TiTeLAN

Lähiverkon toteutus

Rami Kallio

Opinnäytetyö
Maaliskuu 2012
Tietotekniikka
Tietoliikennetekniikka
ja tietoverkot

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka ja tietoverkot

Rami Kallio:
TiTeLAN
Lähiverkon toteutus

Opinnäytetyö on 37 sivua
Maaliskuu 2012

TiTeLAN on TAMKin tietotekniikan koulutusohjelman opiskelijoiden järjestämä verkkopelitapahtuma. Verkkopelitapahtuma on tilaisuus, johon kukin osallistuja tuo mukanaan oman tietokoneensa ja pelaa sillä pelejä lähiverkossa muiden osallistujien kanssa. Verkkopelitapahtuman ideana on tuoda pelaamisesta pitäviä ihmisiä yhteen pitämään hauskaa samanhenkisten ihmisten kanssa. Tämä opinnäytetyö käsittelee TiTeLAN-verkkopelitapahtuman lähiverkon toimintaa.

Työn alussa käsitellään verkkotopologian suunnitelua pelitapahtumalle sopivaksi. Verkon toimintaa käsittelevän osuuden on tarkoitus antaa lukijalle kuva lähiverkossa toimivista palveluista, verkkoon kohdistuvista uhista ja miten niitä voidaan torjua. Työn lopussa käsitellään uusi palomuuri/reititin-käyttöjärjestelmä pfSense, joka on ollut käytössä vasta kahdessa tapahtumassa ja on osoittautunut hyväksi ratkaisuksi. Sen ominaisuuksista käydään läpi vain verkkopelitapahtuman kannalta tärkeimmät asetukset.

Verkon ylläpitäjältä odotetaan vähintään CCNA-kurssin läpäisemistä, koska vain tapahtuman kannalta tärkeimmät asetukset käydään läpi. Ciscon peruskonfiguraatioita käsitellään vain niissä tapauksissa, joissa ne ovat osana suurempaa kokonaisuutta.
Turvallisuus syistä kaikki verkon tunnukset ja IP-osoitteet on vaihdettu.

Asiasanat: verkkopelitapahtuma, lähiverkko, kytkin, reititin

ABSTRACT

Tampere University of Applied Sciences
Bachelor of Engineering (Computer Systems)
Specialization in Telecommunication

Rami Kallio:
TiTeLAN
Implementation of local area network

Bachelor's thesis is 37 pages
May 2012

TiTeLAN is a LAN party organized by the Computer Systems Engineering students. LAN party is an event where each participant brings his/hers computer and plays computer games in the local area network with other participants. The idea of a LAN party is to bring together game loving people to play videogames and have fun together. This thesis takes a look at the thing that makes this kind of event possible, the functions of the local area network.

At the beginning of the thesis we will take a look at the network topology designed specifically for a LAN party. After that we will go through what kind of services run in the LAN, what threats there can be and how they can be prevented. At the end of the thesis we will take a look at our new firewall/router operating system pfSense.

The reader is required to have completed at least CCNA-course, since only the most important configurations will be looked at. Only some basic configurations are included as they are needed for the advanced ones to work.
For security reasons, all login details and IP addresses are changed from the originals.

Key words: LAN party, network, switch, router

SISÄLLYS

LYHENTEET JA TERMIT

ACL	Access Control List, pääsylista johon voidaan määrittää toimintatapoja eri verkkoprotokollille
Agregointi	Verkkolaitteiden liittämistä toisiinsa, kahdella tai useammalla linkillä, tarkoittava termi
DHCP	Dynamic Hosting Configuration Protocol, lähiverkon tietoja ja asetuksia välittävä palvelu
DDoS	Distributed Denial of Service, laaja DoS-hyökkäys johon osallistuu useita laitteita samanaikaisesti
DNS	Dynamic Name Server, nimipalvelin joka pitää listaa sivustoista ja niiden palvelimien IP-osoitteista
DoS	Denial of Service, palvelunestohyökkäys jonka tarkoituksena on häiritä tai kaataa kohteena oleva palvelin
GUI	Graphical User Interface, graafinen käyttöliittymä
HTTP	Hyper Text Transfer Protocol, salaamaton internetselain protokolla
HTTPS	Hyper Text Transfer Protocol Secure, salattu versio HTTP:stä
LAN	Local Area Network, lähiverkko joka sijoittuu maantieteellisesti pienelle alueelle
NIC	Network Interface Controller, verkkokortti
Proxy	Välityspalvelu, välittää yhteyksiä esim. internetsivustoille
PVST / PVST+	Per-VLAN Spanning Tree, Ciscon kehittämä spanning tree protokolla
QoS	Quality of Service, verkkoliikenteen eri tyyppisten pakettien priorisointia tarkoittava termi
STP	Spanning Tree Protocol, verkon rakennetta tutkiva toiminto joka estää silmukoiden syntymisen topologiaan

VPN	Virtual Private Network, menetelmä jolla kahta tai useampaa maantieteellisesti eri paikassa sijaitsevaa lähiverkkoa voidaan yhdistää julkisen verkon yli yhdeksi loogiseksi lähiverkoksi
WAN	Wide Area Network, ison alueen kattava verkko esim. kaupunginosan tietoverkko
wizard	velho, helppokäyttötoiminto jonka tarkoitus on yksinkertaistaa monimutkaisten asetusten tekeminen käyttäjälle
WLAN	Wireless Local Area Network, langattomalla tekniikalla toteutettu lähiverkko

1 JOHDANTO

TiTeLAN on Tampereen ammattikorkeakoulun tietotekniikan koulutusohjelman opiskelijoiden järjestämä verkkopelitapahtuma. Tapahtuma on täysin ilmainen TAMKin opiskelijoille. Tämä projekti aloitettiin vuonna 2008, kun silloiset ensimmäisen vuoden opiskelijat keksivät, ettei TAMKissa oltu aikaisemmin järjestetty verkkopelitapahtumaa.

Tämän opinnäytetyön tarkoitus on toimia apuna TiTeLAN-projektia jatkaville opiskelijoille tai samankaltaista tapahtumaa suunnitteleville henkilöille.
Työn alussa käydään läpi verkontopologiaa ja DHCP-palvelun toimintaa. Topologian suunnittelu on varsinkin tärkeää, koska se vaikuttaa ratkaisevasti verkon toimivuuteen.

Topologian jälkeen perehdytään verkon tietoturvallisuuteen, jonka tarkoitus on antaa lukijalle kuva, miten erityyppiset hyökkäykset toimivat ja kuinka niitä voidaan estää.
Kommentoiduilla esimerkki konfiguraatioilla, jotka on kehystetty selvyyden vuoksi, esitetään kuinka turvallisuutta voidaan lisätä.

Työn lopussa keskitytään esittelemään palomuuri/reititin-käyttöjärjestelmä pfSenseä, joka vaihdettiin aikaisemmin käytössä olleen Ciscon reitittimen tilalle. Kappaleen alusta löytyy pfSenselle tehty ohje asennukseen ja perusasetusten tekemiseen. Sen ominaisuuksista käydään läpi mm. web cache –toiminto, sivustosuodatin ja kuormantasaus.

2 VERKKOTOPOLOGIA

Verkon topologiaksi on valittu tornityyppi, koska osa kytkimistä pitää olla aina siirreltävissä tarpeen mukaan. Ainoastaan pääkytkin, palvelin/admin-kytkin ja reititin ovat samassa räkkikaapissa (kuvassa 1 punaisella merkitty alue). Mobiilin laitekaapin suunnitteli ja rakensi Kalle Koivumäki, joka oli myös vastuussa ensimmäisten tapahtumien tietoverkon suunnittelemisesta.

