HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

# Analiza Linux Devil operacijskog sustava

**CCERT-PUBDOC-2005-05-121**

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

**CARNet CERT**, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

**LS&S**, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

# Sadržaj

# 1. Uvod

Linux Devil operacijski sustav spada u grupu sustava namijenjenih podizanju s CD-ROM medija. Ovakav način rada višestruko podiže razinu sigurnosti samog sustava, budući da neovlašteni korisnici u slučaju uspješno izvršenog napada nisu u mogućnosti trajno mijenjati podatke na sustavu. Razlog tomu je taj što su svi podaci potrebni za rad sustava pohranjeni na CD-ROM mediju dostupnom samo za čitanje, a tijekom rada sve operacije i procesi izvršavaju se isključivo unutar radne memorije. Nakon zaustavljanja ili ponovnog pokretanja sustava, svi se podaci brišu iz radne memorije i sve promjene su trajno izgubljene.
Iako ovakav način rada ima i svoje nedostatke, ovakav tip sustava već je duže vrijeme iznimno popularan u krugovima sistem administratora i sigurnosnih stručnjaka. U slučaju detekcije bilo kakvih neovlaštenih aktivnosti ili nepravilnosti u radu, "čisti sustav" moguće je u vrlo kratkom vremenu podići sa izvornog CD-ROM medija. Navedene karakteristike ovakav tip sustava čine iznimno pogodnim za implementaciju sigurnosnih uređaja od kojih se u prvom redu očekuje pouzdanost i stabilnost.
Dokument opisuje ranije spomenutu Linux Devil distribuciju, njene osnovne karakteristike i način rada te mogućnost primjene kao sustava za vatrozidnu zaštitu.

## 1.1. Mogućnosti sustava

Sustav omogućava korištenje većine standardnih Linux servisa. Osim što je moguće konfigurirati sustav kao vatrozid, postoji mogućnost da računalo radi i kao poslužitelj pri čemu su dostupni sljedeći *open source* servisi:

- HTTP poslužitelji (Apache 2 s PHP podrškom, THTTPD, proxy poslužitelj SQUID)
- FTP poslužitelji (TFTP, VSFTPD, proxy poslužitelji JFTPGW i Frox)
- SAMBA poslužitelj
- Mail poslužitelji (Cyrus POP3/IMAP, Dovecot, Postfix) i SpamAssassin filter za detekciju spam poruka
- DNS poslužitelj (Bind)
- DHCP poslužitelj (Dnsmasq)
- NTP poslužitelj (NTPD)
- SNMP poslužitelj (NET_SNMP)
- VOIP poslužitelj (SIP Express Router)

Osim navedenih poslužitelja raspoložive su i *open source* baze podataka:

- MySQL
- PostrgreSQL

U svrhu zaštite sustava raspoloživi su različiti sigurnosni alati:

- SSH poslužitelj (SSHD)
- Iptables – alat za kreiranje naredbi filtriranja mrežnog prometa
- Snort – alat za detekciju malicioznih aktivnosti (eng. *IDS - Intrusion Detection System*)
- Saslauthd – Cyrus SASL autentikacijski poslužitelj
- Sagator –program za zaštitu od virusa i spam poruka
- Oidentd – identifikacijski poslužitelj za konekcije s promjenom (eng. *Network Address Translation*) i maskiranjem (eng. *Masquerading*) mrežnih adresa
- Net-Acct – registrira mrežni promet
- VTUN – kreira virtualne tunele (eng. *VPN – Virtual Private Network*) s kompresijom i enkripcijom podataka
- Pptdp – VPN poslužitelj baziran na P2P (eng. *Point To Point*) protokolu
- IPSec – VPN alat zasnovan na IPSec protokolu
- CIPE – VPN paket zasnovan na UDP mrežnom prometu
- L2TPD – VPN baziran na L2TP (eng. *Layer Two Tunneling Protocol*) protokolu
- OpenVPN – VPN poslužitelj za zaštitu UDP prometa
- Clam Antivirus – antivirusni program

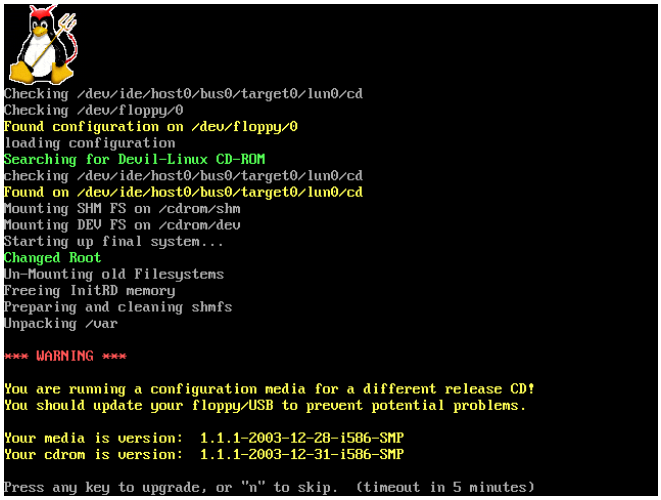
Zbog sigurnosnih razloga i boljih performansi sustav ne posjeduje grafičko sučelje. Iz tog razloga potrebno je sve raspoložive programe podesiti ručnim uređivanjem konfiguracijskih datoteka. Ipak,

