18.12.2006
HF - “Redrum”
maoanimal(cat)gmail.com

# Netin jakaminen Linuxin ja Shorewall-palomuurin avulla

## 2. Sisällysluettelo



Huom! Tämän dokumentin ohjeita saa käyttää vain omalla vastuullasi. En vastaa mahdollisista ongelmista jos niitä ilmentyy. Vikatilanteissa suosittelen http://forums.gentoo.org foorumia, jonka kautta voin yrittää auttaa parhaani mukaan.

## *3. Esipuhe*

Tämän dokumentin tarkoituksena on valaista sitä, miten Linux koneesta voi tehdä palomuurikoneen joka jakaa Internetliittymää lähiverkolle. Lisämausteena kerron pikaisesti miten helposti samaan koneeseen saa päälle DHCP-palvelun, jotta lähiverkon koneisiin ei laittaa käsin asetuksia. Lähtökohtana pidän kuitenkin sitä että lukija tuntee hieman Linux-käyttöjärjestelmää, osaa asentaa sen ja siihen ohjelmia sekä osaa käyttää komentokehotetta tekstieditorin kera. Lisäksi lukijan tulee tietää IP-verkkojen sielunelämää. Lopputuloksena on helposti ylläpidettävä tehokas verkonjakomenetelmä.

## *4. Vaatimukset*

Jotta palomuurisovellus ja verkon jakaminen toimisi, on vaatimukset täytettävä koneen sekä käyttöjärjestelmän osalta. Lisäksi on hyvä pohtia lähiverkon nopeusluokka käyttötarpeen mukaan riittäväksi.

### 4.1 Laitteisto

Minimissään jopa Pentium-tasoinen tietokone riittäisi palomuurikoneeksi. Mutta kun nykyliittymien nopeudet nousevat tiheään tahtiin ja käyttömukavuus on tärkeää, suosittelisin Pentium 3 tason konetta. Yleisinä vaatimuksina koneeseen vaaditaan verkkokortti lähiverkkoon ja toinen kortti riippuen omistajan Internetliittymästä eli esimerkiksi ADSL-modeemi. Esimerkeissä käytän järjestelmää kahdella verkkokortilla, joista toinen on kytkettynä ulkoiseen modeemiin. Keskusmuistia olisi hyvä olla ainakin 256mb ja kovalevytilaa vähintään 5 gigaa, jotta muuttuville lokitiedostoille olisi tilaa vielä swap-osionkin jälkeen.

### 4.2 Lähiverkko

Lähiverkon taas olisi hyvä olla tasoa 10/100 Mbps. Nykyisin yleistymässä oleva liittymän nopeusluokka, 8 Mbps, venyttää periaatteessa jo10 Mbps lähiverkon äärirajoilleen. Vapaata kapasiteettia olisi hyvä olla, koska on todennäköistä että Internetin ja palomuurin takana olevien koneiden välillä kulkee paljon pieniä paketteja moniin eri osoitteisiin. Tämä synnyttää paljon piilossa olevaa liikennettä joka rasittaa verkkoa, muttei näy varsinaisesti Internetin nopeudessa, toisin kuin klassisesti ajateltuna tiedon lataaminen vain yhdestä kohteesta.

**HUOM!** Varoituksen sana langattomien verkkojen käyttäjille: Jos lähiverkossa on langaton tukiasema käytössä, on sen asetukset parasta tarkastaa. Lähiverkkoon ei saa päästää asiattomia tai kaikki turva-asetukset ovat turhia. Palomuuri ei toimi jos sen pystyy kiertämään ilman estoja!

Esimerkissäni käyttämäni verkon perustiedot:

– eth0: Ulkoinen verkko WAN(modeemi): Dynaamisesti (DHCP) haettu palveluntarjoajan toimittama IP-osoite.
– eth1: Sisäinen verkko LAN(verkkokortti): Kiinteä osoite 196.168.0.1
– Internetistä katsottuna kaikki lähiverkon koneet käyttävät palomuurin osoitetta.

### 4.3 Ohjelmisto

Käyttöjärjestelmänä käy mikä tahansa Linux distribuutio. Minimissään kernelivaatimuksena on versio 2.4, mutta uusin 2.6:n vakaa versio on suositeltava. Palomuuriohjelmana toimii Shorewallin uusin versio 3. Käytän tekstin esimerkissä kernelin versiota 2.6.16. Jos asennat kernelin käsin, täytyy siitä aktivoida liitteiden 1 ja 2 mukaiset optiot. Jos asentaminen lankeaa jonkin automaattisen kernelinluontityökalun käsiin, on tarkistettava onko nämä optiot päällä ja jos ei ole, niin ne on ladattava moduuleina. Useimmiten Internetin jakamisongelmat johtuvat juuri puutteellisesta kernelituesta.

