**Universitatea Politehnică Bucureşti**

**Facultatea de Electronică Telecomunicaţii şi Tehnologia Informaţiei**

**Specializarea Calculatoare şi Tehnologia Informaţiei**

**Tema RC**

**Retele virtuale private(VPN)**

**Nechifor Cosmin Adrian**

**Grupa 443A**

**Cuprins**

**Capitolul 1. Introducere..................................................................................................3**

**Capitolul 2. Transmisia datelor folosind VPN .............................................................4**

 **2.1. Principiul tunelarii.........................................................................................4**

 **2.2. Protocolul PPP...................................................................................6**

**Capitolul 3. Principii de functionare ale Hamachi.......................................................9**

**Capitolul 4. Concluzii...................................................................................................10**

**Capitolul 1. Introducere**

Retelele virtuale (VPN) reprezinta o extensie a unei retele private creata in cadrul unei retele publice, cum ar fi Internetul. Caracteristicile cele mai importante ale VPN sunt urmatoarele :

- se pot crea retele izolate in cadrul unei retele private(cum ar fi reteaua unei companii)

- posibilitatea de a transmite datele intre 2 sau mai multe calculatoare din domeniull VPN de-a lungul unui domeniu public

- securitatea datelor este asigurata de obicei de chei de criptare, facand aproape imposibila intelegerea datelor in cazul in care au fost interceptate



**Poza 1 : Arhitectura generala a unei retele virtuale**

 **Capitolul 2. Transmisia datelor folosind VPN**

**Capitolul 2.1. Principiul tunelarii**

O retea privata trimite datele prin legaturi punct la punct. Aceste legaturi se creaza adaugand informatii de rutare aditionale pachetelor de date. Legaturille sunt formate este compusa din 2 domenii :

- domeniul public, in care datele sunt incapsulate; poarta denumirea de tunel

- domeniul privat, in care datele sunt criptate poarta denumirea de VPN

Tunelerea reprezinta o metoda de a transfera datele dintr-o retea in alta retea in cadrul Internetului. Acestea sunt incapsulate de protocolul de tunelare folosind un antet suplimentar cu informatii de rutare.

 Pachetele sunt astfel rutate de-a lungul unei rute intre cele 2 capete ale tunelului. In momentul sosirii, pachetul este decapsulat si este transmis mai departe la destinatia finala.

Exista mai multe tehnologii de transmisie prin tunele, cum ar fi :

 **- SNA tunneling over IP internetworks**

 **- IPX tunneling for Novell NetWare over IP internetworks**

 **- Point-to-Point Tunneling Protocol (PPTP**

 **- Layer Two Tunneling Protocol (L2TP)**

 **- IPSec tunnel mode**

Pentru ca tunelarea sa functioneze corect, ambele capete ale tunelului trebuie sa foloseasca acelasi protocol de tunelare. Acestea pot fi de mai multe tipuri :

 **a) protocoale bazate pe nivelul 2 OSI**

- se formeaza o conectiune intre cele 2 capete ale tunelului ; pe baza protocolului se decid parametrii de compresie, criptare, etc

 - datele se transmit de-a lungul tunelului folosind un protocol bazat pe diagrame

 - se foloseste un protocol de mentinere a tunelului pentru a a asigura transferul/configurarea

 - exemple: PPTP si L2TP

 **b) protocoale bazate pe nivelul 3 OSI**

 **-** spre deosebire de protocoalele bazate pe nivelul 2, acestea nu au nevoie de crearea unei legaturi initiale pentru a negocia setarile ; acestea sunt preconfigurate, de obicei de catre utilizator

 - este necesara cunoasterea doar a adresei IP a celor 2 capete pentru a putea transmite datele

 - prezinta un nivel de securitate crescut

 - exemplu: IPSec

Protocoalele de tunelare de nivelul 2 sunt bazate pe protocolul punct la punct (PPP) si prezinta urmatoarele caracteristici :

 **a) Autentificarea utilizatorului**

 - pentru a se crea legatura, protocoalele necesita ca ambele capete sa prezinte informatii de autentificare

 - se bazeaza pe schemele de autentificare apartinand protocolului PPP, cum ar fi EAP(Extensible Authentication Protocol) sau IKE (Internet Key Exchange ).

