Lucrarea 12.

REȚELE PRIVATE VIRTUALE.

12.1. Instalarea unui server VPN pe un sistem Linux.

12.1.1. Prezentarea componentelor.

Sistemul de operare **Linux** oferă suport pentru conexiuni securizate de tip VPN, prin implementarea unor **protocoale de tunelare**, care pot fi încapsulate în pachete **IP**. Sistemele de operare din familia UNIX oferă mai multe soluții de implementare a transferului datelor prin tunele, între care cele mai des întâlnite sunt cele bazate pe **SOCKS**, **SSL** şi **PPTP**.
Implementarea **SSL** se poate face cu ajutorul suportului oferit de comunitatea **OpenSSL**, pentru transferul datelor criptate într-o gamă extinsă de servicii. Situațiile cele mai des întâlnite, care folosesc **tunelare SSL**, sunt `https`, `pop3s`, sau `imaps`.

OpenSSL este un pachet de aplicații de criptare, conceput pentru implementarea **SSL** şi **TLS** şi a standardelor asociate acestora. Se poate utiliza sub forma unor comenzi de sine stătătoare, în lanțuri de procese de tip `pipe`, sau sub forma de module apelabile din alte aplicații, cum este cazul serverelor de web securizate (`mod_ssl` pentru transfer `https`). **OpenSSL** foloseşte pentru autentificarea părților, aflate la capetele tunelului, certificate de autenticitate (CA) [21].

O altă variantă de implementare este utilizarea pachetului `stunnel`, o aplicație de sine stătătoare, care permite **criptarea SSL** a datelor, transferate între terminale. Aceasta se poate face în absența unui nivel suplimentar de tunelare, prin conectarea aplicațiilor client cu cele de tip server prin intermediul acesteia.

În cazul utilizării sistemului **Linux** ca echipament de comunicație şi interconectare între rețele (ruter), este foarte utilă instalarea suportului pentru protocolul de tunelare **PPTP**.

12.1.2. Instalarea şi configurarea serviciului de tunelare `pptpd`.

Pachetul de instalare pentru implementarea serviciulului de tunelare prin PPTP **nu** este, în general, **inclus** în distribuțiile de bază Linux, ci trebuie **descărcat** de la cei care au dezvoltat acest produs, comunitatea **Poptop**. Pachetul `pptp-x.y.z` (`x, y, z` reprezentând versiunea) se găseşte sub forma unor arhive de tip `.tar.gz` sau `.rpm`, în funcție de distribuția de Linux folosită. Deoarece `pptpd` (serviciul de tunelare **PPTP**) operează împreună cu `pppd` (serviciul care controleată protocolul **PPP**) trebuie corelate versiunile şi verificată, în prealabil, compatibilitatea lor. Pentru instalarea şi configurarea unui server **VPN** trebuie parcurse următoarele etape:

Despachetarea arhivei.

După descărcarea pachetului şi despachetarea arhivei, se vor urma instrucțiunile de compilare şi instalare. De exemplu, pentru un pachet în format de arhivare `.tgz`, se va aplica comanda:

```
root@masserv:~# tar zxf pptpd-x.y.z.tar.gz
root@masserv:~#
```

Aceasta va **despacheta** arhiva în **directorul curent**, creând un subdirector cu **numele fişierului**, mai puțin extensia `tar.gz,` în care se găsesc fişierele, în formă de **cod sursă**, scrise în limbajul de programare **`C++`**, împreună cu fişierele *script* necesare **compilării** acestora.