## *5. Palomuurikone*

Palomuurin ideanahan on se, että se estää kaiken turhan liikenteen ulkoisen verkon eli Internetin ja oman lähiverkon välillä. Palomuuri yksin ei kuitenkaan takaa täysin ötökkä- ja ilkimysvapaata aikaa. Verkon heikoin lenkki on yleensä käyttäjä, joka sallii turhan liikenteen tai hakee ulkoisesta verkosta vahingossa haittaohjelmia. Kotikäytössä oleva nettiä jakava palomuurikone ottaa yleensä monia rooleja kotiverkossa. DHCP-, Samba-, aika-, tiedosto-, WWW- ja muut palvelut ovat yleisiä ja ymmärrettäviä. Palomuurikoneessa ei kuitenkaan ideaalitapauksessa saisi olla mitään muuta palvelua päällä, kuin palomuuriohjelma. Jokainen palvelu on lisäaukko turvallisuudelle. Jokainen palvelu vaatii yleensä oikeuksien myöntämistä ja lisää mahdollisuuksia päästä palomuurin läpi. Esimerkissäni asennan netin jakamisen lisäksi vain DHCP-palvelun helpottaakseni mielikuvitusverkon omistajan elämää.

### 5.1 Turvallisuus

Turvallisuuteen kuuluu kuitenkin muitakin seikkoja, kuin vain palomuuriohjelmaan liittyvät. Tärkeimmät ovat salasanaturvallisuus ja fyysinen sijainti. Koneen käyttäjien salasanojen pitää olla kunnollisia. Palomuurikoneen pitää lisäksi olla sellaisessa paikassa jossa siihen ei pääse käsiksi, sillä jos koneeseen pääsee käsiksi kuka tahansa, niin järjestelmänvalvojan tunnus on helposti muutettavissa. Kun kuitenkin puhutaan kotikäytössä olevasta palvelimesta, niin on fyysisen turvallisuuden käsite tietenkin suhteellinen. Jos ei pysty samassa asunnossa asuviin luottamaan, niin keneen sitten.

Jälleen yksi ideaalinen periaate on, että kaikki liikenne, jopa lähiverkossa tapahtuva sallitaan vain tarpeen mukaan. Esimerkissä kuitenkin käytän mallia jossa palomuurin takana olevilla koneilla on vapaa pääsy lähiverkkoon ja ulospäin Internetiin. Vain sisäänpäin tulevat portit ovat estettyjä. Kyse on käyttömukavuudesta ja siitä luottaako lähiverkon käyt-

täjiin. Jos haluaa rajoittaa esimerkiksi perheen lapsien netin käyttökohteita, on se erittäin helppoa palomuurin asetuksilla, vaikka konekohtaisesti.

On tärkeää muistaa, ettei esimerkin malli poista tarvetta suojata lähiverkon koneita omilla palomuureilla ja virusohjelmalla. Koska palomuurikoneen tehtävä on vain jakaa verkkoa ja suojata liikennettä, se ei seuraa tarkasti mitä tavaraa lähiverkon ja Internetin välillä kulkee. On olemassa ohjelmia jotka voivat seurata liikennettä, mutta ne saattavat olla hankalia asentaa niin hyvin että ne huomaisivat kaiken haitallisen. Lisäksi tällaiset ohjelmat tuppaavat olemaan raskaita ja vaativat yleensä isoja tietokantoja. Ne toimivat tavalleen kuten palveluntarjoajan välityspalvelimet jotka tallettavat tiedon ensin omalle kiintolevylle ja jakavat sitä verkkoon tarvittaessa.

## *6. Shorewall versio 3*

Shorewall on eräänlainen päällinen tutulle iptables-palomuuriohjelmalle. Se yksinkertaistaa asennuksen, käyttöönoton ja sääntöjen hallinnan. Asentaminen nykypäivän pakettihallinnalla pitäisi olla helppoa. Kaikki Shorewallin asetustiedostot sijaitsevat /etc/shorewall hakemistossa, jossa jokaiselle eri asetuksen osa-alueelle on oma tiedostonsa. Yksi erittäin hyvä puoli näissä tiedostoissa on se, että niissä on kattavat ohjeet asetuksista esimerkkeineen. Komentoja ei siis välttämättä tarvitse muistaa ulkoa vaan muistia voi virkistää joka kerta kun tekee uutta sääntöä palomuurille. Tämä alentaa huomattavasti normaalin käyttäjän käyttöönottokynnystä.