 - autentificarea se poate face prin parole, chei de criptarea sau smart cards

 **b) Alocarea dinamica a adreselor**

- adresa fiecarui capat este alocata folosind un mecanism de negociere al NCP(Network Control Protocol)

 - in cazul protocoalelor de tunelare de nivel 2 se considera ca adresele au fost alocate inainte de crearea legaturii.

**c) Compresia datelor**

- compresia se face bazandu-se pe mecanismele de compresie specifice protocului PPP, cum ar fi MPPC(Microsoft Point-To-Point Compression)

**d) Criptarea datelor**

- protocoalele de tunelare de nivel 2 pot folosi mecanismele de criptare ale protocolului PPP sau pot fi folosite altele, cum ar fi MPPE (Microsoft Point-to-Point Encryption).

**e) Support pentru diferite protocoale**

- in cazul protocoalelor de tunelare de nivel 2, se pot folosi forma legaturi intre retele folosind conectiuni diferite, cum ar fi IP,IPX, NetBEUI, etc

- in contrast, protocoalele de nivel 3 pot forma legaturi doar intre retele ce folosesc protocolul IP.

**Capitolul 2.2. Protocolul PPP**

 Protocolul PPP(Point-to-point) a fost creat pentru a transmite date de-a lungul unor conectiuni punct la punct dedicate. In general, PPP incapsuleaza pachete IP, IPX sau NETBEUI folosind cadre PPP si le transmite de-a lungul unei legaturi punct la punct.



**Poza 2 : Structura unui cadru PPP**

Un cadru PPP este format din urmatoarele campuri :

 **1) Flag**

- un octet folosit pentru a indica inceputul sau sfarsitul unui cadru. Are valoarea binara 01111110.

 **2) Adress**

 - un octet ce continea adresa standard de broadcast. Are valoarea binara 11111111

 **3) Control**

- un octet ce specifica transmisia datelor printr-u mod ‘fara conectiune’. Are valoarea binara 00000011.

 **4) Protocol**

 - doi octeti ce identifica protocolul incapsulat in campul de informatii al cadrului

 **5) Data**

 -numar variabil de biti ce contin datagrama pentru protocolul folosit. Dimensiunea maxima este de 1500 de octeti.

 **6) FCS**

 - 2 octeti folositi pentru identificarea si corectarea erorilor

 Fiind un protocol de nivel 2, PPP este nevoit sa negocieze parametrii conectiunii inainte de transmisia datelor. De aceea exista 3 faze distincte de negociere :

**1) Crearea unei legaturi PPP**

 - PPP foloseste LCP(Likn Control Protocol) pentru a forma, a mentine si a sfarsi conectiunea fizica. In cadrul fazei 1 acesta este folosit pentru a alege optiuni de comunicare, compresie, criptare precum si protocoalele de autentificare. Implementarea efectiva a acestora se face in fazele ulterioare.

**2) Autentificare**

- In aceasta faza capatul apelat prezinta date de autentificare capatului transmitator. Se folosesc diferite protocoale, de exemplu :

**a) Password Authentification Protocol (PAP)**

- transmitatorul cere un nume de utilizator si o parola iar receptorul transmite inapoi informatia fara nicio criptare.

- este extrem de rar folosit deoarece nu prezinta nicio protectie impotriva interceptarii datelor

**b) Challenge-Handshake Authentication Protocol (CHAP)**

- transmitatorul trasmite un identificator al sesiunii precum si un sir de caractere receptorului

- receptorul se foloseste de algoritmul MD5 pentru a return numele de utilizator precum si o criptare a sirului,indentificatorului si a parolei.

Daca transmitatorul a primit cu succes datele de atuentificare, verifica intai daca acestea sunt valide. In cazul in care validarea a reusit, se trece la faza urmatoare.

**3) Implementarea optiunilor folosind protocoalele alese**

- in aceasta faza sunt apelate protocoalele pentru alegerea adresei, criptare, compresie, etc.

Dupa ce succesiunea de 3 faze a fost terminata se incepe transmisia efectiva a datelor. Fiecare pachet de date este criptat, compresat si incapsulat intr-un cadru PPP si este transmis de-a lungul legaturii.