Verkko koostuu yhdestä reitittimestä, kahdesta runkokytkimestä, useasta verkkokytkimestä ja valtavasta määrästä verkkokaapelia. Runkokytkin eroaa tavallisista verkkokytkimistä siten, että se kykenee käsittelemään tietoa useita kertoja nopeammin. Molemmat runkokytkimet on sijoitettu mobiiliin laitekaappiin.
Verkossa toimi Ciscon reititin vuodesta 2008 lähtien, kunnes 2011 syksyllä otettiin käyttöön uusi palomuuri/reititin-järjestelmä pfSense. Sen ominaisuuksiin perehdytään tämän työn kappaleessa 5. Reitittimen pääasiallinen tehtävä, tämän kaltaisessa tapahtumassa, on suodattaa liikennettä ja toimia palomuurina. Reititys toteutetaan staattisena, koska topologia sisältää vain yhden reitittimen. Staattista reititystä on suositeltavaa käyttää pienissä verkoissa, jolloin konfiguroinnista tulee yksinkertaisempi ja nopeampi toteuttaa.

2.1 IP-osoitesuunnitelma

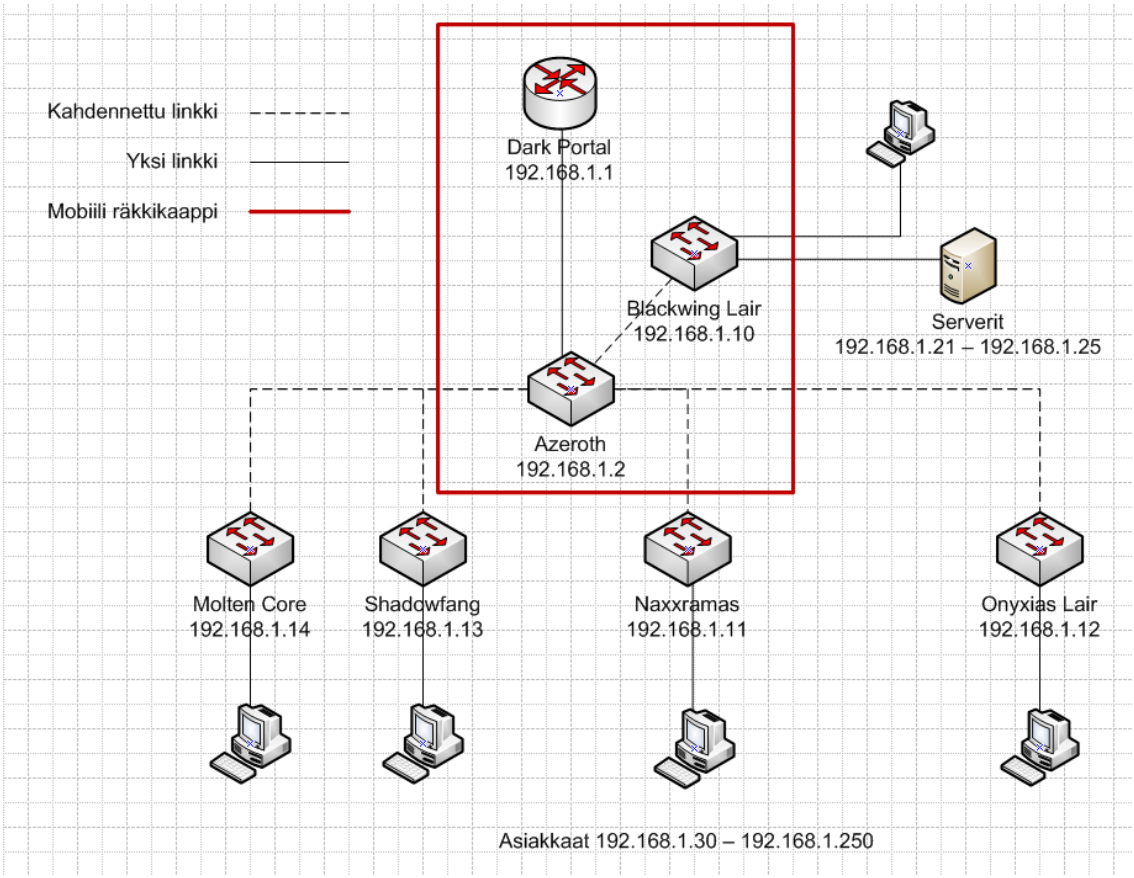
Turvallisuus syistä kaikki tapahtuman IP-osoitteet on vaihdettu ja tilalle on luotu verkko toimimaan esimerkkinä. Esimerkkinä luotuun verkkoon valitaan 192.168.1.0 /24 aliverkko, jonka IP-osoitteiden jako toteutetaan seuraavasti:

- Verkkolaitteet: 192.168.1.1 – 192.168.1.20
- Palvelimet: 192.168.1.21 – 192.168.1.25
- Asiakaskoneet: 192.168.1.30 – 192.168.1.250

Verkkolaitteita on ollut käytössä normaalisti 8. Osoiteita on varattu 20, jos tapahtumaa laajennetaan ja käyttöön otetaan toinen toinen verkko. Palvelimia on enimmillään ollut 5 kappaletta ja jokaisessa on toiminut n. 4 palvelua samanaikaisesti. Palvelinlaitteistoon

saatiin lahjoituksena 2 tehokasta HP:n palvelinta, joten tarvittavien IP-osoitteiden määrä väheni huomattavasti. Osallistujia on ollut enimmillään 120 ja järjestäjiä noin 15, joten 220 osoitetta riittää hyvin asiakkaille. Palvelimille ja asiakkaille varattujen osoitteiden väliin on jätetty tarkoituksella muutama käyttämätön osoite varalle, jos laitteita tuleekin käyttöön ennakoitua suurempi määrä.

Microsoft Visiolla luotu topologia- ja IP-osoitesuunnitelma on esitetty kuvassa 1.



Kuva 1. Verkon topologia

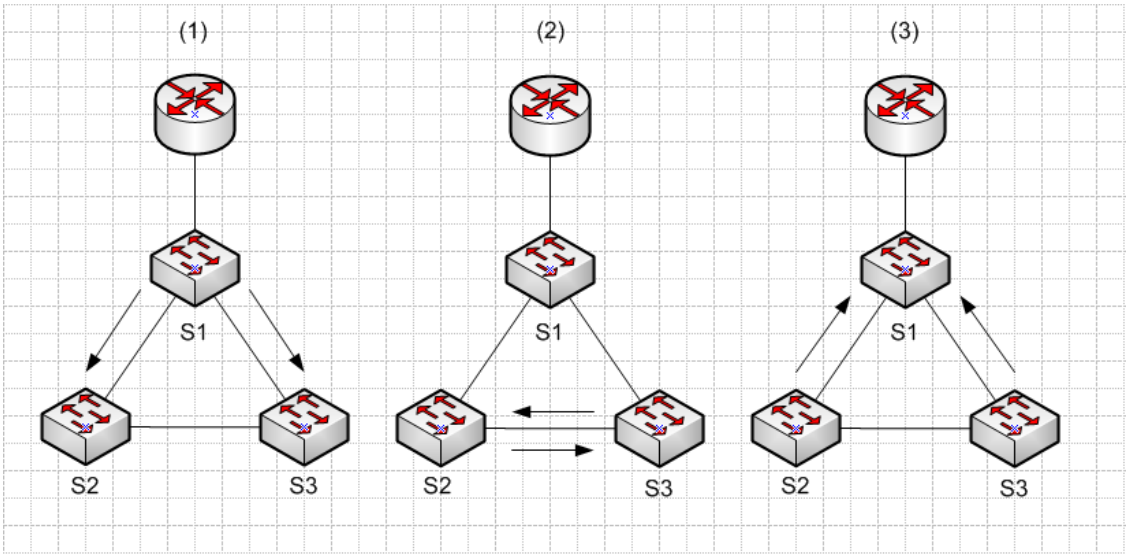
2.2 Kuormantasaus

Yksi ongelmallisimpia tekijöitä tietoverkoissa on käytettävän kaistan riittävyys. Kaikissa verkoissa kaistankäyttö muuttuu kellonajan mukaan ja tiettyinä aikoina esiintyy käytössä piikki, jolloin verkon kapasiteetti on äärirajoillaan. Piikkiä ei voida

estää, mutta sitä voidaan pienentää. Tästä syystä järjestelmästä tulisi tehdä mahdollisimman kevyt, jolloin minimoidaan ruuhka-aikana tapahtuva hidastuminen.