Compilarea codurilor sursă

Pentru compilarea fişierelor sursă trebuie schimbat directorul curent cu directorul care conține aceste fişiere, utilizând comanda `cd`, ca în exemplul de mai jos:

```
root@masserv:~# cd pptpd-x.y.z
root@masserv:~/pptpd-x.y.z#
```

Compilarea se face cu ajutorul unor fișiere script, parcurgând instrucțiunile conținute de acesta, care permit automatizarea procesului. Pentru configurarea procesului de compilare și „personalizarea" acestuia în funcție de sistemul de operare, distribuție, sau versiune, trebuie apelat mai întâi fișierul script `configure`:

```
root@masserv:~/pptpd-x.y.z# ./configure
Mesaje generate de scriptul de configurare
...
root@masserv:~/pptpd-x.y.z#
```

Dacă procesul de configurare a decurs fără erori, se trece la faza de compilare propriu-zisă:

```
root@masserv:~/pptpd-x.y.z# make
Mesaje generate de scriptul de configurare
...
```

Dacă nu sunt erori la compilare se poate trece la faza de instalare a pachetului executabil și a documentației utilizând comanda:

```
root@masserv:~/pptpd-x.y.z# make install
```

Configurarea serviciului.

Serviciul `pptpd` folosește pentru configurare fișierul `/etc/pptpd .conf` care trebuie să conțină următoarele linii:

```
#....
# Următoarea linie specifică locația fișierului
# de configurare PPP care conține opțiunile
# necesare operării cu pptpd. Dacă nu se specifică
# altfel, PPP va utiliza /etc/ppp/options
option /etc/ppp/options.pptpd
#
# Pentru a înregistra evenimentele apărute cu ocazia
# conectării prin pptpd, se poate activa utilizarea
# serverului syslog cu opțiunea debug.
debug
#
# Pentru a permite transmiterea pachetelor cu adresă de
# broadcast spre o anumită interfață, trebuie activată
# opțiunea bcrelay
bcrelay eth0
#
# unde eth0 este interfața spre care trebuie transmise
# pachetele cu adresă de broadcast
#
# pentru alocarea dinamică a adreselor IP pentru
# fiecare client VPN, în parte, acestea trebuie
# specificate aici sub formă de listă.
localip 192.168.122.1
remoteip 192.168.122.2-10
#
# Local IP reprezintă adresa interfeței serverului
# PPTP, iar remote IP, cea alocată dinamic clientului
#
# Linia de mai jos determină locația unde pptpd scrie
# fișierul cu identificatorul de proces, pid
pidfile /var/run/pptpd.pid
#
```

Opțiunile de configurare ale serviciului `pppd` se află în fișierul `/etc/ppp/options.pptp`, al cărui conținut este asemănător cu cel al fișierului folosit de `pppd` în cazul conexiunilor prin linie serială, sau telefonică `/etc/ppp/options.ttyS1`, prezentat în cursul „Protocolul Punct la Punct". Un exemplu de ce ar trebui să conțină acest fișier, pentru ca `pppd` să poată opera alături de `pptpd`, se poate vedea în rândurile de mai jos:

```
# Pentru configurare avansată și opțiuni dependente de
# versiunea pachetului, se va consulta documentația
# însoțitoare.
lock
#
```

```
# Maximum transmit Unit (mtu) trebuie să fie mai mic
# decât dimensiunea maximă acceptată pentru cazurile
# obişnuite (1500), datorită dimensiunii suplimentare
 a antetelor adăugate de protocoalele VPN
#
mtu 1450
mru 1450
debug
login
auth
nodetach
proxyarp
asyncmap 0
require-chap
require-mppe
#require-mppe-stateless
lcp-echo-failure 30
lcp-echo-interval 5
```

Autentificarea clienților.

Autentificarea se face de către componenta `pppd`, în funcție de opțiunile utilizate pentru acest scop. Aşa cum s-a putut vedea în cursul „Protocolul Punct la Punct", autentificarea se poate face în mai multe moduri: prin utilizarea aplicației `login` şi a listelor de utilizatori înscrişi în sistem, sau pe baza celor înscrişi în fişierul `/etc/ppp/chap-secrets`, al cărui conținut poate să arate ca în exemplul următor:

```
# client    server        secret     adresă IP
# nume_client  *          <parolă>       *
florind        *         ProTocOalE      *
```

Pornirea serviciului `pptpd`.

