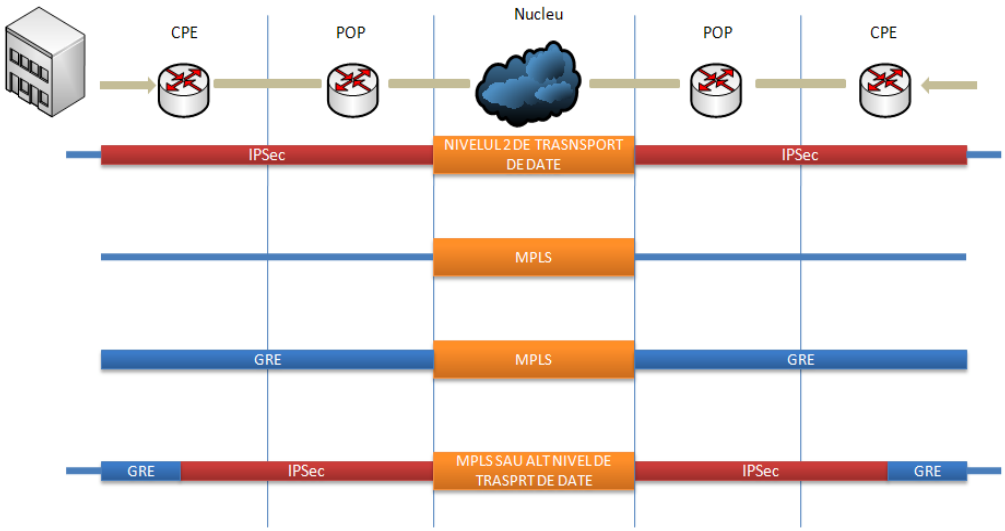
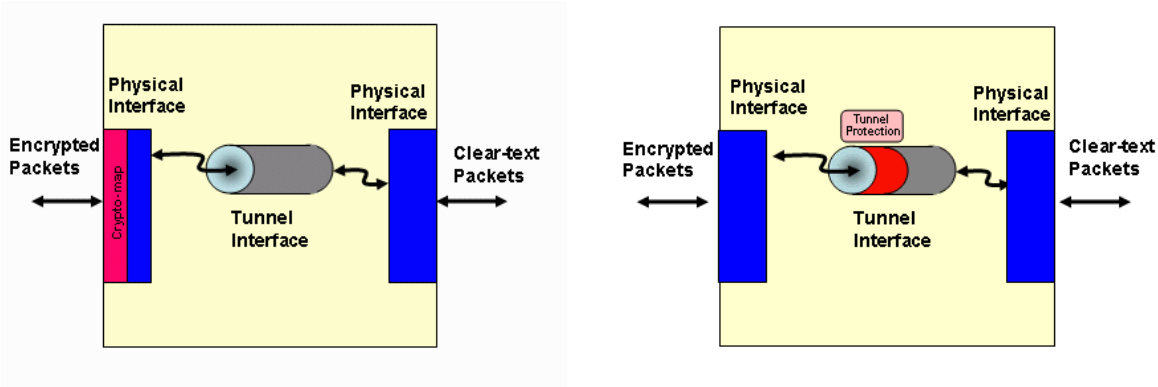


Figura 6: Încapsulare generică [7]

Cu toate acestea trebuie observata ideea că, protocolul GRE nu furnizează criptare de la sine. Pentru a cripta traficul care parcurge un tunel protocolul GRE va trebui să implementăm protocolul special IPSec. Există două metode diferite prin care un protocol IPSec poate cripta pachetele GRE. Prima este cu utilizarea *hărţii de criptare* prin folosirea acesteia pe interfaţa fizică a unui router, ca în imaginea de mai jos (fig. 7):



a. b.

Figura 7: Hartă-criptare şi protecţia tunelului [7]

Odată ce pachetele de date sunt de-criptate şi despachetate îşi vor continua traseu către destinaţia IP, ca şi text clar.

Cea de-a doua metodă utilizata este cea de *protecţie a tunelului* folosita pe interfaţa tunelului, ca în imaginea de mai sus. Pachetele de date ce patrund într-un router prin interfaţa tunelului sunt criptate, apoi sunt de-criptate şi despachetate înainte ca acestea să-şi continue drumul lor către destinaţie, ca şi text clar.

Protecţia tunelară ţine de funcţionalitatea criptării din tunelul GRE şi face verificări după ce pachetul este înpachetat, dar înainte ca informaţia să fie expediata către interfaţa fizică. [4]

Într-un VPN *cu acces la distanţă*, tunelarea este realizata utilizand protocolul PPP(Protocolul Punct-la-Punct). Protocol de face parte din stiva TCP/IP, PPP este cel care transporta alte protocoale IP atunci cand un calculator host comunica prin reţea cu un sistem la distanţă. PPP permite unui PC să se conecteze la reţea via modem, calculatorul operând ca şi cum ar fi conectat la reţea direct. acest amanunt inlesneste exploatarea interfeţelor grafice cu utilizatorul, la accesul serviciilor de genul Web, ftp, e-mail sau telnet.

Sunt folosite trei componente in protocolul PPP: *clientul PPTP*, *server-ul PPTP* şi o *reţea de acces la server*. Pentru a putea observa cum funcţionează acest protocol putem presupune un scenariu în care clientul se conectează la reţeaua de acces la server (NAS – network acces server) prin functionalitatea creată de ISP (Internet Service Provider) său. In momentul in care este conectat clientul poate expedia şi primi pachete de date prin internet cu ajutorul TCP/IP.[3]

După ce este realizata conexiunea iniţială dintre PPP si distribuitorul său de internet (fig. 8), al doilea apel dial-up de reţea se face pe legătura existenta. Datele expediate folosesc această a doua conexiune sub formă de datagrame IP ce conţin pachete PPP, cu referire la pachetele încapsulate PPP (fig. 9).