Shorewall siis jakaa asetukset moneen tiedostoon. Tämä saattaa kuulostaa oudolta, mutta siihen on syynsä. Asetukset pysyvät omissa ”huoneissaan”, tiedostot pysyvät siisteinä eikä niitä voi vahingossa muuttaa kun myöhemmin vaihtaa palomuurin sääntöjä. Lisäksi on huomattava että asennuksen jälkeen käytetään oikeastaan vain yhtä tiedostoa, joten kaikkien asetusten sullominen yhteen tiedostoon olisi turhaa.

### 6.1 Lokitaso

Asetustiedostoissa määritetään myös lokitaso. Omasta käytännön kokemuksesta tasot kannattaa pitää critical-tasolla, jolloin vain kaikkein kriittisimmät tapahtumat kirjautuvat lokitiedostoon. Jos tason pitää vakiona eli info-tasolla, kirjoittaa ohjelma miltei kaiken ylös eli useita tapahtumia sekunnissa. Seurauksena on se että järjestelmän lokitiedosto paisuu ja muuttuu lukukelvottomaksi. Tämä saattaa myös rasittaa konetta. Ohjelmassa on kuitenkin mahdollisuus määrittää rajoitin määrälle jota se kirjoittaa tietyllä aikavälillä.

Joka tapauksessa koneessa pitää olla asennettuna palvelu joka kierrättää lokitiedostoja, jotta tiedostojen koko ei pääse kasvamaan liian suureksi. Suosittelemani critical-taso soveltunee useimpien käyttäjien tarpeeseen, sillä en usko että peruskäyttäjä tarkkailisi säännöllisesti verkon lokitietoja. Jos critical-tasolla lokiin kirjautuu tietoa, on syyn selvittämisen arvoista. Kyseessä voi olla jopa hyökkäys konetta kohtaan, joka on nykyään valitettavan yleistä.

## 6.2 /etc/shorewall/shorewall.conf

Tässä tiedostossa sijaitsevat kaikki yleisen tason asetukset. Tiedostosta tarvitsee muuttaa kaikki lokitasot edellä mainitsemaani critical-tasoon. Tiedosto on hyvä lukea läpi että asetukset ovat varmasti oikein omaa verkkoa ajatellen, vaikka perusasetukset ovatkin yleisesti pätevät. Kaksi tärkeää kohtaa täytyy joka tapauksessa muuttaa.

```
– IP_FORWARDING=On
– STARTUP_ENABLED=Yes
```

Näistä ensimmäinen sallii IP-osotteiden eteenpäin lähetyksen eli Internetin jakamisen. Toinen on Shorewallin kehittäjien tapa saada ihmiset lukemaan tiedosto läpi ennen palomuurin käynnistämistä eli arvo pitää muuttaa että palomuuri käynnistyy.

## 6.3 /etc/shorewall/zones

Ensin määritetään oman verkon alueet joita käytetään myöhemmin muissa asetuksissa. Käytännössä siis luodaan helposti muistettavat nimet ja määritetään mitä niillä tarkoitetaan.

```
#ZONE    TYPE     OPTIONS                 IN                    OUT
#                                         OPTIONS               OPTIONS
fw       firewall
net      ipv4
loc      ipv4
```

Käyttäen vakionimiä, koska niitä käytetään läpi Shorewallin dokumentaation: fw on siis palomuuri, net tarkoittaa Internettiä ja loc on lähiverkko. Molemmat verkonalueet käyttävät IP-protokollaa versio 4 eli perinteistä osoiteavaruutta.

## 6.4 /etc/shorewall/policy

Tässä tiedostossa määritetään runko, jonka päälle palomuurin säännöt luodaan.

```
#SOURCE     DEST        POLICY      LOG LEVEL
loc         net         ACCEPT
net         all         DROP        crit
all         all         REJECT      crit
```

Edellisessä kohdassa määritetyt lyhenteet ovat käytössä. Tässä siis määritetään se että kaikki liikenne lähiverkosta (loc), on sallittua Internetiin (net). Seuraavaksi määritetään että kaikki liikenne Internetistä on kielletty. Lopuksi on tärkeä asetus jolla määritetään että kaikki muut liikenne on kielletty kumpaakin suuntaan, tällöin kaikki mahdollinen liikenne tulee mukaan sääntöihin. Poikkeustapauksia tai oikeuksia liikenteeseen määritetään myöhemmin erillisessä rules-tiedostossa eli lisäsääntöjä voi luoda vaikka tässä viimeiseksi kaikki kiellettiinkin.

