Iiro Auvinen

Reititin- ja palomuurikäyttöjärjestelmä Pfsensen käyttöönotto

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

6.5.2013

Metropolia

Tekijä Otsikko Sivumäärä Aika	Iiro Auvinen Reititin- ja palomuurikäyttöjärjestelmä Pfsensen käyttöönotto 36 sivua + 1 liite 6.5.2013
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkot
Ohjaaja	lehtori Erik Pätynen

Insinöörityön tarkoituksena on perehtyä ja käyttöönottaa avoimeen lähdekoodiin perustuva reititin- ja palomuuri-käyttöjärjestelmä. Alustana käytettiin Pfsense-distribuutiota, joka on FreeBSD-pohjainen käyttöjärjestelmä. Insinöörityö pyrittiin kirjoittamaan niin, että lukija pystyy sen avulla onnistuneesti käyttöönottamaan Pfsense-järjestelmän.

Pfsense on suosittu ja helppokäyttöinen tietoturvaratkaisu, ja sitä käytetään paljon koti-, yritys- ja yliopistoympäristöissä. Pfsensen hienous perustuu sen tehokkuuteen ja siihen, että sen käyttö ei vaadi tietämystä FreeBSD-alustasta.

Järjestelmä toteutettiin kotiympäristöön mahdollisimman kustannustehokkaasti, käyttäen suurimmaksi osaksi vanhoja tietokoneen osia. Projektissa otettiin käyttöön Pfsensen ohella Squid- ja HAVP-välityspalvelin sekä Snort-tunkeutumisenestosovellus, jotka osoittautuivat ilmaisien tunnistuskantojen kanssa kotikäyttäjälle riittäviksi.

Projekti osoitti, että Pfsense ohittaa suorituskyvyn ja ominaisuuksien osalta osan halvemmista kaupallisista laitteista, koska osa kehittyneimmistä ominaisuuksia löytyy vain kalleimmista kaupallisista laitteista. Koska Pfsense on ilmainen ja vain tekninen tuki on maksullista, on Pfsensen hinta-laatusuhde huippuluokkaa, vaikkakin käyttö yritysympäristössä vaatii investointia kaupalliseen Antivirus-ohjelmistoon ja tunkeutumisenesto-sääntökantoihin.

Avainsanat	UTM, palomuuri, reititin, Pfsense

Author Title Number of Pages Date	Iiro Auvinen Deploying Pfsense router and firewall operating system 36 pages + 1 appendix 6 May 2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data networks
Instructor	Erik Pätynen, Senior Lecturer

The purpose of this thesis is to describe how an open source router and firewall operating system is deployed. The chosen platform was Pfsense distribution which is a FreeBSD based operating system. The thesis was written so that the reader could easily deploy the Pfsense system after having read this thesis.

Pfsense is a popular and easy to use security solution and it is widely used in home, corporate and university environments. The magnificence of Pfsense is based on its performance and that the usage does not require knowledge of the underlying FreeBSD platform.

The system was deployed in home environment as cost effectively as possible, using mostly old computer parts. In addition to Pfsense, Snort IPS and HAVP proxy were deployed, which proved to be sufficient to home users when using free signature databases.

The results showed that Pfsense outruns some of the cheaper commercial products with features and performance because some of the advanced features are usually found only on the most expensive commercial products. Because Pfsense is free and only the technical support is charged, the quality-price ratio is excellent although usage in corporate environment requires investing in a commercial antivirus program and IPS rules.

Keywords	UTM, Firewall, Router, Pfsense

Sisällys

Lyhenteet

AD	*Active Directory*. Windows-käyttäjätietokanta ja hakemistopalvelu.
b	Bitti. Pienin informaation yksikkö.
B	Tavu. Kahdeksan bitin muodostama informaation yksikkö.
CIDR	*Classless Inter-Domain Routing*. Luokaton reititys.
DOS	*Denial Of Service*. Palvelunestohyökkäys.
FMS	*Firewall Maximum States*. Palomuurin tilataulussa sijaitsevien yhteyksien maksimimäärä.
FMT	*Firewall Maximum Tables*. Palomuurin tilataulujen maksimimäärä.
FMTE	*Firewall Maximum Table Entries*. Palomuurin tilataulujen tietueiden maksimimäärä
LFUDA	*Least Frequently Used with Dynamic Aging*. Tiedonvarastointi käytäntö, jossa vähiten käytetyt ja pisimpään säilytetyt tieto korvataan uudella tiedolla.
LDAP	*Lightweight Directory Access Protocol*. Hakemistopalvelujen verkkoprotokolla
Mb/s	Megabittiä sekunnissa. Tiedonsiirtonopeuden mittayksikkö.
NAT	*Network Address Translation*. Osoitteenmuunnos-tekniikka
TCP	*Transmission Control Protocol*. Tiedonsiirto-protokolla.
UDP	*User Datagram Protocol*. Yhteydetön tiedonsiirto-protokolla.

1 Johdanto

Kuluttajille soveltuvia kohtuuhintaisia tietoturvalaitteita on markkinoilla verrattain vähän, koska kunnolliset tietoturvalaitteet ovat usein kalliita ja monimutkaisia. Kuluttajille suunnattujen verkkolaitteiden, kuten tukiasemien, tietoturva on lähinnä nimellistä ja monelle, varsinkin Windows-ympäristöön kasvaneiden, kynnys käyttää avoimeen lähdekoodiin perustuvia käyttöjärjestelmiä voi olla suuri.

Insinöörityön tavoitteena on perehtyä ja käyttöönottaa avoimeen lähdekoodiin perustuva Pfsense reititin- ja palomuurikäyttöjärjestelmä. Valinnassa käytin suurimpana kriteerinä käyttöjärjestelmän helppokäyttöisyyttä ja sitä, että käyttö ei vaadi pohjalla toimivan alustan eli FreeBSD:n tuntemusta. Toinen kriteeri oli, että valitsemani käyttöjärjestelmä soveltuu koti- ja yrityskäyttöön. Järjestelmä rakennettiin kotiympäristöön mahdollisimman kustannustehokkaasti käyttäen ylimääräiseksi jääneitä vanhoja tietokoneen osia.

Insinöörityö raapaisee vain pintaa siitä, mihin kaikkeen Pfsense-käyttöjärjestelmä todellisuudessa pystyy. Työ kirjoitettiin niin, että sen avulla lukija voi onnistuneesti ottaa käyttöön kyseisen käyttöjärjestelmän ja siltä pohjalta jatkaa tutustumista tietoturvan maailmaan.

Konfiguroinnit ovat suuntaa antavia, eivätkä ne takaa täydellistä tietoturvaa, riippuen tietysti verkon fyysisestä ja loogisesta rakenteesta, käytettävistä palveluista ja Pfsenseen asennetuista moduuleista.

2 Pfsensen ominaisuudet ja laajennuspaketit

2.1 Pfsensen historia

Pfsense sai alkunsa vuonna 2004 Chris Buechlerin ja Scott Ullrich toimesta [1]. Idea lähti m0n0wall-nimisestä projektista, joka oli myös FreeBSD-pohjainen sulautettuihin järjestelmiin keskittynyt palomuurikäyttöjärjestelmä [1]. Pfsensen ensimmäinen versio 1.0 julkaistiin vuoden 2006 lokakuussa ja 5 vuotta ensijulkaisun jälkeen julkaistiin versio 2.0 [14]. Pfsense-projekti kulki aluksi nimettömänä, mutta myöhemmin Scott keksi nimen Pfsense, jossa alkukirjaimet pf tulevat sanoista packet filtering eli pakettisuodatus [2].

2.2 Yleiset ominaisuudet

Pfsense on tilallinen palomuuriratkaisu, eli se pitää kirjaa kaikista TCP- (Transmission Control Protocol) ja UDP (User Datagram Protocol)-yhteyksistä ja näin ollen joko sallii tai kieltää yhteydet, riippuen palomuuri määrittelyistä [3]. Pfsense ei itsessään ole pelkästään palomuuri, vaan siitä löytyy myös monia reititin- ja palvelinsovelluksia. Työssä on esitelty vain käytetyt ominaisuudet.

Pfsense sisältää NAT:n (Network Address translation), joka kääntää sisäverkon osoitteet ulkoverkon osoitteiksi [3]. NAT:in avulla useat sisäverkon käyttäjät voivat käyttää ulkoverkkoa yhden tai useamman ulkoverkon IP-osoitteen takaa.

CARP:illa (Common Address Reduncancy Protocol) voidaan luoda klustereita kahdesta tai useammasta Pfsense laitteesta [3]. Klusterin pääasiallinen tarkoitus on tuoda vikasietoisuutta verkkoon. Jos klusterin yksi jäsen kaatuu, käyttäjien liikenne kierrätetään automaattisesti toista kautta. Klusterin jäsenet voivat myös jakaa verkon liikennettä, jotta kuormitus jakautuisi tasaisesti klusterin jäsenien kesken.

Pfsense sisältää neljä tapaa, jolla voidaan luoda virtuaalinen erillisverkko eli VPN (Virtual Private Network). VPN:llä voidaan esimerkiksi yhdistää kaksi toimipistettä toisiinsa. Pfsense voidaan myös konfiguroida mVPN-päätepisteeksi, jolloin käyttäjien koneet voidaan yhdistää Pfsensen takana olevaan lähiverkkoon ja sen resursseihin internetin välityksellä.

Pfsensen dynaamisella DNS-asiakasohjelmalla voidaan päivittää IP-osoite automaattisesti ulkopuoliselle nimipalvelimelle, jolloin siihen voidaan ottaa yhteyttä käyttämällä www-osoitetta [3]. Yritysmaailmassa tämä yleensä toteutetaan ostamalla kallis kiinteä IP-osoite, johon on kiinnitetty www-osoite.

Captive portal on todennussivu, joka jaetaan verkkoon yhdistyneille käyttäjille [3]. Sivu pyytää kirjautumistunnuksia ennen käyttäjän päästämistä verkon resursseihin tai internettiin. Captive portal voidaan asettaa myös esimerkiksi avoimen vierailijaverkon reunalle.

VLAN (Virtual LAN) eli virtuaalinen lähiverkko, jolla voidaan jakaa yrityksen lähiverkko useaan osaan, joilla kaikilla on oma IP-osoitealueensa, yhdyskäytävä ja yleislähetysosoite eli broadcast osoite [3]. Se tuo tietoturvallisuutta verkkoon esimerkiksi siten, että vain hallintaverkolla on oikeus luoda yhteys laitteiden hallintaliittymään. VLAN:lla voidaan myös hallita pääsyä vierailijaverkosta sisäverkon muihin resursseihin.

DHCP (Dynamic Host Configuration Protocol) -server on palvelin, joka jakaa osoitteita lähiverkon laitteille [3]. Pfsense pitää sisällään myös DHCP-välityspalvelun, jolla voidaan ohjata osoitepyynnöt erilliselle palvelimelle.

Muita mainittavia ominaisuuksia ovat sovellustason pakettisuodatus, DNS-palvelin, kuormanjako ja -tasaus, liikenteenmuokkaus, UPnP (Universal Plug and Play), SNMP (Simple Network Management Protocol), IGMP (Internet Group Management Protocol) -välityspalvelin ja monia muita. Pfsensen ominaisuudet kehittyvät jatkuvasti.

2.3 Laajennuspaketit

Pfsenseen on saatavilla huikea määrä erilaisia laajennuspaketteja, joilla voidaan laajentaa sen käyttötarkoitusta. Näiden laajennuspakettien suuren määrän vuoksi esittelen vain työssä käyttämäni sovellukset. Käytännössä Pfsenseen voidaan myös asentaa paketteja, jotka eivät ole suorassa jakelussa, mutta tukevat FreeBSD alustaa.

Squid on välityspalvelinsovellus, jolla voidaan suodattaa ja nopeuttaa sisäverkosta tapahtuvaa internetselausta tallentamalla internetsivustojen sisältöä omalle palvelimelle. Sivustojen sisällön ajantasaisuus tarkistetaan oikealta sivustolta, mutta materiaali jae-

taan suoraan välityspalvelimelta. Välityspalvelimen käytöllä voidaan estää käyttäjien pääsy esimerkiksi haitallisille sivuille ja samaan aikaan nopeuttaa käyttäjien internetselausta hitaiden ulkoyhteyksien takaa. Squid voidaan myös asettaa hakemaan ja jakamaan esimerkiksi Windows- ja antiviruspäivityksiä. Squidiin saa myös paketin nimeltä LightSquid, jolla voidaan luoda raportteja välityspalvelimen kautta käytettävistä sivustoista päivä-, kuukausi- ja vuositasolla.

HAVP (HTTP Anti Virus Proxy) on Antivirus-välityspalvelin, joka tarkistaa käyttäjien lataamia tiedostoja viruksien varalta ja estää lataamisen, jos haitallinen sovellus löydetään. HAVP voidaan asettaa toimimaan Squidin kanssa esimerkiksi siten, että liikenne kulkee ensin HAVP-välityspalvelimen kautta ennen kuin se välitetään Squidille ja sitä kautta käyttäjälle. HAVP käyttää virusten tunnistamiseen avoimen lähdekoodin antivirussovellusta ClamAVta, mutta se voidaan asettaa käyttämään myös kaupallisia sovelluksia, jotka tukevat FreeBSD alustaa kuten AVG-sovellusta.

