Universitatea „Politehnica” din București

 Facultatea de Electronică, Telecomunicații și Tehnologia Informației

***Rețele de Calculatoare și Internet***

***Rețea privată virtuală de tip Layer Socket Securizat/Layer Transport Securizat (SSL/TLS)***

 *Stundent:* ***Mihai-Gabriel PETRESCU***

 *Grupa:* ***2-IISC***

***2017***

**Cuprins**

[Capitolul 1. Introducere 4](#_Toc474161968)

[1.1 Pro si contra VPN 5](#_Toc474161969)

[1.2 Tehnologiile din spatele VPN-ului 6](#_Toc474161970)

[1.3 SSL VPN 6](#_Toc474161971)

[Capitolul 2. Arhitectura 8](#_Toc474161972)

[Capitolul 3. Cetificatele SSL 10](#_Toc474161973)

[3.1 Descriere la nivel înalt al protocolului 10](#_Toc474161974)

[3.2 Cifruri folosite la SSL 13](#_Toc474161975)

[Capitolul 4. Protocoalele ce stau la baza TLS 16](#_Toc474161976)

[Capitolul 5. Proiectul OpenVPN ce are la baza SSL/TLS 18](#_Toc474161977)

[Capitolul 6. Concluzii 19](#_Toc474161978)

[Bibliografie 20](#_Toc474161979)

# Capitolul 1. Introducere

 Rețea privată virtuală (VPN) pune la dispozitie utilizatorilor posibilitatea de a trimite si a primi informatii intr-o retea publica ca si cum calculatoarele lor sunt direct conectate la o retea privata. Aplicatiile ce ruleaza cu VPN pot beneficia de securitate si administrarea de retea privata.

 Carcateristica principala este abilitatea de a folosi retelele publice in loc sa se bazeze pe liniile private. Are la baza o metoda numita **tunneling** [1]**.** Tehnologiile VPN implementeaza retele cu acces restrictionat ce utilizeaza acelasi cablu si router ca o retea oublica si fac acest lucru fara a renunta la proprietati sau la securitatea de baza.



Un VPN suporta cel putin 3 moduri de folosire:

* Conexiunea ce acceseaza clientul de la distanta
* LAN - catre - LAN
* Acces controlat intr-un intranet

VPN-uri pentru acces de la distanta au solutia client/server urmatoare [1]:

1. Un host la distanta ce asteapta sa se contecteze in reateaua companiei prima data se contecteaza la orice public ISP (Internet Service Provider)
2. In continuare, gazda initalizeaza o conexiune catre serverul VPN al companiei. Aceasta conexiune este facuta print-o aplicatie client VPN instalata.
3. O data ce conexiunea a fost reusita, cientul comunica cu sistemul intern al companiei prin intermediul internetului ca si cum a fi o retea locala.

 Un VPN ne permite sa facem lucruri pe care nu le-am putea face conectati la o retea de internet standard. Acestea includ:

* Retea privata si securizata
* Se poate accesa de la distanta calculatorul de lucru
* Se poate accesa reteaua de acasa
* Se poate accesa o locatie cu continut restrictionat
* Pot fi depasine anumite restrictii la retele
* Se poate trece peste cenzura

De ce ar trebui sa folosim VPN:

 Chiar daca nu exista dorinta de avea acces la o retea privata de la distanta, un VPN este vital sa asigure securitatea traficului de internet.

 Folosind un VPN, user-ul este protejat de astfel de atacuri deoarece trafic-ul este autentificat si criptat ceea ce il face securizat si privat.

Cum merge un VPN:

 Un VPN tipic este format din doua componente: client-ul si server-ul.

 Un client VPN este software-ul care permite unui utilizator să isi conecteze computerul la

serverul VPN și stabileste conexiunea VPN. Acesta este instalat pe calculatorul utilizatorului și comunică cu serverul VPN pentru a crea o legătură sigură pentru traficul de rețea al utilizatorului. Clientul VPN-ul este ceea ce folosește utilizatorul final pentru a controla conexiunea lor VPN.

