Universitatea Politehnica Bucuresti

Facultate de Electronica, Telecomunicatii si Tehnologia Informatiei

Securizarea retelelor de date – IPSEC

Tema de casa – Retele de Calculatoare si Internet

**Masterand:**

**Burlacu Alina**

Cuprins

[Introducere 2](#_Toc265663770)

[Asigurarea securitatii prin metode criptografice 3](#_Toc265663771)

[Securizarea Infrastructurii 5](#_Toc265663772)

[Ameninţări posibile 5](#_Toc265663773)

[Securizarea Comunicatiei 5](#_Toc265663774)

[Reţele virtuale private 6](#_Toc265663775)

[Concepte generale 6](#_Toc265663776)

[Cum funcţionează VPN ? 6](#_Toc265663777)

[Soluţii VPN 6](#_Toc265663778)

[Standardizarea reţelelor VPN – protocolul IPSec 8](#_Toc265663779)

[Concepte generale 8](#_Toc265663780)

[Structura IPSec 9](#_Toc265663781)

[Cum funcţionează IPSec 12](#_Toc265663782)

[Tunele GRE cu protecţie IPSec 13](#_Toc265663783)

[Bibliografie 14](#_Toc265663784)

# Introducere

Problemele securităţii reţelei pot fi împărţite, în mare, în patru domenii strâns interconectate: confidenţialitate, autentitficare, nerepudiere şi controlul integrităţii. Păstrarea secretului, denumită de asemenea şi **confidenţialitate**, se referă la păstrarea informaţiei departe de utilizatorii neautorizaţi. **Autentificarea** reprezintă determinarea identităţii persoanei cu care vorbeşti înainte de a dezvălui informaţii importante sau de a intra într-o afacere. **Nerepudierea** implică semnături: cum poţi fi sigur că un mesaj pe care l-ai primit a fost cel trimis cu adevărat şi nu unul pe care o persoană rău intenţionată l-a recodificat.

Înainte de a intra în prezentarea acestor soluţii, stabilim unde anume în stiva de protocoale se situează securitatea reţelei. Fiecare nivel poate contribui cu ceva.

La ***nivelul fizic***, ascultarea firelor poate fi zădărnicită prin încapsularea liniilor de transmisie în tuburi sigilate conţinând gaz de argon la presiuni înalte. Orice incercare de a perfora tubul va duce la pierderi de gaz, reducând presiunea şi tragând alarma. Câte­va sisteme militare folosesc această tehnică.

La nivelul ***legatură de date***, pachetele transmise pe o linie punct-la-punct pot fi codificate când părăsesc una dintre maşini şi decodificate când intră în cealaltă. Toate detaliile pot fi manipulate la nivelul legatură de date, fără ca nivelurile mai inalte să aibă cunoştinţă de ceea ce se petrece. Această solutie eşuează, totuşi, atunci când pachetele trebuie să traverseze mai multe rutere, deoarece pachetele trebuie decriptate în fiecare ruter, făcându-le astfel vulnerabile la atacurile din interiorul echipamentelor.

La nivelul ***reţea***, pot fi instalate ziduri de protecţie pentru a păstra pachetele în interior sau pentru a păstra pachetele în afara acestuia. Securitatea IP funcţionează de asemenea la acest nivel.

La nivelul ***transport***, pot fi criptate conexiuni întregi, de la un capat la celălalt, adică de la un proces la celălalt. Pentru o securitate maximă, este necesară securitatea capăt-la-capăt (eng.: *end-to-end security*).

În sfârşit, problemele cum sunt autentificarea utilizatorilor şi nerepudierea nu pot fi tratate decât la nivelul ***aplicaţie***.

# Asigurarea securitatii prin metode criptografice

Criptografia este o metoda de transformare a informaţiilor originale într-o formă care pare a fi aleatoare şi ilizibilă. O definiţie şi mai simplă a criptării ar fi că aceasta este metoda de stocare şi transmitere a datelor într-o formă care poate fi citită sau procesată doar de către destinatarul asignat. Stiinţa comunicării secrete şi sigure, criptografia, permite emiţătorilor să transforme informaţia într-un mesaj codat folosind o cheie secretă, ştiută doar de cel care trimite si de destinatarul autorizat. În cazul în care persoane neautorizate interceptează transmisia şi primesc mesajul, ar trebui să fie incapabile să-l decodeze. Cheia, care este de obicei un şir de biţi de lungime variabilă lucrează cu algoritmul de criptare pentru a coda/decoda mesajul. Algoritmul, un set de reguli matematice, dictează cum are loc cifrarea, respectiv descifrarea textului. Majoritatea algoritmilor de criptare sunt cunoscuţi, nu reprezintă partea secretă a procedului de codare; cheia este cea care nu trebuie să fie cunoscută.

Profesioniştii fac o distincţie între cifruri şi coduri. Un *cifru* este o transformare caracter-cu-caracter sau bit-cu-bit a mesajului, fără a ţine cont de structura lingvistică a acestuia. Prin contrast, un *cod* înlocuieşte un cuvant cu un alt cuvant sau cu un simbol. Codurile nu mai sunt foiosite, deşi au avut o istorie glorioasă.

* **Cifruri clasice**
	+ - **Cifruri cu substitutie** - fiecare literă sau grup de litere este înlocuit pentru a-l deghiza, cu altă literă sau grup de litere. Dacă textul clar este văzut ca o secvenţă de biţi, substituţia implică înlocuirea textului clar cu modele criptate de biţi.

*Cifrul lui Caesar*- fiecare literă a alfabetului va fi înlocuită cu litera cu trei locuri mai departe în alfabet; astfel, *a* devine *D, b* devine *E, c* devine *F,*..., *z* devine C.

* + - **Cifruri cu transpozitie -** reordonează literele, dar nu le deghizează.

 **-** se caracterizează prin faptul că textul în clar rămâne acelaşi, doar ordinea caracterelor se schimbă. O simplă transpoziţie permite păstrarea proprietăţilor statistice ale textului în clar şi textului cifrat; o nouă transpoziţie a textului cifrat măreşte securitatea cifrului.

* **Algoritmi cu cheie secreta**

Criptografia modernă utilizează aceleaşi idei de bază ca şi criptografia tradiţională (transpoziţia şi substituţia) dar accentul este diferit. Tradiţional, criptografii foloseau algoritmi simpli. Astăzi este valabilă ipoteza contrarie: obiectivul este de a face algoritmi de criptare atât de complecşi şi ireversibili, încât, chiar dacă un criptanalist achiziţionează cantităţi imense de text cifrat la alegerea sa, el nu poate face nimic făra a avea cheia.