Snort on avoimeen lähdekoodiin perustuva IPS (Intrusion Prevention System) eli tunkeutumisenestosovellus. Snort tunnistaa erilaiset porttien skannailuyritykset [4] ja suorittaa pakettien sisällön analysointia ja protokollien vertailua. Snort voidaan asettaa kirjaamaan mahdolliset tunkeutumisyritykset, tai estämään kielletyt toimet lähde- tai kohdeosoitteen perusteella.

FreeRadius on avoimen lähdekoodin Radius-palvelin. Sitä voidaan käyttää todennuspalveluna esimerkiksi langattomille tukiasemille, Captive portalille tai muille Radius-todennusta tukeville palveluille. FreeRadius voidaan asettaa myös suorittamaan todennus LDAP:ia vasten, jolloin esimerkiksi yrityksen työntekijät voivat käyttää omia AD-tunnuksia kirjautuessaan langattomaan verkkoon tai Captive portaliin. Radius voidaan asettaa todentamaan käytännössä lähes mitä tahansa käyttäjätietokantaa vasten.

Quagga OPSF- ja OpenBGPD-sovelluksilla Pfsense saadaan vaihtamaan reititystietoja muiden verkon laitteiden, kuten kytkimien ja reitittimien kanssa, jotka tukevat OSPF- tai BGP-protokollaa.

TFTP-sovelluksella Pfsense voidaan asettaa vastaanottamaan ja jakamaan esimerkiksi asetuksia ja lokeja verkon laitteilta. Vikatilanteessa, jossa laite kadottaa asetuksensa, ne ovat helposti palautettavissa TFTP-palvelimelta.

Syslog-ng-sovelluksella Pfsense saadaan vastaanottamaan lokiviestejä muilta verkon laitteilta, ja näin kaikkien laitteiden lokit ovat helposti tarkasteltavissa yhdestä paikasta. Syslog-ng:llä voidaan myös tallentaa Pfsensen omia lokitietoja, koska esimerkiksi palomuurilokeja Pfsense säilyttää oletusarvoisesti hyvin rajallisen määrän.

Unbound on DNS-palvelinsovellus, joka tallentaa välimuistiinsa DNS-tietoja myöhempää käyttöä varten ja vähentää näin ulospäin suuntautuvia nimikyselyitä. Unbound tukee nimipalvelun tietoturvalaajennusta DNSSEC:ä, ja se havaitsee mahdolliset väärennetyt DNS-tietueet.

Zabbix-agent ja -proxy ovat monitorointityökaluja. Zabbix-proxyllä Pfsense voi toimia verkon muille laitteille monitorointi viestien välityspalvelimena. Zabbix-agentilla Pfsenseä voidaan monitoroida laajemmin kuin pelkillä SNMP-viesteillä. Myös Nagios-ohjelmiston sovelluksia on saatavilla Pfsenselle.

3 Asennus

3.1 Laitteisto

Pfsense voidaan asentaa normaaliin pc-järjestelmään tai sulautettuun järjestelmään. Sulautetun järjestelmän asennuksessa alustana toimii nanoBSD, ja se voidaan asentaa esimerkiksi Flash-pohjaisille muistikorteille, kuten CF-korteille. Sulautetussa järjestelmässä pyritään välttämään kirjoittamista asennusmedialle Flash-muistikorttien rajallisen eliniän takia, joten lokit pyritään säilyttämään RAM-muistissa.

PC-järjestelmässä pohjana toimii FreeBSD, ja se voidaan asentaa niin ikään muistikorteille tai kovalevyille. PC-asennuksessa kovalevyn käyttö tallennukseen on priorisoidumpaa, joten lokit tallennetaan suoraan kovalevylle [6].

Laitteisto rakennettiin vanhoista ylimääräiseksi jääneistä tietokoneen osista ja sitä laajennettiin koulusta lainaksi saaduilla kahdella verkkokortilla. Energiatehokkuuteen panostaminen olisi vaatinut uusien osien hankkimista, mutta koska kriteerinä oli kustannustehokkuus, päätettiin pitäytyä vanhojen osien käytössä. Seuraavana on listattu kaikki käytetyt komponentit, mukaan lukien tukiasema.

- Intel core 2 duo 2,4 Ghz -prosessori
- Asus P5B deluxe/Wifi AP -emolevy
- 4 Gt Kingston Hyper- X DDR2 muistia
- 100 Gt Serial-ATA kovalevy
- 550 W virtalähde
- 2 kpl Realtek piirisarjan PCI-verkkokorttia
- Asus RT-N56U Langaton tukiasema

Pfsensen valmistajan ilmoittamien laitevaatimusten mukaan käytetyllä laitteistolla odotettiin päästävän noin reiluun 300 Mb/s:n suorituskykyyn, koska tiedettiin etukäteen PCI-väyläisten verkkokorttien toimivan pullonkaulana. Pfsensen valmistajan ilmoittamat laitevaatimukset on kuvattu taulukossa 1.

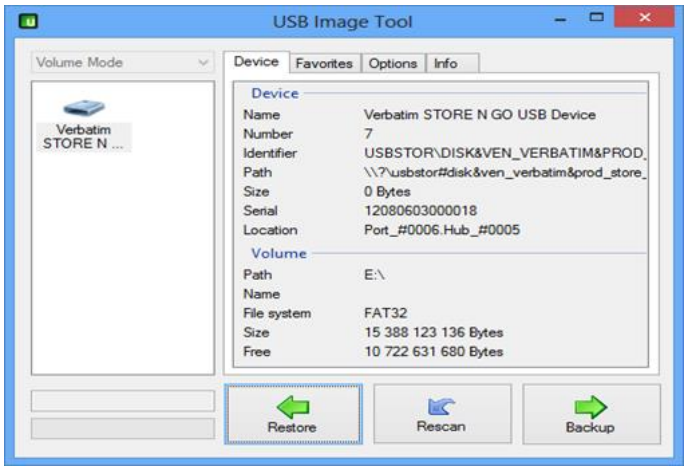
Taulukko 1. Valmistajan ilmoittamat laitevaatimukset nopeus luokittain [5].

Verkon suorituskyky	**Laitteisto vaatimukset**
10-20 Mb/s	Vähintään 266Mhz prosessori
21-50 Mb/s	Vähintään 500Mhz prosessori
51-200 Mb/s	Vähintään 1Ghz prosessori
201-500 Mb/s	Serveri tason laitteisto PCI-X tai PCI-E verkkokorteilla ja vähintään 2Ghz prosessori
501+ Mb/s	Serveri tason laitteisto PCI-X tai PCI-E verkkokorteilla ja vähintään 3Ghz prosessori

3.2 PC:n asennus

PC-asennus voidaan suorittaa joko cd-levyltä tai usb-muistikortilta. Muistikortilta asennettaessa tarvitaan sovellus, joka osaa kirjoittaa levykuvan suoraan muistikortille, kuten esimerkiksi kuvassa 1 esitetty Usbit usb image tool.

Valitaan oikea muistikortti listasta sekä purettava levykuva. Pfsense-levykuvat on jaettu gzip-pakattuina, mutta Usbit-sovellusta käytettäessä niitä ei tarvitse erikseen purkaa, koska Usbit osaa lukea pakattujen tiedostojen sisällön.



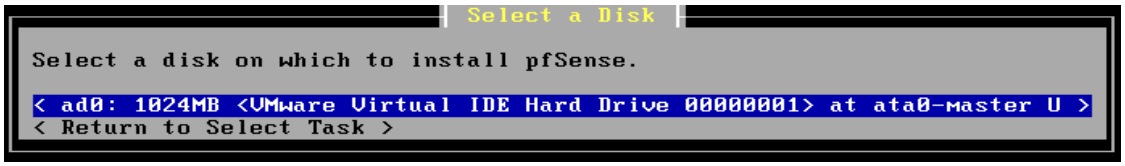
Kuva 1. USB Image tool.

Kun levykuva on saatu kirjoitettua muistikortille tai cd-levylle, tapahtuu itse asentaminen. Valitaan käynnistysmedia bios-valikosta vastaamaan asennusmediaa eli USB-tikkua tai cd-asemaa. Joissakin tapauksissa vaihtoehtoinen käynnistysasema valitaan käynnistyksen alussa painamalla esimerkiksi F12 tai F8, riippuen emolevyn mallista.

Kun järjestelmä on käynnistetty käyttäen asennusmediaa, käyttäjältä kysytään, ajetaanko Pfsense nykyiseltä medialta vai asennetaanko se kovalevylle. Pfsense voidaan siis ajaa ensin samaiselta medialta ja suorittaa alustavia konfiguraatioita webportaalin kautta ennen asennusta. Nämä konfiguraatiot siirtyvät asennettuun versioon automaattisesti asennuksen yhteydessä. Asennus käynnistetään valitsemalla 99 shell-valikosta [7].

Asennuksen ensimmäisessä vaiheessa käyttäjältä pyydetään konfigurointikonsolin asetuksia, kuten näppäimistön merkistöä ja videofonttia. Nämä asetukset voidaan muuttaa myös asennuksen jälkeen käyttämällä keymap-, kbdcontrol- ja vidfontkomentoja [7].

Kuvassa 2 Pfsense tunnistaa tallennusmedioita, joille Pfsense pystytään asentamaan. Asennuksen kohteeksi kannattaa valita sellainen kovalevy, jolla ei ole tärkeää tietoa, koska myöhemmässä vaiheessa levy pyydetään alustamaan uudelleen, jolloin aikaisemmat tiedot häviävät levyltä. Pfsense kannattaakin asentaa tallennusmedialle, joka on sille omistettu [7].



Kuva 2. Tallennusmedia, jolle Pfsense asennetaan [7].

Asennukseen valittu levy olisi hyvä aina alustaa onnistuneen asennuksen varmistamiseksi. Pfsense ei välttämättä toimi kunnolla tai ollenkaan, jos levyä ei alusteta [7].

Seuraavaksi Pfsense ilmoittaa asennukseen valitun levyn tunnistetun geometrian, kuten liitteen 1 kuvassa 3. Näitä asetuksia ei tarvitse muuttaa, ellei asennuksessa ilmene virheitä. Jos asennuksessa ilmenee virheitä, kannattaa vian selvitys aloittaa emolevyn biosista, jotta levyn geometria tunnistettaisiin oikein [7].

Osiointivaiheessa asennus tarjoaa mahdollisuuden lohkoa levy pienempiin osioihin, kuten kuvassa 3, jos levylle halutaan esimerkiksi asentaa muita käyttöjärjestelmiä rinnakkain tai jos lokitiedostoille halutaan oma osio levyltä. Asennus tarjoaa automaattisesti yhtä osiota, joka on koko levyn kokoinen [7].

Kuva 3. Levyn osiot [7].

Osiointivaiheen jälkeen asennus pyytää valitsemaan osion, jolle käynnistyslohko eli bootblock asennetaan, kuten liitteen 1 kuvassa 4. Tämän tulisi olla se osio, jolle Pfsense valitaan asentumaan. Vaihtoehtoisesti käynnistyslohkoja voi asettaa myös useille levyille.

Aliosiointivaiheessa asennus tarjoaa esiasetettuja määrityksiä, kuten kuvassa 4. Näitä asetuksia ei tarvitse välttämättä muuttaa, ellei halua esimerkiksi kasvattaa Swap-osion kokoa tai luoda omia aliosiota erilaisiin tarpeisiin.

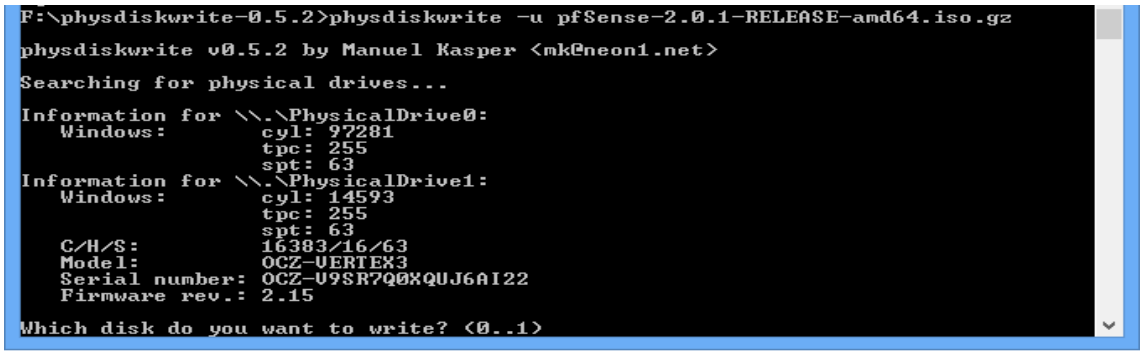
Kuva 4. Ali osiot [7].

Seuraavaksi käyttäjää pyydetään valitsemaan Pfsensen kernelin versio. Jos käytössä on prosessori, jossa on enemmän kuin yksi ydin, valitaan Symmetric multiprocessing kernel. Aliosioiden asettamisen ja kernelin valitsemisen jälkeen asennus alkaa kopioida tiedostoja valitulle levylle, minkä jälkeen käyttäjää pyydetään poistamaan asennusmedia laitteesta ja käynnistämään laite uudelleen [7].