konfiguracijske datoteke moguće je prenijeti i s postojećih sustava uz eventualne modifikacije. U skladu s tim, proizvođač Linux Devil operacijskog sustava predlaže korištenje Firewall Builder alata za kreiranje konfiguracijske datoteke vatrozida.
Minimalni sklopovski zahtjevi koje je proizvođač naveo kao potrebne za rad Linux Devil operacijskog sustava su sljedeći: PC 486 s 32 MB radne memorije i CD-ROM jedinica ili USB priključak potrebni za podizanje sustava. Ukoliko sustav radi kao vatrozid potrebna je barem jedna mrežna kartica (kontrola virtualnih LAN-ova). Iako je konfiguraciju moguće uklopiti u sam *boot*-abilni CD, jednostavnije ju je učitavati s USB priključka ili diskete.

# 2. Instalacija sustava

Linux Devil operacijski sustav ne instalira se na klasičan način. Za korištenje sustava nije potrebno imati tvrdi disk već samo CD-ROM jedinicu ili USB priključak s kojeg će se sustav podići. Pri tome se konfiguracijski podaci ujedinjuju sa sustavom ili se učitavaju preko diskete odnosno USB priključka. Izvorni kod operacijskog sustava može se dohvatiti sa službenih Web stranica Linux Devil projekta (http://www.devil-linux.org/downloads/index.php).

Ukoliko se prilikom instalacije ne koristi IDE CD-ROM jedinica, tada je potrebno modificirati izvorni kod operacijskog sustava pri čemu se promjene obavljaju na sistemskoj `etc/sysconfig/config` datoteci pohranjenoj u `etc.tar.bz2` arhivi. U njoj treba definirati dodatne module koje je potrebno učitati prilikom podizanja sustava. Također, ukoliko se ne koristi IDE CD-ROM jedinica, konfiguracijsku arhivu `etc.tar.bz2` potrebno je pohraniti na *floppy* disketu ili USB priključak. A ukoliko je sustav potrebno podizati s USB priključka, u izvornom paketu raspoloživa je skripta `install-on-usb` koja obavlja sve pripremne radnje za instalaciju s USB-a.




**Slika 1:** Učitavanje konfiguracijskih podataka

# 3. Podešavanje sustava

Konfiguracija Linux Devil operacijskog sustava svakako nije preporučljiva za Linux početnike. Budući da distribucija ne sadrži napredne grafičke alate za podešavanje sustava, već se sva podešavanja baziraju na ručnom uređivanju konfiguracijskih datoteka, od administratora se zahtjeva određena razina znanja i iskustva u održavanju Linux sustava. Grafičko sučelje opravdano je izostavljeno, budući da bi ono nepotrebno moglo utjecati na performanse i stabilnost sustava.

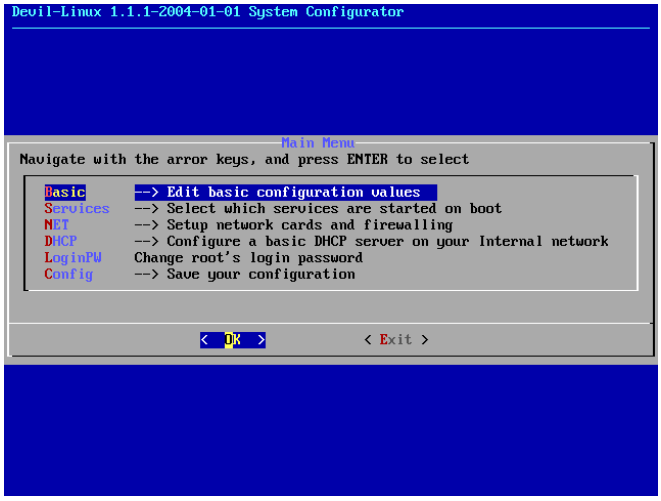
Sustav raspolaže sa specijaliziranim programom System Configurator koji se koristi za osnovno podešavanje sustava te uključivanje ili isključivanje pojedinih servisa. Korištenjem System Configurator programa moguće je konfigurirati mrežne postavke, vrstu tipkovnice i miša, vremensku zonu, praćenje log zapisa i sl. Program omogućava i podešavanje vrste mrežne zaštite pri čemu je raspoloživ standardni sustav s dvije mrežne kartice ili sustav s tri mrežne kartice (DMZ uključena). Pri tome je potrebno dodatno proći kroz definirane naredbe i odabrati koje su potrebne te unijeti one koje nedostaju. Nažalost, s konfiguracijskim programom nije moguće podešavati pojedine servise, već ih samo aktivirati.