* **Algoritmul DES -** a fost adoptat extensiv în industrie pentru a fi utilizat în produsele de scuritate. Textul clar este cripiat în blocuri de câte 64 de biţi, rezultând blocuri de 64 de biţi de text cifrat. Algoritmul, care este parametrizat cu o cheie de 56 de biţi, are 19 runde distincte:prima rundă este o transpoziţie independentă de cheie, aplicată asupra textului clar de 64 de biţi iar ultima este inversa acestei transpoziţii. Algoritmul a fost proiectat pentru a permite ca decriptarea să se facă cu aceeaşi cheie ca şi criptarea, o proprietate necesară în orice algoritm cu cheie secretă. Paşii sunt parcurşi în ordine inversă.
* **Algoritmul Triplu-DES –** foloseste tripla criptare. În prima rundă textul clar este în mod obişnuit criptat cu K1*,* în a doua rundă, este rulat DES în mod de decriptare, folosind cheia K2. În final, este efectuată o altă criptare cu K1.
* **Algoritmul AES**- Criteriile pe baza cărora au fost evaluate propunerile pentru AES au fost *securitatea* (rezistenţa la atacuri criptanalitice), *costurile* (eficienţa computaţională, complexitatea spaţială, precum şi licenţierea liberă şi gratuită) şi *particularităţile algoritmului* (flexibilitatea, simplitatea, şi uşurinţa de realizare a implementărilor atât software cât şi hardware). Operaţiile AES sunt definite sub formă de operaţii pe matrice, unde atât cheia, cât şi blocul sunt scrise sub formă de matrice. La începutul rulării cifrului, blocul este copiat într-un tablou denumit *stare* (în engleză *state*), primii patru octeţi pe prima coloană, apoi următorii patru pe a doua coloană, şi tot aşa până la completarea tabloului.Algoritmul modifică la fiecare pas acest tablou de numere denumit *state*, şi îl furnizează apoi ca ieşire.
* **Algoritmi cu cheie publica**

Un astfel de sistem foloseşte o pereche de chei aflate într-o relaţie matematică: o cheie privată, menţinută în secret în cadrul sistemului şi o cheie publică, ce poate fi cunoscută de oricine. Astfel crearea şi distribuţia cheilor, prin cheia publică, poate fi realizată mult mai simplu faţă de cazul unui criptosistem cu cheie privată. Există două tipuri de criptosisteme utilizate în mod curent în cazul unor reţele VPN; Diffie-Hellman (DH) şi Rivest Shamir Adlemen (RSA).

* **Diffie-Hellman** - combinaţia dintre cheia privată a utilizatorului A şi cheia publică a lui B va genera acelaşi rezultat ca şi combinaţia dintre cheia privată a lui B şi cheia publică a lui A. Această proprietate poate fi extinsă la orice combinaţie de două chei, astfel încât cheia publică a oricărui partener de comunicaţii poate fi distribuită liber, fără a pune în pericol securitatea criptositemului. Cele două părţi, care schimbă propriile chei publice, sunt singurele care pot genera ceea ce se numeşte secretul comun (eng. *shared secret*). Sistemul devine foarte sigur, fără ca o altă parte să poată crea sau cunoaşte secretul comun.
* **Rivest Shamir Adleman (RSA) -** un algoritm criptografic cu chei publice, primul algoritm utilizat atât pentru criptare, cât şi pentru semnătura electronică. Puterea sa criptografică se bazează pe dificultatea problemei factorizării numerelor întregi, problemă la care se reduce criptanaliza RSA şi pentru care toţi algoritmii de rezolvare cunoscuţi au complexitate exponenţială. Dacă A îşi foloseşte cheia privată RSA pentru criptarea unui mesaj, oricine deţine cheia sa publică poate decripta acel mesaj.
* **Semnaturi digitale**

Un mesaj este introdus într-un algoritm matematic cunoscut sub numele de funcţie **hash** (de mixare) care mapează valori mai mari pe valori mai mici. Mărimea mesajului este micşorată, astfel încât să se asigure performanţele maxime la transmisia pe reţea - cu cât un mesaj este mai scurt, cu atât mai puţine calcule sunt neceasare, deci şi performanţele sunt mai mari.

Rezultatul funcţiei hash, cunuscut sub numele de **message digest (sumar de mesaj)** este apoi criptat cu cheia privată a emiţătorului. Sumarul de mesaj astfel criptat formează semnătura digitală, care va fi ataşată la mesajul original, ambele componente fiind apoi criptate şi trimise destinatarului. Acesta poate autentifica mesajul după cum urmează. Mai întâi, prin folosirea aceleiaşi funcţii de mixare de mai sus, stabilite de comun acord, se regenerează sumarul de mesaj. Semnătura digitală încorporată în mesaj este apoi decriptată cu cheia publică a expeditorului. În final, se compară cele două rezultate. Dacă şi numai dacă cele două sumare coincid, se poate concluziona cu siguranţă că:

- mesajul a fost transmis prin utilizarea cheii private corespondente;

- mesajul nu a fost alterat în decursul transferului.

Unele dintre funcţiile de mixare criptografice folosite în procesul de semnătură digitală sunt: MD4, MD5, SHA-1 şi CBC- DES-MAC, între ele fiind diferenţe de lungime a cheilor şi de metodă de hash. Funcţiile hash/de mixare pot fi utilizate şi pentru a verifica dacă mesajul a fost recepţionat în forma originală (integritatea datelor), caz în care funcţiile hash (ca şi semnăturile digitale rezultate) sunt mult mai cunoscute sub numele de algoritmi de autentificare a datelor.

Prin folosirea unei combinaţii între: schema de semnături digitale RSA, sistemul de distribuţie a cheilor Diffie-Hellman şi sistemul simetric de criptare cu cheie, se poate stabilii o sesiune criptată VPN care facilitează confidenţialitatea datelor, autentificarea datelor şi integritatea datelor. Odată cu stabilirea unei sesiuni criptate VPN, ea este protejată în faţa unor forme diferite de atac.

# Securizarea Infrastructurii

Una din marele probleme de securitate cu care astăzi se confruntă instituţiile este faptul că sunt necesare măsuri de protecţie sofisticate şi uneori complicate, pentru a se apăra de cele mai noi ameninţări reprezentate de intruşi şi de a reduce vulnerabilităţile în activitate. Un alt obstacol major implică hotărârea dacă o soluţie de securitate este sau nu corespunzătoare pentru a se potrivi afacerii respective; un număr vast de produse specializate funcţionează doar pe anumite părţi ale reţelei şi nu reuşesc să fie o o soluţie bună pentru conectivitatea capăt-la-capăt (***eng.*** *end-to end)*.