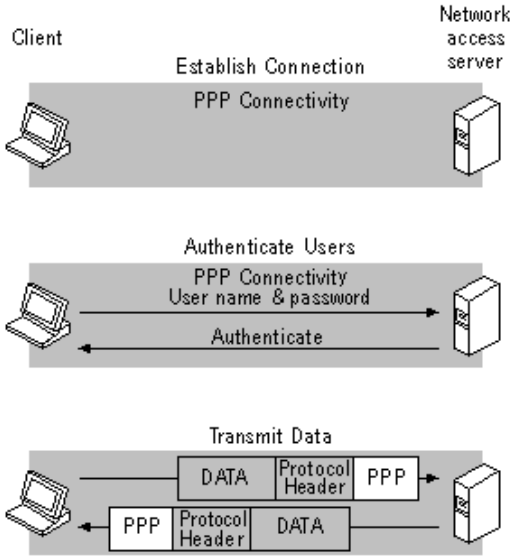


Figura 8: Conectarea cu ISP [7]

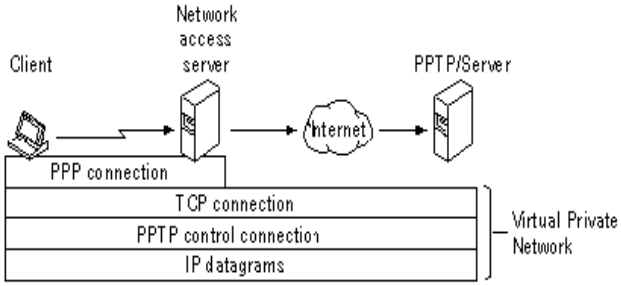


Figura 9: Tunelarea cu PPTP [7]

Deoarece server-ul PPTP este conceput să realizeze conexiuni peste reţelele private folosid protocoale de reţea privată are capacitatea de a citi şi pachete multi-protocol.

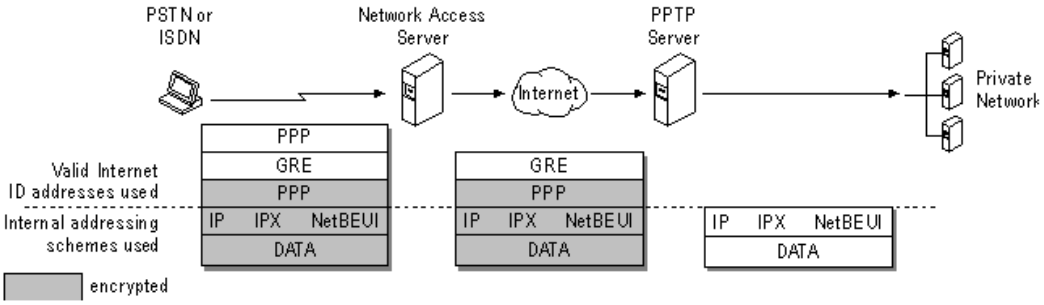


Figura 10: Pachete multi-protocol [7]

PPTP încasulează pachetele de date PPP comprimate şi criptate în datagrame IP pentru a le transporta pe reţeaua internet. Aceste datagrame IP sunt rutate pe internet înainte să ajungă la server-ul PPTP care este conectat la reţeaua privată şi internet.

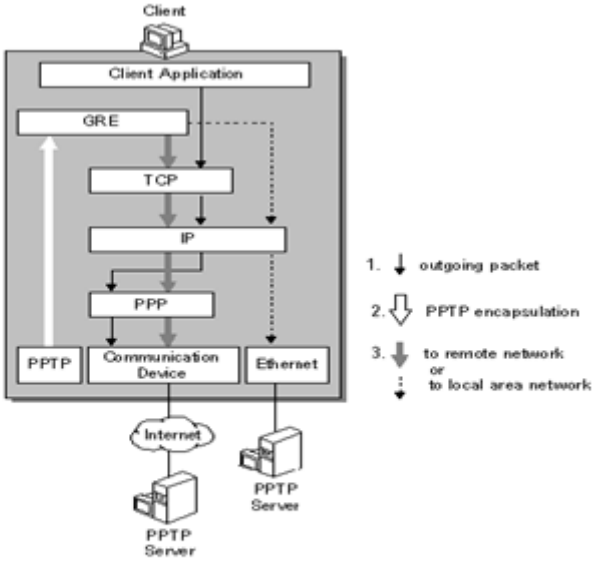


Figura 11: Plasarea de pachete PPTP pe suportul de reţea

Pachetele clientului PPTP cu acces la distanţă sunt procesate diferit faţă de cele ale unui client PPTP de reţea locală. Pachetul de date la accesul la distanţă este plasat pe suportul fizic al dispozitivului de telecomunicaţii, în timp ce datele dintr-o reţea LAN sunt plasate pe suportul fizic al adaptorului de reţea, aşa cum este ilustrat în fig. 11.

Protocolul de nivel 2(L2TP) este o prelungire a protocolului PPTP, descris în documentul RFC 2661 şi utilizat pentru a permite futilizarea unui VPN în Internet. Companiile Cisco şi Microsoft au ajuns la acordul să-şi unifice protocoalele L2TP, avand astfel caracteristicile cele mai bune ale celor două protocoale pentru tunelare prin Internet: PPTP (Microsoft) şi Layer 2 Forwarding (L2F- Cisco System). această colaborare a dus la imbunatatirea in domenii ca cel al protejării datelor confidenţiale.