 Un server VPN este setată la locația unde utilizatorii doresc să se conectezeß, cum ar fi la un loc de muncă sau la domiciliu. Un VPN Server este de obicei configurat și întreținute de către personalul IT, cu toate acestea utilizatorii de acasă pot setat adesea propriul lor ßVPN personal la domiciliu sau de la o locație la distanță. Utilizatorii finali au rareori trebuie sa interacționeze cu serverul VPN. Un server VPN, va efectua, de asemenea, autentificarea pentru a se asigura ca, doar utilizatorii înregistrați se pot conecta la VPN.

## 1.1 Pro si contra VPN

 La fel ca multe tehnologii de rețea comercializate, o cantitate semnificativă de vânzări și marketing înconjoară VPN.

 In realitate, VPN-urile oferă doar câteva avantaje față de formele mai tradiționale de zonă largă de rețele. Aceste avantaje pot fi semnificative, dar ele nu vin gratis.

 Potențiale probleme cu rețeaua VPN sunt mai numeroase decât avantajele și sunt în general mai dificil de înțeles. Dezavantajele nu depășesc în mod necesar avantajele, cu toate acestea.

 Problemele legate de securitate și de performanță se referă o gamă largă de produse de furnizor, uneori incompatibile, decizia de a utiliza o rețea VPN nu poate fi făcută fără o planificare și pregătire semnificativă [2].

## 1.2 Tehnologiile din spatele VPN-ului

Mai multe tipuri de protocoale de rețea au devenit populare ca urmare a evoluției VPN:

* PPTP
* L2TP
* IPsec
* SOCKS

 Aceste protocoale empatizeaza autentificarea și criptarea în VPN-uri. Autentificarea permite clienților VPN și serverelor sa stabileasca în mod corect identitatea persoanelor în rețea. Criptarea permite datelor potențial sensibile să fie ascunse publicului larg [2].

 Mulți furnizori si-au dezvoltat hardware-ul VPN și(sau) produse software. Din păcate, standardele VPN imature înseamnă că unele dintre aceste produse rămân incompatibile între ele.

## 1.3 SSL VPN

 Pe măsură ce organizațiile au crescut și devin mai complexe, acces-ul de la distanță securizat la resursele de rețea a devenit critic pentru operațiunile de zi cu zi. In plus, este de așteptat ca majoritatea companiilor să ofere clienților servicii eficiente, convenabile, inclusiv baze de cunoștințe și portaluri ale clienților [3]. Angajații care călătoresc în întreaga țară sau in întreaga lume au nevoie de acces în timp util și cuprinzător la resursele rețelei. Ca urmare a nevoii tot mai mari pentru furnizarea de clienți la distanță, cost-eficiente și accesul sigur la o multitudine de resurse, a fost dezvoltat conceptul de Virtual Private Network (VPN).

 SSL VPN stabileste o conexiune utilizând SSL, care funcționează la niveluri 4 - 5 (straturi de transport și de sesiune). Informatiile sunt încapsulate la niveluri 6 - 7 (straturi de prezentare si aplicatii), si SSL VPN comunica la cele mai înalte niveluri ale modelului OSI. SSL nu este strict o tehnologie de Virtual Private Network (VPN), care permite clienților să se conecteze la rețele la distanță într-un mod securizat [3]. Un VPN este o rețea logică securizată creată de rețele separate fizic. VPN-urile folosesc criptarea și alte metode de securitate pentru a se asigura că doar utilizatorii autorizați pot avea acces la rețea. De asemenea, să se asigure că rețelele VPN datele transmise între calculatoare nu pot fi interceptate de către utilizatori neautorizați. Atunci când datele sunt codificate și transmise prin internet, datele se spune că este trimis printr-un "tunel VPN". Un tunel VPN este un tunel orientat non-aplicație care permite utilizatorilor și a rețelelor de a face schimb de o gamă largă de trafic, indiferent de aplicație sau protocol.