Ensimmäisessä käynnistyksessä Pfsense pyytää käyttäjää asettamaan WAN- ja LAN-liitännät, ellei niitä ole tehty ennen asennusta. Liitäntöjen valinta on helppo tehdä valitsemalla a, jolloin järjestelmä pyytää kiinnittämään johdon verkkokorttiin. Järjestelmä seuraa, mikä liitäntä ilmoittaa nousseensa ylös ja tekee valinnan sen perusteella. Liitännän valinnan voi myös tehdä kirjoittamalla liitännän nimen, kuten esimerkiksi re0, msk0 ja sk0.

3.3 Sulautetun järjestelmän asennus

Pfsensen asentaminen sulautettuun järjestelmään tapahtuu helpoiten käyttämällä Physdiskwrite-nimistä ohjelmaa, joka näkyy kuvassa 5. Physdiskwrite kirjoittaa levykuvat binääritasolla levylle, ja se osaa lukea levykuvat suoraan pakatuista tiedostoista. Ohjelma täytyy aina ajaa järjestelmänvalvojana, tai muuten kirjoitus epäonnistuu [7].



Kuva 5. Levykuvan kirjoittamis parametrit.

Kirjoittaminen käynnistetään käynnistämällä Physdiskwrite-ohjelma parametrilla –u, joka poistaa 2 Gt:n rajoituksen. Tätä parametria ei siis tarvita, jos käytössä on 2 Gt tai pienempi tallennusmedia. Ohjelma listaa tämän jälkeen järjestelmästä löytämänsä levyt ja pyytää käyttäjää valitsemaan haluamansa levyn. Tässä vaiheessa tulisi käyttää varovaisuutta, sillä valitsemalla väärän levyn kaikki kyseisellä levyllä oleva tieto tuhoutuu [7].

Levyn valinnan jälkeen Physdiskwrite-ohjelma kirjoittaa levykuvan kiintolevylle, jonka jälkeen kiintolevy voidaan asentaa palomuurilaitteeseen. Jos kirjoitus kuitenkin epäonnistuu jostain syystä, kannattaa kaikki vanhat osiot poistaa kyseiseltä levyltä ja yrittää uudelleen. Osioiden poisto voidaan Windows-järjestelmässä suorittaa komentoriviltä, käyttäen diskpart-komentoa tai ohjauspaneelin levynhallinta osiota.

4 Konfigurointi

4.1 Yleiset asetukset

Pfsensen Webkonfiguraattoriin pääsee käsiksi internetselaimella yhdistämällä http://ip-osoite, joka on alussa yleensä 192.168.1.1. Käyttäjätunnus ja salasana ovat alkutilassa admin ja pfsense.

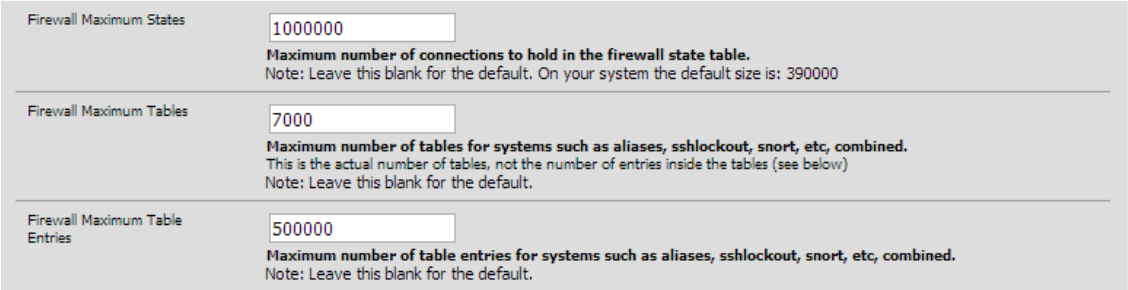
Pfsensen konfigurointi voidaan aloittaa käyttämällä Setup wizardia eli ohjattua asennusta, joka löytyy System-välilehdestä. Ohjattu asennus käy läpi kohta kohdalta kaikki tärkeimmät alkuasetukset. Käyttäjää pyydetään ensimmäiseksi asettamaan laitteen

hostname eli isäntänimi sekä domain name eli verkkotunnus. Pfsenseen voidaan myöhemmin yhdistää selaimella käyttämällä osoitteena isäntänimi.verkkotunnus.

Seuraavaksi asetetaan aikapalvelimen osoite. Tämä voidaan jättää oletusarvoon, ellei välttämättä haluta käyttää jotain muuta NTP-palveluntarjoajaa. Tämän jälkeen asetetaan Pfsensen WAN-liitännän asetukset. Yleensä internet-palveluntarjoaja jakaa IP-osoitteet DHCP:tä käyttäen varsinkin kotiliittymissä, mutta yritysliittymissä voi olla staattiset IP-osoitteet. Alareunasta valitaan Block private networks ja Block bogon networks. Tämä luo automaattiset palomuurisäännöt, joilla estetään väärennetyillä lähdeosoitteilla tulevat paketit. Viimeisissä asetuksissa asetetaan sisäverkon osoite sekä adminsalasanat.

System->advanced->Admin access -välilehdestä vaihdetaan Webkonfiguraattorin TCP-portti normaalista portti 80:stä, esimerkiksi porttiin 54321. Tämä sen takia, että jos päätetään käyttää muuta kuin Transparent proxyä, jolloin kaikki porttiin 80 tulevat yhteydet estetään, vältetään sulkemasta käyttäjä ulos Webkonfiguraattorista. Webkonfiguraattorin yhteysprotokolla olisi myös hyvä asettaa HTTPS:ksi, jotta liikenne kulkisi salattuna. Konsoli SSH-yhteydet voidaan myös sallia kytkemällä ne käyttöön Enable secure shell -kohdasta.

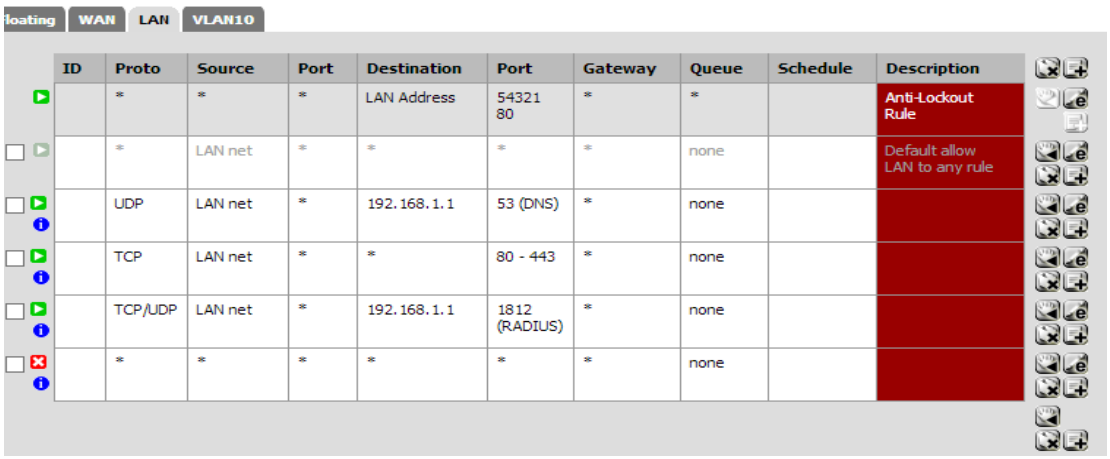
System->advanced->Firewall/NAT -välilehdestä voidaan kasvattaa palomuurin yhteystaulujen kokoa ja määrää. Asetukset tulisi määritellä käytettävissä olevan muistin mukaan, esimerkiksi, jos käytössä on vapaata muistia 1 Gt, kun muiden moduulien muistin käyttö on laskettu pois. Yksi yhteys käyttää noin 1 kt muistia, joten teoriassa taulun kooksi voidaan asettaa esimerkiksi noin miljoona yhteyttä. Kotikäytössä Pfsensen ei todennäköisesti tarvitse käyttää näin suurta yhteystaulua, mutta yrityskäytössä miljoonan yhteyden taulu riittäisi teoriassa noin 500–1000 käyttäjälle. Käytännössä tällaiselle käyttäjämäärälle tarvitaan todennäköisesti useampi Pfsense-laite, joista muodostetaan klusteri, jottei yksittäisen laitteen kuormitus kasvaisi liian suureksi. Nämä asetukset voidaan jättää oletusarvoon, mikäli kyseessä on kotiverkko.



Kuva 6. Yhteystaulujen asetukset.

Kytketään IP random id generation käyttöön, joka vaihtaa IP-pakettien header-tunnisteen satunnaiseksi arvoksi. Asetetaan FMS-arvoksi miljoona, koska tässä tapauksessa käytössä on yli 1 Gt muistia, FMT-arvoksi 7000 ja FMTE-arvoksi 500 000, kuten kuvassa 6. Muihin System->Advanced -välilehden alta löytyviin muihin asetuksiin palataan myöhemmässä vaiheessa. Tämän jälkeen voidaan siirtyä System->packages -välilehteen asentamaan paketit, joita tarvitaan seuraavissa luvuissa, kuten File manager, HAVP Antivirus Proxy, Squid, Snort ja Freeradius2.

Palomuurisääntöjä suunnitellessa yleisenä toimintaohjeena kannattaa pitää sitä, että sallitaan vain tarvittavat portit ja estetään loput. Palomuurisäännöt löytyvät Firewall->rules -välilehdestä. Wan-liitännässä estetään automaattisesti kaikki tulevat yhteydet ennen ensimmäisen sallimissäännön luontia. Kun ensimmäinen sallimissääntö on luotu, tulee luoda myös estämissääntö, jossa estetään kaikki yhteydet. Koska säännöt luetaan ylhäältä alaspäin, tulee uudet sallimissäännöt luoda aina viimeisen estosäännön yläpuolelle.



Kuva 7. Palomuurisäännöt.

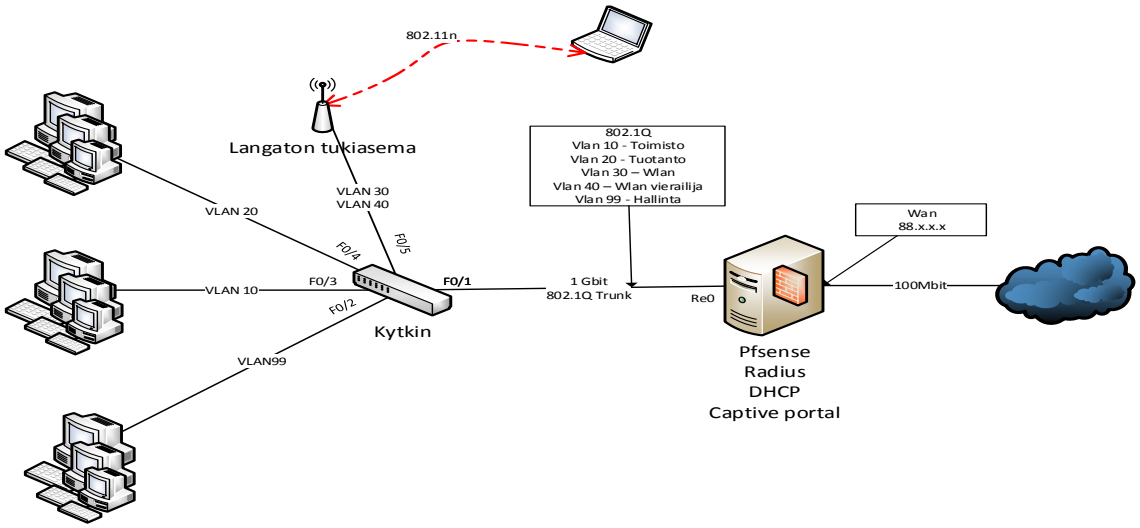
Lan-liitännän säännöistä löytyy Anti-lockout rule, kuten kuvassa 7, joka varmistaa, että käyttäjä ei sulje itseään ulos Webkonfiguraattorista. Lisätään sallimissääntö portille 53, jotta DNS-kyselyt pääsisivät läpi. Sääntö lisätään painamalla plusmerkkiä sääntölistan oikeasta alareunasta. Valitaan action-kohtaan pass ja protokollaksi UDP. Valitaan source eli lähdeosoitteeksi listasta Lan subnet, ja destination-kohtaan kirjoitetaan Pfsensen Lan-osoite. Tehdään uusi sääntö, jolla sallitaan HTTP ja HTTPS, mutta tällä kertaa laitetaan destination-kohtaan any.

Estosääntöjä ei alkutilassa ole, joten viimeiseksi säännöksi luodaan estosääntö, jolla kielletään kaikki yhteydet, jotka eivät osu sallimissääntöihin. Estosäännöt voidaan luoda joko Block- tai Reject-sääntöinä. Näiden ero on se, että Reject-sääntöihin osuviin paketteihin vastataan TCP-RST-paketilla ja Block-sääntöihin osuvat paketit tiputetaan vastaamatta mitään. Järkevintä on siis luoda Block-sääntöjä, jotta laite ei näkyisi ulkoverkkoon.

4.2 VLAN-verkot ja DHCP-palvelin

Pfsensellä pystytään jakamaan sisäverkko useisiin loogisiin segmentteihin fyysisestä toteutuksesta riippumatta. Jokaisella virtuaaliverkolla eli VLAN:lla on oma osoitealueensa ja yhdyskäytävänsä, vaikkakin kaikki liikenne kulkee trunkin osalta samaa fyysistä johtoa pitkin. Paketit merkitään matkan varrella omalla VLAN-tagilla, jotta vastaanottopäässä tiedetään, mistä segmentistä paketti tulee.