Protocolul L2TP este alcatuit din doua componente principale: L2TP access Concentrator (LAC-concentrator de acces), dispozitiv care încheie fizic un apel şi L2TP Network Server (LNS- server de reţea), dispozitiv care încheie şi poate autentifica fluxul PPP. Din acest punct de vedere, L2TP este similar cu PPTP când este vorba de utilizarea protocolului PPP, atât ca funcţie cât şi ca structură (fig. 12).[5]

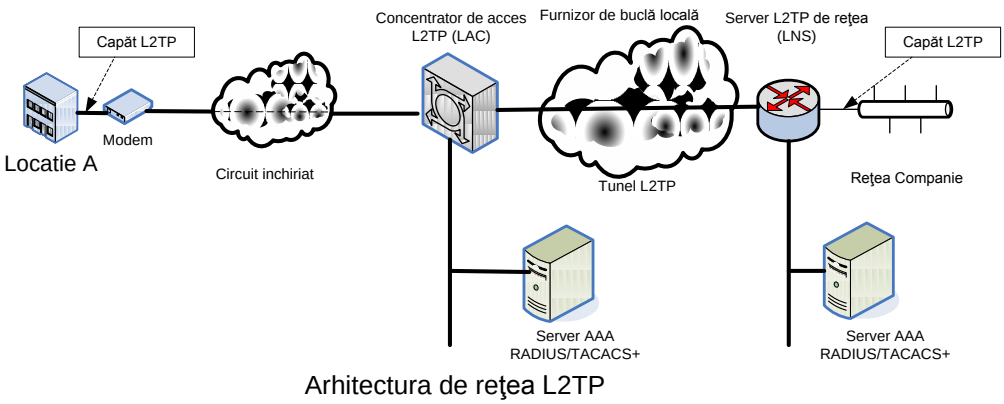


Figura 12: Structura reţelei L2TP [10]

L2TP prin IP internet utilizează UDP (User Datagram Protocol) şi o serie de mesaje tipice protocolului pentru întreţinerea tunelului creat. L2TP foloseste UDP şi pentru a trimite cadre PPP încapsulate ca şi date de tunel. Încărcătura cadrelor PPP încapsulate poate fi criptată şi/ori comprimată, aşa cum apare în figura de mai jos:

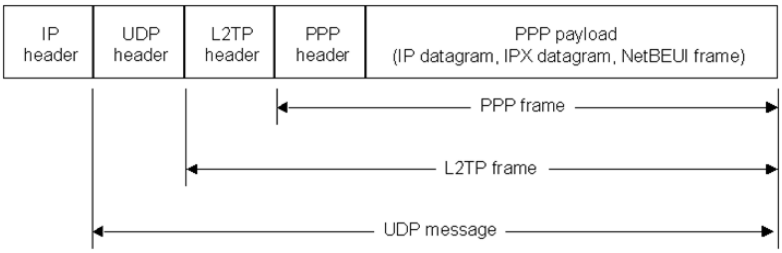


Figura 13: Structura unui pachet L2TP care conţine date utilizator [10]

Iar un pachet L2TP conţine :

0 - 15 bit	**16 - 31 bit**
Indicatori şi info versiune	Lungime(opt)
Tunel ID	Sesiune ID
Număr secvenţial a datelor (opt)	Număr secvenţial primit (Opt)
Dimensiune offset (opt)	Pad offset (Opt).....
Încărcătura de date	

Figura 14: pachet L2TP [10]

Când se stabileste o conexiune cu L2TP mai multe pachete de control se schimbă între server şi client pentru realizarea tunelului şi a sesiunii în fiecare direcţie. Un capăt îi cere permisiunea celuilalt capăt pentru asignarea un indicator de tunel şi sesiune printre aceste pachete de control. Folosind id-ul tunelului şi sesiunii, cadrele PPP comprimate ca şi încărcătură de date inlocuiesc pachetele de date. astfel, în schema din dreapta se poate urmări stabilirea unei legături de tip „handshaking" între server-ul de reţea si concentratorul de acces şi, prin mesajele de control. (fig. 15) [5]

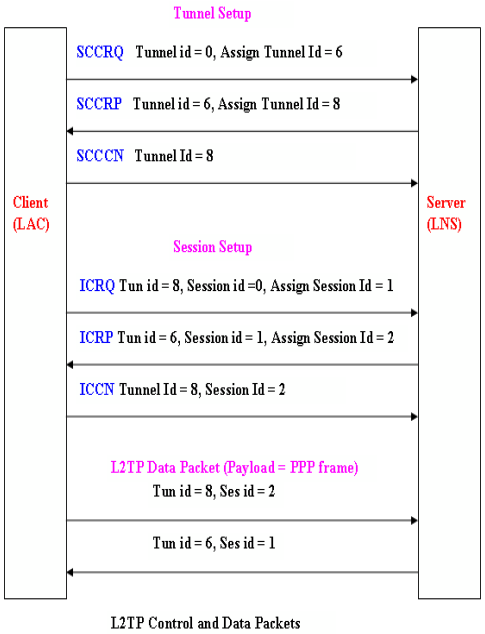


Figura 15: L2TP Pachete de date si control [11]

Deşi protocoalele L2TP şi PPTP sunt asemanatoare, diferă prin următoarele:

- în cazul L2TP, criptarea datelor începe după ce se termina procesul de conectare PPP (şi deci după autentificarea PPP). În cazul L2TP/IPSec, criptarea datelor începe înainte de procesul de conectare PPP;
- Protocolul PPTP necesită doar o autentificare la nivelul utilizatorului, iar L2TP necesită aceaşi autentificare la nivelul utilizatorului dar şi o autentificare la nivelul calculatorului, printr-o certificare a calculatorului.