 Avantajele unui VPN printr-o rețea privată fizică reală sunt de două ori mai mari. Mai degrabă decât folosind linii scumpe închiriate sau alte infrastructuri, se poate utiliza banda Internet relativ ieftin, de mare lățime [3]. Poate și mai importantă, deși este disponibilitatea universală a internetului. În cele mai multe zone, accesul la Internet este ușor de obținut, fără nici un regim special sau de ori mai mult timp asteptati.

 SSL (Secure Sockets Layer) ca HTTPS este suportat de majoritatea browser-elor web pentru schimbul de informații sensibile între un server de web și un client. SSL stabileste un link criptat, asigurându-se că toate datele transmise între serverul web și browser-ul rămâne privat și sigure. Protecție SSL este inițiată automat atunci când un utilizator (client) se conectează la un server de web, care are activat SSL. Odată ce conexiunea de succes este stabilit, browser-ul criptează toate informațiile înainte de a părăsi calculatorul. Atunci când informația ajunge la destinație, acesta este decriptat folosind o cheie secretă (privată). Datele trimise înapoi este mai întâi criptat, și este decriptat atunci când ajunge la client.

#  Capitolul 2. Arhitectura

 Pentru cei ce doresc să stabilească o conexiune VPN, sunt disponibile mai multe metode (bazate pe nivelele 2 și 3 din Modelul  OSI), împreună cu tehnologiile respective. Rețeaua VPN poate fi stabilită și administrată la sediul clientului, sau și de către furnizorul de servicii de telecomunicații. De asemenea, pentru a satisface cerințe speciale, există și posibilitatea de a combina mai multe din aceste metode între ele.



Fig1. Arhitectura unei reţel VPN [4]

 Transport Layer Security (SSL / TLS) poate crea un tunelul de trafic pentru o întreagă rețea (așa cum o face în proiectul OpenVPN și proiectul SoftEther VPN [8]) sau asigurara o legătura individuala [4]. Un număr de vânzători furnizează capabilități VPN la distanță de acces prin SSL. Un SSL VPN se poate conecta la locații unde Ipsec se execută în probleme cu regulile Network Address Translation și firewall.

 Arhitectura MPLS / VPN oferă posibilitatea de a comanda o infrastructură de rețea IP care furnizează servicii de rețele private pe o infrastructură comună. Tehnologia MPLS / VPN este destul de complexa în sine.

 Suprapunerea adreselor, de obicei, care rezultă din utilizarea de adrese IP private în rețelele de client, reprezintă una dintre cele mai mari obstacole în calea desfășurării cu succes a peer-to-peer implementari VPN. Tehnologia MPLS / VPN oferă o soluție elegantă la dilema: Fiecare VPN are propria sa de rutare și tabelul de redirecționare în router, astfel încât orice client sau site care aparține acelui VPN este asigurat accesul numai la setul de rute conținute în acel tabel [5]. Orice router PE într-o rețea MPLS / VPN conține, prin urmare, un număr de per-VPN tabele de rutare și o tabelă de rutare globală, care este utilizat pentru a ajunge la alte routere din rețeaua furnizorului, precum și destinații la nivel global accesibile de externe (de exemplu, restul internetul). În mod eficient, un număr de routere virtuale sunt create într-un singur router fizic.

Acces de la distanță VPN

 O conexiune de acces VPN la distanță se face de către un client de acces de la distanță. Un client de acces la distanță este un singur utilizator de computer care se conectează la o rețea privată dintr-o locație la distanță. Serverul VPN oferă acces la resursele rețelei la care este conectat serverul VPN. Pachetele trimise prin conexiunea VPN provin de la clientul VPN.

VPN Site-to-site

 O conexiune VPN fata in fata face legătura între două porțiuni ale unei rețele private sau a două rețele private. De exemplu, acest lucru permite o organizație să fi rutate legături cu birouri separate, sau cu alte organizații, prin Internet. O conexiune VPN rutate prin Internet operează în mod logic, ca un link dedicat Wide Area Network (WAN) [5].



Fig2. VPN Conectarea unui client la distanță la un Intranet Privat [5]

# Capitolul 3. Cetificatele SSL

 SSL (și succesorul său, TLS) este un protocol care opereaza direct pe partea de sus a TCP (deși există și alte implementări pentru protocoale bazate pe datagrame, cum ar fi UDP). In acest fel, protocoalele pe straturile superioare (cum ar fi HTTP) pot fi lăsate neschimbate oferind în același timp o conexiune securizată. Sub stratul SSL, HTTP este identic cu HTTPS.