Ameninţări posibile

 Când vorbim de securitate în zona reţelelor trebuie să avem în vedere două aspecte: protecţia împotriva accesului neautorizat şi recuperarea datelor în urma unor evenimente neprevăzute.

 Protecţia împotriva accesului neautorizat este asigurată prin politici de securitate şi prin intermediul sistemului de operare folosit, oricare ar fi acesta. Metodele folosite de persoanele neautorizate pentru a-şi câştiga accesul pe echipamentele de reţea sunt definie ca şi ameninţări.

 Este suficient de rău să existe o problemă de securitate în sistem dar uneori este sfidat orice efort de a grupa pe categorii problemele şi de a defini metodele de a proteja reţeaua de acestea prin numărul, natura şi tipurile de de **ameninţări de securitate** care există astazi:

* **Eavesdropping**(Aflarea conţinutului mesajelor) - este o metodă de a captura pachetele TCP-IP sau a oricărui alt protocol, deci permite intrusului să decodeze conţinutul pachetului folosind un analizator de protocoale. Intercepţia pachetelor (Packet sniffing) este un termen mai comun folosit pentru a descrie acţiunea de eavesdropping (exemplu: numere de card de credit sau de asigurări sociale furate).
* **Manipularea datelor** - este un simplu act de alterare a fişierelor pe calculatoare, vandalizarea site-urilor Web sau înlocuirea fişierelor FTP.
* **Defectele protocolului** - cel mai utilizat protocol astăzi este TCP-IP. Acest protocol a fost conceput acum mult timp de aceea un număr de imperfecţiuni de creare pot conduce către posibile probleme de securitate: atacuri smurf, spoofing IP (modificarea header-elor pachetelor IP), predicţia numărului de secvenţă TCP sau inundări SYN.
* **Replicarea sesiunii** - pot fi ascultaţi unul sau mai mulţi utilizatori implicaţi într-o sesiune de comunicare şi sa se manipuleaze informaţiile în funcţie de ceea ce se urmăreşte să se facă.

Atacurile asupra reţelei sunt împărţite în trei mari categorii:

 -**Recunoaştere** - sunt asociate cu desoperirea şi maparea neautorizată a resurselor unei reţele. Un exemplu tipic de astfel de atac este **ping sweep** (scanare ping). Atacatorii pot folosi scanarea pentru a identifica dacă o adresă IP răspunde sau nu la ping; odată ce au identificat o adresă IP activă pot determina ce servicii şi ce porturi sunt deschide pe aceasta. Un atac de recunoaştere este primul pas spre un atac de negare a serviciilor (Denial of Services).

 -**Acces** - poate fi identificat cu refacerea neautorizată a datelor, care se clasifică prin citirea, scrierea, copierea, ştergerea, sau chiar mutarea fişierelor de orice tip de date. Exemple pot fi accesul la baza de date a companiei şi manipularea unei singure tabele sau modificarea privilegiilor unui utilizator într-un sistem. Atacurile de acces conduc la situaţii în care intruşii pot dobândi acces explorând vulnerabilităţile unui sistem ţintă.

 -**Negarea serviciilor** - are loc atunci când un hacker dezactivează sau corupe serviciile şi resursele găzduite de o reţea. Exemple tipice de atacuri DoS sunt **"ping-ul morţii"** şi atacul **TCP SYN**. Ambele atacuri sunt comune şi conduc către o saturare a serviciilor reţelei, adică acelea care nu sunt disponibile utilizatorilor autorizaţi. Al doilea exemplu presupune ca cineva să execute un atac TCP SYN (practic se face o inundaţie cu pachete de solicitare a conexiunii) împotriva unui server web al unei companii. Server-ul îşi va folosi o parte din resurse pentru a administra sesiunile TCP pe jumătate deschise şi răspunde persoanelor legitimate care sunt logate din ce în ce mai încet.

# Securizarea Comunicatiei

Securitatea reţelelor are ca scop protejarea acestora şi a aplicaţiilor de reţea împotriva unor atacuri. Pentru a realiza acest lucru, companiile abordeaza securitatea reţelelor creând o politică de securitate şi pe baza acestei politici, o arhitectură de securitate a reţelelor.

Confidenţialitatea datelor sau conectivitatea securizată a reţelei poate fi realizata prin implementarea Reţelelor Private Virtuale (VPN), care permit companiilor să îşi extindă reţeaua securizată a companiei către birouri aflate la distanţă, lucrători mobili sau parteneri extrareţea. Tehnologiile de criptare asigură că datele care circulă printr-un VPN nu pot fi interceptate sau citite de receptori neautorizaţi.

 Instrumente de monitorizare a securităţii permit supravegherea, recunoaşterea şi testarea vulnerabilităţilor în infrastructură a reţelei, astfel încât să poată fi rezolvate înainte ca intruşii să le exploateze.

 Tehnologia VPN oferă conexiuni private, separând datele în "tuneluri". În acest mod, o reţea privată poate fi creată prin reţele publice cum ar fi Internetul, folosind protocoale ca Generic Routing Incapsulation (GRE) sau Layer 2 Tunneling Protocol (L2TP). Pentru a oferi protecţia datelor pe care le transportă, echipamentele hardware şi software VPN susţin tehnologia de criptare. Tot traficul care circula printr-un tunel între două puncte într-un VPN este criptat.

 Uneori, separarea datelor folosind tehnologii de tunelare oferă confidenţialitate eficientă, de exemplu în cadrul reţelei locale. Deseori însă, cerinţele suplimentare de confidenţialitate necesită protecţie mai mare, de exemplu prin folosirea unor tehnologii sau protocoale de criptare digitale ca IPSec.

## Reţele virtuale private

### Co**ncepte generale**

Simplu definit, o reţea virtuală privată (VPN) este o reţea a companiei implementată pe o infrastructură comună, folosind aceleaşi politici de securitate, management şi performanţă care se aplică de obicei într-o reţea privată.

 Tehnologiile VPN oferă o cale de a folosi infrastructurile reţelelor publice cum ar fi Internetul pentru a asigura acces securizat şi privat la aplicaţii şi resurse ale companiei pentru angajaţii din birourile aflate la distanţă sau cei care lucrează de acasă, pentru partenerii de afaceri şi chiar pentru clienţi.