## 3.1. Korištenje System Configurator programa

System Configurator pokreće se naredbom `setup`, a sastoji se od šest glavnih cjelina:

- **Basic** – dio za definiranje imena računala, domene, vremenske zone, vrste tipkovnice, vrste miša, razine zapisivanje log zapisa jezgre operacijskog sustava i sl.

- **Services** – cjelina za odabir servisa koji će biti aktivni. Odabiranjem pojedinih servisa isti se zapisuju u konfiguracijsku datoteku `/etc/sysconfig/config`.
- **NET** – dio za postavljanje mrežnih kartica i definiranje modela mrežne zaštite (sustav s dvije mrežne kartice ili sustav s tri mrežne kartice). Postavke za pojedine mrežne kartice zapisuju se u pripadne konfiguracijske datoteke `/etc/sysconfig/nic/ifcfg-ethX`.
- **DHCP** – cjelina za definiranje DHCP poslužitelja. Postavke se spremaju u konfiguracijsku datoteku `/etc/sysconfig/network/dhcp`.
- **LoginPW** – cjelina za promjenu administratorske zaporke koja na početku nije postavljena.
- **Config** – sučelje za pokretanje `save-config` naredbe koja zapisuje definirane postavke u obliku `etc.tar.bz2` arhive na *floppy* disketu ili USB priključak.



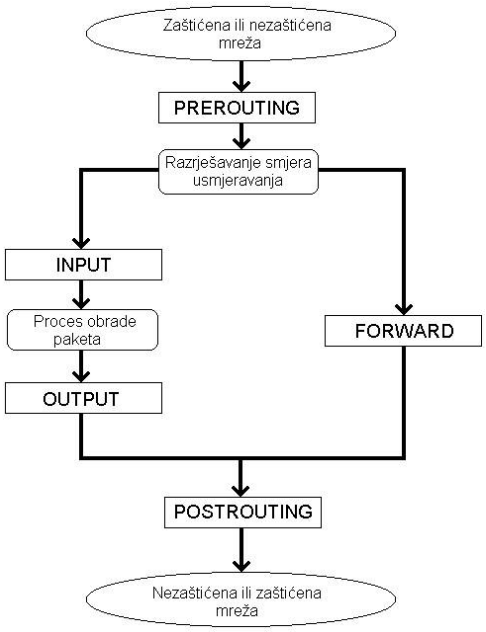

**Slika 2:** Sučelje System Configurator programa

# 4. Sustav kao vatrozid

Glavni zadatak vatrozida je kontrola mrežnog prometa pri čemu se određeni mrežni paketi propuštaju dok se drugi odbacuju. Odluke o tome koji će se paketi propustiti, a koji odbaciti donose se na temelju zaglavlja paketa u kojem se nalaze osnovni podaci o paketu i stanju konekcije.
Izgradnja vatrozida zasnovana je na standardnim Linux programima, prvenstveno na Iptables programskom alatu (http://www.netfilter.org). Korišteni alat omogućava različite napredne mogućnosti kod filtriranja mrežnog prometa. Sustav raspolaže skriptama za podešavanje vatrozida s dvije mrežne kartice, odnosno s tri mrežne kartice kad se koristi i zaštićena mreža poslužitelja (DMZ – *Demilitary Zone*). Osim definiranih skripti za spomenute sheme, na sustavu su raspoložive i Shorewall skripte (http://www.shorewall.com) koje isto koriste Iptables naredbe.
Glavna prednost korištenja Linux Devil operacijskog sustava kao vatrozida je u tome što se sustav podiže i izvršava u potpunosti s CD-ROM ili slične jedinice. Tako udaljeni napadači ne mogu modificirati sustav čak i ako uspiju dobiti administratorske ovlasti na napadnutom računalu.

## 4.1. Iptables programski alat

IPtables čini osnovi element za izgradnju Linux Devil vatrozida. Program je dio Netfiler *open-source* projekta, a raspoloživ je za Linux jezgre >=2.4. Svi mrežni paketi provjeravaju se od strane Iptables naredbi te ukoliko udovoljavaju zadanim pravilima paketi se prihvaćaju, a ako ne odbacuju se. Cijeli sustav provjere mrežnih paketa baziran je na određenim fazama obrade mrežnih paketa. Glavne faze obrade nazivaju se još i karike (eng. *chains*). Na slici 3 vidljive su glavne faze unutar vatrozida.




**Slika 3:** Usmjeravanje paketa unutar jezgre operacijskog sustava

Svi paketi namijenjeni samom vatrozidu prosljeđuju se na INPUT (ulaznu) fazu. Tu je moguće definirati pravila u vezi s dolaznim paketima. Neka od tipičnih pravila bila bi da se paket proslijedi na neku drugu, na slici nespomenutu fazu koja je zadužena za obradu i provjeru paketa određenog tipa (npr. UDP ili TCP paketi). Nakon što uspješno prođe INPUT fazu paket odlazi na obradu određenom aplikacijskom procesu.