 Atunci când se utilizează corect SSL / TLS, ce poate vedea pe cablu un atacator este care IP și portul la care sunteți conectat, in mare cantitatea de date care este trimisa, și ce criptare și compresie au fost utilizate [6]. El se poate termina, de asemenea, conexiunea, dar ambele părți vor ști că conexiunea a fost întreruptă de către o parte externa.

 În utilizarea tipică, atacatorul va fi, de asemenea, în măsură să dau seama care numele de gazdă pe care îl conectați la (dar nu și restul URL): cu toate că HTTPS în sine nu expune numele gazdei, browser-ul dvs. va avea nevoie, de obicei, pentru a face un DNS cere mai întâi pentru a afla ce adresa IP pentru a trimite cererea [6].

## 3.1 Descriere la nivel înalt al protocolului

 După construirea unei conexiuni TCP, strângere de mână SSL este pornit de către client. Client (care poate fi un browser precum și orice alt program, cum ar fi Windows Update sau PuTTY) trimite o serie de specificații:

* ce versiune SSL / TLS este în execuție
* ce algoritmi de criptare se doreste utilizat, și
* ce metode de compresie se vrea folosita.

 Serverul verifică ce cea mai mare versiune SSL / TLS este acceptat de ei amândoi, alege un ciphersuite la una dintre opțiunile clientului (dacă acesta acceptă unul), și opțional alege o metodă de comprimare [6].

 După această configurarea de bază, serverul trimite certificatul său. Acest certificat trebuie să fie de încredere fie de clientul în sine sau de o parte in care are încredere client-ul. De exemplu, în cazul în care clientul are încredere GeoTrust, atunci clientul poate avea încredere în certificatul de la Google.com, deoarece GeoTrust a **semnat digital** certificatul de la Google.

 O semnătură digitală este o schemă matematică pentru a demonstra autenticitatea mesajelor digitale sau a documentelor. O semnătură digitală validă dă un motiv pentru destinatar să creadă că mesajul a fost creat de către un cunoscut expeditor (autentificare), că expeditorul nu poate nega faptul că a trimis mesajul (non-repudiere), și că mesajul nu a fost modificat în tranzit (integritate).

O schemă de semnătură digitală de obicei este format din trei algoritmi;

* Un algoritm de generare de chei care selectează o cheie privată la întâmplare, dintr-un set de posibile chei private. Algoritmul scoate cheia privată și o cheie publică corespunzătoare.
* Un algoritm de semnare, folosind un mesaj și o cheie privată, produce o semnătură.
* Un algoritm de verificare a semnăturii, folising mesajul, cheia publică și semnătura, fie acceptă sau respinge pretenția mesajului de autenticitate.

 Semnăturile digitale sunt bazate pe criptografie cu chei publice, de asemenea, cunoscut sub numele de criptografie asimetrică. Cu ajutorul unui algoritm de chei publice, cum ar fi RSA, se poate genera două chei, care sunt legate în mod matematic: una privată și una publică. Pentru a crea o semnătură digitală, semnând software-ul (cum ar fi un program de e-mail) creează un hash într-un fel de date electronice care urmează să fie semnate. Cheia privată este apoi utilizată pentru a cripta hash. Criptat hash - împreună cu alte informații, cum ar fi algoritmul hashing - este semnătura digitală. Motivul pentru criptarea hash în locul întregului mesaj sau a documentului este că o funcție hash poate converti o intrare arbitrar într-o valoare de lungime fixă, care este de obicei mult mai scurt. Acest lucru economisește timp, deoarece hashing este mult mai rapid decât semnarea.

 Exista mai multe modalitati de a genera o cheie publica/privata, mai jos este un exemplu pe pasi de cum se genreaza si cum se decodifica:

Ne gandim la 2 numere prime.

p = 3, q ​​= 11

Se calculează modulul pentru cheia publică / privată.