VLAN:ien käyttö vaatii 802.1Q-protokollan tuen verkossa sijaitsevilta kytkimiltä ja reitittimiltä. Esimerkkinä käytettiin Router-on-a-stick-tyyppistä topologiaa, jossa luodaan 802.1Q-trunkki, kuten kuvassa 8.



Kuva 8. Router-on-a-stick-tyyppinen verkkotopologiaesimerkki.

Konfigurointi aloitetaan Interface -> assign -> VLANs -välilehdestä. Luodaan jokainen VLAN erikseen ja valitaan haluttu liitäntä, joka tässä tapauksessa on re0. Kun VLAN:it on luotu, luodaan VLAN:eille liitännät interface-välilehdestä. Luonti tapahtuu painamalla plussamerkkiä oikeasta reunasta ja valitsemalla haluttu VLAN listasta. Uudet liitännät nimetään automaattisesti OPT [numero].

Taulukko 2. VLAN segmentit ja osoitealueet.

VLAN / Nimi	**Verkkoalue/CIDR verkkomaski**	**Yhteyskäytävä osoite**
10 / Toimisto	10.10.10.0/24	10.10.10.1
20 / Tuotanto	10.10.20.0/24	10.10.20.1
30 / Wlan	10.10.30.0/24	10.10.30.1
40 / Vierailija Wlan	10.10.40.0/24	10.10.40.1
99 / Hallinta	10.10.99.0/24	10.10.99.1

Kun liitännät on luotu VLAN:eille, asetetaan liitäntöjen tyypit staattisiksi sekä taulukon 2 mukaiset osoitteet ja verkkomaskit Interface->OPT[numero] välilehdestä. Tässä vaiheessa voidaan muuttaa myös liitännän nimet kuvaavammaksi, kuten esimerkiksi VLAN 10 ja VLAN 20..

Seuraavaksi kytketään DHCP-palvelu liitännöille Service->DHCP-Server -välilehdestä. Valitaan haluttu liitäntä, esimerkiksi VLAN 10, ja kytketään palvelu käyttöön enable-kohdasta. Available range -kohdassa on ilmoitettu verkkomaskin perusteella laskettu verkkoalue, josta osoitteita voidaan jakaa. Asetetaan range -kohtaan alue, josta en-

simmäinen osoite on otettu pois, koska se asetettiin liitännän osoitteeksi eli 10.10.10.2 to 10.10.10.254. Mikäli verkossa on laitteita, jotka tarvitsevat kyseisestä VLAN:ista staattisia osoitteita, annetaan ne vapaana olevan alueen alusta, ja poistetaan jaettavasta alueesta kyseiset osoitteet. Toistetaan sama prosessi kaikille VLAN-liitännöille.

Jotta VLAN:it toimisivat verkossa, täytyy myös kytkimille tehdä VLAN-asetukset. Asetukset voivat vaihdella kytkimen valmistajasta ja mallista riippuen. Esimerkiksi HP:n kytkimissä luodaan ensin VLAN:it ja sen jälkeen asetetaan halutut portit tagged-tilaan esimerkiksi komennolla `vlan 10 tagged [portti numero]`. Tietysti tarvitaan muitakin komentoja näiden lisäksi, mutta oletetaan, että alkukonfiguroinnit on tehty jo aikaisemmin.

Kytkin konfiguraatioiden valmistuttua voidaan toimintaa testata liittämällä kone kytkimen porttiin. Mikäli kaikki on tehty oikein, riippuen porttiin ohjatusta virtuaaliverkosta, pitäisi DHCP-palvelimelta saada kyseiseen virtuaaliverkkoon kuuluva osoite.

4.3 Squid- ja HAVP-Proxy

4.3.1 HAVP-välityspalvelin

HAVP (HTTP Anti Virus Proxy) voidaan konfiguroida niin, että internetistä tulevat paketit kulkevat ensin Antivirus-tarkistuksen läpi, jonka jälkeen ne jaetaan Squidin välivarastoon ja sitä kautta käyttäjälle. Konfiguraatio voidaan myös suorittaa päinvastoin, mutta koska Squid toimii välivarastona kyseiselle materiaalille, on järkevämpää tarkistaa paketit jo ennen välivarastoon sijoittamista. Vaikka käytössä on Antivirus-proxy, tulisi silti huolehtia, että myös verkonkäyttäjien koneilla on käytössä ajan tasalla oleva Antivirus-ohjelmisto.

Aloitetaan konfigurointi HAVP-Antivirus-välityspalvelusta, vaikka käytännössä konfigurointi järjestyksellä ei ole toiminnan kannalta merkitystä. HAVP-asetukset löytyvät Service->antivirus->HTTP Proxy -välilehtien takaa.

Asetetaan välityspalvelin päälle Enable proxy -kohdasta ja valitaan Proxy mode, joka on tässä tapauksessa Parent for Squid, koska internetistä tulevien pakettien halutaan

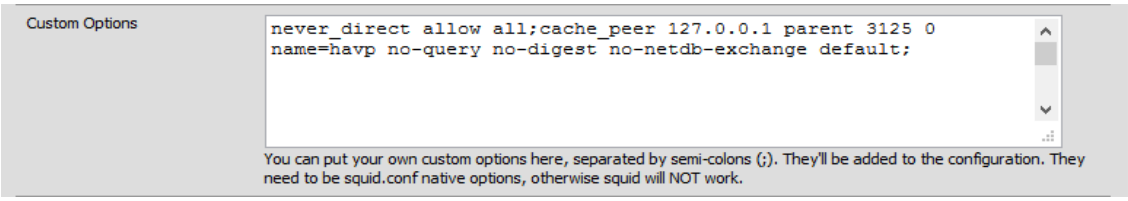
kulkevan ensin virustarkistuksen läpi. Asetetaan portti, jota Proxy-serveri kuuntelee eli esimerkiksi 3125. Proxy-portin tulee olla eri kuin Squidiin asetettava portti.

Seuraavaksi valitaan skannattavien tiedostojen maksimikoko ja mediat, joita HAVP tarkistaa. Asetetaan Scan max file size -kohtaan suurin mahdollinen eli 10 Mb. Tätä suurempien tiedostojen skannaus jätetään käyttäjän koneen Antivirus-ohjelmiston harteille. Vaihtoehtoisista skannattavista medioista valitaan myös kaikki mahdolliset, eli kuvat, video- ja -äänivirrat ja rikkinäisten käynnistettävien tiedostojen heuristinen skannaus. Stream-skannaus hidastaa esimerkiksi Youtube-videoiden lataamista, koska HAVP lataa tiedostot ensin omaan varastoonsa. Tämän voi kuitenkin kiertää asettamalla luotettavat medialähteet ns. valkoiseen listaan, jolloin niistä sivustoista tulevia tiedostoja ei tarkasteta. Tallennetaan muutokset, jonka jälkeen voidaan siirtyä Squidin puolelle.

4.3.2 Squid

Squid voidaan konfiguroida kahdella eri tavalla. Ensimmäinen tapa on konfiguroida Squid läpinäkyvään tilaan, jolloin kaikki TCP-porttiin 80 tulevat kyselyt ohjataan välityspalvelimeen, eikä käyttäjän puolella tarvitse tehdä muutoksia. Toinen tapa on konfiguroida Squid direct Proxy -tilaan eli karkeasti suomennettuna suoraan välityspalvelintilaan, jolloin käyttäjien pitää asettaa ohjaamaan kaikki HTTP-liikenne välityspalvelimen tiettyyn porttiin sekä asettaa mahdolliset autentikointimäärittelyt. Palomuurin puolelta pitää avata portti, jota välityspalvelin kuuntelee [8].

Squid-asetukset löytyvät Service->Proxy server -välilehden takaa. Valitaan liitäntä, jota Squid kuuntelee, eli tässä tapauksessa LAN. Asetetaan Allow users on interface ja Transparent proxy päälle. Nämä asetukset asettavat välityspalvelimen transparent-tilaan ja lisäävät automaattisesti sallittujen aliverkkojen listaan valitun liitännän. Kytketään lokien kirjoitus käyttöön ja valitaan lokitiedostojen tallennuspaikaksi /var/squid/logs-kansio. Asetetaan lokirotaatio, eli kuinka kauan lokeja pidetään tallessa, esimerkiksi 20 päiväksi, sekä Proxy-portti, esimerkiksi 3128 [8]. Asetetaan supress Squid versio -kohtaan valintamerkki, joka poistaa mahdollisista virheilmoituksista Squid-versiotiedot. Tämä tehdään sen takia, että mahdollinen tunkeutuja ei saa tietoonsa käytössä olevan Squid-versiota. Versiotiedon avulla tunkeutuja voi käyttää hyväkseen tietoturva-aukkoja, joita eri versioista voi löytyä. Mitä vähemmän annamme tietoja ulos, sitä parempi.



Kuva 9. HAVP:n luomat asetukset.

Kuten kuvasta 9 voidaan todeta, Pfsense on jo luonut alustavia asetuksia, jotta Squid toimisi HAVP:n kanssa yhteen. Kyseinen rivi asettaa Squidin lähettämään isäntä-proxylle siihen tulleet HTTP-kyselyt. Mikäli kyseiset asetukset eivät ole ilmestyneet, ne voidaan lisätä käsin, tai vaihtoehtoisesti käydään sulkemassa Antivirus-Proxy ja käynnistetään se uudelleen, jolloin asetuksien pitäisi ilmestyä.

Seuraavaksi siirrytään Squid-välimuistiasetuksiin, jotka löytyvät cache mgmt-välilehden takaa. Välimuistiasetukset tulisi tehdä käyttötarkoituksen ja kovalevyn koon mukaan. Tässä tapauksessa Squid:in halutaan nopeuttavan verkkoselausta, sekä erilaisten päivitysten latausta, kuten Antivirus- ja Windows-päivitysten latausta.

Asetetaan välimuistille kovalevyltä varattava tila noin 3–10 Gt ja tiedostojärjestelmäksi ufs. Välimuistin tallennus sijainniksi asetetaan /var/squid/cache. Squidille varatun tilan järjestelmän käyttömuistista ei tulisi ylittää 50 % järjestelmään asennetusta muistista [8]. Asetetaan sille 1,5 Gt käyttömuistista, koska kyseisessä järjestelmässä on yhteensä 4 Gt käyttömuistia [8].

Tallennettavien objektien minimikooksi laitetaan 0 ja maksimikooksi 512 Mt eli 512000, koska koko on ilmoitettu kilotavuina. Maksimikoko asetetaan isoksi sen takia, että esimerkiksi Windows-päivitykset voivat olla kookkaita, ja ne halutaan säilyttää välimuistissa. Squid poistaa maksimikokoa suuremmat tiedostot välimuistista, vaikka kyseiset tiedostot olisi asetettu säästettäväksi muista asetuksista [9].

Käyttömuistiin tallennettavien objektien maksimikokoa ei kuitenkaan tulisi kasvattaa liian isoksi, koska se voi vaikuttaa negatiivisesti Squidin suorituskykyyn. Level 1 subdirectory -kohta määrittelee, kuinka moneen kansioon Squid tallentaa internetsisältöä. Jokainen kansio pitää sisällään 256 alikansiota, joten 16 kansiota sisältää 4096 kansiota. Mikäli kansioiden määrää kasvatetaan, tulee Squid sammuttaa ja käynnistää konsolista komennolla `squid -z`, jolloin Squid luo kansiorakenteensa uudestaan.

Kuvien, videoiden, päivitysten ym. internetistä ladattujen objektien vaihtokäytännöksi käyttömuistin ja välimuistin osalta valitaan Heap LFUDA. Tämä käytäntö pitää tallessa objektit, joihin kohdistuu eniten kyselyitä välittämättä kyseisten objektien koosta.

4.3.3 Optimointi

Squidin toimintaa voidaan nopeuttaa monella eri tavalla, kuten nostamalla MBUF-arvoa, tai jos käytössä UFS-tiedostojärjestelmä, nostamalla vfs.read_max-arvoa. Myös välimuisti-asetuksia muuttamalla Squidin suorituskykyä voidaan parantaa [9].

MBUF-arvo on kernelin optio, jolla määritellään verkkotoiminnoille varatun muistin koko. Tässä muistissa säilytetään verkkopuskureita ja paketteja. MBUF-asetus löytyy kansiosta `/boot` tiedostosta `/loader.conf.local`. MBUF-asetus tehdään lisäämällä rivi `kern.ipc.nmbclusters=32768` edellä mainittuun tiedostoon. Tiedostoa voidaan muokata esimerkiksi konsolin kautta vi-komennolla tai diagnostics-välilehdestä löytyvällä edit file -toiminnolla [9].

Vfs.read_max -arvo määrittelee UFS-tiedostojärjestelmässä kovalevyn etukäteen luettavien lohkojen määrän. Tätä arvoa nostamalla voidaan siis tehostaa kovalevyltä tapahtuvaa lukemista. Liiallinen nosto voi kuitenkin aiheuttaa käynnistysvaikeuksia, joten nyrkkisääntönä korotetaan nykyinen arvo 32 itsellään eli saadaan 64, ja mikäli virheitä ei ilmene, voidaan korottaa se vielä arvoon 128. Vfs.read_max asetus löytyy System->Advanced->System tunables -välilehden alta [9].