Mrežni paketi generirani od strane vatrozida prvo dolaze na OUTPUT fazu. Tu je moguće obaviti filtriranje paketa, tj. provesti zabranu prolaska neodgovarajućim paketima.

Ako je paket potrebno samo proslijediti s jedne na drugu mrežu on mora proći kroz FORWARD faze. U FORWARD fazi obavljaju se provjere prema pravilima koje određuju koji paketi smiju prolaziti na koju mrežu. Uobičajeni skup naredbi sadrži zabranu prosljeđivanja paketa s vanjske mreže prema zaštićenoj i dozvolu prosljeđivanja odgovora s vanjske mreže prema zaštićenoj mreži. Također, često se korisnicima zaštićene mreže u FORWARD fazi zabranjuje pristup određenim vanjskim računalima (poslužitelji sa igrama i sl.) ili određenim nesigurnim uslugama (ftp, tftp, itd...).

Faza PREROUTING omogućava manipulaciju paketima na razini promjene TOS (eng. *Type of Service*) varijabli i sl. Važnija primjena ove faze je DNAT (eng. *Destination Network Address Translation*), transformacija koja se koristi za promjenu odredišne adrese kada je potrebno pakete koji sadrže javnu IP adresu vatrozida kao odredište preusmjeriti na neko drugo računalo.

Fazi POSTROUTING glavna je funkcija SNAT (eng. *Source Network Address Translation*), transformacija izvorne adrese. SNAT transformacija koristi se za promjenu izvorne adrese paketa. Umjesto SNAT-a u ovoj fazi moguće je koristiti i proces maskiranja (eng. *Masquerading*) privatnih adresa iz zaštićene mreže. Vatrozid mijenja IP adrese iz zaštićene mreže svojom adresom pridruženom vanjskom mrežnom sučelju i prosljeđuje tako modificirane pakete na vanjsku mrežu. Razlika između SNAT-a i maskiranja je u tome što SNAT zamjenjuje IP adrese s definiranom adresom, a maskiranje zamjenjuje IP adrese s adresom pridruženom određenom mrežnom sučelju.

## 4.2. Stateful inspection

*Stateful Inspection* danas je jedna od ključnih tehnologija za kvalitetan i pouzdan rad modernih vatrozidnih sustava. Bazira se na kontinuiranom praćenju i analizi pojedinih segmenata paketa koji prolaze kroz vatrozid, kako bi se na temelju njih u stvarnom vremenu mogle donositi pravilne odluke o filtriranju paketa. Ovakav način filtriranja dodatno podiže sigurnosni nivo sustava jer smanjuje broj nepotrebno otvorenih portova na vatrozidu.

Iptables programski alat podržava *stateful inspection* za TCP pakete i pri tome pojedinim vezama dodjeljuje određena stanja. Stanja ključna za filtriranje prometa baziranog na Iptables alatu su *NEW*, *ESTABLISHED* i *RELATED*. *NEW* stanje označava pakete koji nisu dio uspostavljene veze i to su obično paketi koji pokušavaju uspostaviti vezu. Nakon što se uspostavi, veza prelazi u *ESTABLISHED* stanje. Ukoliko je neka veza povezana s drugom vezom onda je ta veza označena *RELATED* stanjem. Primjer za takvu vezu je FTP podatkovna veza koja je povezana s FTP kontrolnom vezom. Osim spomenutih postoji i *INVALID* stanje koje označava sve pakete koji se ne mogu identificirati, ili im nije pridruženo niti jedno stanje. Da bi Iptables program za određeni mrežni paket znao u kojem se stanju nalazi, analiziraju se izvorna i ciljna IP adresa, TCP portovi, brojevi TCP sekvenci, te dodatno TCP zastavice mrežnih paketa.
Za svaki paket koji dolazi s nepovjerljive mreže provjerava se koje mu je stanje pridruženo pomoću vatrozidovih internih tablica. Ukoliko je paket dio *ESTABLISHED* ili *RELATED* konekcije paket se prosljeđuje. Ako paketi nisu dio *ESTABLISHED* ili *RELATED* konekcije, a ispravni su i s postavljenom SYN zastavicom, onda su oni dio *NEW* konekcije. Svi se takvi paketi, koji dolaze s povjerljivih mreža, prihvaćaju, a ukoliko dolaze s nepouzdanih mreža odbacuju.
Primjer naredbi koje osiguravaju *stateful inspection*:

```
${IPTABLES} -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
${IPTABLES} -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED
  -j ACCEPT
```

Navedene naredbe definiraju propuštanje svih dolaznih i odlaznih mrežnih paketa koji su dio uspostavljene veze (*ESTABLISHED* i *RELATED* stanja).