Numarul care este aceeași în ambele chei, si il numim n. Este folosit ca modulul în criptare su decriotare și decriptare. Ai calcula prin a face:

n = 3 \* 11

Se calculează totient de n.

totient (n) = (p - 1) \* (q - 1)

În cazul nostru vom face:

totient (33) = (3 - 1) \* (11 - 1)

Acest lucru este egal cu 20.

Până în prezent, avem:

p = 3

q = 11

n = 33

totient (n) = 20

Alegeți un număr pentru e

Acest număr este este un pic mai greu decât ceilalți. Ea trebuie să fie între 1 și n, de asemenea, la n prime între ele.

Acest lucru înseamnă practic că cel mai mare divizor comun al ambelor numere este 1. Dacă alegeți un număr prim pentru e tot ce trebuie să faci acum este să verificați că e nu este un divizor de n. Vom alege numărul:

e = 17

Calcularea inversul modular multiplicativ e \* (totient mod (n))

 Exprimate în mod simplu ai putea spune: Care este soluția ecuației:

(E \* x - 1) mod (totient (n)) = 0

Aceasta ar dura destul de mult timp să-l opereze manual, asa ca am scris o funcție mică Javascript, care face acest lucru pentru mine:

Funcția doLoop (e, totient) {

  var i = 1, x;

  în timp ce (true) {

    x = (e \* i - 1)% totient;

    if (x === 0) {

      console.log (i);

      pauză;

    }

  }

}

Functia ia 2 argumente, unul este e celălalt este totient (n). În funcție de procesorul dumneavoastră și dimensiunea numerelor pe care o alegeți poate dura mai mult sau mai scurt pentru a rula.

În cazul nostru funcția va înregistra valoarea 13, pe care o voi suna d. Acum ai toate valorile necesare pentru public criptare și decriptare / privat-cheie.

Rezumând

Toate valorile de până acum:

p = 3

q = 11

n = 33

totient (n) = 20

e = 17

d = 13

- Cheie publica este acum: e = 17, n = 33

- Cheie privată este acum: d = 13, n = 33

Cu această privat și public-cheie, puteți cripta date. Ne vom cripta valoarea:

m = 9

Pentru a cripta cu cheia publică, vă luați m la puterea lui e (în cheie publică) n mod

m ^ e mod n

9 ^ 17 mod 33 = 15

Valoarea noastra este criptat:

c = 15

Acest lucru poate fi decriptat doar cu cheia privată.

Pentru a-l decripta, să luați c la puterea d (în particular-cheie) n mod

c ^ d mod n

15 ^ 13 mod 33 = 9

Acum avem valoarea noastră originală!

## 3.2 Cifruri folosite la SSL

 Protocolul SSL include două sub-protocoale: protocolul de înregistrare SSL și protocolul SSL strângere de mână. Protocolul de înregistrare SSL definește formatul utilizat pentru a transmite date [8]. Protocolul SSL implică strângere de mână, utilizând protocolul SSL de înregistrare pentru a face schimb de o serie de mesaje între un server SSL activat și un client SSL activat atunci când stabilesc mai întâi o conexiune SSL. Acest schimb de mesaje este conceput pentru a facilita următoarele acțiuni:

* Autentifica serverul catre client
* Permitețe clientului și serverului sa aleaga algoritmi de criptare sau cifruri, ce suporta ambele.
* Optional autentifica clientru catre server
* Se foloseste tehnica de cheie publica criptata sa genereze secrete
* Se stabileste o conexiune criptata SSL

 Protocolul SSL acceptă utilizarea unei varietăți de algoritmi de criptare sau cifruri, pentru a fi utilizate în operații cum ar fi autentificarea pe server și client in ambele sensuri, transmiterea certificatelor, precum și stabilirea cheilor de sesiune.

 In tabelul de mai jos sun prezentate diferite tipuri de criptari ce sunt folosite pentru generarea de chei private si chei publice. La baza se afla algoritmi DES, MD5, SHA-1.