Unele din avantajele specifice protocolului L2TP sunt următoarele:

- acceptă medii cu mai multe protocoale deoarece, prin proiectare, L2TP poate transporta orice protocoale rutabile, inclusiv IP, IPX şi appleTalk.
- L2TP acceptă, de asemenea, orice tehnologie WAN de transmitere, inclusiv Frame Relay, ATM, X25 sau SONET.
- de asemenea acceptă medii LAN, precum Ethernet, Fast ethernet, Token Ring şi FDDI.

L2F (Layer 2 Forwarding), proiectat de firma Cisco Systems Inc., poate fi de asemenea folosit. Protocolul L2F nu furnizează criptarea sau confidenţialitatea datelor de unul singur. El se bazează pe realizarea protocolului de tunelare pentru a oferi un plus de intimitate a datelor. Protocolul folosit la nivelul data-link al modelului OSI a fost în special conceput pentru realizarea tunelelor PPP îmbunătăţite.

3. Avantajele VPN-urilor

Popularitatea tehnologiei VPN este legată direct de potenţialul acesteia de recuperare semnificativă a investiţiilor (return of investment). Pentru firmele care plătesc costuri adesea ameţitoare pentru conexiunile private prin linii închiriate sau prin Frame Relay (releu de cadre), este semnificativă reducerea cheltuielilor asociată cu instalarea reţelelor VPN, care înlocuiesc conexiunile costisitoare.

Cu ajutorul unor echipamente aparte de concentrare a accesurilor VPN remote-connection, se pot examina pachetele aplicaţiilor in parte identificând orice pachete considerate a fi periculoase. aplicaţii de control pot cerceta pachetele pentru a fi corelate cu conexiuni acceptate de management. In cazul unei neconcordante pachetele sunt descărcate. aceste capabilităţi creaza un sistem pe mai multe nivele de apărare în mediile reţelelor curente în care schimbarea este un factor important. Politici de securitate detaliate sunt aplicate traficului VPN, astfel încât ultilizatorii şi grupurile de utilizatori au acces la resursele reţelei la care au dreptul.

Echipamentele de securizare a VPN-urilor permite unui administrator să definească politici ce monitorizează atât accesul între locaţiile conectate cât şi între utilizatorii conectaţi de la distanţa. Tehnologia a evoluat, iar soluţia de frunte pentru aceste necesităţi este cea a reţelelor private virtuale (VPN) criptate bazate pe protocolul IPSec. [6]

IP Security (IPSec) a fost proiectat de către organizaţia IETF (Internet Enginnering Task Force) ca şi un mecanism de asigurare a securităţii datelor la nivelul comunicaţiilor bazate pe Internet Protocol. au fost definite de a serie de documente RFC 2401, 2402 şi 2406, care au stabilit în arhitectura globală, un antet de autentificare (AH - authentication Header) pentru a verifica integritatea datelor şi o încărcătură securizată încapsulată (ESP- Encapsulating Security Payload) pentru asigurarea celei de-a doua funcţii de asigurare a confidenţialităţii: criptarea datelor.

Antetul de autentificare pe lângă rolul de a garanta integritatea datelor transmise poate optional proteja pachetele împotriva atacurilor de întoarcere folosind tehnica ferestrelor glisante (sliding window) şi descărcarea pachetelor vechi.[6]

- În IPv4, AH protejează încărcătura IP şi toate antetele câmpurilor din datagramele IP, cu excepţia pentru câmpurile variabile: DSCP/TOS, ECN, Flags, Fragment Offset, TTL and Header Checksum;
- În IPv6, AH îşi protejează antetul propriu, opţiunile destinaţiei antetului extins după antetul său, şi apoi încărcătura IP; de asemenea protejează şi antetul IPv6 fix şi toate antetele extinse înainte de AH, excepţie făcând urătoarele câmpuri: DSCP, ECN, Flow Label, and Hop Limit.

Pachet datagramă cu antet de autentificare, din figura 16 mai jos, arată cum este acest pachet construit şi interpretat:

Offsets	Octet$_{16}$	0								1								2								3							
Octet$_{16}$	Bit$_{10}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Next Header								Payload Len								Reserved															
4	32	Security Parameters Index (SPI)																															
8	64	Sequence Number																															
C	96	Integrity Check Value (ICV)																															
...	...	...																															

Figura 16: Formatul antetului de autentificare (AH) [11]

Next Header (8 bits)

Tipul antetului următor indică ce protocol de nivel superior a fost protejat; Valoarea este luată din lista cu numerele de protocole IP.

Payload Len (8 bits)

Lungimea acestui antet de autentificare în 4 unităţi de octeţi minus 2. Deşi mărimea este măsurată în 4 unităţi de octeţi, lungimea acestui antet are nevoie SA fie multiplicat cu 8 octeţi dacă este purtat într-un pachet IPv6. această restricţie nu este aplicată unui AH purtat într-un pachet IPv4.

Reserved (16 bits)

Rezervaţi pentru utilizări viitoare (toate zerourile pâna atunci).

Security Parameters Index (32 bits)

Valoarea arbitrară care este folosită (împreună cu adreSA IP a sursei) pentru a identifica asocierei de securitate a unei sesiune de trimitere.

Sequence Number (32 bits)

O secveţă monotonă de creştere a numărului (incrementat cu 1 pentru fiecare pachet trimis) pentru prevenirea atacurilor de întoarcere (reply attacks).

Integrity Check Value (multiplu de 32 bits)

Lungime variabilă ICV verifică valoarea. Este posibil să conţină paduri de aliniere de câmp în limita de 8 octeţi pentru IPv6 sau în limita a 4 octeţi pentru IPv4.