TiTeLAN-verkon kuormantasauksesta saadaan suurinosa aikaan käyttämällä agregoituja linkkejä. Agregointi tarkoittaa kahden verkonlaitteen esim. kytkimien yhdistämistä kahdella tai useammalla linkillä toisiinsa. Oletuksena verkkokytkimissä on päällä Spanning Tree Protocol (STP), joka estää agregoinnista sytyviä silmukoita muodostumasta verkkotopologiaan. Tämä tekniikka kehitettiin estämään broadcast-myrskyjen syntymistä.

Jos verkkotopologiassa on silmukoita, kuten kuvan 2 esimerkissä, se saattaa aiheuttaa vakavan ongelman. Ongelma johtuu pääasiallisesti kytkimien pakettien käsittelytavasta. Kun kytkin saa broadcast-viestin, se lähettää viestin eteenpäin jokaiseen porttiinsa. Tässä esimerkki tapauksessa ylin kytkin lähettää broadcast-viestin molemmille alimmille kytkimille (1). Nämä kaksi taas lähettävät toisilleen saman viestin (2) ja sen jälkeen ylemmälle kytkimelle (3). Tämä jatkuu loputtomiin, ellei silmukkaa rikota esim. ajamalla yksi linkeistä alas. Tätä tapahtumaa kutsutaan nimellä broadcast-myrsky (broadcast storm) (Donahue 2007, 66-67.)



Kuva 2. Esimerkki silmukasta

Broadcast-myrsky syö verkon suorituskykyä valtavat määrät ja pahimmillaan se voi aiheuttaa verkon täydellisen pysähtymisen.

Verkkokytkimissä käytetään Ciscon Per-VLAN-Spanning-Tree protokollaa, joka kehitettiin päivitykseksi IEEE:n STP-standardiin. Jälkeenpäin Cisco paranteli PVST:tä, koska se käytti Ciscon omaa paketointimenetelmää (encapsulation) ja ei tästä syystä ollut yhteensopiva muiden laitevalmistajien laitteiden kanssa. Näin syntyi PVST+, joka oli yhteensopiva IEEE:n standardin kanssa. PVST on siitä hyödyllinen, että se käsittelee VLANit eri instansseina. Tämä mahdollistaa kuorman jakamisen agregoitujen linkkien yli.

2.3 Quality of Service

Quality of Service (QoS), lyhyesti selitettynä, on tietotekniikassa resurssien priorisointia tarkoittava termi. Koska kyseessä on pakettikytkentäinen järjestelmä, verkossa kulkevia paketteja voidaan merkitä käsiteltäväksi tietyllä prioriteetillä. Korkea prioriteettisiä paketteja ovat esimerkiksi puhedataa sisältävät VOIP-paketit, joiden myöhästyminen kohteesta aiheuttaa haittaa (äänen pätkiminen). Pienen prioriteetin omaavia paketteja ovat mm. sähköposteja ja tiedostoja sisältäviä data-paketteja, joita ei haittaa vaikka ne saapuisivatkin väärässä järjestyksessä kohteeseensa.

Verkkopelitapahtumassa tulisi asettaa verkkopelit aina samalle tai korkeammalle prioriteetille, kuin VOIP-liikenne. Lisäksi P2P-liikenne kannattaa asettaa pienelle prioriteetille, koska se yleensä vie valtavasti käytettävänä olevasta kaistasta.
Kaikki muu liikenne on toissijaista ja voidaan asettaa pienelle prioriteetille.

3 DHCP-PALVELIN

DHCP (Dynamic Hosting Configuration Protocol) on palvelu, joka mahdollistaa IP-osoitteiden ja muiden verkonasetusten jakamisen automaattisesti verkon sisällä. Jos tätä palvelua ei käytettäisi, kaikki asetukset pitäisi laittaa käsin jokaiselle laitteelle. Tämän palvelun käyttö on erittäin suositeltavaa kaiken kokoisissa verkoissa, koska se säästää valtavasti aikaa ja vaivaa.

Kun tietokone liitetään verkkoon, se lähettää kyselyn DHCP-palvelimesta broadcastina. Tämä kysely sisältää tietoja tietokoneesta esim. verkkokortin (NIC) MAC-osoitteen. DHCP-palvelimen saadessa tämä paketti, se vertaa tietokoneen tietoja lokiinsa. Jos asiakaslistasta ei löydy ko. tietokonetta, palvelin lähettää tietokoneelle tiedot IP-osoitteesta ja verkonasetuksista. Paketin saapuessa, tietokone kirjoittaa saadut tiedot muistiin ja tekee tarvittavat muutokset. Lisäksi se lähettää kuittausviestin DHCP-palvelimelle. Jos vastausta ei kuulu, yrittää lähettävä osapuoli uudestaan muutamia kertoja ennen kuin luovuttaa (Koivumäki 2010, 7.)

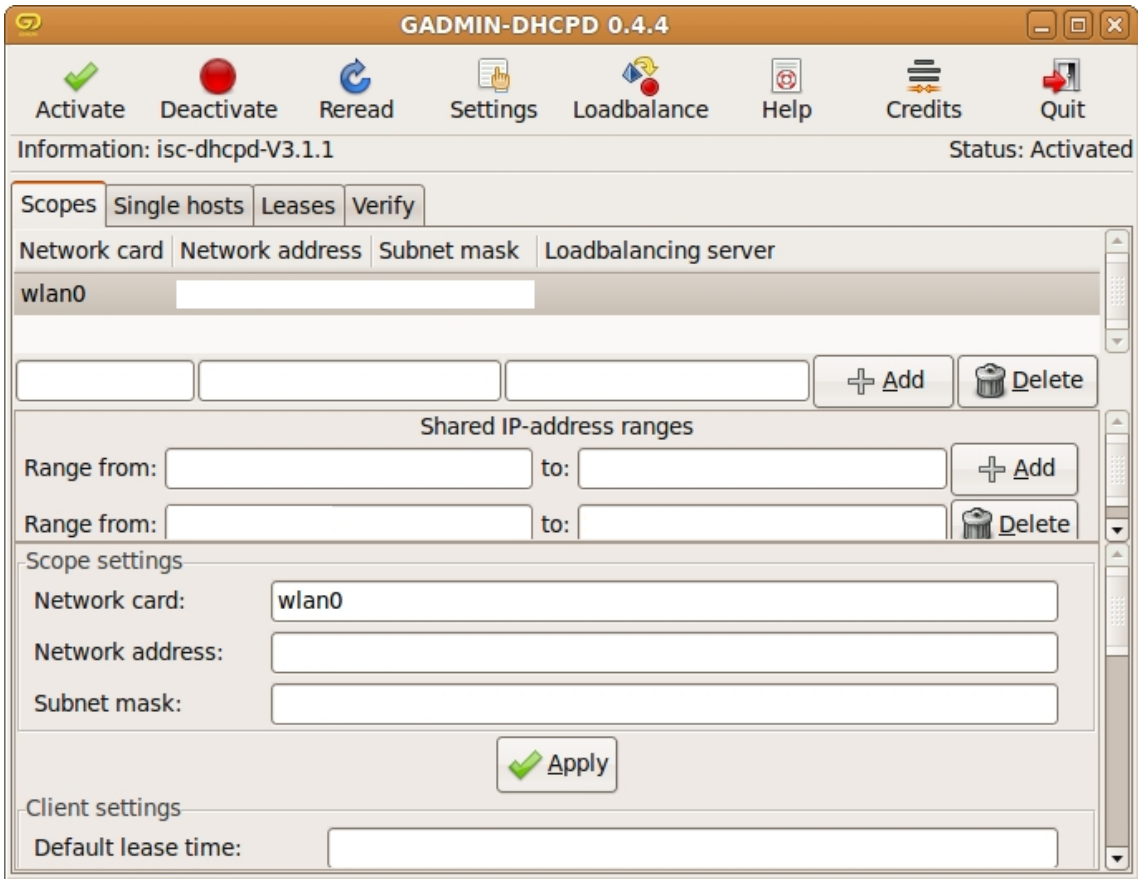
DHCP-palvelin voi jakaa osoitteita kolmella eri tavalla, jolloin se käsittelee verkkolaitteiden pyynnöt eri tavoin.