Avantaje si dezavantaje:

* Numarul de biti indica complexitatea algoritmului astfel incat sa fie mai grei de decriptat de catre persoanele ce vor sa fure datele
* O data cu cresterea complexitatii algoritmului creste si procesarea datelor cat si creste timpul acestuia
* Pentru a scurta timpul de procesare, criptarea datelor se face pe un calculator mai performant si cateodata costul acostora nu se justifica

Standardul de Criptare a Datelor (DES) este un cifru (o metodă de criptare a informației), selectat ca standard federal de procesare a informațiilor. Algoritmul are la baza

MD5, SHA-1 sunt tot cifruri one way, adica se pot doar cripta nu si decripta. Cine receptioneaza mesajul trebuie sa stie modalitatea de criptare pentru a afla mesajul final.

Tabelul 1. Cifrurile suportate de protocolul SSL, care utilizează RSA Key [8]

|  |  |
| --- | --- |
| Forța de aderență Domeniu și utilizare recomandate | Cifruri |
| Fortezza = Cifrul SuiteStrongest, Cifrul Suite  | DES (criptare tripla) 168-bit și SHA-1. Triple DES este cel mai puternic cifrul sprijinit de SSL folosit la programele bancilor mari. **Avantajul** este securitatea ridicata, pentru a “sparge” o astfel de criptare este nevoie de cateva sute de ani. **Dezavantajul** este nivelul de procesare pe care il solicita atat la cripate cat si la decriptare. |
| **Strong Cipher Suites**  | RC4 cu criptare pe 128 de biți și MD5 pentru mesaj de autentificare. Spre deosebire de Fortezza nu cripteaza de 3 ori, ci doar o data. Foloseste MD5 ca si generare de mesaj de autentificare.**Avantajul** esteprocesarea mai rapida a criptarii si decriptare dar si o securitate destul de ridicata.**Dezavantajul** este ca nu poate fi utilizat la programele cu date secrete.  |
| RC4 cu criptare pe 128 de biți și MD5 pentru mesaj de autentificare. Diferenta este viteza de compresie - mai rapida la RC4 |
| DES cu 56 de biți de criptare și SHA-1 mesaj de autentificarea |
| Exportabile Cipher Suites Aceste suite de cifrare nu sunt la fel de puternice ca cele enumerate mai sus, dar pot fi exportate în majoritatea țărilor  | RC4 cu criptare pe 40 de biți și MD5 pentru mesaj de autentificare  |
| RC2 cu criptare pe 40 de biți și MD5 pentru mesaj de autentificare |
| Cel mai slab cifru | Fără criptare, autentificare MD5. Se foloseste doar autentificarea folosind. Oricine incearca sa se pacaleasca autentificarea si ghiceste cifrul este doar o chestiune de timp pana se rezolva. |

# Capitolul 4. Protocoalele ce stau la baza TLS

 Transport Layer Security (TLS) și predecesorul său, Secure Sockets Layer (SSL), frecvent denumite "SSL", sunt protocoale criptografice care asigură securitatea comunicațiilor prin intermediul unei rețele de calculatoare. Mai multe versiuni ale protocoalelor sunt utilizate pe scară largă în aplicații cum ar fi navigarea pe web, e-mail, Internet fax, mesagerie instant și voice-over-IP (VoIP). Site-urile folosesc TLS pentru a securiza toate comunicațiile între serverele lor și browsere web.

 Protocolul de securitate al Transport Layer își propune în primul rând, sa asigure integritatea vieții private și a datelor între două aplicații informatice care comunică [9]. Când este securizat prin TLS, conexiunea între un client (de exemplu, un browser web) și un server (de exemplu, wikipedia.org) au una sau mai multe din următoarele proprietăți:

* Conexiunea este privat (sau securizat), deoarece este utilizată criptarea simetrică pentru criptarea datelor transmise. Cheile de la această criptare simetrică sunt generate în mod unic pentru fiecare conexiune și se bazează pe un secret comun negociat la începutul sesiunii (a se vedea protocolul de strângere de mână TLS). Serverul și clientul să negocieze detaliile algoritmului de criptare și cheile criptografice pentru a le utiliza înainte de primul octet de date sa fie transmis (a se vedea algoritmul de mai jos). Negocierea unui secret partajat este atât securizat (secret negociat este disponibil pentru eavesdroppers și nu pot fi obținute, chiar și de către un atacator care se plasează în mijlocul conexiunii) cat și de încredere (fără atacator poate modifica comunicațiile în timpul negocierii, fără a fi detectat).
* Identitatea părților care comunică pot fi autentificate folosind criptografia cu cheie publică. Această autentificare poate fi opțională, dar este în general necesara pentru cel puțin una dintre părți (de obicei serverul).
* Conexiunea asigură integritatea, deoarece fiecare mesaj transmis include un mesaj de verificare a integrității folosind un cod de autentificare mesaj pentru a preveni pierderea nedetectate sau alterarea datelor în timpul transmisiei.

 TLS a fost definit pentru prima dată în RFC 2246, în ianuarie 1999 ca un upgrade al SSL-ului, și a fost scris de Christopher Allen și Tim Dierks de consens pentru dezvoltare. După cum se menționează în RFC, "diferențele dintre acest protocol și SSL nu sunt dramatice, dar ele sunt suficient de importante pentru a exclude interoperabilitatea între TLS și SSL" [9]. TLS nu include un mijloc prin care o implementare TLS poate retrograda conexiunea la SSL, slăbind astfel securitatea.

 Cele mai importante functionalitati adaugate in ultimul deceniu ce au ajutat la securizarea datelor ce se transmit in **WEB** prin **HTTPS** sunt:

* Elimina sprijin-ul pentru curbe eliptice slabe și mai puțin folosite pe nume (vezi criptografie curbe eliptice)
* Elimina support pentru MD5 și SHA-224 funcții hash criptografice
* Necesită semnăturile digitale chiar și atunci când se utilizează o configurație anterioară
* Inlocuirea cu reluarea [PSK](https://en.wikipedia.org/wiki/Pre-shared_key) (Pre-shared key)
* Sprijinirea strângeri de mână 1-[RTT](https://en.wikipedia.org/wiki/RTT) si suport initial pentru 0-[RTT](https://en.wikipedia.org/wiki/RTT) (a se vedea tur-retur timp de întârziere)
* Dropping suport pentru multe caracteristici nesecurizate sau depășite, inclusiv prin compresie, renegociere, cifrurile non-[AEAD](https://en.wikipedia.org/wiki/Authenticated_encryption) (Authenticated encryption), statică RSA și DH schimbul de chei statice, grupuri [9] personalizate DHE, negocierea formatului punct, protocolul Change Cipher Spec, Hello mesajul timp UNIX, iar intrarea AD câmpul de lungime la [AEAD](https://en.wikipedia.org/wiki/Authenticated_encryption) cifrurile [9]
* Interzicerea SSL sau RC4 negociere pentru compatibilitate
* Utilizarea de integrare a hash sesiune
* Depreciativă utilizarea numărului de înregistrare versiunii strat și înghețarea numărului pentru o mai bună compatibilitate
* În mișcare unele legate de detaliile de securitate algoritm dintr-o anexă la caietul de sarcini și relegating ClientKeyShare unui apendice

# Capitolul 5. Proiectul OpenVPN ce are la baza SSL/TLS

 [OpenVPN](https://en.wikipedia.org/wiki/OpenVPN) este o aplicație software open-source care implementează tehnici de rețea virtuală privată (VPN). In acest moment este unul dintre cele mai utilizate retele private oferind un pachet complet server/client.

Sunt diferite module pentru sistemul de operare Linux ce creaza usor un server OpenVPN plus certificate pentru useri. Pe site-ul lor exista niste pasi ce trebuie indepliniti pentru a duce la bun sfarsit integrarea sistemului: <https://openvpn.net/index.php/open-source/documentation/howto.html>

Pe partea de client este mult mai simplu, exista diverse programe pentru fiecare sistem de operare, cele mai cunoscute fiind aplicatiile lor.

P Configurarea pe Mac necesita logarea pe web pe pagina lor de unde se poate descarca aplicatia direct cu configurarile pentru serverul dorit.