Încărcătura securizată încapsulată (ESP- Encapsulating Security Payload) este un membru a protocolului IPSec care suportă numai configuraţii de criptare şi autentificare dar folosirea criptării fără autentificare este puternic descurajată deaorece este nesigură. Spre deosebire de AH, ESP nu oferă protecţie antetului pachetului IP.

În figura 17 este ilustrat cum este construit şi interpretat pachetul datagaramă ESP:

Security Parameters Index (32 bits)

Valoarea arbitrară care este folosită (împreună cu adreSA IP a sursei) pentru a identifica asocierei de securitate a unei sesiune de trimitere.

Sequence Number (32 bits)

O secveţă monotonă de creştere a numărului (incrementat cu 1 pentru fiecare pachet trimis) pentru prevenirea atacurilor de întoarcere (reply attacks).
aici se găseşte un contor separat ţinut pentru fiecare asociere de securitate.

Offsets	Octet16	0								1								2								3							
Octet16	Bit10	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Security Parameters Index (SPI)																															
4	32	Sequence Number																															
C	96	Payload data																															
...	...																																
...	...									Padding (0-255 octets)																							
...	...																																
...	...																	Pad Length								Next Header							
...	...	Integrity Check Value (ICV)																															
...	...	...																															

Figura 17: Formatul ESP [11]

Payload data (variable)

Conţinutul protejat în pachetul IP original ce include orice date folosite pentru protecţie. Tipul conţinutului care a fost protejat este indicat ăn câmpul antetului vecin.

Padding (0-255 octets)

Încărcarea pentru criptare, pentru extinderea datelor de încărcare la dimensiunea unui chiper de criptare, şi aliierea cîmpului următor.

Pad Length (8 bits)

Mărimea padding-ului în octeţi .

Next Header (8 bits)

Tipul antetului următor indică ce protocol de nivel superior a fost protejat; Valoarea este luată din lista cu numerele de protocole IP.

Integrity Check Value (multiple of 32 bits)

Lungime variabilă ICV verifică valoarea. Este posibil să conţină paduri de aliniere de câmp în limita de 8 octeţi pentru IPv6 sau în limita a 4 octeţi pentru IPv4.

Pentru a stabili adevărul, ***autentificarea*** verifică identitatea a două puncte de capăt VPN şi a utilizatorilor ce transmit traficul prin reţeaua VPN. Un punct de capăt ar putea fi un client VPN, un concentrator VPN, un sistem firewall sau un router. autentificarea este un proces ce ţine de securitatea IP şi care are loc după criptarea datelor şi înainte de decriptare, la capătul receptor. Este o funcţie necesară în cadrul securităţii IP, prin care se asigură că ambele părţi, expeditorul şi destinatarul, sunt cine pretind a fi. In cazul IPSec, fiecare participant trebuie configurat manual cu o cheie partajată anterior (de obicei se convine asupra ei în afara unei conexiuni) şi o listă statică de participanţi valabili, creând astfel un tabel mare în cadrul routerului, care necesită resurse de memorie.[6]

Integritatea datelor este o altă funcţie din IPSec. Integritate înseamnă că pachetul primit de destinatar nu a fost modificat în timpul transmisiei. acest lucru

se realizează folosind un algoritm hash ireversibil. Un algoritm hash ireversibil este echivalent cu o sumă de control criptată. După ce expeditorul criptează şi autentifică un pachet, algoritmul hash ireversibil este rulat pe valoarea întregului pachet. O valoare hash este interesantă pentru că rezultatul acesteia va avea întotdeauna o dimensiune fixă, indiferent de intrare.

IPSec are două moduri de criptare***: tunel şi transport***. Fiecare mod diferă prin aplicaţiile sale şi prin cantitatea de informaţii adăugate în antetul pachetului pasager. aceste moduri diferite de operare sunt rezumate astfel: modul tunel criptează antetul pachetului şi segmentul de date utile al fiecărui pachet, pe când modul transport criptează doar segmentul cu datele utile.[6]

Modul tunel este metoda normală prin care IPSec este implementat între două sisteme IPX Firewall (sau alte porţi de securitate) care sunt conectate printr-o reţea lipsită de încredere, cum este Internetul public. Întreaga prezentare legată de IPSec implică modul tunel. Modul tunel încapsulează şi protejează un pachet IP complet. Deoarece încapsulează sau ascunde pachetele pentru a fi transmise în continuare cu succes, chiar routerele de criptare posedă adresele IP folosite în aceste antete noi. Folosirea modului tunel duce la o creştere suplimentară a pachetului, cu aproximativ 20 de octeţi asociaţi la antetul IP, căci trebuie să se adauge un antet IP nou la pachet, ca în figura 18.[6]

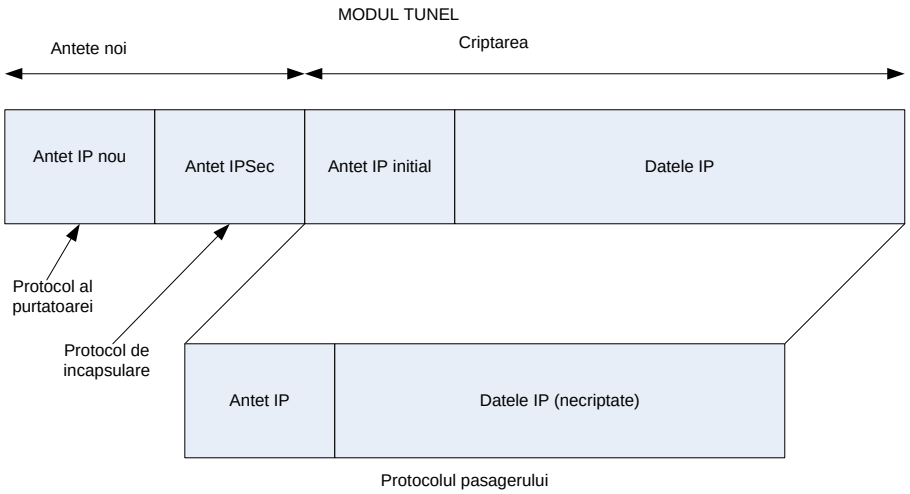


Figura 18: Modul Tunel [9]