Dynaamisesti toimivassa DHCP-palvelimessa ylläpitäjä antaa sille yhden tai useamman IP-osoite avaruuden, joista asiakaslaitteille jaetaan omat osoitteet. Nämä osoitteet on varattu ko. laitteiden käyttöön ajaksi, jonka ne ovat liitettynä verkkoon. Kun laite irroitetaan verkosta, DHCP-palvelin huomaa ko. laitteen tavoittamattomaksi ja vapauttaa laitteen käytössä olleen IP-osoitteen.

Automaattinen DHCP-palvelin toimii lähes samalla tavalla kuin dynaaminen. Erona on kuinka pitkään saatu IP-osoite on laitteen käytössä. Vaikka laite irroitetaan verkosta, se kuitenkin säilyttää varauksen määrätyn ajan. Kun laite liitetään takaisin verkkoon, ennen kuin varausaika loppuu, se saa vanhan osoitteensa uudelleen. Esimerkiksi internet operaattorit jakavat IP-osoitteet asiakkailleen tällä periaatteella.

Staattinen DHCP-palvelin jakaa verkonlaitteille MAC-osoitteisiin sidotut IP-osoitteet. Esimerkiksi TiTeLANien palvelimien IP-osoitteet jaetaan tällä tavalla.

DHCP-palvelimena käytettiin tavallista tietokonetta, johon asennettiin DHCP-palvelinohjelmisto.
Käyttöjärjestelmänä tässä tietokoneessa käytettiin Debianin Linux-jakeluun pohjautuvaa Ubuntua, koska se on ilmainen käyttöjärjestelmä. DHCP-ohjelmistona käytettiin Gadminin DHCP-palvelinohjelmistoa (kuva 3). Ohjelma on yksinkertainen käyttää ja sillä pystyy luomaan nopeasti uusia osoitealueita.



Kuva 3. Gadmin DHCP-palvelin

4 TIETOTURVALLISUUS

Ensimmäinen ja ehdottomasti tärkein asia tietoturvallisuudessa on estää fyysinen pääsy laitteistoon. Valitettavasti tämän asian tärkeyttä vähätellään liian usein ja laitteisto sijoitetaan vain lukittavaan tilaan. Yleensä tämä on riittävä toimenpide ehkäisemään vahingontekoa. Lisäksi olisi erittäin tärkeää sijoittaa kaikki käytössä oleva ja käyttämätön tietotekniikka lukittuihin kaappeihin. Avaimia tulisi valvoa tarkasti, etteivät ne eivät joudu vahingossakaan ulkopuolisten henkilöiden käsiin.

Kun fyysinen pääsy on estetty, seuraavaksi rajataan pääsy laitteisiin verkon kautta. Vaikka kaikissa laitteissa olisikin kirjautumisen taakse asetettu pääsy, voidaan se silti murtaa. Vaikeutta tähän saadaan lisää sallimalla etäkäytön yhteydenotot vain tietyistä osoitteista. Alapuolella on esimerkki kuinka kytkimeen S1 sallitaan etäyhteys ainoastaan lähdeosoitteista 192.168.1.1 ja 192.168.1.2, käyttämällä Access Control Listiä (ACL) eli pääsylistaa apuna.

```
Sallitaan ip 192.168.1.1.
S1 (config) # access-list 1 permit 192.168.1.1
Sallitaan ip 192.168.1.2.
S1 (config) # access-list 1 permit 192.168.1.2
Estetään yhteys, jos lähdeosoite ei vastaa ylempänä annettuja osoitteita.
S1 (config) # access-list 1 deny any
Määritetään etäyhteys käyttämään access-list 1:ssä määritettyjä sääntöjä suodattamaan
sisääntulevia yhteyksiä.
S1 (config) # line vty 0 15
S1 (config-line) # access-class 1 in
```

4.1 MAC-tulva

MAC-tulva (MAC flooding) on hyökkäystapa, jota käytetään sekoittamaan verkkokytkimiä. Sekaisin olevat kytkimet vuotavat kaikkialle verkkoon, sinne kuulumatonta dataa. Tatum (2012) kuvaa MAC-tulvaa seuraavasti:

MAC flooding is a method that can be used to impact the security protocols of different types of network switches. Essentially, MAC flooding inundates the network switch with data packets that disrupt the usual sender to recipient flow of data that is common with MAC addresses. The end result is that rather than data passing from a specific port or sender to a specific recipient, the data is blasted out across all ports.
The basics of MAC flooding begin with a corruption of the translation table that is part of the function of the network switch. When functioning properly, the table will map each individual MAC address that is found on the network. Each MAC address is associated with a physical port on the network switch. This approach makes it possible to designate a specific and single point of termination for data sent across the network.
By flooding the switch with data packets, the translation table is thrown out of kilter and the connection between the ports and specific MAC addresses is destroyed. Instead, any data that is intended for a single MAC address is now sent out on all ports associated with the network. This means that any type of data that was intended for a single address is received by multiple addresses.

Käytännössä hyökkääjä hukuttaa verkkokytkimen data-paketeilla, joiden tarkoitus on sekoittaa MAC-kohdeosoitteita käyttävä liikenne. Tämän seurauksena kytkin alkaa lähettää saamiansa paketteja kaikista porteista.
Hyökkäyksen toimintaperiaate on yksinkertainen: Korruptoidaan kytkimen MAC-käännöstaulukko. Normaalisti tähän taulukkoon kytkin merkitsee kaikki verkosta löytyvät MAC-osoitteet ja jokainen osoite on sidottu tiettyyn kytkimen porttiin.
Kun kytkin hukutetaan paketteihin, käännöstaulukko menee sekaisin. Kaikki sidokset porttien ja MAC-osoitteiden välillä tuhoutuvat. Paketit, joiden päämääränä on tietty

MAC-osoite, lähetetäänkin kaikista kytkimen porteista. Normaalisti paketti kulkisi ainoastaan tietystä portista, koska kaikki tarvittava tieto löytyisi MAC-käännöstaulusta. Tämän jälkeen kuuntelemalla verkonliikennettä pystytään helposti saamaan selville salasanoja, käyttäjätunnuksia, lukemaan sähköposteja jne. (Tatum 2012.)

Koska MAC-tulva aiheuttaa vakavan tietoturvariskin, laitevalmistajat sisällyttävät toimintoja estämään mahdollisia urkkimisyrityksiä. Ciscon kytkimissä MAC-osoitteiden rajoittamiseen löytyy port-security –toiminto, jolla rajoitetaan sallittuja MAC-osoitteita kytkimen porteissa.

```
Määritetään samat asetukset kaikille FastEthernet porteille.
S1 (config) # interface range FastEthernet 0/1-24
Määritetään porttien olevan access-tyyppisiä.
S1 (config-if-range) # switchport mode access
Asetetaan porttisuojaus sulkemaan portti, jos siinä esiintyy enemmän kuin 3 MAC-osoitetta.
S1 (config-if-range) # switchport port-security
S1 (config-if-range) # switchport port-security maximum 3
S1 (config-if-range) # switchport port-security violation shutdown
```

Tämä aiheuttaa ristiriidan VPN-ohjelmisto Hamachin kanssa. Hamachilla voidaan luoda virtuaalinen lähiverkko, johon voi liittyä kuka tahansa. Yleisesti sitä käytetään luomaan lähiverkko, jossa toimii pelipalvelin.
Käytännössä Hamachi luo virtuaalisia MAC-osoitteita, jolloin aiemmin tehty rajoitus aiheuttaa rikkomuksen ja kytkin sulkee ko. portin. Tämä aiheutti valtavan määrän päänvaivaa ensimmäisessä tapahtumassa, ennen kuin ongelma löydettiin. Tästä syystä Hamachin käyttö kiellettiin.