**Capitolul 3. Principii de functionare ale Hamachi**

Hamachi reprezinta un program folosit pentru crearea unei retele virtuale private. Acesta implementeaza un protocol de tunelare de nivel 3 pentru transmisia de date si prezinta avantajul de a crea legaturi intre dispozitive ce se afla in spatele unui firewall.

Arhitectura retelei este de tip punct la punct. Fiecare nod Hamachi schimba informatii intre ele dupa terminarea autentificarii/selectarea optiunilor. Exista un server central folosit pentru a crea legaturile initiale intre noduri.

Fiecare nod primeste o adresa IP in momentul cand se conecteaza la serverul central. In mod curent se alege o adresa din subreteaua 25.0.0.0/8. De asemenea, adresei IP alocate ii corespunde o cheie criptare publica unica pentru autentificare.

Legaturile intre noduri pot conduce la formarea unor retele de tip mesh, hub sau inel, prima fiind cea mai comuna.

Fiecare nod este autentificat de catre serverul central folosind un set de chei RSA. Acest sistem de securitate consta intr-o cheie de criptare care este publica si o cheie de decriptare care este ascunsa. Astfel, nodurile cripteaza datele de autentificare si le transmit serverului pentru a fi validate.

Dupa ce perioada de autentificare s-a terminat, nodurile pot incepe sa trimita date intre ele direct, fara interventia serverului central.

Criptarea datelor se face folosind codul AES de 256 de octeti.



**Poza 3: Exemplu de retea Hamachi de tip hub**

**Capitolul 4. Concluzii**

In concluzie, se poate afirma ca retelele virtuale au aparut in urma necesitatii de critpare a datelor precum si pentru a rezolva probleme legate de conectarea unor calculatoare ce se afla in spatele unor routere/firewaluri.

**Capitolul 7. Bibliografie**

**Bibliografie** :

[**https://technet.microsoft.com/en-us/library/bb742566.aspx**](https://technet.microsoft.com/en-us/library/bb742566.aspx)

[**http://en.wikipedia.org/wiki/Virtual\_private\_network**](http://en.wikipedia.org/wiki/Virtual_private_network)

[**http://www.quora.com/Difference-between-layer-2-vpn-and-layer-3-vpn**](http://www.quora.com/Difference-between-layer-2-vpn-and-layer-3-vpn)

[**http://searchnetworking.techtarget.com/definition/PPP**](http://searchnetworking.techtarget.com/definition/PPP)

[**http://www.cisco.com/c/en/us/tech/wan/point-to-point-protocol-ppp/index.html**](http://www.cisco.com/c/en/us/tech/wan/point-to-point-protocol-ppp/index.html)

**http://docwiki.cisco.com/wiki/Point-to-Point\_Protocol**

[**http://en.wikipedia.org/wiki/Point-to-Point\_Protocol**](http://en.wikipedia.org/wiki/Point-to-Point_Protocol)

[**http://en.wikipedia.org/wiki/LogMeIn\_Hamachi**](http://en.wikipedia.org/wiki/LogMeIn_Hamachi)

[**https://secure.logmein.com/products/hamachi/security.aspx**](https://secure.logmein.com/products/hamachi/security.aspx)

[**http://en.wikipedia.org/wiki/RSA\_%28cryptosystem%29**](http://en.wikipedia.org/wiki/RSA_%28cryptosystem%29)

[**https://secure.logmein.com/welcome/documentation/EN/pdf/Hamachi/LogMeIn\_Hamachi\_GettingStarted.pdf**](https://secure.logmein.com/welcome/documentation/EN/pdf/Hamachi/LogMeIn_Hamachi_GettingStarted.pdf)

**http://en.wikipedia.org/wiki/Advanced\_Encryption\_Standard**

**Poze**

 **1 - http://upload.wikimedia.org/wikipedia/commons/thumb/0/00/Virtual\_Private\_Network\_overview.svg/2000px-Virtual\_Private\_Network\_overview.svg.png**

**2 -** [**http://docwiki.cisco.com/w/images/e/ed/CT841301.jpg**](http://docwiki.cisco.com/w/images/e/ed/CT841301.jpg)

**3 - http://wmpoweruser.com/wp-content/uploads/2010/02/hamachi\_thumb.jpg**