Modul transport este o metodă de implementare a tehnologiei IPSec este aplicată mai ales cu protocolul L2TP pentru a permite autentificarea clienţilor VPN- Windows 2000 aflaţi la distanţă. În modul tunel, IPSec criptează întregul pachet şi scrie un nou antet IP în pachet, ceea ce maschează informaţiile despre surSA iniţială şi destinatar. Modul tunel este evident mai sigur decât modul transport (deoarece întregul pachet iniţial este criptat, nu numai segmentul de date propriu-zise ca în modul transport), cum este arătat în figura 19.[6]

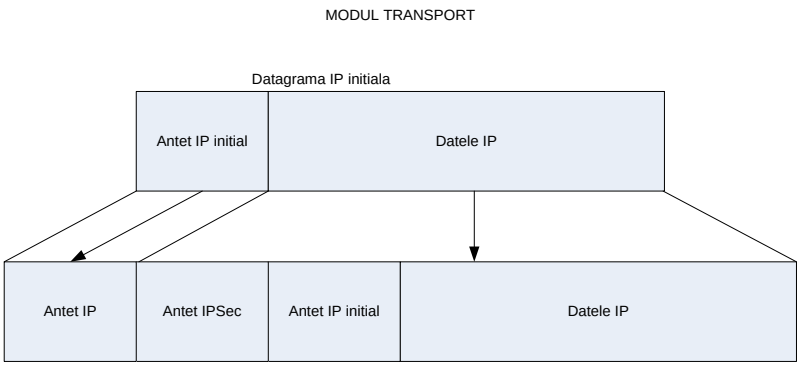


Figura 19: Modul Transport [9]

Asocierile de securitate (Sa) stabilesc încrederea între două dispozitive într-o relaţie egal-la-egal şi activează punctele de capăt VPN pentru a conveni asupra unui set de reguli de transmitere, folosind politici de negociere cu un participant potenţial. O asociere de securitate poate fi văzută ca un contract prin care se negociază şi apoi se stabilesc diferiţi parametri ai conexiunii. O asociere de securitate este identificată printr-o adresă IP, printr-un identificator de protocol de securitate şi o valoare unică de index al parametrului de securitate SPI — (Security Parameter Index). Valoarea SPI este un număr de 32 de biţi înglobat în antetele pachetelor. Cele două tipuri de asocieri de securitate sunt:

1. ***Internet Key Exchange*** (IKE — schimbul de chei în Internet). Conţine negocierea, autentificarea unui participant, managementul cheilor şi schimbul de chei. Fiind un protocol bidirecţional, IKE oferă un canal de comunicare protejat între doua dispozitive care negociază un algoritm de criptare, un algoritm hash, o metodă de autentificare şi orice informaţie relevantă de grup. Foloseşte schimbul de chei bazat pe algoritmi Diffie-Hellman, iar administratorii de reţea pot lega bine protocolul IKE de sistemele de gestionare a politicilor. [7]

2. ***IPSec Security association*** (IPSec SA — asociere de securitate IPSec) — IPSec SA este o asociere unidirecţională şi de aceea este necesar să se stabilească asocieri IPSec SA pentru fiecare direcţie. IPSec SA este o procedură în două faze şi trei moduri. în faza 1, pot fi folosite două moduri: main mode (modul principal) şi aggressive mode (modul agresiv). In faza 2, singurul mod disponibil este numit quick mode (modul rapid). Utilizatorul final nu are nici un control asupra alegerii modului, selectarea fiind automată şi depinzând parametrii de configurare stabiliţi de ambii participanţi. [7]

Modul principal cuprinde un număr de şase mesaje care se schimbă între iniţiatorul şi responderul de IPSec.

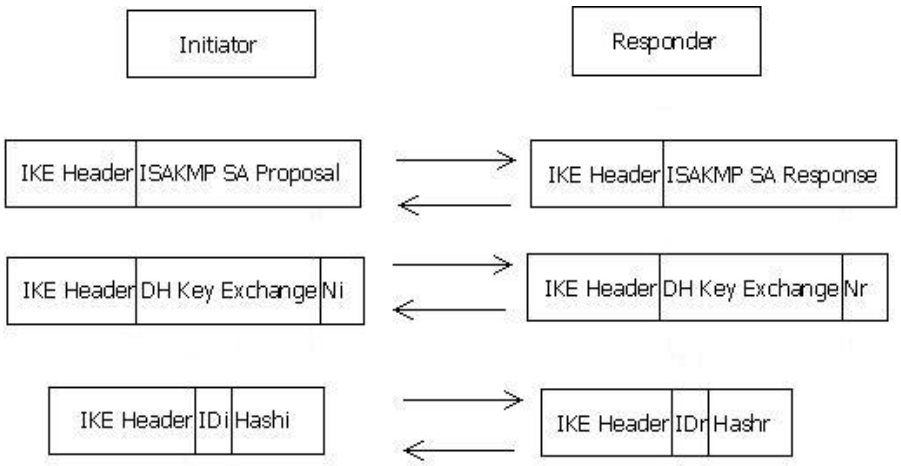


Figura 20: Modul principal de autentificare IKEv1 [9]

Modul agresiv cuprinde un număr de trei mesaje schimbate şi este considerat un schimb nesigur, de aceea nu se mai recomandă utilizarea lui.