Pe windows este necesar adaugarea datelor serverului, cum ar fi adresa, portul si cum dorim sa se numeasca conexiunea.

#

# Capitolul 6. Concluzii

 In ultimii ani a crescut tot mai mult dorinta de avea acces la o retea privata de la distanta, iar un VPN este vital sa asigure securitatea traficului de internet.

 Retelele publice, pun la dispozitie o modalitate usoara ca hackerii sa asculte reteaua ("sniff") si sa vada ce face fiecare utilizator. Acesta le permite sa vada ce pagini web sunt deschise, sa fure parole, sa fure informatii ale sesiunii si sa fie capabil sa se logheze in site-uri drept un alt utilizator si sa preia alte informatii private. In plus, hackerii calificați pot efectua un "om în mijloc" atac. Acest lucru le permite să monitorizeze nu numai în profunzime a traficului de rețea, dar, de asemenea, modifica traficul sau injectați propria lor într-o încercare de a păcăli un utilizator pentru a dezvălui date importante.

 Se incearca gasirea unor algoritmi de generare a cheii private incat sa fie foarte securizate dar procesarea lor sa nu fie costisitoare la nivel de resurse. De aceea au aparut noile cifruri MD5 si SHA224.

 In acest moment exista posibilitatea de a avea sisteme private atat la companii cat si acasa dar sub un anumit pret. Multe firme ofera atat useri nelimitati cat si suport in functie de cerintele fiecarui client.

 Microsoft a implementat de cativa ani un sistem de retea private ce nu mai oblige oamenii sa plateasca diferite companii de suport. Aceasta functionalitate permite crearea unui server pe masina locala cat si crearea de utilizatori ce se pot conecta folosind un client-ul oferit in functie de platforma pe care este.

 Limitarea este la server deoarece nu se poate crea decat pe sistemul de operare oferit de Microsoft, adica Windows.

 OpenVPN au venit cu aceeasi implementare ca si Microsoft dar eliminan limitarea serverului de a fi doar pe o platforma, aceastia punan la dispozitie functionalitatea pe toate platformele si in special pe Linux. Clientii exista pe toate platformele desktop si de cativa ani au fost integrate si pe platformele mobile.

 In acest moment se incearca securizarea tuturor retelelor publice, mai ales cele din spatiile publice (ex: parcuri, facultati) cat si pe cele din restaurante sau alte locuri ce pot sa ii expuna pe utilizatori.

 Orange a inceput sa adopte aceasta strategie punan la dispozitii un numar destul de mare de wireless-uri ce au integrate in ele retele private. In viitor or sa apara tot mai multe companii ce o sa puna la dispozitie aceste retele securizate si o sa inlocuiasta retelele publice actuale ce nu sunt foarte sigure.

# Bibliografie

[1] Online, Articol, https://www.lifewire.com/vpn-software-hardware-and-protocols-818175, publicat in 13.10.2016

[2] Online, Articol, https://www.sparklabs.com/viscosity/introtovpn/, modificat in 2016

[3] Online, Articol, http://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-sslvpn-52/SSLVPN\_Overview\_52/SSLVPN\_Overview\_52.htm, modificat in 2017

[4] Online, https://en.wikipedia.org/wiki/Virtual\_private\_network, modificat in 2016

[5] Online, Articol, https://technet.microsoft.com/en-us/library/cc779919(v=ws.10).aspx#w2k3tr\_vpn\_how\_kkgn, publicat in 2013

[6] Online, Articol, http://security.stackexchange.com/questions/20803/how-does-ssl-tls-work, publicat in 04.07.2014

[7] Online, https://en.wikipedia.org/wiki/Digital\_signature, 23.01.2017

[8] Online, Articol, https://developer.mozilla.org/en-US/docs/Archive/Security/Introduction\_to\_SSL#The\_SSL\_Protocol, 04.06.2015

[9] Online, https://en.wikipedia.org/wiki/Transport\_Layer\_Security, 09.01.2017

[10] Online, https://en.wikipedia.org/wiki/OpenVPN, 23.01.2017