## 4.3. Definiranje naredbi filtriranja

Definiranje naredbi za filtriranje mrežnog prometa obavlja se u `/etc/init.d/firewall.rules` skripti. Tu je potrebno prvenstveno pomoću Iptables naredbi definirati sigurnosnu politiku vatrozida. Naredbe je potrebno unositi slijedno pri čemu treba paziti na redoslijed izvršavanja naredbi jer iako je pojedina naredba potrebna i ispravna, ako nije smještena na pravu poziciju u lancu naredbi, ona neće biti funkcionalna.
Testirani sustav kao vatrozid posjeduje predefinirane skripte za mrežnu shemu s dvije spojene mreže (zaštićenom i nezaštićenom) i s tri spojene mreže (zaštićena, nezaštićena i mreža poslužitelja). Linux Devil operacijski sustav omogućava aktiviranje tih predefiniranih skripti, ali prilagodbu je potrebno napraviti modificiranjem glavne skripte. Sustav u predefiniranim skriptama osigurava postojanje naredbi koje osiguravaju *stateful inspection* način rada te pokretanje određenih zaštitnih mehanizama. Administrator treba unijeti sve naredbe kojima želi postići omogućavanje odnosno onemogućavanje određenih servisa i resursa. Primjer naredbe koja omogućava pristup HTTP poslužitelju u DMZ zoni s Interneta:

```
# Definirana lokacija iptables programa
IPTABLES=/usr/sbin/iptables

# Definirana mrežna sučelja
OUT_DEV=eth0  # Internet
INT_DEV=eth1  # Zaštićena mreža
DMZ_DEV=eth2  # DMZ mreža

# Definirana IP adresa i port HTTP poslužitelja
HTTP_SERVER_IP=192.168.1.1   # Skriveni poslužitelj
HTTP_PORT=80  # Port za pristup

# Naredba koja omogućava pristup HTTP poslužitelja s Interneta
${IPTABLES} -A FORWARD -p TCP -i ${OUT_DEV} -o ${DMZ_DEV}
  -d ${HTTP_SERVER_IP} --dport ${HTTP_PORT} -j ACCEPT
```

Konfiguriranje naredbi za vatrozid moguće je napraviti i korištenjem Firewall Builder programa (http://www.fwbuilder.org/). Firewall Builder je program s intuitivnim sučeljem namijenjen izradi pravila za više vrsta vatrozida, pa tako i za Linux vatrozide bazirane na Iptables naredbama.
Osim korištenja Firewall Builder programa, vatrozid je moguće konfigurirati i korištenjem Shorewall skripti. Pomoću različitih skripti kreiraju se Iptables naredbe koje se potom izvršavaju od strane

sustava. Konfiguracijske skripte pozicionirane su u `/etc/shorewall/` direktoriju. Skripta `/etc/shorewall/zones` definira mreže ili tzv. zone na koje je vatrozid spojen pri čemu je i vatrozid jedna zona. Povezivanje mrežnih sučelja s pojedinim zonama obavlja se u skripti `/etc/shorewall/interfaces`. Globalne politike o prihvaćanju ili ne prihvaćanju mrežnih paketa s jedne na drugu zonu definiraju se u skripti `/etc/shorewall/policy`. Iznimke koje odstupaju od globalnih politika definiraju se u `/etc/shorewall/rules` skripti. Uz navedene postoje i druge skripte, ali spomenute su najvažnije za rad vatrozida.

Primjer `/etc/shorewall/zones` skripte:

```
#ZONE      DISPLAY        COMMENTS
net        Net            Internet
loc        Local          Local networks
dmz        DMZ            Demilitarized zone
```

Primjer `/etc/shorewall/policy` skripte:

```
#SOURCE    DEST      POLICY    LOG LEVEL    LIMIT:BURST
loc        net       ACCEPT
net        all       DROP      info
all        all       REJECT    info
```

Primjer `/etc/shorewall/interfaces` skripte:

```
#ZONE    INTERFACE    BROADCAST    OPTIONS
net      eth0         detect       dhcp,norfc1918,blacklist
```

Primjer `/etc/shorewall/policy` skripte:

```
#ACTION    SOURCE      DEST                 PROTO      DEST
ACCEPT     net         dmz:155.186.235.222  tcp        www
ACCEPT     loc         dmz:155.186.235.222  tcp        www
```

## 4.4. Pretvorba i maskiranje mrežnih adresa

Programski alat Iptables osigurava podršku kako za pretvorbu mrežnih adresa (eng. *Network Address Translation*), tako i za maskiranje mrežnih adresa (eng. *Masquerading*). Te funkcionalnosti ostvarene su u PREROUTING i POSTROUTING fazama obrade mrežnih paketa, a uključuju se preko modula sljedećim naredbama:

```
/sbin/modprobe iptable_nat
/sbin/modprobe ipt_MASQUERADE
```

Dio *nat* PREROUTING faze osigurava podršku za promjenu ciljnih adresa (eng. *Destination NAT*), dok *nat* POSTROUTING faze osigurava podršku za promjenu izvornih adresa (eng. *Source NAT*), tj. maskiranje istih. Sve naredbe koje se odnose na promjenu mrežnih adresa unose se u `/etc/init.d/firewall.rules` konfiguracijsku datoteku.