Un VPN poate fi realizat pe diverse reţele de transport deja existente: Internetul public, reţeaua furnizorului de servicii IP, reţele Frame Relay şi ATM. Astăzi, tot mai multe VPN-uri sunt bazate pe reţele IP. Tehnologia VPN foloseşte o combinaţie de tunneling, criptare, autentificare şi servicii de control al accesului, folosite pentru a transporta traficul pe Internet, o reţea IP administrată, sau reţeaua unui furnizor de servicii.

### Cum funcţionează VPN ?

Pentru a utiliza Internetul ca o reţea privată virtuală, de tip Wide Area Network (WAN), trebuie depăşite două obstacole principale. Primul apare din cauza diversităţii de protocoale prin care comunică reţelele, cum ar fi IPX sau NetBEUI, în timp ce Internetul poate înţelege numai traficul de tip IP. Astfel, VPN-urile trebuie să găsească un mijloc prin care să transmită protocoale non-IP de la o reţea la alta.

 Când un dispozitiv VPN primeşte o instrucţiune de transmitere a unui pachet prin Internet, negociază o schemă de criptare cu un dispozitiv VPN similar din reţeaua destinaţie Datele în format IPX/PPP sunt trecute în format IP pentru a putea fi transportate prin reţeaua mondială. Al doilea obstacol este datorat faptului că pachetele de date sunt transportate prin Internet în format text clar. În consecinţă, oricine poate „vedea” traficul poate să şi citească datele conţinute în pachete. Aceasta este cu adevărat o problemă în cazul firmelor care vor să comunice informaţii confidenţiale şi, în acelaşi timp, sa folosească Internetul. Soluţia la aceste probleme a permis apariţia VPN şi a fost denumită „tunneling". În loc de pachete lansate într-un mediu care nu oferă protecţie, datele sunt mai întâi criptate, apoi încapsulate în pachete de tip IP şi trimise printr-un „tunel" virtual prin Internet.

### Soluţii VPN

VPN-urile se împart în două mari categorii:

* **RemoteAccess VPN** – permite conectarea individuală (utilizatori mobili) sau a unor birouri la sediul central al unei firme, aceasta realizându-se în cele mai sigure condiţii.
* **Site-to-Site VPN** sau **LAN-to-LAN–** implică o conexiune sigură între două dispozitive de capăt, cum ar fi două routere, firewall-uri sau echipamente dedicate VPN; maşinile conectate la aceste puncte de capăt pot accesa reţeaua locală a celuilalt capăt prin conexiunea sigură bazată pe tactica de securitate a organizaţiei şi plasamentul resurselor comune.

#### Site-to-Site VPN



***Figura 4 -3.***  *Site-to-Site VPN*

**Intranet VPN**

Permite realizarea unei reţele interne complet sigură pentru o firmă şi a unor medii client-server foarte performante prin utilizarea conexiunilor dedicate care pot să atingă rate de transfer foarte bune (E1) limita fiind determinată de suma pe care firma respectivă este dispusă să o investească în infrastructura sa informaţională .

Arhitectura aceasta utilizează două routere la cele două capete ale conexiunii, între acestea realizându-se un tunel criptat. În acest caz nu mai este necesară folosirea unui client de VPN ci folosirea IPSec. IPSec este un protocol standardizat care asigură autentificarea, confidenţialitatea şi integritatea transferului de date între o pereche de echipamente care comunică. Foloseşte ceea ce se numeşte Internet Key Exchange ( IKE ) care necesită introducerea la ambele capete ale conexiunii a unor chei de autentificare care mai apoi vor permite logarea reciprocă.

Schematic conexiunea arată cam aşa :



**Extranet VPN**

Acest tip de VPN seamănă cu precedentul cu deosebirea că extinde limitele intranetului permiţând legarea la sediul corporaţiei a unor parteneri de afaceri, clienţi etc.; acest tip permite accesul unor utilizatori care nu fac parte din structura firmei. Pentru a realiza acest lucru se folosesc certificate digitale care permit ulterior realizarea unor tunele criptate .Certificatele digitale sunt furnizate de o autoritate care are ca activitate acest lucru.



În cel mai simplu sens, un VPN conectează două puncte de capăt peste o reţea publică pentru a forma o conexiune logică, ce poate fi făcută la nivel 2 sau 3 al modelului OSI. Conceputal, stabilirea unei conexiuni între două locaţii printr-un VPN de nivel 2 sau 3 se face la fel. Conceptul implică adăugarea unui "antet de expediere" în faţa înformaţiei utile (payload) pentru a-l transporta la destinaţie. În cazul unui VPN de nivel 2, antetul este plasat la acest nivel iar în celălalt caz, la nivel 3.

* ***VPN de nivel 2 -*** sunt reţele punct-la-punct şi stabilesc conexiuni între capete printr-un circuit virtual. Acest termen se referă la o conexiune logică capăt-la-capăt între două puncte şi poate cuprinde mai multe elemente şi mai multe segmente fizice ale unei reţele. ATM şi Frame Relay sunt două dintre cele mai populare tehnologii de VPN de nivel 2. Unul dintre avantajele acestui tip de VPN este independenţa de informaţia de trafic de nivel 3 care poate fi transportată (IP, IPX, AppleTalk, IP multicast).
* ***VPN de nivel 3 -*** aici există mai multe exemple, VPN-ul de nivel 3 încadrându-se între două posibilităţi:

*Tunele GRE* - Un tunel GRE între două locaţii care au rază de acoperire IP poate fi descris ca VPN, pentru că datele sunt încapsulate într-un antet GRE. În acest model, fiecare locaţie a corporaţiei necesită doar conectivitate la furnizorul său de Internet. Deşi VPN-urile construite peste Internet folosind GRE sunt posibile, sunt foart rar folosite de companii datorită riscurilor şi lipsei de mecanisme de securitate.

*MPLS* - Furnizorii de Internet dezvoltă din ce în ce mai mult MPLS-ul pentru a oferi soluţii de VPN clienţilor. Pentru încapsulare MPLS foloseşte etichete. Unul din avantajele acestei soluţii este flexibilitatea de configurare arbitrară a topologiilor între locaţiile din VPN. Tehnica folosită de MPLS este comutaţia de etichete. O etichetă de lungime fixă este codată într-un antet MPLS şi este folosită pentru îndrumarea pachetelor.