Lansarea serviciului `pptpd` se poate face simplu, direct prin apelarea acestuia cu numele său, precedat de calea spre el:

```
root@masserv:~# /usr/sbin/pptpd
```

Pentru automatizarea lansării în execuție a serviciului se poate adăuga, în fişierul `/etc/rc.d/rc.local`, o linie conținând această comandă. Pe de altă parte, în timpul instalării se creează şi fişierul `/etc/rc.d/rc.pptpd` care conține scripturile necesare lansării în execuție, opririi, sau repornirii serviciului. Pentru aceasta, fişierul trebuie să aibă setat atributul de „executabil", pentru utilizatorul `root` şi grupul din care face parte acesta:

```
root@masserv:~# chmod 750 /etc/rc.d/rc.pptpd
root@masserv:~# ls -ax /etc/rc.d/rc.pptp
-rwxr-xr-x  1 root root 508 Sep 13  2004 /etc/rc.d/rc.pptpd*
root@masserv:~#
```

Pentru a ne asigura că acest serviciu este activ şi „ascultă", adică este apt să primească cereri de acces, se poate interoga sistemul de operare pentru a vedea dacă este deschis portul `TCP 1723`, utilizând comanda `netstat`, aşa cum se poate vedea în exemplul de mai jos:

```
root@masserv:~# netstat -an
...
tcp       0      0 0.0.0.0:1723        0.0.0.0:*    LISTEN
...
root@masserv:~#
```

12.1.3. Testarea funcționării serviciului.

După pornirea serviciului, se va testa funcționarea conexiunii, cu ajutorul unui terminal client, conectat la rețea, pe care se va porni plicația care permite conectarea prin „interfața" VPN.

Notă: Această lucrare nu îşi propune să dezvolte modul de configurare, bazat pe meniuri cu ferestre, a unor aplicații. Pentru aceasta se va consulta documentația explicativă, însoțitoare. Se porneşte aplicația client, de conectare prin VPN, configurată cu opțiunile de securitate dorite, în cazul de față autentificare prin **CHAP**, tunelare prin **PPTP** şi criptare **MPPE**, şi se vor trece adresa

IP a serverului de **VPN**, recent configurat şi instalat, numele de utilizator şi parola acestuia. Se apasă butonul de conectare şi se urmăreşte evoluția procesului de conectare. După mesajul „Validating", se poate verifica activarea interfeței PPP, pe sistemul Linux, utilizând următoarea secvență de comenzi, la care sistemul de operare trebuie să trimită răspunsuri asemănătoare cu acestea:

```
root@masserv:~# netstat -an
...
tcp  0  0  0.0.0.0:1723       0.0.0.0:*         LISTEN
...
tcp  0  0  193.226.5.178:1723 89.137.96.190:3497 ESTA-BLISHED
...
root@masserv:~#ifconfig ppp0
ppp0    Link encap:Point-to-Point Protocol
        inet addr:192.168.122.1  P-t-P:192.168.122.3
Mask:255.255.255.255
        UP POINTOPOINT RUNNING NOARP MULTICAST
MTU:1400  Metric:1
  RX packets:54 errors:0 dropped:0 overruns:0 frame:0
  TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:3
  RX bytes:4775 (4.6 Kb)  TX bytes:152 (152.0 b)

root@masserv:~#
```