Primjer preusmjeravanja mrežnih paketa pristiglih na mrežno sučelje `eth0` i usmjerenih HTTP port računala s IP adresom `A.B.C.D` na port 8080 računala s IP adresom `A.B.C.E`:

```
${IPTABLES} -t nat -A PREROUTING -p TCP -i eth0 -d A.B.C.D --dport 80
  -j DNAT --to-destination A.B.C.E:8080
```

Promjena ciljnih adresa najčešće se obavlja za mrežne pakete koji su usmjereni na poslužitelje. Pri tome se mogu koristiti mapirane IP adrese i virtualne IP adrese. Korištenjem virtualnih IP adresa sav dolazni mrežni promet preusmjerava se na temelju ciljnog porta dolaznog paketa. Na ovaj način moguće je različite pakete za pojedine mrežne servise (npr. Web, E-mail, FTP), preusmjeriti na odgovarajuće interne poslužitelje koji su zaduženi za navedeni servis. Kod mapiranih IP adresa kompletni se promet upućen na definiranu javnu IP adresu vatrozida prosljeđuje odabranom internom računalu. U ovom slučaju potrebno je posebno odvojiti jednu javnu IP adresu koja će na Internetu zastupati odabrano interno računalo. Nažalost, Linux Devil sustav ne posjeduje predefinirane skripte za podizanje mapiranih sučelja, ali iste je moguće definirati u nekoj od skripti koja se podiže prilikom dizanja sustava ( npr. u `/etc/init.d/firewall.rules`):

```
ifconfig eth0 up
ifconfig eth0:1 A.B.C.D netmask 255.255.255.0 up
route add default gw A.B.C.1 eth0:1
```

Promjena izvornih adresa najčešće se obavlja za mrežne pakete koji imaju IP adrese rezervirane za privatne mreže. Sljedeće dvije naredbe primjer su promjene i maskiranja izvorne adrese mrežnih paketa koje napuštaju računalo preko mrežnog sučelja `eth0` pri čemu se kod SNAT-a paketima dodjeljuje IP dresa `A.B.C.D`, odnosno kod maskiranja se dodjeljuje IP adresa pridružena sučelju `eth0`:

```
# SNAT
${IPTABLES} -t nat -A PREROUTING -p ALL -o eth0 -j SNAT
  --to-source A.B.C.D
# Masquerading
${IPTABLES} -t nat -A PREROUTING -p ALL -o eth0 -j MASQUERADE
```

Osim što NAT tehnologija omogućuje simultano dijeljenje Internet veze između više korisnika, ista ujedno pruža dodatni nivo zaštite, budući da računalima za koje se provodi prepisivanje adresa nije moguće direktno pristupiti izvana (ukoliko to nije eksplicitno dozvoljeno na vatrozidu).

## 4.5. Virtualne lokalne računalne mreže – VLAN

Tehnologija virtualnih LAN-ova omogućava logičko grupiranje korisnika, neovisno o njihovoj fizičkoj lokaciji, u manje logičke cjeline, u tzv. virtualne lokalne računalne mreže (VLAN). Ovakvim pristupom moguće je unutar jednog fizičkog LAN-a kreirati nekoliko manjih, međusobno odvojenih virtualnih LAN-ova, od kojih svaki zadržava svojstva klasične računalne mreže. Svaki virtualni LAN predstavlja jednu *broadcast* domenu, a komunikaciju između pojedinih VLAN-ova moguće je kontrolirati.
Linux sustavi podržavaju VLAN komunikaciju. U tu svrhu potrebno je kreirati posebne skripte, po jednu za svaki pojedini VLAN. Skripte trebaju biti spremljene u `/etc/sysconfig/nic/` direktoriju s nazivima `ifcfg-vlanX` pri čemu `X` označava redni VLAN identifikacijski broj (0-4095).

## 4.6. VPN funkcionalnost

*Virtual Private Networks* (VPN) tehnologija omogućava sigurno povezivanje udaljenih korisnika putem nesigurnog medija kao što je Internet. Moguće je međusobno povezivanje udaljenih lokalnih računalnih mreža (*LAN-to-LAN VPN*) te povezivanje udaljenih mobilnih korisnika s centralnim lokacijama (*Host-to-LAN VPN*). Korištenjem VPN tehnologije moguće je kreiranje sigurnog kanala (eng. *tunnel*) između udaljenih lokacija, gdje se kompletni promet enkripcijom štiti od neovlaštenog promatranja. Ovisno o tome koji se protokol koristi, VPN tehnologija omogućuje autentikaciju korisnika, enkripciju podataka te vjerodostojnost podataka.
Testirani vatrozid posjeduje više različitih poslužitelja koji podržavaju VPN funkcionalnost. Na sustavu je moguće aktivirati PPTDP poslužitelj baziran na P2P (eng. *Point to Point*) protokolu ili L2TPD poslužitelj baziran na (eng. *Layer Two Tunneling Protocol*) protokolu. Također, raspoloživ je i OpenVPN poslužitelj (http://openvpn.net/) baziran na SSL/TLS autentikaciji te IPSec protokolu za kreiranje sigurnog tunela korištenjem UDP paketa. Još jedan od VPN programa zasnovan na UDP protokolu je i CIPE (eng. *Crypto IP Encapsulation*). Osim navedenih VPN poslužitelja raspoloživi su i multifunkcionalni poslužitelj VTUN (http://vtun.sourceforge.net/) te FreeS/WAN VPN baziran na IPSec protokolu (http://www.freeswan.org/).