4.2 Palvelunestohyökkäys

Denial of Service (DoS) on MAC-tulvan kaltainen hyökkäys, joka kohdistetaan yleensä palvelimiin. DoS-hyökkäyksen tarkoitus on saada palvelin jumiutumaan kuormasta tai kaatumaan. Tästä syystä hyökkäysten kohteina ovat usein suurien internetsivujen tai yritysten palvelimet. Käsiteltäessä DoS-hyökkäyksiä, tulee usein vastaan termi DDoS eli Distributed Denial of Service (laaja palvelunestohyökkäys). DDoS eroaa DoS-hyökkäyksestä siten, että hyökkääviä laitteita on useita.

Tulvaaminen tapahtuu, kun palvelin yrittää vastata valtavalle määrälle käyttäjiä samanaikaisesti. Tämä syö palvelimen resursseja ja pakottaa sen olemaan vastaamatta osaan pyynnöistä. Pelkkä tulvaaminen ei yleensä riitä kaatamaan palvelinta, vaan siihen joudutaan käyttämään hyödyksi palvelinohjelmistossa olevaa haavoittuvuutta. Yleensä tulvaamiseen käytetään tietokoneohjelmaa, joka luo monta valekäyttäjää ja alkaa tulvata kohdepalvelinta näiden valekäyttäjien pyynnöillä (Wiesen 2012.)

Tapahtumassa ei tarvitse pelätä DoS-hyökkäystä kolmesta syystä: Tapahtuma kestää 3 päivää, pääsy ulkoverkosta sisäverkkoon on estetty ja tekijä pystytään helposti jäljittämään jos hyökkäys tapahtuu sisäverkosta. Kaikki häiritsevä ja haitallinen toiminta tietoverkoissa on Suomen riskoslain luvussa 38 (578/1995) määrätty rangaistavaksi teoksi.

4.3 Man in the middle -hyökkäys

Man in the middle on hyökkäystyyppi, jossa hyökkääjä sijoittaa itsensä käyttäjän ja palvelun väliin. Tätä menetelmää käytetään usein langattomissa verkoissa, joissa hyökkääjä luo WLAN-verkon samalla nimellä, kuin verkon laillinen omistaja. Tietämättömät käyttäjät ottavat yhteyttä todennäköisimmin valeverkkoon, joka kuuluu yleensä paremmin. Yleensä käyttäjille tulee ensimmäisenä vastaan sivu, jolla kalastellaan tunnuksia, luottokorttitietoja jne.

Jos tällainen sivu tulee vastaan, kannattaa käydä kysymässä ensin paikan työntekijältä sivun aitoutta ennen kuin antaa tietojansa.

Langallisessa verkossakin voidaan toteuttaa tämän tyyppisiä hyökkäyksiä. Jos topologiassa, kuten esimerkki verkossa, kytkimet ovat hajautetusti, voidaan käyttää vale DHCP-palvelinta. Kuten kappaleessa 3 todettiin, tietokone lähettää pyynnön broadcastina eli kytkin lähettää sen kaikkiin portteihinsa. Pyyntöön ensimmäisenä vastaava DHCP-palvelin nappaa käyttäjän itselleen ja seuraavaksi hyökkääjä pystyy toteuttamaan saman tietojenkalastelun, kuin langattomassakinverkossa.

Vale DHCP-palvelinten toiminta on estetty käyttämällä DHCP snooping toimintoa.
DHCP snooping on tekniikka, jonka avulla pystytään määrittelemään hyvin tarkasti mitä portteja lähtevät pyynnöt saavat käyttää.

Aktivoidaan DHCP snooping globaalisti ja määritetään sille käytettävä VLAN.
S1 (config) # ip dhcp snooping
S1 (config) # ip dhcp snooping vlan 1
Määritetään GigabitEthernetportit luotettaviksi lähteiksi. Kaikki pyynnöt menevät näihin portteihin.
S1 (config) # int range GigabitEthernet 1/0-1
S1 (config-if-range) # ip dhcp snooping trust

4.4 Sivustosuodatus

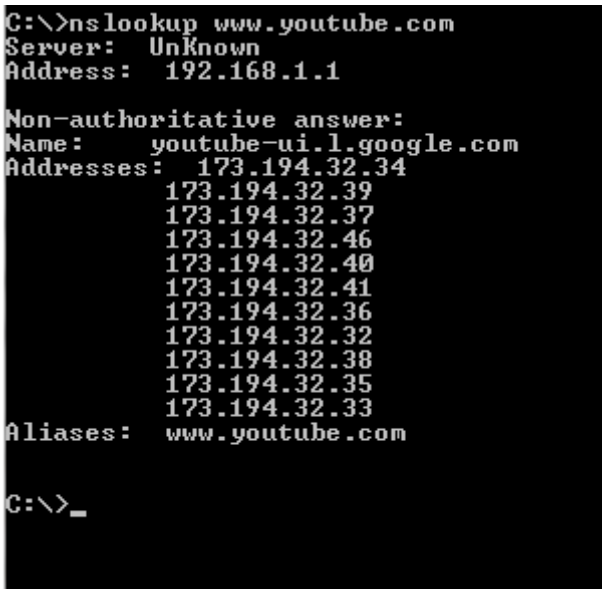
TiTeLAN on julkinen tapahtuma, joka tarkoittaa että noudatamme Suomen lakia tiukasti ja tästä syystä ohjelmitopiratismi on ankarasti kielletty. Lisäksi pornograafisen materiaalin katsominen on kielletty. Vieressä istuva tai ohi kävelevä henkilö voi kuitenkin nähdä mitä näytöllä on, jolloin tätä voidaan pitää julkisena esittämisenä.

Sivujen suodattamiseen käytetään Ciscon urlfilter-toimintoa, joka luodaan reitittimeen. Alla olevassa esimerkissä näytetään kuinka luodaan yksinkertainen URL-suodatin.

Luodaan http osoitesuodatin nimellä Block.
R1 (config) # ip inspect name Block http urlfilter
Lähdeporttina toimii sisäverkon liitäntä.
R1 (config) # ip urlfilter source-interface FastEthernet0/0
Suodatus tehdään black-listauksena, jolloin allow-mode tulee olla päällä.
R1 (config) # ip urlfilter allow-mode on
Estetään pääsy domainiin.
R1 (config) # ip urlfilter exclusive-domain deny torrentz.com
Esto voidaan myös tehdä antamalla merkkijono, jota osoitteesta etsitään.
*-merkki ilmaisee merkkijonon alkamisen ja loppumisen.
R1 (config) # ip urlfilter exclusive-domain deny * porn *
Suodatin pitää lopuksi sijoittaa käytettävään porttiin. Tässä tapauksessa ulkoverkkoon olevaan liitäntään.
R1 (config) # interface FastEthernet 0/1
Tutkitaan ulospäin menevää liikennettä ja estetään liikennettä Block-listassa määriteltyjen parametrien mukaan.
R1 (config-if) # ip inspect Block out

Valitettavasti tämä toimii ainoastaan salaamattomaan liikenteeseen, jolloin suodatus voidaan kiertää vaihtamalla esim. youtube käyttämään https-protokolla.

Tämä kiertäminen voidaan yksinkertaisesti estää tekemällä extended ACL, johon lisätään kyseisen domainin IP-osoitteet. Nämä osoitteet saa helposti selville esimerkiksi kirjoittamalla komentoriville nslookup www.youtube.com, jolloin dns palvelin antaa pyydettyä url:ia vastaavan osoitteen tai osoitteet (kuva 4).



Kuva 4. Youtuben IP-osoitteet

Gmailin palvelimet sijaitsevat samassa aliverkossa, joten pelkästään youtuben estäminen on hankalaa. Alapuolella olevassa esimerkissä luodaan laajennettu pääsylista, jonka avulla estetään yhteydet youtuben palvelimille.