4.4 Snort IPS

Snortin asetukset voivat aluksi tuntua epäselviltä ja monimutkaisilta. Sen vuoksi onkin tärkeää luoda ensin vain lokitussääntöjä, joita seuraamalla voidaan pois sulkea väärät tunnistukset. Sen jälkeen asetetaan Snort estämään osoitteet, joista kielletyt toimet tulevat. Snortin asetukset löytyvät Service->Snort -välilehdestä.

Aloitetaan konfigurointi Global settings -välilehdestä. Tunnistussääntöjen päivitysten lataaminen vaatii Oinkmaster-koodin, joka on saatavilla ilmaiseksi osoitteesta www.snort.org. Vaihtoehtoisesti voi asentaa myös yrityskäyttöön soveltuvat Sourcefiren maksulliset tunnistussäännöt tai ilmaiset Emergingthreats-säännöt. Sääntökantoja voi

olla samanaikaisesti käytössä myös useita, koska Snort osaa poistaa käytöstä päällekkäiset säännöt.

Kuva 10. Sääntökannat ja automaattinen päivitys.

Asetetaan Oinkmaster-koodi sille varattuun kenttään sekä valitaan asennettavaksi myös Emergingthreats-säännöt. Automaattiset päivitykset asetetaan esimerkiksi päivän välein, kuten kuvassa 10. Asetetaan kansion kokoraja, joka tulisi olla maksimissaan noin 20 % kovalevyllä vapaana olevasta tilasta. Tallennetaan tehdyt muutokset ja käydään päivittämässä säännöt Updates-välilehdestä.

Seuraavaksi siirrytään Snort interface -välilehteen määrittelemään liitännät, joita Snort seuraa. Aloitetaan luomalla WAN-liitännän säännöt painamalla plusmerkkiä oikeasta reunasta. Kytketään liitännän valvonta enable-kohdasta, valitaan WAN-liitäntä listasta, ja annetaan sille kuvaus description-kenttään, kuten esimerkiksi WAN IPS. Valitaan suorituskykykäytäntö vastaamaan käytössä olevaa laitteistoa, joka tässä tapauksessa on AC-BFNA, eli vähän muistia ja huono suorituskyky. Tässä vaiheessa ei vielä asetetа Snort:a estämään yhteyksiä.

Preprocessors-välilehdestä kytketään HTTP-tarkistus käyttöön ja asetetaan HTTP Server flow depth -arvoksi maksimi eli 65535 ja HTTP client flow depth -arvoksi 1460. Liian matala flow depth -arvo voi aiheuttaa vääriä hälytyksiä. General preprocessor -kohdasta asetetaan kaikki mahdolliset esikääntäjät päälle, paitsi SCADA-esikääntäjät. Tallennetaan muutokset, jonka jälkeen siirrytään Category-välilehteen valitsemaan käytössä olevat säännöt.

Kytketään Resolve Flowbits käyttöön ja valitaan Snortin IPS-käytännöksi balanced. Snortin IPS-käytännöt vastaavat Snort.org-sääntökantoja ja käytännöt valitsevat automaattisesti tiettyjä sääntöjä Snort.org-sääntökannoista käyttöön. Valitaan kaikki Emerging Threats -säännöt käyttöön tai jätetään sellaisia sääntöjä pois, joita ei haluta seurata. Tämän jälkeen voidaan käynnistää Snort interface -välilehdestä kyseinen prosessi painamalla vihreän nuolen kuvaa. Mikäli kyseinen nuoli ei muutu punaiseksi, eli prosessi ei käynnisty, voidaan katsoa järjestelmä lokeista, mikä estää Snortia käynnistymästä.

Yleisin syy on päällekkäiset säännöt, jos sääntökantoja on useita tai preprocessor-välilehdestä on jäänyt joku esikääntäjä asettamatta. Vanhentuneet säännöt voivat myös aiheuttaa käynnistysongelmia uusien Snort-versioiden kanssa. Lan-liitännän asetukset tehdään samalla tavalla kuin WAN-liitännän asetukset, mutta poikkeuksena valitaan seurattavaksi liitännäksi LAN-liitännän.

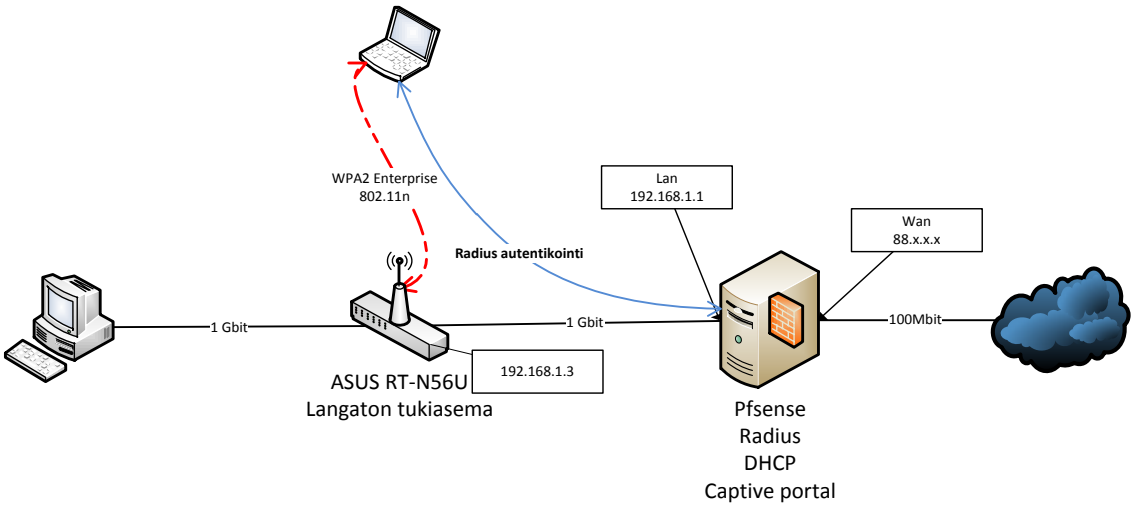
Seuraavaksi käytetään kaikkia mahdollisia palveluita, kuten esimerkiksi Skype, MSN messenger, Facebook, Windows update, ja seurataan Snortin varoituksia alerts-välilehdestä. Väärät hälytykset voidaan lisätä suodatuslistaan painamalla kyseisen hälytyksen SID-kohdassa olevaa plusmerkkiä. Tämän voi tehdä myös manuaalisesti Rules-välilehdestä poistamalla ongelmia aiheuttavat säännöt käytöstä. Mikäli käytetään Suppress-listaa, täytyy se myös ottaa käyttöön IF interface -välilehdestä. Jos hälytyksiä on paljon, eikä niiden oikeellisuudesta voida olla varmoja, voidaan Snortin estotila kytkeä käyttöön, jotta nähdään käytännössä, mitkä yhteydet Snort estää. Tämä taktiikka voi helpottaa väärien hälytysten poistamisen konfigurointia, mutta helpoin tapa on kuitenkin käydä suoraan Category-välilehdestä poistamassa sääntökannat, jotka tuottavat eniten ongelmia.

Suurimmat virheelliset tunnistukset tulevat yleensä HTTP-tarkistuksesta. HTTP-tarkistuksen voi kytkeä kokonaan pois preprocessor-välilehdestä kohdasta Disable HTTP alerts. Tämä ei ole kuitenkaan suositeltavaa.

Kun Snort on saatu toimimaan, kytketään estotila Snortin interface-välilehdestä. Estotila täytyy kytkeä jokaiselle liitännälle erikseen sekä määritellä, mikä osoite estetään hälytyksen sattuessa. Yleensä kannattaa valita estettäväksi molemmat osoitteet eli lähde- ja kohdeosoite. Global settings -välilehdestä voidaan asettaa aika, jolloin estolista tyhjennetään. Tämä voi olla tunnista useisiin päiviin tai vaihtoehtoisesti ei koskaan.

4.5 FreeRadius

FreeRadiuksen konfigurointi kannattaa aloittaa tekemällä ensin hyvin yksinkertainen ja toimiva konfiguraatio ja vasta sen jälkeen suorittaa tarkempia määrittelyjä, jolloin vikatilanteiden selvittäminen on helpompaa. FreeRadius-todennusta voidaan käyttää esimerkiksi langattomien laitteiden todentamisessa tai Captive portalin todentamisessa. Periaatteessa kaikki mahdolliset todentamista vaativat toiminnot ja palvelut on todennettavissa Radiuksella.



Kuva 11. Esimerkki kotiverkkototeutus.

Käytetään esimerkkinä kuvassa 11 esitettyä kotiverkkototeutusta ja aloitetaan radiuksen konfigurointi määrittelemällä kuunneltava liitäntä interface-välilehdestä. Osoite kentässä on automaattisesti *-merkki, joka tarkoittaa sitä, että radius kuuntelee kaikkia liitäntöjä. Asetetaan osoitteeksi sen liitännän osoite, josta radius ottaa vastaan todennuspyyntöjä, eli tässä tapauksessa 192.168.1.1. Määritellään portti 1812 ja liitännän tyyppi authentication eli todennus [11].

Seuraavaksi siirrytään NAS/clients-välilehteen asettamaan laitteet, joilta todennuspyyntöjä otetaan vastaan. Tässä määritellään laite, joka välittää todennuspyynnöt palvelimelle, eli tässä tapauksessa langaton tukiasema. Asetetaan osoitekenttään tukiaseman osoite eli 192.168.1.3, nimetään kyseinen tukiasema lyhyesti, esimerkiksi accespoint1, ja asetetaan salasana. Asetetaan protokollaksi UDP ja client-tyypiksi, tässä tapauksessa other [11].

Asetetaan Settings-välilehdestä kohdasta Logging configuration, Radiuksen lokitus käyttöön ja siirtymään suoraan Pfsensen järjestelmä lokeihin. Tämä helpottaa myöhemmässä vaiheessa vikatilanteiden selvittämistä. Lokit voidaan muuttaa takaisin siirtymään omaan tiedostoon, kun kokoonpano on saatu toimivaksi. Asetetaan lokitus hyväksytyille ja hylätyille todennusyrityksille sekä asetetaan Radius näyttämään myös tunnukset ja salasanat, joilla hylätyt todennusyritykset ovat tapahtuneet. Tunnukset ja salasanat saadaan näkyviin lisäämällä `%{User-Name}` `%{User-Password}` additional information -kohtaan [11].

Siirrytään Users-välilehteen asettamaan tunnukset, joilla käyttäjät ottavat yhteyttä langattomaan verkkoon. Käyttäjiä voidaan lisätä oikeasta reunasta löytyvällä plusmerkillä. Asetetaan käyttäjätunnus, salasana ja viimeinen voimassaolopäivä. Käyttäjätunnuksille voidaan myös asettaa mahdollisia kaistarajoituksia tai asettaa päiviä, jolloin tunnus on voimassa, mikäli sitä halutaan rajoittaa. Jokaiselle käyttäjälle voidaan myös määritellä Radiuksen välittämä IP-osoite ja VLAN id. Tämän jälkeen voidaan siirtyä tukiasemalle tekemään vastaavat konfiguraatiot ja testata radiuksen toimintaa.

Kuva 12. RT-N56U-tukiaseman radius-asetukset.

Tehdään tukiaseman puolelle vastaavat asetukset palvelimen osoitteen, portin ja salasanan osalta, kuten kuvassa 12. Tämän jälkeen Radius-yhteyttä voidaan testata yhdistämällä langattomaan verkkoon. Mikäli yhteysyritys epäonnistuu, voidaan epäonnistumisen syytä etsiä Pfsensen lokista, joka löytyy Status->System logs -välilehdeltä. Yleisin syy yhteyden epäonnistumiseen on väärin kirjoitetut käyttäjätunnus ja salasana tai tukiaseman Radius-salasana. Tässä vaiheessa olisi tärkeää myös asettaa DHCP-

palvelimen puolelta tukiasemalle kiinteästi jaettava IP-osoite, koska jos tukiasema saa eri osoitteen kuin sen, mikä asetettiin Radius-asetuksista, todennus ei toimi.

Siirrytään FreeRadiuksen EAP-välilehteen asettamaan turvallisuusmäärittelyjä. Aloitetaan poistamalla heikot EAP-protokollat käytöstä ja asetetaan ensisijaiseksi tyypiksi TLS. Koska tässä tapauksessa varmenteita ei käytetä todentamiseen, voidaan siirtyä suoraan listan pohjalle EAP-PEAP-asetuksiin ja asettaa EAP-protokollaksi TLS. Nyt Radius-todennuksen pitäisi toimia langattomassa verkossa, ja haluttaessa voidaan tehdä tarkempia turvallisuusmäärityksiä.

4.6 VPN-tunnelit

OpenVPN

Konfigurointi aloitetaan luomalla Pfsensen cert managerista CA-varmenne. Varmennekanta löytyy System->Cert manager -välilehden alta. Painetaan oikeasta reunasta plusmerkkiä, valitaan luontimetodiksi sisäinen ja täytetään tarvittavat tiedot. Annetaan varmenteelle nimeksi, esimerkiksi VPN CA. Tämän jälkeen luodaan Certificate-välilehdestä palvelinvarmenne. Nimetään palvelinvarmenne kuvaavasti, esimerkiksi VPN Server Cert. Valitaan metodiksi taas sisäinen varmenne ja Certificate authority -kohtaan aikaisemmin luotu VPN CA. Valitaan varmenteen tyypiksi palvelinvarmenne ja täytetään loput kohdat.