*IPSec* - Una dintre principalele griji ale oricărei persoane care foloseşte VPN este securizarea datelor când traversează o reţea publică.Criptarea datelor este o posibilitate şi se poate realiza prin implicarea unor dispozitive de reţea în fiecare locaţie. IPSec este o suită de protocoale dezvoltate sub auspiciile lui IETF pentru a dobândi servicii sigure reţelelor cu comutare de pachete IP. Totodată, dezvoltarea VPN-urilor pe baza reţelei publice Internet poate însemna reducerea costurilot semnificant de mult comparativ cu liniile închiriate. Serviciile IPSec permit autentificare, integritate, controlul accesului şi confidenţialitare. Cu IPSec, schimbul de informaţii între locaţiile la distanţă poate fi criptat şi verificat. Cu IPsec pot fi dezvoltate soluţii atât la distanţă, cât şi site-to-site.

## Standardizarea reţelelor VPN – protocolul IPSec

### Concepte generale

Este cunoscut faptul că numai standardele susţinute de industrie vor asigura interoperabilitatea aplicaţiilor. Administratorii care implementează o soluţie VPN sunt puşi în faţa unor anumite probleme, din cauza absenţei standardelor. Internet Engineering Task Force (IETF) a stabilit un grup de lucru numit IP Security (IPSec), dedicat definirii standardelor şi protocoalelor legate de securitatea Internetului.

**IPSec** a apărut în cadrul efortului de standardizare pentru IPv6 şi reprezintă singura soluţie 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 informaţiei, între două sisteme firewall, de exemplu. În modul *transport*, informaţia este încapsulată altfel încât ea poate fi securizată între punctele terminale ale conexiunii, deci "ambalajul" nu ascunde informaţia de rutare cap-la-cap. Modul tunel este cea mai sigură metodă de securizare, însă creşte gradul de încărcare a sesiunii de comunicaţie, prin mărirea dimensiunilor pachetelor.

Lucrarea îşi propune să furnizeze o persectivă asupra metodelor de control al securităţii care oferă protecţie pentru reţelele TCP/IP, foarte folosite astăzi. Controlul securităţii se poate face la oricare dintre cele patru nivele ale stivei TCP/IP; datele sunt pregătite pentru transport şi sunt tranzitate de la cel mai înalt la cel mai jos nivel, adăugându-se treptat noi informaţii. Astfel, nivelele de mai sus nu pot asigura protecţie totală pentru nivelele de jos pentru că acestea adaugă informaţii după ce s-au aplicat măsurile de securitate mai sus. Controlul la nivel reţea a devenit doarte utilizat în reţelele de date pentru că propune o soluţie mai balansată şi are marele avantaj de a priva utilizatorul de implicarea în configurarea echipamentelor.

### Structura IPSec

Există deja două idei majore în IPSec: Authentification Header (AH) şi Encapsulated Security Payload (ESP), definite după cum urmează:

- **Authentification Header** (AH) este folosit pentru a furniza integritatea şi autentificarea originii pentru orice datagramă IP, fără ca aceste atribute să fie orientate pe conexiune. Această proprietate este denumită generic "autentificare".

- **Encapsulated Security Payload** (ESP) furnizează autentificarea şi criptarea datagramelor IP folosind algoritmul de criptare stabilit de către utilizator. În autentificarea ESP, sumarul de mesaj este inserat la sfîrşitul pachetului (în timp ce în AH, sumarul se află în interiorul cîmpului de autentificare).

Standardul IPSec stabileşte că înainte de orice transfer de date trebuie negociată o asociere de securitate (Security Association - SA) între cele două noduri VPN (de tip gateway sau client), care să conţine toate informaţiile necesare pentru execuţia diferitelor servicii de securitate pe reţea, cum sunt serviciile corespunzătoare nivelului IP (autentificarea antetului şi încapsularea datelor), serviciile nivelurilor de transport sau aplicaţie, precum şi autoprotecţia traficului de date din negociere.

IPSec poate fi privit ca un nivel intermediar sub stivă TCP/IP. Acest nivel este controlat de o politică de securitate pe fiecare maşină şi de o asociere de securitate negociată între emiţător şi receptor. Politica constă într-un set de filtre şi un set de profile de securitate asociate. Dacă un pachet are adresa, protocolul şi numărul de port corespunzătoare unui filtru, atunci pachetul este tratat conform profilului de securitate asociat.

În afara protocoalelor de securitate prezentate anterior, IPSec mai conţine şi **protocolul Internet Key Exchange (IKE).** IPSec foloseşte IKE pentru a negocia setările de conexiune IPsec, pentru a autentifica vecinii unul cu celălalt, pentru a defini parametrii IPSec pentru conexiuni private, pentru a negocia cheile secrete şi pentru a administra, îmbunătăţi şi şterge canalele de comunicaţie IPSec.

#### Protocolul AH

AH, unul dintre protocalele de securitate IPSec, asigură integritatea datelor şi autentificarea utilizatorilor. Opţional, poate oferi protecţia accesului şi împotriva atacurilor de replicare. Nu poate cripta nicio porţiune din pachet. În versiunea iniţială IPSec, AH şi ESP erau des utilizaţi împreună (ESP nu asigura autentificarea), dar în cea de-a doua versiune, AH devine mai puţin semnificativ, până la stadiul îm care unele sisteme nu mai suportă AH. Totuşi, acest protocol este valoros pentru că poate autentifica porţiuni de pachet pe care ESP nu poate.

*Modurile AH*

AH are două moduri: transport şi tunel.

În modul **tunel**, AH crează un nou antet IP pentru fiecare pachet iar în modul **transport** nu. În arhitecturile IPSec care utilizează o poartă(gateway), sursa şi destinaţia adevărată a pachetelor trebuie să fie modificate pentru a fi adresa IP a porţii. Pentru că modul transport nu poate modifica antetul original IP sau să creeze un alt antet, acesta este utilizat în general în arhitecturile staţie-la-staţie.

Împreună cu protocolul AH, procesul NAT nu poate avea loc. AH protejează întregul pachet IP, incluzând câmpurile invariante ale antetului (adresele IP sursă şi destinaţie), printr-un sumar de mesaj pentru a produce un hash cifrat. Receptorul va folosi acest hash pentru a autentifica pachetul, deci dacă orice câmp din pachetul IP original este modificat, autentificarea va eşua şi pachetul va fi aruncat.