Luodaan extended access-list nimellä Blacklist.

R1 (config) # ip access-list extended Blacklist

Kommentointi siitä mitä estetään.

R1 (config-ext-nacl) # remark youtube

Estetään tcp liikenne mistä tahansa osoitteesta youtuben palvelimille porttiin 443 (https). Koska osoitteita on paljon, käytetään wildcardia estämään useampi osoite.

R1 (config-ext-nacl) # deny tcp any 173.194.32.32 0.0.0.15 eq 443

Lopuksi pitää sallia IP-liikenne kaikkialle ja tcp-liikenne porttiin 443. Jos tätä ei tehdä, kaikki liikenne jää suodattimeen.

R1 (config-ext-nacl) # permit tcp any any eq 443

R1 (config-ext-nacl) # permit ip any any

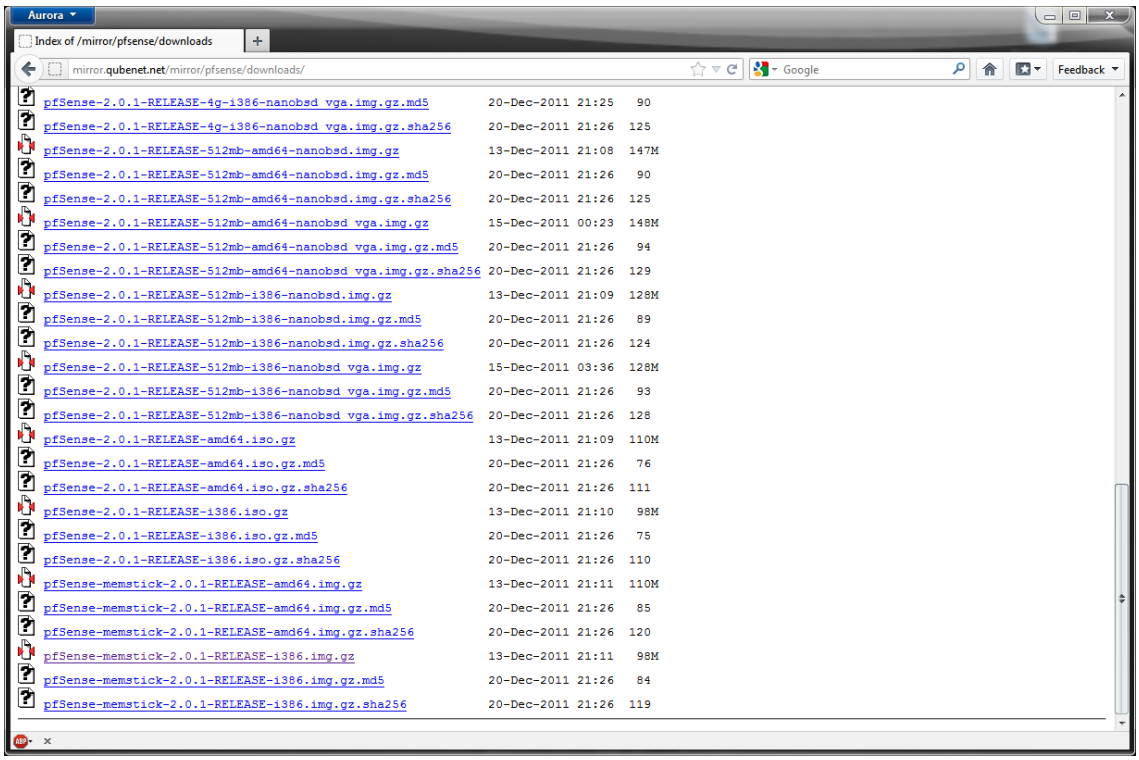
5 PFSENSE-KÄYTTÖJÄRJESTELMÄ

pfSense on avoimen lähdekoodin palomuuri/reititin jakelu (distribuutio), joka perustuu FreeBSD-käyttöjärjestelmään. pfSensen suurin hyöty on se, että se voidaan asentaa myös tavalliselle PC:lle. Toiminnoiltaan se menee helposti kaupallisten reitittimien ohi, koska suurinosa sen sisältämistä ominaisuuksista on saatavilla vain kalleimmissa laitteissa ja useimmiten vielä lisämaksua vastaan.

pfSense on yksinkertainen asentaa, eikä se vaadi käyttäjältään minkäänlaista perehtymistä FreeBSD-maailmaan. Konfigurointi on helppoa ja tapahtuu web-käyttöliittymän kautta.

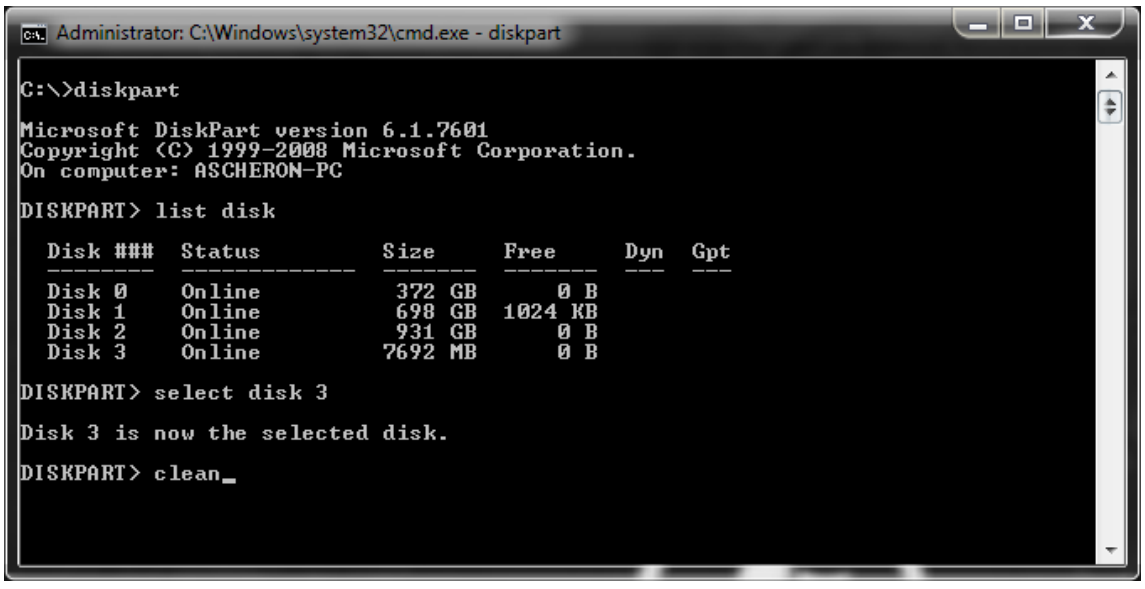
5.1 pfSensen asennus

pfSensen levykuva on ladattavissa ilmaiseksi osoitteesta www.pfsense.org. Levykuvia on saatavilla todella monta, koska ohjelma pystytään asentamaan melkein miltä tahansa medialta. Lisäksi kaikissa vaihtoehdoista on olemassa 32- ja 64-bittinen versio.
Asennus tehdään USB-muistitikun kautta, jolloin valitaan memstick vaihtoehto (kuva 5). Levykuva on pakattu .gz-tiedostoksi, jonka saa purettua esimerkiksi 7-Zip –pakkausohjelmalla.