## 4.7. Praćenje log zapisa

Log zapisi svakako su jedna od najvažnijih komponenti svakog vatrozida. Preglednost i temeljitost log zapisa administratoru u velikoj mjeri olakšavaju održavanje i nadgledanje sustava te poduzimanje odgovarajućih mjera u slučaju detekcije neovlaštenih aktivnosti. Praćenje i analiza log zapisa ostvarena je korištenjem syslog poslužitelja. Pri tome se modificira `/etc/syslog.conf` ili `/etc/syslog-ng/syslog-ng.conf` konfiguracijska datoteka tako da se definira lokacija gdje će se log zapisi pohranjivati.
Na sustavu je predefinirano nezapisivanje log zapisa pa ih je potrebno omogućiti. Prvo je potrebno kreirati određenu particiju na tvrdom disku na koji će se zapisivati log zapisi, a potom omogućiti zapisivanje na istu modificiranjem syslog konfiguracijske datoteke.
Log zapisi zapisuju se samo za one pakete za koje se to odabere prilikom definiranja naredbi obrade mrežnih paketa. Ukoliko se registriranje log zapisa odabere za velik broj pravila tada je potrebno paziti

na raspoloživu veličinu tvrdog diska na koji se ti log zapisi zapisuju jer u suprotnom mogu brzo onesposobiti ili otežati rad vatrozida.
Predefinirano je da se log zapisi spremaju pod *warning* razinom, ali kao što je vidljivo na sljedećoj naredbi moguće je pojedine mrežne pakete spremati pod različitom razinom, tj. u različite datoteke. Navedena naredba zapisuje izvornu i ciljnu IP adresu, TCP sekvencijalni broj te u datoteku umeće prefiks kako bi se znalo o kojoj se naredbi radi.

```
${IPTABLES} -A INPUT -p TCP -j LOG --log-level debug
  --log-tcp-sequence  --log-tcp-options --log-ip-options
  --log-prefix "[FW][INPUT: ACCEPT]"
```

Iptables naredbe za zapisivanje log zapisa preporuča se zapisivati pred naredbom koja će paket odbaciti ili prihvatiti.

## 4.8. Zaštita od neovlaštenih aktivnosti

Linux Devil operacijski sustav iskoristio je određene metode i servise standardne na Linux operacijskim sustavima za zaštitu od neovlaštenih aktivnosti. No, administrator sustava može proširiti postavljene naredbe s novim pri čemu treba modificirati konfiguracijsku datoteku `/etc/init.d/firewall.rules`. U nastavku je dan pregled određenih uobičajenih napada te načini zaštite od istih.
Prvi od napada koji je onemogućen na testiranom sustavu je *Smurf* napad čijim izvršavanjem se postiže tzv. DoS (eng. *Denial of Service*) napad:

```
# stop some smurf attacks.
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
```

Navedena naredba ignorira primljene ICMP *echo request* pakete na *broadcast* adresu cijele lokalne mreže. Kad ne bi postojala navedena zaštita sva računala bi odgovarala na jedno računalo (najčešće poslužitelj) koji bi zbog toga bio onesposobljen za funkcionalan rad. Zaštita se može postići i Iptables naredbom koja u potpunosti zabranjuje ICMP *echo request* pakete.
Linux operacijski sustavi raspolažu i sa zaštitom od promjene rute paketa (eng. *Source routing*). Definiranjem rute paketa pošiljatelju je omogućeno da definira kojim putem će mrežni paket putovati do odredišta te kojim putem će se vratiti. Time pošiljatelj može zavaravati ciljano računalo da komunicira s drugim računalom. Zaštita se postiže sljedećom naredbom:

```
# Don't accept source routed packets.
echo "0" > /proc/sys/net/ipv4/conf/all/accept_source_route
```

*Syn-Flood* napad zasniva se na napadačevom slanju velikog broja početnih TCP paketa koji imaju postavljenu SYN zastavicu, i ignoriranjem TCP odgovora s postavljenim SYN i ACK zastavicama. Time su resursi ciljanog računala zaokupljeni odgovaranjem na pakete. Za sprečavanje ovakvog oblika napada moguće je na vatrozidu ograničiti broj dolazećih TCP paketa s postavljenom SYN zastavicom:

```
${IPTABLES} -A INPUT -p TCP –syn -m limit  --limit 45/minute
   -j ACCEPT
${IPTABLES} -A FORWARD -p TCP --syn --limit 30/second
   -j ACCEPT
```