User manager -välilehden alta voidaan luoda uusi käyttäjä ja uudelle käyttäjälle uusi sisäinen varmenne VPN CA:n pohjalta. Painetaan plusmerkkiä User certificates-kohdasta, josta luodaan uusi käyttäjäkohtainen varmenne. Valitaan Create Internal certificate ja valitaan Certificate authorityksi aikaisemmin luotu VPN CA. Nimetään varmenne kuvaavasti, täytetään kaikki loput kentät ja siirrytään OpenVPN-asetuksiin VPN->OpenVPN -välilehdestä [12].

Aloitetaan VPN-palvelimen luonti OpenVPN->Server -välilehdestä. Valitaan Server Mode-kohtaan Remote Access SSL/TLS + User Auth. Valitaan Backend for authentication -kohtaan tässä tapauksessa lokaali tietokanta, jos todennukseen halutaan käyttää LDAP:a tai Radiusta, täytyy ne ensin määritellä System->User manager->Servers -välilehdestä. Valitaan protokollaksi UDP ja Device Mode -kohtaan tun. Asetetaan liitän-

tä, josta palvelin kuuntelee saapuvia yhteyksiä, ja koska internetin puolelta halutaan yhdistää sisäverkon resursseihin, valitaan kuunneltavaksi liitännäksi WAN-liitäntä. Asetetaan portti esimerkiksi 1195 tai joku muu portti, jonka tiedetään olevan vapaana [12].

Kytketään TLS-todennus ja TLS-avaimien luonti käyttöön, ja asetetaan muut salaustekniset asetukset, kuten salaus-parametrit ja -algoritmit, Diffie-Hellman-avaintenvaihtoprotokollan pituus ja mahdolliset laitepohjaiset kryptoprosessorit. Valitaan Peer Certificate Authority- ja Server Certificate -kohtiin aikaisemmin luodut VPN CA ja VPN Server Cert. Asetetaan tunneliverkko eli tunnelin sisäinen verkkoalue, esimerkiksi 192.168.2.0/24. Asetetaan myös paikallisverkko, johon asiakkaat päästetään eli esimerkiksi LAN-verkko 192.168.1.0/24. Jos halutaan, että käyttäjien kaikki liikenne kulkee tunnelin kautta, asetetaan Redirect gateway -kohtaan valintamerkki. Concurrent connections eli samanaikaiset yhteydet -kohtaan laitetaan erimerkiksi 10. Käyttäjien välinen liikenne asetetaan sallituksi kohdasta Inter-client communications. Client settings -kohdasta voidaan asettaa määrityksiä, jotka jaetaan yhdistyneille käyttäjille, kuten DNS, NTP ja WINS. Viimeiseksi tulee luoda WAN-liitännälle VPN-yhteydet salliva palomuurisääntö, UDP-protokollalle ja portille 1195 [12].

Käyttäjäpuolen konfiguroinnin helpoittamiseksi, asennetaan OpenVPN client exporter utility -paketti. Tämän avulla voidaan ladata asennukseen tarvittavat ohjelmat ja konfiguraatiot käyttäjien koneille suoraan Pfsensestä.

Kun palvelin on luotu, voidaan tunnelin toimintaa testata. Avataan Client export -välilehti. Jos kaikki on tehty oikein, pitäisi listassa näkyä uusi käyttäjä. Export -kohdassa näkyvät kaikki tavat, joilla tarvittavat konfiguraatiot voidaan toimittaa käyttäjille. Käyttäjille voidaan toimittaa myös koko OpenVPN-asiakasohjelmiston valmiiksi konfiguroituna asettamalla valintamerkki Management Interface OpenVPNManager kohtaan ja valitsemalla käyttäjän kohdalla export-kohdasta Windows installerin alta löytyvä vaihtoehto. Mikäli käyttäjälle halutaan toimittaa vain konfiguraatiot ilman asiakasohjelmaa, valitaan configuration archive, joka sisältää asetukset ja avaimet OpenVPN-asiakasohjelmaan [12].

IPSec

IPSec:illä voidaan luoda niin sanottu kahden toimipisteen välinen VPN-tunneli eli site-to-site VPN. Site-to-site-tunnelia luodessa tulee huomioida, että toimipisteiden sisäverkkojen täytyy olla eri osoitealueilla, jos käytössä ei ole kaksisuuntaista NAT:a [13].

Mobiili IPSec VPN -konfigurointi asettaa Pfsensen toimimaan dynaamisena päätepisteenä käyttäjien VPN-yhteyksille. Käyttäjille voidaan jakaa joko tunnelin takana olevan verkon resurssit tai vaihtoehtoisesti kierrättää käyttäjän kaikki internetliikenne tunnelin kautta [13].

Kuva 13. IPsec VPN -välilehti.

Mobiili IPSec -konfigurointi aloitetaan VPN-välilehdestä, kuten kuvassa 13. Valitaan Mobile clients -välilehti ja kytketään mobiilikäyttäjätuki kohdasta Mobile client support. Valitaan käyttäjä todennuksen lähteeksi paikallinen tietokanta ja ryhmätodennukseen system eli järjestelmä. Virtual address pool -kohtaan asetetaan verkkoalue, josta yhdistyneille käyttäjille jaetaan osoitteita. Mikäli sisäverkossa on käytössä esimerkiksi 192.168.1.0/24 -alue, voidaan tunneliverkoksi asettaa esimerkiksi 192.168.2.0/24. Asetetaan tunnettujen verkkojen listan jako päälle, jotta käyttäjät voivat yhdistää sisäverkon resursseihin tunnelin ylitse. DNS- ja WINS-kohtiin asetetaan Pfsensen sisäverkon osoite, jos ne halutaan jakaa VPN-käyttäjille. Phase2 PFS Group-kohtaan valitaan ryhmä 2, joka määrittelee avaimen salauksen algoritmin pituudeksi 1024 bittiä. Tämä asetus tulee olla sama myös käyttäjänpuolelta [13].

Kun mobiilitila on kytketty käyttöön, Pfsense ilmoittaa, että mobiilitila on toiminnassa, mutta vaihe 1 ei ole määritelty. Määritellään vaihe 1 painamalla create phase1. Valitaan käytettävä internet-protokolla sekä liitäntä, josta käyttäjäyhteyksiä kuunnellaan. Asetetaan todennusmetodiksi mutual PSK eli yhteinen esijaettu avain ja neuvottelutila aggressiiviseksi eli tehostetuksi [13].

Valitaan tunnisteeksi IP-osoite ja käytännön generointimenetelmäksi unique. Salausalgoritmiksi voidaan valita esimerkiksi AES. Tiivistealgoritmiksi valitaan sha1, ja tämä asetus täytyy muistaa asettaa käyttäjän puolelta samaksi. DH-avainryhmäksi valitaan sama kuin mobiilikäyttäjä asetuksista eli ryhmä 2. Kytketään NAT-T toimintaan ja DPD eli Dead Peer Detection pois, jonka jälkeen siirrytään vaiheen 2 määrittelyihin [13].

Vaiheessa 2 luodaan itse tunneli ja määritellään käytettävät salausalgoritmit. Aloitetaan valitsemalla tunnelin tilaksi IPv4. Lähiverkkokohtaan asetetaan LAN-subnet. Ilman tätä tunnelin käyttäjiä ei voi yhdistää sisäverkon resursseihin. Valitaan protokollaksi ESP, joka salaa liikenteen, ja salausalgoritmiksi esimerkiksi AES. Hash eli tiivistealgoritmiksi voidaan valita sha1. Tämän tulee olla sama myös käyttäjäpuolella. Pfsense tukee AES:n lisäksi muun muassa 3DES-, Blowfish-, Cast- ja DES-salausalgoritmeja [13].

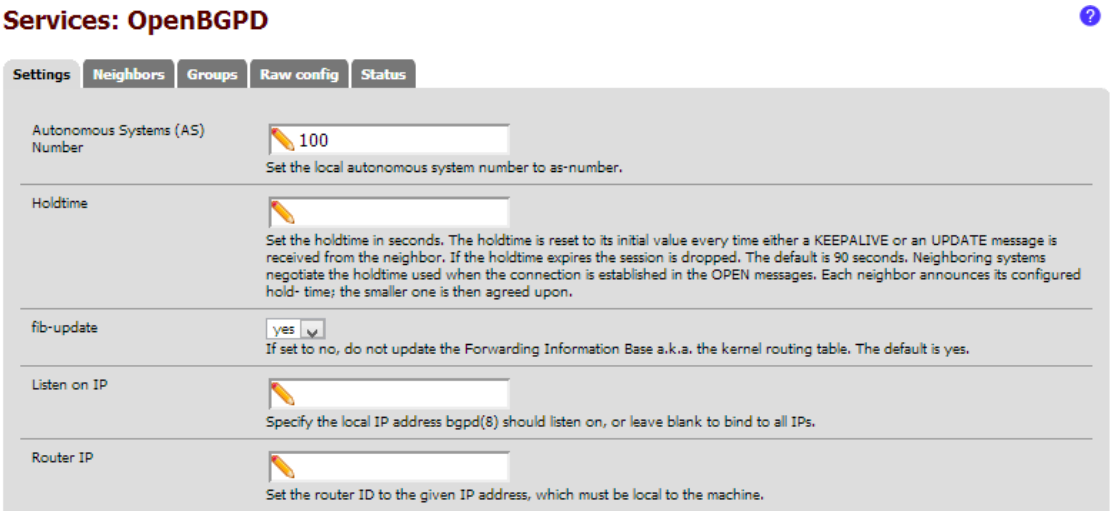
Kun asetukset ovat valmiit, Pfsense luo automaattisesti palomuuriin määrittelyt tunnelia varten. Tunnelin toimintaa voidaan testata käyttämällä esimerkiksi Shrew soft VPN -ohjelmaa. Käyttäjäpuolen asetuksien tulee olla täysin samat kuin Pfsensessä, jotta tunneli saataisiin käyttöön. Mikäli tunneli ei jostain syystä toimi, tutkitaan virhe ilmoituksia Pfsensen järjestelmälokeista.

4.7 Reititysprotokollat

BGP-protokolla

BGP-protokollan käyttöönotto aloitetaan lataamalla OpenBGPD-paketti. Kun paketti on asentunut, siirrytään Service->OpenBGPD -välilehteen tekemään asetukset. Jokaisella BGP-alueella on oma AS eli Autonomous system -numero ja jokaisella BGP-alueen jäsenellä oma ID-numero. ID-numero on yleensä samassa muodossa kuin IP-osoite ja Ciscon laitteissa, joissa ID-numeroa ei määritellä, se on automaattisesti suurin loopback-osoite. Kun BGP vaihtaa reititystietoja saman AS-alueen sisällä muiden reitittimi-

en kanssa, sitä kutsutaan IBGP:ksi eli Internal BGP:ksi. Jos BGP vaihtaa reititystietoja muiden AS-alueiden kanssa, sitä kutsutaan EBGP:ksi eli External BGP:ksi.



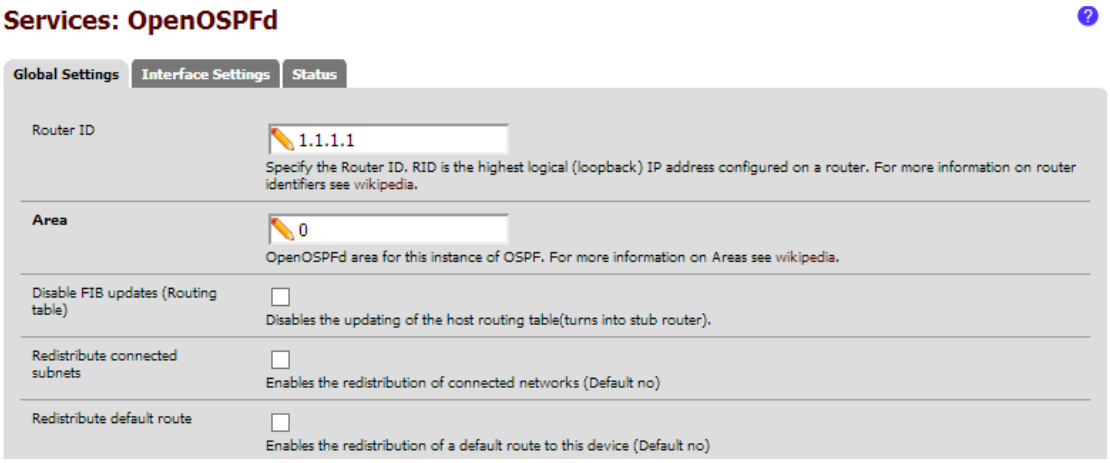
Kuva 14. BGP-asetukset.

Aloitetaan BGP-konfigurointi asettamalla AS-numero, kuten kuvassa 14. Asetetaan holdtime-kohtaan noin 90 sekuntia ja Fib-update-kohtaan kyllä, jos halutaan jakaa Pfsensen kernelin reititystaulun tietoja. Listen IP -kohtaan asetetaan 192.168.1.1, joka vastaa LAN-liitäntää. Router IP -kohtaan, joka käytännössä toimii kyseisen laitteen ID-numerona, voidaan asettaa sama LAN-osoite tai mielivaltainen osoite, jolla laite on helposti tunnistettavissa, kuten 1.1.1.1. Networks-kohtaa asetetaan ne verkot, joita halutaan mainostaa. Jos kyseiseen kenttään kirjoitetaan connected, BGP jakaisi reitit verkkoihin, jotka ovat yhteydessä kyseiseen laitteeseen. Static-määrittely jakaisi kaikki staattisesti luodut reitit.