Kuva 5. Levykuvat

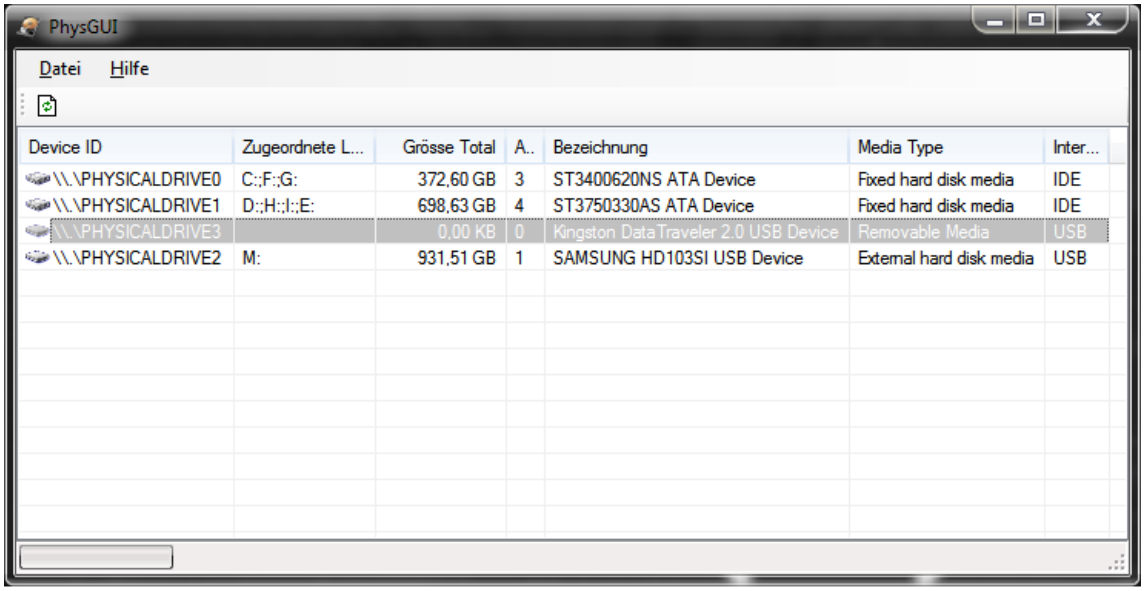
USB-muistitikun alustukseen tulisi käyttää windowsin diskparttia, koska normaali alustus ei tyhjennä koko tikkua. Diskpartin saa käynnistettyä avaamalla komentorivi ja kirjoittamalla siihen ”diskpart” (kuva 6).



Kuva 6. Diskpart

Komennolla ”list disk” saadaan listattua kaikki käytössä olevat asemat. Listasta etsitään oikea asema, joka vastaa muistitikun kokoa. Tässä esimerkissä käytetään 8 Gt:n muistitikkua, jolloin disk 3 on oikea vaihtoehto. Asema valitaan aktiiviseksi käyttämällä ”select disk”-komentoa, joka tässä tapauksessa on muotoa ”select disk 3”. Lopuksi alustetaan muistitikku ”clean”-komennolla.

USB-tikulle kirjoittamisen voi tehdä monella eri ohjelmalla. Tässä esimerkissä käytetään m0n0wallin physdiskwriteä, koska se pystyy kirjoittamaan .img-tiedoston suoraan tikulle. Ohjelman voi ladata osoitteesta http://m0n0.ch/wall/physdiskwrite.php ja on suositeltavaa ladata GUIn sisältävä versio, jollei välttämättä halua tehdä koko työtä komentoriviltä. Ohjelma on yksinkertainen käyttää, vaikka se onkin suurimmaksi osaksi saksankielinen.

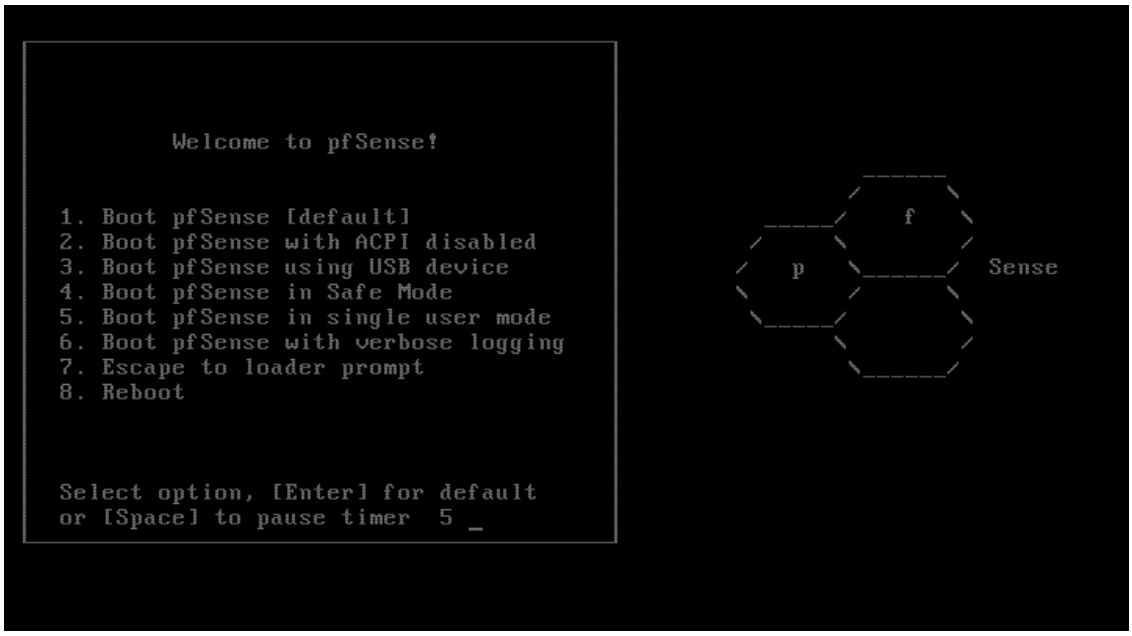


Kuva 7. Physdiskwriten GUI

Ohjelma listaa käytössä olevat mediat samalla tavalla kuin diskpart. Oikean median tunnistaminen on kuitenkin helpompaa, koska ohjelma antaa kuvauksen laitteesta ja liityntärajapinnan tyypistä. Valitaan listasta oikea asema (kuva 7.) ja oikealla hiirennapilla avataan valikko. Valikosta valitaan Image laden (load image) ja sen alta öffnen (open). Ohjelma avaa uuden ikkunan, jonka kautta avataan aikaisemmin

internetistä ladattu levykuvatiedosto. Seuraavaksi ohjelma voi kysyä otetaanko 4 Gt:n rajoitus pois käytöstä, jolloin kannattaa vastata kyllä. Physdisk alkaa kirjoittaa muistitikulle levykuvaa ja se kestää, koneesta riippuen, noin muutaman minuutin.

Jotta kone saadaan käynnistymään USB-muistitikulta, pitää ensimmäisenä muuttaa boot device priorityä BIOSin asetuksista. Koska emolevyjen valmistajilla on erilaiset BIOSin asetukset, boot device priorityn muuttamista ei käsitellä tässä työssä. Apua tähän saa esimerkiksi etsimällä googlella lauseita ”How to change boot device priority” tai ”How to boot from memorystick”.
Jos käynnistys tikulta onnistuu, ruudulle tulee kuvan 8 mukainen näkymä.