Se deschide apoi, pe sistemul client, o fereastră text în care se vor utiliza următoarele comenzi pentru verificarea tabelei de rutare şi apoi a conectivității cu terminalul server.

```
C:\Documents and Settings\Administrator>route print
===========================================================
Interface List
0x1 ........................ MS TCP Loopback interface
0x2 00 30 05 3d f9 3e ... Intel(R) PRO/1000 Network Connection - Packet
Scheduler Miniport
0x60004 00 53 45 00 00 00 . WAN (PPP/SLIP) Interface
===========================================================
Active Routes:
Network Dest. Netmask       Gateway       Interface Metric
...
192.168.122.0 255.255.255.0 192.168.122.3 192.168.122.3     1
192.168.122.3 255.255.255.255 127.0.0.1   127.0.0.1         5
192.168.122.255 255.255.255.255 192.168.122.3 192.168.122.3 5
193.226.5.178 255.255.255.255   192.168.0.1   192.168.0.17  2
...
255.255.255.255 255.255.255.255 192.168.122.3 192.168.122.3 1
Default Gateway:       192.168.122.3
===========================================================
Persistent Routes:  None

C:\Documents and Settings\Administrator>ping 192.168.122.1
Pinging 192.168.122.1 with 32 bytes of data:
Reply from 192.168.122.1: bytes=32 time=21ms TTL=64
Reply from 192.168.122.1: bytes=32 time=20ms TTL=64
...
Ping statistics for 192.168.122.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 21ms, Average = 18ms

C:\Documents and Settings\Administrator>
```

Filtrarea accesului terminalelor, la acest serviciu, se poate face introducând în fişierul `/etc/rc.d/rc.firewall` câte o linie pentru fiecare terminal client, astfel [16, 22]:

```
# VPN florind
iptables -A INPUT  -p tcp -s 89.137.96.190/32 --dport 1723 -j ACCEPT
```

În această linie, aplicația `iptables` instruieşte nucleul sistemului de operare cum să manipuleze pachetele IP şi segmentele TCP. Semnificația argumentelor este următoarea:

- **-A** (Append) regula din această linie nu anulează o altă regulă ci se adaugă la cele existente;
- **INPUT** – regula se referă la pachetele care intră în sistem;
- **-p <***protocol***>** - protocolul de transport pentru care este stabilită regula;

- **-s <*adresa IP*>** - adresa terminalului de la care se primesc pachetele care fac obiectul regulii curente;
- **--dport <port>** - portul destinație la care se referă regula;
- **-j** (jump) – indică saltul spre următoarea regulă de filtrare, în cazul în care regula curentă se verifică;
- **ACCEPT** – regula are ca scop acceptarea condițiilor înscrise în argumente.

În funcție de scopul pentru care se foloseşte **serverul de VPN** se pot adăuga, sau modifica şi alte opțiuni, în acest caz fiind nevoie de consultarea documentației care însoțeşte aplicațiile, prezentate mai sus.

12.2. VPN alături de Firewall.

Accesul spre şi dinspre rețelele private este, de cele mai multe ori, restricționat prin filtrare pe baza unor liste de acces. Filtrarea se poate face de către echipamentele de rutare, sau de aplicații care operează pe terminalele din rețea, numite în general „ziduri de foc” *(firewall)*. Criteriile de filtrare pot să fie foarte variate, începând cu adresa terminalelor, aplicațiile care transferă date (prin numărul de port de la nivelul de transport), fluxul de date transferate, sau frecvența cererilor de acces.

Pentru a permite deschiderea „tunelului”, este nevoie ca serviciile care asigură funcționarea conexiunilor **VPN** să fie acceptate de către sistemele de filtrare. Se presupune că este necesară conectarea unei rețele locale (**LAN** A), izolată prin *fireqall*, la un server **VPN** care utilizează protocolul de tunelare **PPTP**. Astfel, pentru ca un terminal să poată avea acces la un server **VPN**, trebuie ca „zidul de foc” să permită transferul pachetului **IP**, cu segmentul **TCP** care poartă cererea de stabilire a conexiunii virtuale spre serviciul **PPTP**, reprezentat prin portul destinație cu numărul 1723, aşa cum se poate vedea în **figura 12.1**.