Jotta BGP keskustelisi muiden verkon laitteiden kanssa, täytyy ne ensin määritellä naapureiksi. Naapureiden ollessa saman AS-alueen sisällä voidaan kyseiset naapurit lisätä suoraan Neighbor-välilehdestä. Mikäli kuitenkin naapurilaitteet ovat eri AS-alueen sisällä, pitää niille ensin luoda ryhmä Group-välilehdestä, johon määritellään vieras AS-alue. Tämän jälkeen naapuri luodaan Neighbors-välilehdestä, ja Group-kohdasta valitaan luotu ryhmä, johon kyseinen naapuri kuuluu.

OSPF-protokolla

OSPF-protokollan käyttöönotto vaatii hieman tuntemusta kyseisestä protokollasta, ja se voidaan konfiguroida monella eri tavalla. OSPF:ssä käytetään runkoverkossa 0-aluetta, johon muut alueet liittyvät. Liittyvät alueet voivat olla tavallisia alueita tai niiden toimintaa voidaan rajoittaa määrittelemällä ne esimerkiksi tynkäverkoiksi. Tynkäverkot eivät ota vastaan ulkopuolisten alueiden reittejä, vaan niiden reititys perustuu oletusreittiin. Stub- ja Totally stub -verkko ovat esimerkkejä tynkäverkkojen tyypeistä.



Kuva 15. OSPF-asetukset.

OSPF-protokollan käyttöönotto aloitetaan asentamalla OpenOSPFd-paketti. Paketin asennuttua asetukset löytyvät Service->OpenOSPFd -välilehdeltä, joka näkyy kuvassa 15. Konfigurointi aloitetaan antamalla reititin-ID. Mikäli kyseinen kenttä jätetään tyhjäksi, ID:nä käytetään automaattisesti suurinta loogista Loopback-osoitetta. Oletetaan, että Pfsense vaihtaa runkoverkon laitteiden kesken tietoja, joten laitetaan Area-kohtaan 0, jolla kuvataan runkoverkkoa.

Redistribute-asetuksilla voidaan määritellä, mitä tietoja välitetään. Valittavissa on yhdistyneiden verkkojen default eli oletusreitin ja staattisten reittien jako. Jaettavat tiedot voidaan myös määritellä käsin sivun alareunassa olevasta Subnet to route -kohdasta. Subnet to route -kohdassa määritetyt reitit ovat ensisijaisia, ja niillä voidaan täydentää tai korvata muita välityssääntöjä.

Interface settings -välilehdestä määritellään liitäntä, joka osallistuu reititystietojen välitykseen. Metric-arvolla määritellään kyseisen liitännän ensisijaisuus, eli paketit kulkevat

sitä reittiä pitkin, jossa on pienin Metric-arvo. MD5-salattu salasana kannattaa asettaa, jotta OSPF-tietojen välitykseen osallistuvat vain ne laitteet, joilla on oikea salasana.

Router priority -arvolla määritellään kyseisen reitittimen prioriteetti DR eli designated router valinnassa. Mikäli verkossa on paljon reitittimiä, suurimman prioriteetin omaava reititin on pääreititin ja toiseksi suurimman prioriteetin omaava varapääreititin eli BDR. Jos pääreititin kaatuu, varareititin siirtyy pääreitittimeksi sekä suoritetaan valinta uuden varareitittimen osalta.

Seuraavaksi asetetaan Hello- ja Retransmit-intervallit. Hello-paketteja käytetään pitämään naapuruussuhteita yllä. Mikäli naapuri ei vastaa Dead timeriin määritellyn ajan kuluessa Hello-pakettiin, se poistetaan naapurilistasta. OSPF-naapureiden tulee lähettää hyväksyntä jokaisesta uudesta LSA:sta eli linkintilamainostuksesta. Retransmit eli uudelleenlähetysajastin määrittelee, minkä ajan kuluessa lähetetään uusi kysely, mikäli naapuri ei vastaa.

Asetusten valmistuttua voidaan status-välilehdestä katsoa, muodostuuko reitittimien välille naapuruussuhde. Mikäli OSPF-naapuruussuhdetta ei laitteiden välille synny, tarkistetaan, että molemmissa laitteissa on vastaavat asetukset. Joissakin tapauksissa naapuruussuhdetta ei synny, koska laitteet eivät yksinkertaisesti ymmärrä toisiaan, koska kyseessä on kuitenkin avoimen lähdekoodin sovellus. Tällaisissa tilanteissa voidaan kokeilla vaihtoehtoista Quagga OSPF -sovellusta.

RIP-protokolla

RIP-protokollan käyttöönotto aloitetaan asentamalla routed-paketti. Paketin asennuttua asetukset löytyvät service->RIP -välilehden alta. Kytketään RIP toimintaan enable RIP -kohdasta ja valitaan LAN-liitäntä. Valitaan protokollaversioksi RIP versio 2 ja asetetaan salasana. RIP-reititystietojen automaattinen summarointi voidaan kytkeä pois asettamalla ruksi no_ag- ja no_super_ag-kohtiin. Summarointi tarkoittaa sitä, että jos Pfsense saa mainostuksena yhdeltä laitteelta esimerkiksi verkon 192.168.1.0/25 ja toiselta laitteelta verkon 192.168.1.127/25, Pfsense automaattisesti laskee verkkoalueet yhdeksi 192.168.1.0/24 -verkoksi.

4.8 Captive portal

Captive portal voidaan konfiguroida käyttämään todennukseen paikallista tietokantaa tai Radius-tietokantaa. Koska käytössä on Radius jo ennestään, asetetaan Captive portali käyttämään sitä.

Aloitetaan valitsemalla liitäntä, josta käyttäjät ohjataan Captive portaliin eli tässä tapauksessa LAN. Asetetaan idle timeout eli aika, jolloin käyttämätön yhteys katkaistaan esimerkiksi 300 minuutin kuluttua. Kytketään uloskirjautumisponnahdusikkuna eli logout popup window toimintaan, josta käyttäjät voivat katkaista yhteyden.

Autentikaatio-kohdasta kytketään Radius-todennus päälle ja käyttämään mschap v2 -protokollaa. Asetetaan ensisijainen todennuspalvelimen osoite käyttämään Pfsensen LAN-osoitetta eli 192.168.1.1 ja portti 1812. Salasanaksi asetetaan mahdollisimman monimutkainen kirjaimien ja erikoismerkkien yhdistelmä.

Asetetaan Captive portal käyttämään HTTPS-protokollaa, jotta kirjautumistunnus ja salasana lähetetään salattuna. HTTPS:n käyttö vaatii palvelimen nimen, esimerkiksi koti.pfsense. Tämä voidaan asettaa yleisistä asetuksista System -> General settings -välilehden takaa kohdasta Hostname ja Domain.

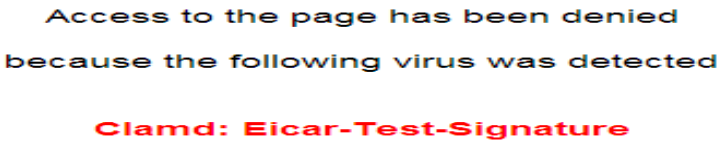
Jotta Captive portal -todennus toimisi Radiuksen kanssa, joudutaan myös muuttamaan FreeRadiuksen-asetuksia seuraavalla tavalla. FreeRadius-asetuksista lisätään NAS/client-välilehteen client Pfsensen LAN -osoitteella eli 192.168.1.1. Salasanaksi asetetaan sama kuin Captive portalin Radius-asetuksiin. Tarkistetaan Interface-välilehdestä, että sieltä löytyy kuunteluliitäntänä Pfsense LAN -osoite. Lisätään Users-välilehteen käyttäjätunnus, jolla voidaan testata todennusta. FreeRadius ja Captive portal voidaan asettaa vaihtamaan todennustietoja paikallisen 127.0.0.1 osoitteen kautta, mutta sen toimintaan saattaminen voi aiheuttaa ongelmia.

Captive portalin toimintaa voidaan kokeilla avaamalla selaimella mikä tahansa sivusto. Pfsensen pitäisi ohjata yhteys suoraan kirjautumissivustolle. Mikäli kirjautumissivusto ei hyväksy tunnuksia, voidaan järjestelmän lokista katsoa epäonnistumisen syytä. Yleensä syy löytyy väärin asetetuista salasanoista, osoitteista tai porteista.

5 Testaus

5.1 Squid- ja HAVP-proxy

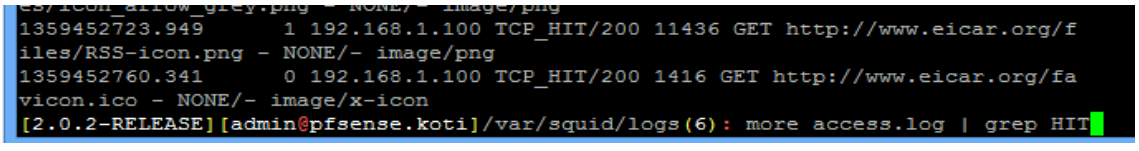
HAVP-proxyn toiminta on helppo testata esimerkiksi Eicar-testivirus tiedoston avulla. Eicar ei ole oikea virus, vaan se sisältää testimerkkijonon, jonka Antivirus-ohjelmistojen valmistajat ovat lisänneet tunnistuskantoihinsa. Eicar-tiedostot löytyvät osoitteesta www.eicar.org. Tarjolla on neljä erilaista tiedostoa. Testitiedostot ovat saatavilla com- ja txt-päätteillä sekä zip-pakattuina tiedostoina.



Kuva 16. HAVP-virheilmoitus.

Aloitetaan lataamalla joku neljästä Eicar-tiedostosta. HAVP:n pitäisi varoittaa viruksesta ja estää tiedoston lataaminen kuten kuvassa 16. Mikäli HAVP ei varoita viruksesta, tarkastetaan, ohjaako Squid liikenteen HAVP:n kautta.

Squid-proxyn toiminnan testaus kannattaa aloittaa vasta, kun Squid on ehtinyt kerätä varastoonsa tiedostoja. Tämän jälkeen voidaan tarkastella /var/squid/logs -kansiosta access.log -tiedostosta, onko välivaraston materiaaliin tapahtunut hakuja. Tämä on helppo toteuttaa komennolla more access.log | grep HIT, kuten kuvassa 17. Kaikki TCP_HIT- tai MEM_HIT-kohdat tarkoittavat osumia välivarastoon tallennettuun materiaaliin.



Kuva 17. Squid-lokien tarkastelu.

Squidin cache.log -tiedostosta voidaan tarkistaa, kuinka paljon materiaalia Squid on ehtinyt tallentaa varastoonsa. Cache.log -tiedostosta voidaan tarkastella myös muita

tietoja, kuten kuinka monta tiedostoa Squid on vapauttanut välivarastosta, välimuistin-koon ja kuinka monesta osoitteesta välimuistin tiedostot on kerätty.

5.2 Snort

Snortin testaus voidaan toteuttaa monella eri tavalla. Esimerkiksi WAN-liitännän tunnistuksia voidaan testata ShieldsUP -sivuston kautta, joka skannaa avonaisia portteja tai Metasploit-ohjelmistolla toisen internet-yhteyden takaa.

Aloitetaan siirtymällä GRC:n Shields up -sivustolle osoitteeseen www.grc.com. Valitaan palveluporttien skannaus ja siirrytään tarkkailemaan Snortin hälytyksiä. Snortin pitäisi hälyttää porttiskannauksesta ja asettaa sivusto torjuttujen listaan, kuten kuvassa 18.

CLASS	SRC	SRCPORT	DST	DSTPORT	SID	DESCRIPTION
Attempted Information Leak	[redacted]		[redacted]		122:5:1	PSNG_TCP_FILTERED_PORTSCAN

Kuva 18. Snort porttiskannaus hälytys.

LAN-liitännän testauksessa voidaan käyttää hieman luovempia tapoja rikkomatta vahingossa tietoturvalakeja. Testaus voidaan toteuttaa esimerkiksi Backtrack-käyttöjärjestelmän avulla. Backtrack sisältää useita tietoturvatestaukseen tarkoitettuja sovelluksia, kuten Nessus ja Metasploit. Backtrack-käyttöjärjestelmän saa ladattua ilmaiseksi osoitteesta www.backtrack-linux.org.

Backtrackilla voidaan esimerkiksi pommittaa SSH-porttia 22 väärennetyillä paketeilla ja samalla seurata Snortin hälytyksiä tai suorittaa laajamittaisen verkkoskannauksen Nessuksella, josta Snortin pitäisi hälyttää.