*Procesul de protejare a integrităţii*

Primul pas este crearea unui **hash** folosind un algoritm de control cifrat, cunoscut şi sub numele de algoritm MAC (cod de autentificare a mesajului). De cele mai multe ori hash-urile sunt confundate cu cu criptarea. Algoritmii hash produc o „amprentă” a unei informaţii, astfel încât aceste date vor produce de fiecare dată aceeaşi valoare. Dacă un singur bit se schimbă, atunci şi amprenta va fi diferită. Aceşti algoritmi sunt utilizaţi pentru a asigura integritatea prin faptul că ne asigură că datele nu au fost modificate în tranzit. Verificarea se face prin adăugarea hash-ului datelor trimise iar la destinaţie se rulează acelaşi algoritm asupra datelor, obţinându-se acelaşi hash (dacă datele nu au fost modificate). Cei mai importanţi algoritmi hash sunt MD5 şi SHA-1. Ambele preiau la intrare date de lungime arbitrară şi produc la ieşire o amprentă de 128 biţi, respectiv 160. SHA-1 conţine măsuri adiţionale de securitate, cum ar fi o rundă în plus pentru calularea valorii.

Pentru a preveni un atac de interceptare a transmisiei se introduce în algoritm şi o cheie secretă, cunoscută de capetele de tunel. Astfel, valoarea aleatoare procesată (cheia) va furniza autentificarea mesajului, mecanismul care dă o astfel de integritate se numeşte Cod de autentificare a mesajului (MAC). Atunci când MAC-urile se utilizează cu algoritmii de tip hash, va purta numele de HMAC.

IPSec foloseşte algoritmi de autenticitate HMAC, care execută două hash-uri acordate. Ca şi exemplu, cei mai utilizaţi algoritmi sunt HMAC-MD5 şi HMAC-SHA-1. Un alt algoritm cunoscut MAC este AES Cipher Block Chaining MAC (AES-XBC-MC-96).

#### Protocolul ESP

ESP este al doilea protocol de securitate, folosit de IPSec. Începând cu a doua variantă IPSec, protocolul poate performa autentificarea, pentru protejarea integrităţii, deşi nu şi pentru antetul IP extrem (cel mai din afară). O altă opţiune a ESP-ului oferă posibilitatea de a dezactiva criptarea prin algoritmul Null ESP.

*Modurile ESP*

ESP are două moduri: **transport şi tunel**. În modul **tunel**, ESP crează un nou antet IP pentru fiecare pachet care afişează capetele de tunel ESP, dar si sursa şi destinaţia pachetului. În această situaţie se poate realiza criptarea şi protejarea integrităţii atât a datelor cât şi a antetului original IP al fiecărui pachet. Dacă se utilizează şi autentificarea, fiecare pachet va avea o secţiune de **autentificare ESP** la sfârşit.

În modul **transport**, ESP utilizează antetul original IP, în loc să creeze unul nou. În acest caz, ESP poate doar să cripteze şi să asigure integritatea doar a anumitor componente ESP şi a informaţiei utile din pachet, nu şi a antetelor IP.Acest mod este incompatibil cu NAT, pentru că NAT modifică pachetul TCP şi trebuie să recalculeze suma de verificare pentru verificarea integrităţii. Pe de altă parte, autentificarea ESP va eşua dacă NAT actualizează suma de verificare TCP iar dacă NAT nu face actualizarea (de exemplu, dacă informaţia utilă este criptată), va eşua verificarea TCP. În modul tunel, ESP şi NAT pot funcţiona împreună pentru că adresa originală IP şi informaţia de transport sunt incluse în informaţia utilă. Astfel, NAT poate avea loc dacă maparea este de tip unu-la-unu.

 ESP utilizează criptografia simetrică. Totodată, ambele capete ale unei conexiuni IPsec, protejată de ESP, trebuie să folosească aceeaşi cheie pentru criptare şi decriptare a pachetelor. Algoritmii de criptare propuşi de ESP sunt: AES, DES şi 3DES.

*Câmpurile pachetelor ESP*

 ESP adaugă un antet şi un subsol porţiunii de informaţie a fiecărui pachet. Fiecare antet ESP conţine două câmpuri:

* **SPI** - fiecare capăt a fiecărei conexiuni IPsec are o valoare SPI arbitrar aleasă, care se comportă ca un identificator unic. Destinatarul foloseşte această valoare, adresa IP destinaţie şi (opţional) tipul protocolului IPSec (în cazul de faţă, ESP), pentru a determina ce SA este folosită.
* **Numărul de secvenţă** - fiecărui pachet îi este asignat un număr secvenţial şi doar pachete dintr-o anumită fereastră sunt acceptate.

 Următoarea parte a pachetului este informaţia utilă, formată din **Date** (criptate) şi **Verctorul de Iniţializare** (IV), care este necriptat. Valoadea acestui vector este diferit în fiecare pachet, deci dacă două pachete au acelaşi conţinut, IV va cauza criptarea diferită a acestora.

 A treia parte a unui pachet este informaţia suplimentară de la sfârşit, care conţine cel puţin două câmpuri (opţional mai poate conţine încă unul.

#### Protocolul IKE

 Scopul protocolului IKE este să negocieze, creeze şi să administreze Asocierile de Securitate (SA). SA este un termen generic pentru un set de valori care definesc caracteristicile IPSec şi protecţiile aplicate unei conexiuni; pot fi create şi manual, folosind valori decise în avans de cele două părţi, dar nu pot fi reînnoite.

O asociere de securitate, mai comun referită ca SA, este un bloc de bază pentru IPSec. Aceasta reprezintă o intrare în baza de date SA (SABD), care conţine informaţii despre securitatea negociată între două părţi pentru IKE sau IPSec. Sunt două tipuri de SA:

1. IKE sau ISAKMP SA -sunt folosite pentru traficul de control, cum ar fi negocierea algoritmilor pentru criptarea traficului IKE şi autentificarea utilizatorilor. Este o singură IKE SA între participanţi şi de obicei are mai puţin trafic şi o durată de viaţă mai mare decât IPSec SA.

2. IPSec SA - sunt folosite pentru a negocia algoritmii de criptare pentru traficul IP, bazându-se pe definirea regulilor de stabilire a traficului ce va fi protejat. Pentru că sunt unidirecţionale, cel puţin două sunt necesare (traficul de intrare şi de ielire)

IKE are probleme cu dispotitivele NAT, care modifică transparent pachetele de ieşire. Prima problemă este că unele echipamente ar putea depinde de negocierea IKE făcută de pachetele de intrare trimise de pe portul 500 UDP. Dacă se introduce un proces NAT, portul pachetului final nu va fi, cu siguranţă, cel aşteptat deci negocierea nu va începe. Alt eveniment neplăcut apare când IKE include adresele IP ca parte a procesului de autentificare, care depinde de modul IKE folosit. Dacă autentificarea se bazează pe adresa IP, schimbările făcute de NAT vor cauza eşuarea procesului IKE.