**HUOM!** Tässä asetuksessa palomuurikone ei pääse Internetiin käsiksi ilman että se erikseen määritetään myöhemmin. Hyödyllinen sääntö saattaisi olla sallia palomuurikoneen pääsy päivityksien hakuun. Tietenkin turvallisempaa olisi hakea päivitykset erillisellä koneella, tarkistaa ne ja sitten kopioida ne palomuurikoneelle.

## 6.5 /etc/shorewall/interfaces

Seuraavaksi tarvitsee määritellä palomuurikoneen verkkoadapterien asetukset. Tiedostossa määritetään yksinkertaisesti se, mikä lyhenne liitetään mihinkin verkkoadapteriin. Samalla määritetään niiden ominaisuudet:

```
#ZONE   INTERFACE       BROADCAST       OPTIONS
net     eth0            detect          dhcp,tcpflags
loc     eth1            192.168.0.255   dhcp
```

Tässä sidotaan eth0-adapteri Internetiin ja eth1-adapteri lähiverkkoon. Ulkoverkon lähetysosoite saadaan palveluntarjoajalta ja lähiverkon osoite tiedetäänkin. Lisäksi molemmille voi määritellä optioita, jotka löytyvät myös interfaces-tiedostosta selityksineen. Esimerkissä sallin molemmille liittymille DCHP liikenteen, koska ulkoinen osoite haetaan sillä ja palvelimeen tullaan asentamaan DHCP-palvelu joka kuuntelee lähiverkkoa. Lisäksi määritin ulkoiseen liittymään tcpflags option joka tarkistaa sisään tulevat paketit tunnettuja ja yleisiä haittatunnisteita vastaan.

## 6.6 /etc/shorewall/masq

Tässä tiedostossa määritetään NAT:n käyttö. Tavoitteena on siis että ulospäin näkyy vain 1 kone, vaikka palomuurikoneen takana olisi kymmeniä koneita. Tiedostossa voisi esimerkiksi määrittää, vaikka mihin jonkin koneen ulossuuntaavat paketit menevät. Esimerkin tarkoitukseen riittää että tiedostoon lisätään vain 1 rivi:

```
#INTERFACE      SUBNET          ADDRESS         PROTO   PORT(S) IPSEC
eth0            eth1
```

## 6.7 /etc/shorewall/rules

Tässä tiedostossa määritellään ne erikoistapaukset jotka jäivät zones-tiedoston määrittelyn ulkopuolelle. Esimerkkitapauksessa tiedostoon ei tarvitse tehdä mitään muutoksia, koska erikoistapauksia ei ole. Jopa myöhemmin asennettava DHCP-palvelu määritettiin jo interfaces-tiedostossa. Listaan kuitenkin pari yleistä esimerkkiä. Tässäkin tiedostossa on hyvät ohjeet ja malliesimerkit apuna, mutta myös Internetistä Shorewallin kotisivuilta löytyy paljon apua tarvittaessa.

```
#ACTION SOURCE          DEST            PROTO   DEST
#                                               PORT
DNAT    net             loc:192.168.0.2 tcp     80
ACCEPT  $FW             net             tcp     80
```

Ensimmäinen sääntö kertoo palomuurille, että sen pitää lähettää kaikki TCP-protokollan porttiin 80 tuleva liikenne lähiverkon osoitteeseen 192.168.0.2. Tämä siis toimisi tapauksessa jos osoitteessa 192.168.0.2 olisi WWW-palvelin. Ulospäin näyttäisi että palvelin olisi palomuurikoneessa. Toinen sääntö antaisi luvan palomuurikoneella lähettää ulos TCP-protokollan porttiin 80 eli selata Internetsivuja. Samaan tapaan voisi sallia aiemmin mainitun pääsyn päivityspalveluun.

### 6.8 Shorewallin käynnistys

Sitten tarvitseekin vain käynnistää palomuuri komennoilla:

| | |
|---|---|
| >shorewall start | = Käynnistää palomuurin |
| >shorewall stop | = Pysäyttää palomuurin |
| >shorewall restart | = Käynnistää palomuurin uudelleen (hyödyllinen jos muuttaa sääntöjä) |

Tietenkin palomuuripalvelu pitää lisätä koneen käynnistyslistaan:

```
>rc-update add shorewall default
```

### 6.9 Asetuksista

Nyt päällä pitäisi olla siis täysin toimiva, Internetiä jakava palomuurikone. Esimerkin asetukset ovat kuitenkin vain raapaisu Shorewallin tai Linuxin ominaisuuksiin tällä saralla. Lisää ominaisuuksia haluaville löytyy Shorewallin kotisivuilta, joilla voi muokata palomuurin haluamakseen.