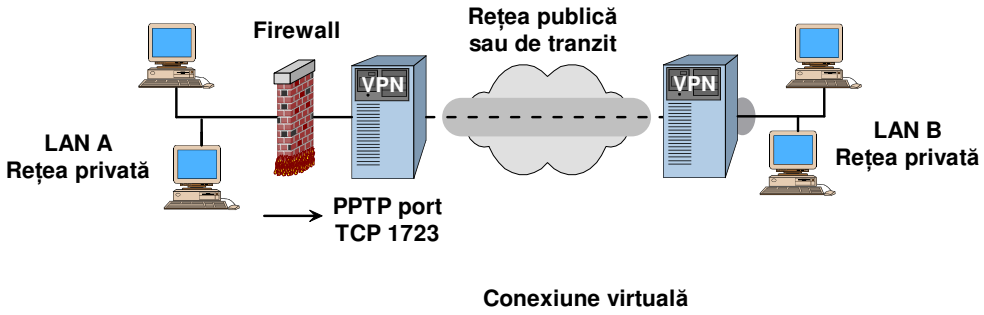

Fig. 12.1. Accesul unei rețele locale, izolată prin firewall, la un server **VPN** aflat în rețeaua publică.

În cazul în care serverul **VPN** este conectat direct la rețeaua locală, este nevoie ca tunelul să poată „străbate” zidului de foc. În acest caz, zidul de foc trebuie să accepte transferul, spre rețeaua locală, a pachetelor care au adresa sursă a clienților rețelei **LAN A** şi a segmentelor care au ca destinație portul cu numărul 1723, aşa cum se poate vedea în **figura 12.2.**

În cazul utilizării protocolului de tunelare L2TP, numărul corespunzător al portului, de identificare, destinație este 1701, protocolul de transport fiind **UDP**.

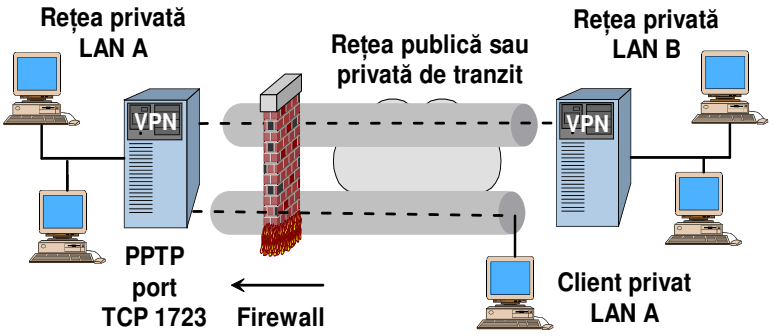

Fig. 12.2. Accesul unui terminal-client la un server **VPN** aflat într-o rețea privată izolată prin firewall.

Pentru a verifica dacă un server de tunelare permite accesul unui terminal, din exterior, la servicii, se poate folosi aplicația `nmap`, lansată la linia de comandă, aşa cum se poate vedea în exemplul următor:

```
root@masserv:~# nmap 192.168.120.2
Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2008-03-08 18:43 EET
Interesting ports on 192.168.120.2:
(The 1660 ports scanned but not shown below are in state: filtered)
PORT     STATE SERVICE
139/tcp  open  netbios-ssn
1701/udp open  L2TP
1723/tcp open  pptp
3389/tcp open  ms-term-serv

Nmap run completed -- 1 IP address (1 host up) scanned in 23.056 seconds
root@masserv:~#
```

Aplicația `nmap` trimite cereri, nivelului de transport, prin care se încearcă deschidere a unor conexiuni virtuale cu numere de port cuprinse într-un anumit interval. Dacă pe terminalul destinație există o aplicație de rețea activă, componenta de transport va accepta deschiderea unei conexiuni pentru aceasta, trimițând înapoi segmente de acceptare a conexiunii. Astfel, fără să cunoască natura aplicației, sau să trimită alte date spre aceasta, nmap determină dacă, sau nu, pe terminalul destinație există permisiuni de acces spre anumite porturi.

Aceste aplicații se numesc exploratoare de porturi *(port scanners)* şi se folosesc pentru verificarea preliminară a funcționării unor servicii şi a drepturilor de acces la acestea.