Ambele tipuri de SA sunt stabilite între participanţii IPSec folosind protocolul IKE (aceasta este principala sa funcţie). IKE operează în două faze pentru a stabili acest asociaţii de securitate:

**Schimbul în faza 1**

Prima etapă asigură autentificarea reciprocă a celor două capete IKE şi stabilirea cheii pentru sesiunea respectivă. Această fază creează o ISAKMP SA (asociere de securitate pentru IKE) care odată ce a fost stabilită, toate comunicaţiile IKE dintre iniţiator şi cel care răspunde sunt protejate cu criptare şi cu o verificare a integrităţii prin autentificare. Trebuie menţionat că există o diferenţă între ISAKMP şi IKE: ISAKMP defineşte cum capetele IPSec comunică, cum realizează schimbul de mesaje şi starea tranziţiilor prin care trec pentru a stabili conexiunea (mai exact arată scopul autentificării şi schimbului de informaţii pentru interschimbul de cheie) iar IKE defineşte cum se realizează schimbul de cheie.

Etapa unu (cunoscută şi ca IKE SA) reprezintă momentul în care cele două capete IPSec negociază cu succes un canal sigur prin care pot fi stabilite şi transmise apoi SA-urile IPSec. Astfel, se garantează criptarea bidirecţională şi autentificarea pentru alte schimburi IKE. Această fază poate fi realizată în două moduri: principal şi agresiv.

*Modul principal* negociază stabilirea unei IKE SA prin trei perechi de mesaje.

În prima pereche de mesaje, fiecare capăt propune parametrii folosiţi de SA. Patru dintre aceştia sunt obligatorii şi alcătuiesc aşa numita sutiă de protecţie:

* **Algoritmul de criptare** - specifică algoritmul care criptează datele: DES, 3DES, AES.
* **Algoritmul de protecţie a integrităţii** -indică ce algoritmi de tip hash de pot folosi: HMAC-MD5 sau HMAC-SHA-1
* **Metoda de autentificare** - sunt 3 posibilităţi de autentificare a utilizatorilor (chei prestabilite, semnături digitale, criptare cu cheie publică)
* **DH Group** - este folosit pentru generarea unui secret comun într-o manieră sigură, astfel încât un observator a etapei 1 IKE să nu îl poată determina.

 A doua pereche de mesaje execută un schimb de cheie prin DH, folosind parametrii negociaţi la primul pas. Conţinutul acestei perechi de mesaje variază în funcţie de metoda de autentificare.

În cea de-a treia pereche de mesaje, fiecare capăt este autentificat (şi aici contează metoda de autentificare folosită). În cazul cheilor prestabilite, rezumatele de autentificare se schimbă acum iar în cazul celorlalte două posibilităţi acesta sunt folosite (au fost schimbate în timpul perechii de mesaje anterioare).

*Modul agresiv*

Acesta oferă o metodă mai rapidă a modului principal. Se negociază stabilirea IKE SA prin trei mesaje în locul celor trei perechi din modul principal. Primele două mesaje negociază parametrii IKE SA şi realizează un schimb de cheie; al doilea şi al treilea mesaj autentifică utilizatorii.

În primul mesaj, prima staţie trimite toţi parametrii suitei de protecţie dar şi porţiunea sa de schimb de cheie DH, un număr folosit o singură dată (nonce) şi identitatea sa. În al doilea mesaj, cealaltă staţie trimite parametrii suitei sale de protecţie, proţiunea sa de DH, numărul folosit o singură dată (nonce), identitatea sa şi informaţia utilă de autentificare.

Al treilea mesaj este utilizat pentru ca prima staţie să trimită propria sa informaţie de autentificare.

**Schimbul în etapa a doua**

A doua etapă furnizează negocierea şi stabilirea asociaţiilor de securitate IPSec (IPSec SA) folosing ESP sau AH pentru protejarea traficului IP.

Scopul celei de-a doua etape este stabilirea asocierilor de securitate pentru o conexiune IPsec actuală (IPSec SA). O conexiune IPSec între două sisteme necesită două IPSec SA, pentru că acestea sunt unidirecţionale. Aceste perechi sunt create prin intermediul unui singur mod, modul rapid, care foloseşte trei mesaje pentru a stabili SA. Comunicaţiile din acest mod sunt criptate prin metoda spacificată în IKE SA-ul stabilit în faza 1.

În primul mesaj, prima staţie trimite cheile, numerele unice şi sugestiile de parametri IPSec SA. Numerele unice sunt o măsură împotriva atacurilor de replicare.

În al doilea mesaj, cealaltă staţie trimite cheile, numerele şi selecţiile parametrilor IPSec SA şi în plus procedurile hash de autentificare.

Al treilea mesaj este utilizat doar pentru ca prima staţie să trimită procedura hash pentru autentificare. După ce a doua staţie validează al treilea mesaj, se poate spune că s-a stabilit o asocieere de securitate IPSec, cele active fiind reţinute într-o bază de date (SADB).

Atât IKE SA cât şi IPSec SA, au o limită de viaţă, care nu poate fi mărită după ce SA a fost creată. Dacă o SA este aproape de sfârşitul duratei de viaţă, capetele ar trebui să creeze una nouă, printr-un proces de restabilire a cheii. Durata de viaţă a unei SA spune cât de des ar trebui fiecare SA să fie restabilită, bazându-se fie pe un anumit timp scurs fie pe cantitatea de trafic din reţea.

Similar cu modelu TCP/IP, IPSec are un număr mare de componente implicate şi caracterizează un set complet de interacţiuni de-a lungul acestora. Structura protocolului asigură avantajul modularizării: când are loc o schimbare a unei componente, celelalte nu se schimbă implicit. Dezavantajul modularizării este că greu de explicat fără scheme, pur şi simplu pentru că multe componente trebuie să lucreze împreună pentru ca protocolul să opereze.