## *7. Dnsmasq DHCP-palvelu*

DHCP-palvelun asentaminen palomuurikoneeseen on ideaaliselta kannalta turhaa, mutta helpottaa elämää. Käytännössä siis kaikki lähiverkkoon liitettävät koneet voivat hakea IP-osoitteen automaattisesti palomuurikoneelta. Tämä ei kuitenkaan estä manuaalista IP-osoitteen määrittämistä. Asetankin palvelun jakamaan osoitteita 192.168.0.10 ja 192.168.0.20 väliltä. Tällöin voin varata muut alueen (eli vaikka 192.168.0.1 – 192.168.0.9) osoitteet kiinteille koneille, mutta samalla ei ole tarvetta pitää kirjaa jokaisen liikkuvan koneen verkkoasetuksista.

### 7.1 Asennus

Tarvitsee vain asentaa Dnsmasq-ohjelma järjestelmän pakettihallinnalla ja sen jälkeen editoida tiedostoa /etc/dnsmasq.conf. Tiedostossa on vakioasetukset valmiina jolla se toimii useimmista tapauksista. Käyttäjää esimerkkitapauksessa kiinnostaa vain 2 kohtaa tiedostosta (jotka löytyvät helpoiten editorin search-komennon avulla):

```
dhcp-range=192.168.0.10,192.168.0.20,12h
```

```
Jossa ensimmäinen osoite on alueen alku ja seuraava osoite loppu. Lopussa on vielä aika, jonka ajan palvelu varaa osoitetta tietylle koneelle.
```

```
interface=eth1
```

Tämä kertoo palvelulle sen että se kuuntelee vain lähiverkkoa. Jos tähän unohtaa arvon ”eth0”, yrittää kone jakaa osoitteita ulkoverkkoon, joka estää toiminnan ja saattaa olla erittäin vaarallista turvallisuuden kannalta.

Sitten palvelu tarvitseekin vain käynnistää ja lisätä palomuurikoneen automaattiseen käynnistyslistaukseen:

```
>/etc/init.d/dnsmasq start
>rc-update add dnsmasq default
```

Ongelmatapauksissa apua löytyy esimerkiksi osoitteesta:
http://www.thekelleys.org.uk/dnsmasq/doc.html

## *8. Loppusanat*

Netin jakaminen on helppoa, kunhan hieman näkee vaivaa sisäistääkseen yhden palomuuriohjelman. On tärkeää suunnitella kotiverkko ennen sen toteuttamista. Mitkä koneet vaativat pääsyä ja minne? Tarvitseeko liikennettä sallia kaikille koneille? Ennen asennusta olisi siis hyvä istahtaa alas paperin ja kynän kanssa suunnittelemaan. Ohjelmavaihtoehtojahan on paljon, kuten esimerkin tekstipohjalla toimiva esimerkin Shorewall tai vaikka graafisella liittymällä varustettu Firestarter, jotka molemmat tosin perustuvat iptables-ohjelman käyttöön. Valita useimpien kohdalla varmaan päätyy siihen joka maistuu parhaimmalta omasta mielestä, mutta Shorewallilla on etunsa. Se ei vaadi graafista käyttöliittymää eli on kevyt ja vakaa, se on helppo omaksua ja on helppokäyttöinen. Kunhan vain muistaa mahdolliset tietoturvariskit.

Kenelle sopii Linux-kone palomuurina käyttöön? Helpompaa olisi ostaa kaupasta noin 100€ hintaluokkaan saatava modeemi, joka jakaa Internetiä, jossa on palomuuri ja DHCP-palvelu. Ajankohtaisesti ajateltuna se vie vielä vähemmän sähköäkin. Linux palomuurikone tuleekin kyseeseen siinä tapauksessa, jos kotona on kone joka on jatkuvassa käytössä esimerkiksi mediakeskuksena ja samaan koneeseen voi integroida useita palveluita. Ideaalisesti ajateltuna, näin ei saisi tehdä. Mutta uskon, että jos suunnitteluun käyttää hieman aikaa niin turvallisuusongelmilta voi välttyä.