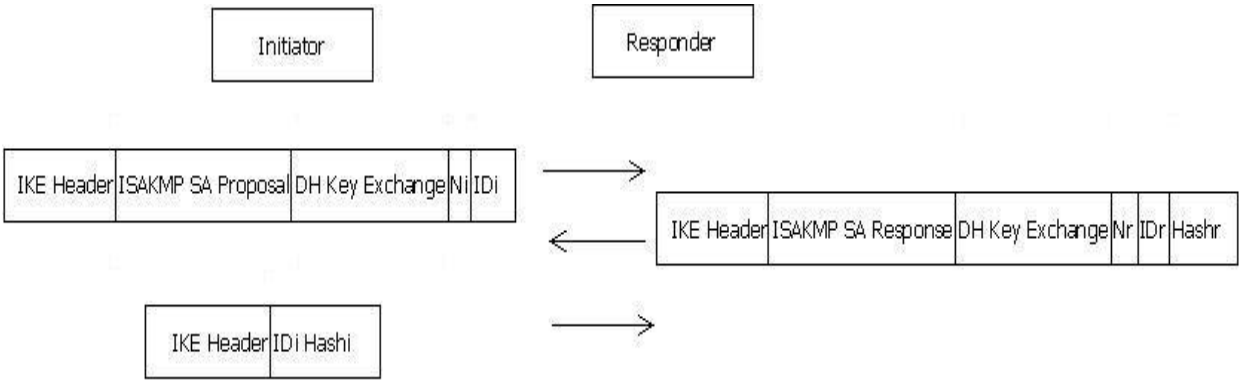


Figura 21: Modul agresiv de autentificare IKEv1 [9]

Negocierea **IKEv2** are un singur mod de stabilire si cuprinde un schimb iniţial - **Initial Exchange** şi un schimb de creare de asocieri de securitate - **CREATE_CHILD_SA Exchange**.

- **Initial Exchange** este un schimb alcătuit din patru mesaje, el fiind oarecum echivalentul primei faze în accepţiunea protocolului IKEv1.
- **CREATE_CHILD_SA Exchange** este un schimb alcătuit din două mesaje, echivalentul celei de-ale doilea faze din IKEv1.
-

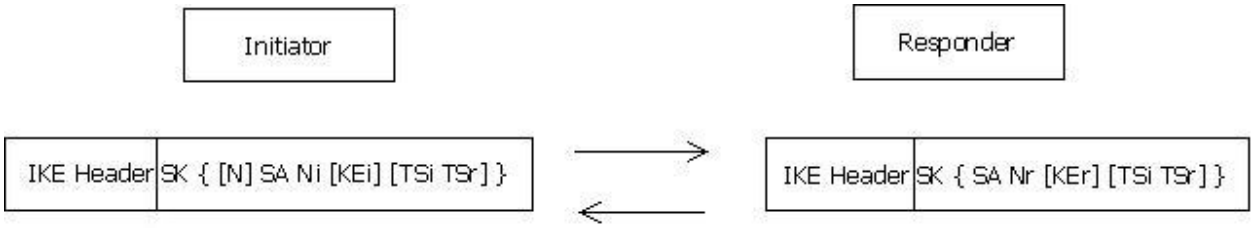


Figura 22: Modul de autentificare IKEv2 [9]

Protocolul Internet Key Exchange (IKE) este un protocol hibrid care foloseşte o parte din protocolul Oakley şi o parte dintr-o altă suită de protocoale numită Secure Key Exchange Mechanism (SKEME) în cadrul format de Internet Security association and Key Management Protocol (ISAKMP — protocolul de asociere pentru securitatea şi managementul cheilor în Internet). In figura de mai jos se poate vedea că IKE este cu adevărat un protocol hibrid.

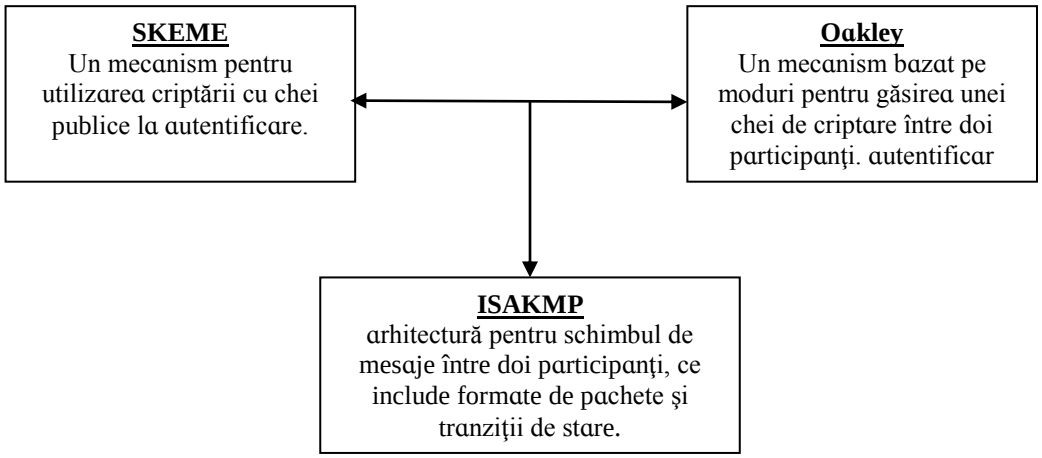


Figura 23: IKE (Internet Key Exchange) – RFC 2409 - este un protocol hibrid. [9]

Protocolul ISAKMP (Internet Security association and Key Management Protocol — protocolul de asociere pentru securitatea şi managementul cheilor în Internet) este un cadru care defineşte mecanismele de implementare a protocolului: de schimb al cheilor şi negocierea unei politici de securitate. ISAKMP este folosi pentru schimburile protejate atât de parametri Sa, cât şi de chei private, între participanţii dintr-un mediu IPSec, precum şi la crearea şi controlul cheilor.