### Cum funcţionează IPSec

Arhitectura IPSec presupune:

1. **nucleul** (IPSec driver or core engine) - această componentă realizează criptarea, decriptarea, autentificarea şi verificarea semnăturii; de asemenea este responsabil pentru coordonarea efortului altor componente IPSec pentru a asigura că poate îndeplini sarcinile.
2. **agentul de politică** (IPSec Policy Agent) - este funcşia cognitivă a protocolului şi examinează setările IPSec ale sistemului specificând ce trafic ar trebui protejat; nu protejeajă datele ci doar avertizeată ca un anumit trafic ar trebui protejat.
3. **ISAKMP** (Internet Security Association and Key Management Protocol) - este negociatorul setărilor de securitate ale Internetului; atunci când două staţii vor să comunice, ISAKMP negociază grupul desetări folosite pentru criptare şi autentificare.
4. **IKE** (Internet Key Exchange) - pentru că IPSecul foloseşte chei secrete împărţite, trebuie să fie un mecanism care să conecteze echipamentele şi să se pună de acord asupra unei chei; acesta depinde de setările furnizate de ISAKMP.

**Interacţiunea componentelor**



***Figura 4-15.*** *Interacţiunea* ***IPSec***

Politica locală sau de grup este aplicată unui dispozitiv în timpul pornirii şi periodic în timp ce activează în reţea. Orice politică IPSec este preluată de angentul de politică IPSec. Atunci când există mai multe reguli stabilite, agentul monitorizează comuniaţia cu protocolul TCP/IP din toate aplicaţiile, caută traficul care se potriveşte acestora, adică acela care trebuie protejat. Când traficul de reţea care necesită protecţie este identificat, agentul de politică îi va comunica dispozitivului IPSec tipul de protecţie de care este nevoie. Apoi, echipamentul IPSec determină dacă există o Asociere de Securitate care poate fi folosită pentru a proteja traficul. Dacă nicio SA nu există, funcţia IKE va fi contactată; aceasta va folosi ISAKMP pentru a negocia autentificarea reciprocă şi pentru a stabilit cheia. Apoi, IKE va furniza o SA activă către IPSec driver, care va proteja traficul. Astfel, traficul protejat va fi returnat către protocolul TCP/IP pentru procesare.

###

### Tunele GRE cu protecţie IPSec

GRE este un protocol de tunelare dezvoltat de Cisco care poate încapsula o mare varietate de tipuri de pachete ale protocoalelor de reţea în interiorul tunelelor IP, creând o legătură virtuală punct la punct, între routere aflate la distanţă, peste o reţea IP.

Tunelele GRE sunt create să fie complete, fără o stare persistentă. Acest lucru înseamnă că fiecare capăt de tunel nu păstrează nicio informaţie despre starea şi disponibilitatea capătului de tunel de la distanţă. O consecinţă a acestui fapt este că router-ul din capătul de tunel nu are abilitatea de a marca protocolul liniei interfeţei tunelului GRE ca fiind inaccesibil dacă router-ul de la distanţă, din celălalt capăt, nu este funcţional. Posibilitatea de a exprima că interfaţa este nefuncţională către celălalt capăt este eficientă pentru retragerea rutelor care o folosesc ca şi interfaţă de ieşire, din tabela de rutare (în special rutele statice).

În mod normal, o interfaţă de tunel GRE este funcţională din momentul în care este configurată şi rămâne aşa cât timp este o adresă sursă a tunelului validă. Adresa IP destinaţie a tunelului trebuie să fie mereu rutabilă. Acest lucru este adevărat chiar dacă celălalt capăt al tunelului nu a fost configurat. Astfel, o rută statică a pachetelor via interfaţa tunelului GRE rămâne în vigoare chiar dacă pachetele tunelului GRE nu găsesc celălalt capăt de tunel.

Construirea unei reţele virtuale private folosind IPSec pentru conectivitatea dintre capete are câteva limitări:

-IPSec poate cripta/decripta doar traficul IP

-traficul IP destinat unei adrese de difuzare nu poate fi procesat de IPSec, ceea ce înseamnă că nu poate traversa tunelul.

-de asemenea, rutarea dinamică folosind procoale ca EIGRP, OSPF, RIPv2 nu pot fi configurate între două capete IPSec

Aceste probleme pot fi rezolvate prin configurarea unui tunel GRE între cele două noduri şi aplicarea ulterioară a protecţiei IPSec pe acest tunel. Este în esenţă că GRE ăncadrează orice informaţie utilă dintr-un pachet unicast destinat unui capăt GRE.

Când se utilizează GRE îmbinat cu IPSec se poate folosi atât modul tunel cât şi cel transport (modul tunel va adăuga un antet IP pachetelor GRE, în timp ce modul transport va folosi antetul original GRE).

Teoretic, modul transport ar fi recomandat atunci când se utilizează colaborarea dintre IPSec şi GRE pentru că deja protocolul de încapsulare GRE adaugă un antet IP nou pachetului util. Totuşi, această situaţie presupune existenţa unor adrese IP sursă şi destinaţie care sunt accesibile prin calea IP dintre noduri.

Utilizarea protocoluli GRE împreună cu IPSec face configurarea echipamentelor VPN mai simplă. În situaţia tradiţională IPSec era nevoie de o politică anume care să specifice subreţelele protejate pentru ca traficul dintre acestea să fie criptat/decriptat şi de fiecare dată când o subreţea era adăugată trebuia să fie reînnoită structura la ambele capete. În cazul utilizării GRE, regulile trebuie să corespundă doar traficului dintre adresele de capăt GRE (tot ce trece prin tunelul GRE este criptat).

Principala motivaţie a folosirii GRE cu IPSec este posibilitatea de a rula protocoale dinamice între locaţii pentru a anunţa subreţelele protejate. Rutarea dinamică ajută implicit şi în situaţii de eşuare a transferului, astfel pot fi detectate interfeţele care nu mai funcţionează şi nu mai participă în VPN.

# Bibliografie

***Cisco Network Security*** – Joe Harris; **Cisco Press**, 2002

***Comunicaţii de date*** – Ioan Bănica; editura Politehnica Press, 2008

***Cryptography and Network Security*** - William Stallings; editura **Prentice Hall**, 16

noiembrie 2005

***Guide to IPSec VPN*** - Sheila Frankel, Karen Kent, Ryan Lewkowski, Angela D.

Orebaugh, Ronald W. Ritchey, Steven R. Sharma; editura **NIST**, Decembrie 2005

***IPSec VPN Design* -** Vijay Bollapragada, Mohamed Khalid, Scott Wainner; editura

**Cisco** **Press**, 07 aprilie 2005

***Reţele de calculatoare*** – Andrew S. Tanenbaum, ediţia a patra

<http://www.wikipedia.org/>

<http://techrepublic.com.com>

<http://www.blindhog.net/>

<http://etutorials.org/>

<http://www.cisco.com>