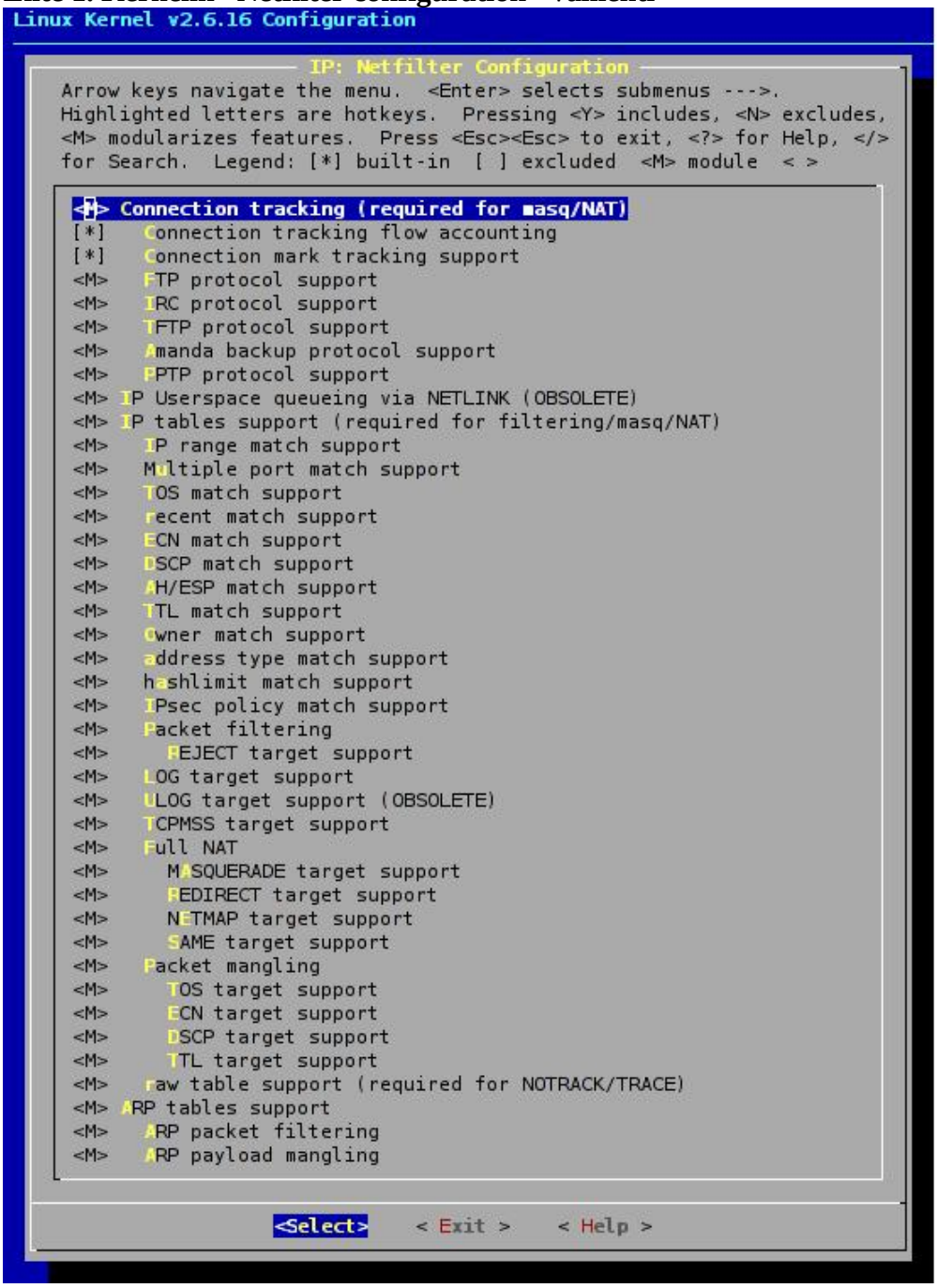
## *9. Lähteet*

1. Shorewallin kotisivujen asennusohje (http://www.shorewall.net/two-interface.htm)
2. Shorewallin kernelohje (http://www.shorewall.net/kernel.htm)
3. Gentoo Linuxin router guide (http://www.gentoo.org/doc/en/home-router-howto.xml)

## *10. Liitteet*

Kuvat lainattu www.shorewall.net sivuilta.

**Liite 1. Kernelin ”Netfilter configuration”-välilehti**



**Liite 2. Kernelin ”Core Netfilter”-välilehti**