Linux operacijski sustav također raspolaže sa zaštitom od *SYN-Flood* napada, a ista se može uključiti sljedećom naredbom:

```
# Syncookies
echo "1" > /proc/sys/net/ipv4/tcp_syncookies
```

Paketi bez zastavica mogu biti indikacija napada pregledavanja otvorenih portova i može se onemogućiti sljedećom naredbom:

```
${IPTABLES} -A bad_tcp_packets -p tcp --tcp-flags ALL NONE -j DROP
```

*IP Spoofing* napad, koji omogućava prosljeđivanje paketa s vanjskog sučelja na neko od internih računala ukoliko napadač kao izvornu adresu uzme neku od adresa unutar lokalne mreže također se može onemogućiti na slijedeći način:

```
# Stop IP spoofing,
for interface in /proc/sys/net/ipv4/conf/*/rp_filter; do
       echo "1" > $interface
done
```

Na Internetu se često koriste ICMP *redirect* paketi koji usmjerivačima definiraju rute do određenih mreža. Ukoliko napadač uspije modificirane pakete poslati usmjerivaču, isti bi krivo prosljeđivao mrežne pakete. Stoga je na sustavu predefinirano ukinuto prihvaćanje spomenutih ICMP mrežnih paketa:

```
# Stop ICMP redirect
for interface in /proc/sys/net/ipv4/conf/*/accept_redirects; do
      echo "0" > ${interface}
done
```

### 4.9. Ostale sigurnosne funkcionalnosti sustava

Osim spomenutih sigurnosnih opcija, sustav podržava i druge funkcionalnosti koje pospješuju sigurnost mreže. Ukoliko se sustav koristi kao mail poslužitelj, administratoru je na raspolaganju Postfix s SSL/TLS podrškom konfiguriran za rad u *chroot* okruženju. Za pristup korisničkoj elektroničkoj pošti koristi se Dovecot IMAP mail poslužitelj. Mail poruke moguće je i filtrirati te odbacivati nepoželjne. Spam poruke moguće je odbacivati korištenjem SpamAssasin programa, dok je mail poruke inficirane virusima i sličnim malicioznim programima moguće filtrirati korištenjem Clam Antivirus programa. Također, za zaštitu od mail poruka inficiranih virusima i sličnim malicioznim programima moguće je koristiti i antivirusni program Sagator.

Na sustavu je raspoloživ i Snort, alat za detekciju mrežnih malicioznih aktivnosti (eng. *IDS - Intrusion Detection System*). Njegovom primjenom moguće je detektirati razne napade (CGI napadi, napadi bazirani na prepisivanju spremnika i sl.) i nedozvoljena skeniranja (skeniranje portova, detektiranje operacijskih sustava).

Sustav posjeduje programe za praćenje mrežnog prometa. Ntop je napredni mrežni analizator koji pokazuje mrežnu iskorištenost, dok Net-Acct radi kao poslužitelj koji zapisuje mrežni promet u obliku log zapisa. Stoga je za njegovo korištenje potrebno posjedovati tvrdi disk na koji će se podaci moći zapisivati.

## 5. Zaključak

Glavna prednost Linux Devil operacijskog sustava je što se sustav podiže i izvršava u potpunosti s CD-ROM ili slične jedinice. Time je razina sigurnosti višestruko podignuta. Zlonamjerni napadač, čak i ako uspije preuzeti kontrolu nad sustavom, ne može trajno sačuvati svoje modifikacije. Konfiguracijski podaci nepromijenjeno se mogu čuvati na "zaključanom" USB priključku ili disketi, a mogu se čak trajno ukomponirati u sam kod sustava na CD-ROM mediju. Takav način zaštite konfiguracijskih podatka bolji je od svih drugih programskih zaštitnih izvedbi.

Sustav ujedno može biti veoma koristan jer raspolaže brojnim poslužiteljskim servisima. Stoga je moguće konfigurirati sustav kao dobro zaštićeni poslužitelj.

Osnovna mana cijelog sustava je način konfiguracije. Raspoloživo konfiguracijsko sučelje System Configurator korisno je isključivo za pokretanje ili gašenje određenih servisa. Svu ostalu konfiguraciju potrebno je obaviti modificiranjem konfiguracijskih datoteka. Iz tog razloga administrator sustava treba biti iskusni Linux korisnik. To je osobito važno kod definiranja Iptables naredbi za filtriranje mrežnog prometa te pretvorbu mrežnih adresa. Pri definiranju naredbi osobitu pozornost treba posvetiti redoslijedu naredbi jer ukoliko se naredbe ne navedu u ispravnom redoslijedu vatrozid neće raditi na ispravan način.