5.3 Suorituskyvyn mittaaminen

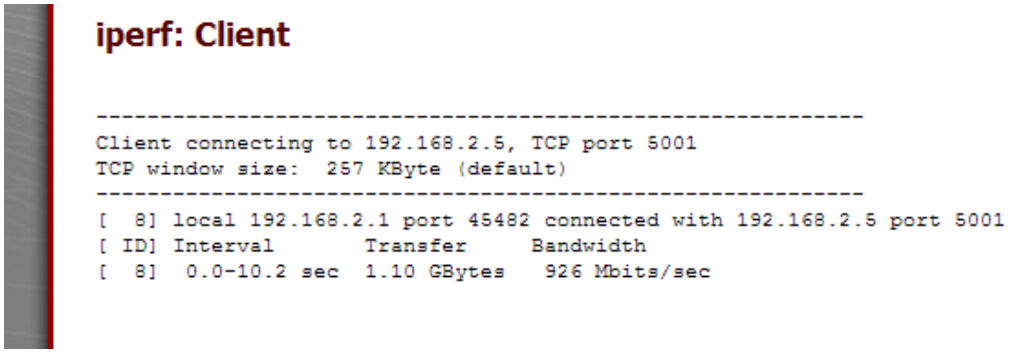
Todellisen suorituskyvyn mittaaminen on hieman hankalaa pienikokoisessa verkossa ilman oikeanlaisia laitteita, eikä mittaustulokset välttämättä pidä täysin paikkaansa. Testaukset pyrittiin suorittamaan mahdollisimman monta kertaa ottaen huomioon tuloksiin vaikuttavat elementit.

Sisäverkon mittauksessa käytettiin FTP-palvelinta, Iperf-sovellusta sekä ilmaista Speedtest mini-verkkosivua, jonka asensin Pfsenseen. Ulkoverkon testauksessa käytin lähinnä Speedtest.net-sivustoa, koska käytössä ei ollut pakettigeneraattoreita tai muita normaalisti vastaaviin testeihin käytettäviä laitteita.

Speedtest minin asentaminen tapahtui luomalla Speedtest-kansio, Pfsensen `/usr/local/www`-juureen. Tämän jälkeen sivustoon pääsi käsiksi selaimella osoitteesta https://ip-osoite/speedtest. Speedtest toimii lähettämällä erikokoisia tiedostoja ja laskemalla, kuinka kauan niiden siirto käyttäjän ja palvelimen välillä kestää.

Ulkoverkon nopeustestausta suoritettiin Speedtest.net -sivuston testillä. Testi suoritettiin myös ilman välityspalvelinta, jotta mahdolliset hidastavat vaikutukset huomattaisiin.

Sisäverkon testauksessa Speedtestin ja Iperf-ohjelmiston avulla saatiin noin 650 Mb/s–900 Mb/s tuloksia, kuten kuvassa 19. FTP-siirrolla maksiminopeus oli luokkaa 60 Mt/s–80 Mt/s, joka vastaa Speedtestin ja Iperfin tuloksia. Testit suoritettiin 1500 ja 9000 MTU-arvoilla. Siirtoja FTP-palvelimelta olisi voitu tehostaa nopeammalla kovalevyllä.



Kuva 19. Iperf tulos.

Ulkoverkon testauksessa Speedtest.net ilmoitti latausnopeudeksi välityspalvelimen kanssa noin 80 Mb/s, ja ilman välityspalvelinta nopeus nousi noin 93 Mb/s. Välityspalvelimenkäyttö siis söi nopeutta noin 10 Mb/s. Kun testausta oli suoritettu useamman kerran ja Squid oli alkanut varastoida Speedtestin testaukseen käyttämiä tiedostoja, latausnopeudet yllättäin nousivat 140–180 Mb/s nopeuteen. Suurella käyttäjämäärällä Squidin kovalevykäyttö voi olla hyvin intensiivistä, mihin kannattaa varautua nopealla SSD-levyllä tai Raid-levypakalla.

6 Yhteenveto

Insinöörityön tarkoituksena oli perehtyä ja käyttöönottaa Pfsense -palomuurikäyttöjärjestelmä, jonka käyttö ei vaadi FreeBSD-alustan tuntemusta. Pfsense saatiin käyttöönotettua onnistuneesti, eikä käyttöönotto tai käyttö vaatinut FreeBSD:n komentoihin perehtymistä. Kaikki konfiguraatiot pystyttiin suorittamaan suoraan Webkonfiguraattorista.

Suorituskyvyssä Pfsense rajoittuu tällä hetkellä käytettävän laitteiston fyysisiin rajoituksiin, eikä sitä sen takia voi varsinaisesti verrata vastaaviin kaupallisiin laitteisiin, jotka ovat räätälöity niissä käytettävien käyttöjärjestelmien ympärille. Kokoonpanossa suorituskyky rajoittui selkeästi verkkokorttien PCI-väylien tiedonsiirtonopeuteen. Tulevaisuudessa PCI-e-väyläisten verkkokorttien yleistyessä Pfsensestä saadaan enemmän tehoa irti. Suorituskykyä testattiin FTP-siirroilla, Speedtest-mini-sivustolla ja Iperf-ohjelmistolla. Suorituskyky oli odotettua suurempi ja joiltain osin verrattavissa Ciscon ASA 5510-palomuuriin, jonka hintalapussa lukee noin 2000 euroa. Mikäli asennuslaitteistoon olisi panostettu kyseinen summa, olisi suorituskyvyssä päästy huomattavasti parempiin tuloksiin.

Antivirus- ja tunkeutumisenesto-ominaisuuksia ei myöskään voida verrata vastaaviin kaupallisiin laitteisiin, koska kaupallisten laitteiden tunnistuskantoja päivitetään useammin. Pfsensessä voidaan toki käyttää kaupallisia tunnistuskantoja kuten AVG-antivirus HAVP:in kanssa tai SourceFiren tunkeutumiseneston tunnistuskantoja Snortin kanssa. Näitä ei kuitenkaan ollut mahdollista opinnäytetyötä tehdessä kokeilla kalleuden vuoksi. HAVP-ominaisuuksia testattiin viruksilla ja niiden pääsy verkkoon estettiin onnistuneesti. Tunkeutumisenesto-ominaisuuksia testattiin monilla menetelmillä, ja Snort esti yritykset useimmissa tapauksissa. Ilmaiset tunnistuskannat aiheuttivat kuitenkin todella paljon vääriä tunnistuksia Snortin ja HAVP:n käytössä.

Pfsense on olevan helposti omaksuttava palomuurikäyttöjärjestelmä, jonka ominaisuudet laajenevat jatkuvasti. Se tarjoaa ominaisuuksia, joita on normaalisti totuttu näkemään vain kalliissa kaupallisissa laitteissa. Avoimen lähdekoodin käyttöjärjestelmät ovat yleensä hitaasti päivittyviä, minkä takia Pfsense onkin loistava esimerkki siitä, mitä yrityksen eteenpäin vievä avoimen lähdekoodin projekti voi parhaimmillaan olla. Pfsenseä päivitetään todella paljon, ja päivityksissä reagoidaan myös paljon käyttäjäkunnan löytämiin ongelmiin, vikoihin, puutteisiin ja toiveisiin.

Kotikäyttäjille ja pienille yrityksille Pfsense voi olla suuri säästö tietoturvan rakentamisessa, jos otetaan huomioon kertamaksut ja vuosittaiset lisenssimaksut. Avoimen lähdekoodin käyttöjärjestelmissä on kuitenkin aina omat riskinsä, mutta kalleinkaan laite ei suojaa verkkoa, jos toteutettava verkko on huonosti suunniteltu.

Lähteet

1 History of Pfsense. 2012. Verkkodokumentti. BSD Perimeter LLC. <http://www.pfsense.org/index.php?option=com_content&task=view&id=68&Itemid=76>. Luettu 18.11.2012

2 Background on the name Pfsense. 2007. Verkkodokumentti. <http://blog.pfsense.org/?p=114>. Päivitetty 21.6.2007. Luettu 18.11.2012.

3 Features of Pfsense. 2013. Verkkodokumentti. BSD Perimeter LLC. <http://www.pfsense.org/index.php?option=com_content&task=view&id=40&Itemid=43>. Luettu 20.11.2012.

4 About Snort. 2012. Verkkodokumentti. <http://www.snort.org/snort>. Luettu 19.11.2012.

5 Hardware Sizing Guidance. 2013. Verkkodokumentti. BSD Perimeter LLC. <http://www.pfsense.org/index.php?option=com_content&task=view&id=52&Itemid=49>. Luettu 21.1.2013.

6 Pfsense foorumi keskustelu. 2012. Verkkodokumentti. BSD Perimeter LLC. <http://forum.pfsense.org/index.php?topic=53743.0>. Luettu 20.11.2012.

7 Installing Pfsense. 2012. Verkkodokumentti. BSD Perimeter LLC. <http://doc.pfsense.org/index.php/Installing_pfSense>. Päivitetty 21.1.2012. Luettu 20.11.2012.

8 Setup Squid as a Transparent Proxy. 2009. Verkkodokumentti. BSD Perimeter LLC. <http://doc.pfsense.org/index.php/Setup_Squid_as_a_Transparent_Proxy>. Päivitetty 28.4.2009. Luettu 6.12.2012.

9 Squid package tuning. 2011. Verkkodokumentti. BSD Perimeter LLC. <http://doc.pfsense.org/index.php/Squid_Package_Tuning>. Päivitetty 31.12.2011. Luettu 6.12.2012.

10 Setup snort package. 2009. Verkkodokumentti. BSD Perimeter LLC. <http://doc.pfsense.org/index.php/Setup_Snort_Package>. Luettu 6.12.2012

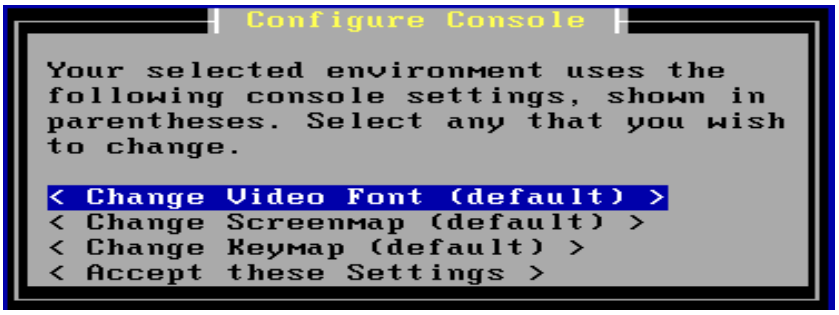
11 FreeRadius 2.x package. 2013. Verkkodokumentti. BSD Perimeter LLS <http://doc.pfsense.org/index.php/FreeRADIUS_2.x_package>. Päivitetty 28.1.2013. Luettu 5.3.2013.

12 Setup & Configuration of OpenVPN on Pfsense 2.0 RC3. 2013. Verkkodokumentti. <http://www.apollon-domain.co.uk/?p=433>. Luettu 5.3.2013.

13 Pfsense VPN Capability. 2010. Verkkodokumentti. BSD Perimeter LLC. <http://doc.pfsense.org/index.php/VPN_Capability_IPsec>. Päivitetty 4.2.2010. Luettu 10.12.2012.

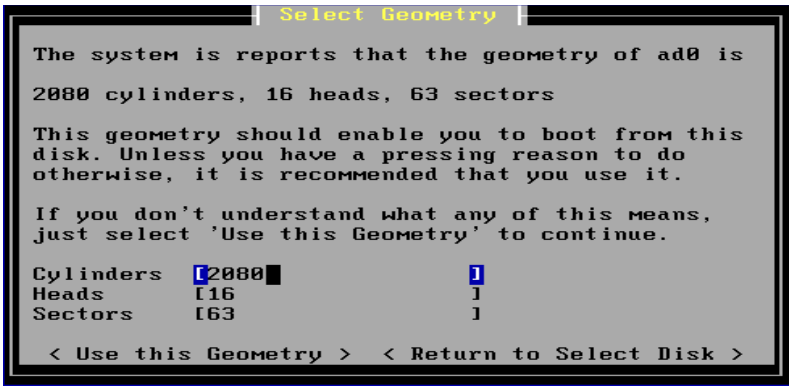
14 Pfsense History. 2013. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/PfSense>. Luettu 5.3.2013.

Asennus kuvia

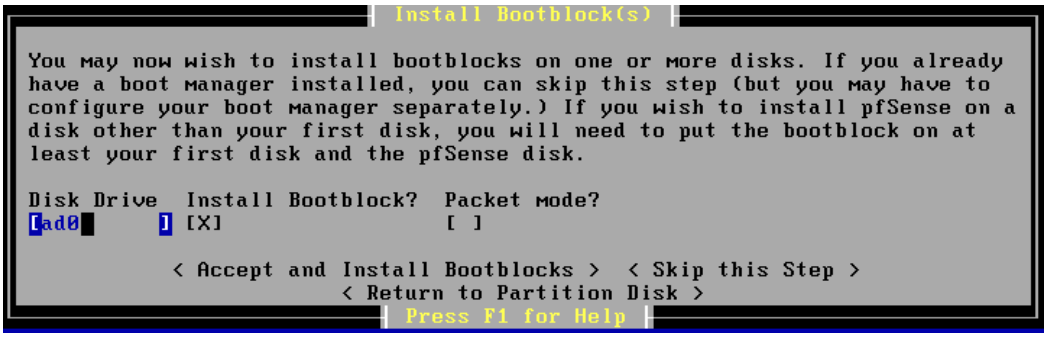


Kuva 1. Konsoli asetukset.

Kuva 2. Levyn formatointi



Kuva 3. Levyn geometria



Kuva 4. Käynnistys lohko