ISAKMP oferă mai multe metode de control al cheilor şi un tranzit protejat al parametrilor IPSec între participanţi. acest lucru este realizat folosind algoritmi similari cu cei folosiţi de IPSec pentru criptarea propriu-zisă a datelor din segmentul de date. Ca şi IPSec, ISAKMP nu este un protocol, ci o simplă interfaţă de control al diferitelor metode de schimb dinamic al cheilor. ISAKMP defineşte diferite metode — cum ar fi semnătura digitală, certificatele şi algoritmii hash ireversibili — pentru a se asigura că negocierea asocierilor de securitate între participanţi se desfăşoară în siguranţă.

În prezent, singurul protocol acceptat din ISAKMP este protocolul Internet Key Exchange (IKE). Când IKE este folosit activ în procesul de criptare, devin disponibile multe funcţii pentru procesul de comunicare IPSec. Folosind criptarea cu chei publice, IKE negociază parametrii de securitate şi schimburile de chei înainte chiar ca prelucrarea IPSec să înceapă. [5]

Concluzii

Această lucrare prezintă utilizarea reţelelor VPN, modul de funcţionare, criptarea oferită de IPSec şi modul în care aceste tehnologii pot asigura păstrarea securităţi unei reţele. Toate firmele au clienţi cărora le oferă servicii într-o oarecare măsură indiferent de domeniu. Dar, în cazul reţelelor VPN, clienţii pot fi definiţi ca persoane a căror afacere necesită conectarea protejată la reţeaua companiei partenere pentru a avea acces la resurse. Clienţii pot fi utilizatori mobili (agenţi de vânzare, inginer de sistem), utilizatori importanţi care sunt conectaţi online în permanenţă, colectivul de conducere (staff-ul) sau parteneri de afaceri care culeg sau furnizează informaţii importante. Resursele sunt definite în acest caz ca fiind orice dispozitiv care nu este direct accesibil din Internet. aceste resurse pot include servere de poşta electronică, servere de fişiere, sau dispozitive de reţea.

Un VPN poate aduce multe beneficii firmei: extinde aria geografică de conectivitate, sporeşte securitatea, reduce costurile operaţionale, creşte productivitatea, simplifică topologia reţelei, oferă oportunităţi de lucru într-o reţea globală, asigură suport pentru telenavetişti şi altele.

Activitatile din ce în ce mai crescânde ale furnizorilor de Servicii Internet (ISP – Internet Service Provider) impulsionează avansările rapide ale tehnologiei în domeniul telecomunicaţiilor. La mijlocul anilor 90 modelul IP-over-ATM a creat multor furnizori de servicii Internet posibilitatea de a oferi o tehnologie performantă pentru traficul de reţea.

Marirea reţelei Internet şi evoluarea tehnologiei WDM (Wavelength Division Multiplexing – Multiplexarea lungimilor de undă) la nivelul fibrei optice au condus la apariţia unei alternative viabile pentru ATM prin multiplexarea multiplă a serviciilor (faţă de circuite individuale). De asemenea, ruterele coloanelor vertebrale Internet depăşesc ca viteză comutatoarele ATM, odinioara considerate foarte rapide şi cu o lăţime de bandă foarte mare. MPLS reprezintă ultimul pas făcut în evoluţia tehnologiilor de comutare/rutare pentru Internet, oferind mecanisme mai simple pentru controlul traficului orientat pe pachete, multifuncţionalitate împreună cu avantajul important al scalabilităţii şi nu în ultimul rînd al costurilor mult mai scăzute faţă de alte tehnologii.

Conform specialiştilor, în anul 2011, vor fi mai mult de 1 milion de conexiuni tip MPLS Multi-Protocol Label Switching VPN .

În concluzie, pentru cerinţele de comunicare ale multor reţele aparţinând diferitelor companii, VPN-urile bazate pe tehnologia MPLS reprezintă cea mai bună alegere. Totuşi pentru reţelele unde se doreşte o securitate crescută a traficului (trafic criptat între două puncte terminale) varianta optimă rămâne VPN cu IPSec.

Bibliografie

[1] - „Primii paşi în securitatea reţelelor” - Thom Thomas, Editura Corint, Bucureşti, 2005;

[2] - **“**QoS în reţelele IP multimedia” - Tatiana Rădulescu, H.G. Coandă, Editura albastră, Cluj-Napoca , 2007;

[3] - „Sisteme de comunicaţii – Reţele ATM şi reţele locale” - H.G. Coandă, Editura Bibliotech, Târgovişte, 2004;

[4] - „Reţele de calculatoare” - andrew Tanenbaum, Ediţia a IV-a, 2003;

[5] - „Reţele digitale în telecomuncaţii” - Virgil Dobrotă, vol.III OSI şi TCP/IP, Editura Mediamira, Cluj-Napova, 2002;

[6] - “Reţele de calculatoare” - Peter Norton;

[7] - http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800c75d1.html#1000872 accesat la data de 15 ianuarie 2015;

[8] - Multiprotocol Label Switching (MPLS) Traffic Engineering, http://www.cisco.com/univered/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s5/mpls_te.htm accesat la data de 17 ianuarie 2015;

[9] - http://ro.wikipedia.org/wiki/Re%C5%a3ea_privat%C4%83_virtual%C4%83#Generic_Router_Encapsulation accesat la data de 15 ianuarie 2015;

[10] - http://technet.microsoft.com/en-u s/library/cc768084.aspx accesat la data de 14 ianuarie 2015;

[11]- http://ro.wikipedia.org/wiki/IPSec accesat la data de 20 ianuarie 2015.