Kuva 8. Käynnistysruutu

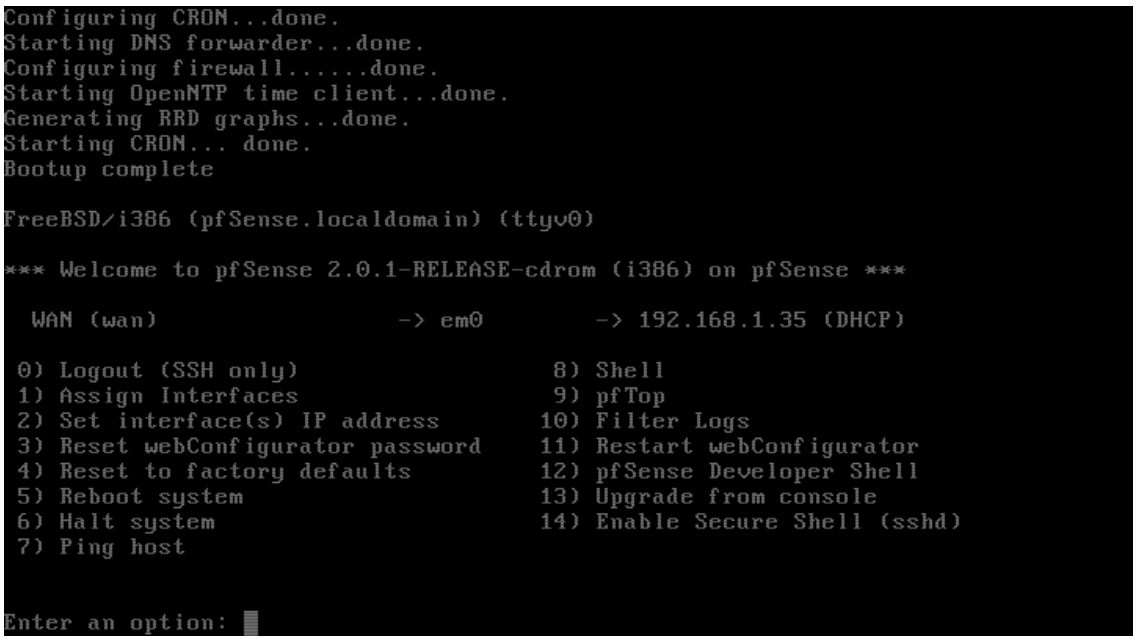
Valitaan Boot pfSense [default] ja pfSense käynnistyy normaaliin tilaan. Vaihtoehtoisesti mitään ei tarvitse painaa, koska oletuksena se käynnistyy normaalin tilaan. Ensimmäisenä pfSense kysyy alustavia tietoja, kuten esimerkiksi haluaako käyttäjä määritellä VLANit. Suositeltavaa on määritellä ne vasta web-käyttöliittymässä, koska se on helpompi tapa toteuttaa. Lisäksi kysytään mitä verkkokorttia käytetään ulkoverkkoon ja mitä sisäverkkoon. pfSense tukee useimpia verkkokortteja, joten ongelmia yhteensopivuuksien kanssa tulee harvemmin vastaan.

Tämän jälkeen siirrytään vasta varsinaiseen asennusohjelmaan. Kannattaa valita Quick and Easy Install, jollei välttämättä ole tekemässä jotain erikoisasetuksia asennukseen. Seuraavaksi asennus kysyy minkä tyyppiselle laitteistolle käyttöjärjestelmä asennetaan. Vaihtoehtoina ovat Symmetric multiprocessing kernel (asennus PC:lle), Embeded kernel (asennus reitittimelle) ja Developers kernel (kehitystyökalut). Valitaan Symmetric multiprocessing kernel, eli tietokoneelle asennus. Asennuksen lopuksi tietokone käynnistetään uudelleen.

5.2 Peruasetukset

Ennen kuin web-käyttöliittymää voidaan käyttää, pitää määritellä pfSensen verkkoliityntöjen IP-osoitteet. Tämä tehdään valitsemalla vaihtoehto 2 komentoriviltä (kuva 9). Ohjelma kysyy tämän jälkeen mitä liityntää muutetaan. WAN-rajapinta määritetään hakemaan IP-osoitteensa DHCP-palvelimelta, jollei staattista IP:tä ole annettu käyttöön. Jos järjestelmä kysyy palautetaanko web-käyttöliittymän protokollaksi http, tulee siihen vastata aina ei ! Jos käytettäisiin http:tä konfiguroinnin aikana, niin verkkoa kuunteleva henkilö pystyy helposti saamaan kaikki tunnukset ja tiedot, koska http liikenne on salaamatonta. Turvallisuussyistä, sitä ei koskaan tulisi vaihtaa http:ksi.

Lopuksi muutetaan sisäverkon portin osoite ja määritetään DHCP-palvelin (pfSense) jakamaan osoitteita sisäverkkoon. Käytettävä osoitealue asetetaan kappaleessa 2 esitetyn IP-suunnitelman mukaiseksi.



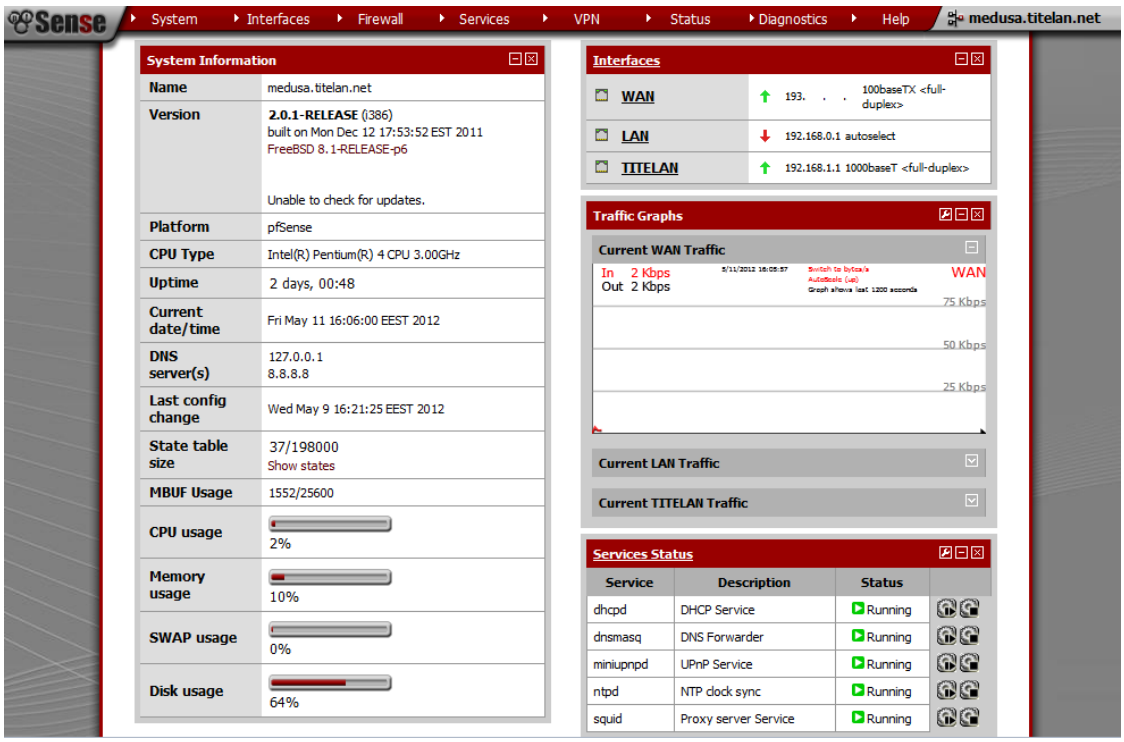
Kuva 9. Valintaruutu

Seuraavaksi liitetään toinen tietokone sisäverkkoon, jotta saadaan otettua yhteys web-käyttöliittymään. Koneelta avataan selain ja otetaan yhteys LAN-liitännän IP-osoitteeseen. Osoitekenttään kirjoitetaan https://192.168.1.1 (kuvan 9 tapauksessa 192.169.1.35). pfSensen web-käyttöliittymä suunniteltu toimimaan Firefoxissa, joten on suositeltavaa käyttää edellä mainittua selainta. Näkyviin pitäisi tulla kuvan 10 mukainen kirjautumisruutu.

Kuva 10. Kirjautumisruutu

Oletus käyttäjätunnus (username) on ”admin” ja salasana (password) ”pfsense”. Jos nämä eivät toimi, kannattaa nollata web-käyttöliittymän tunnukset pfSense-koneelta (kuvassa 9 vaihtoehto 3).

Kirjauduttua sisään, avautuu ensimmäisenä Dashboard, joka on pfSensen ns. yleisinformaatio sivu (kuva 11). Dashboard on siitä hyödyllinen, että siihen voidaan lisätä monenlaisia tietokenttiä, kuten verkonkuormituskäyriä tai käytössä olevia palveluita. Oletuksena sivulla ei näy muuta, kuin System Information- ja Interfaces-ikkuna.

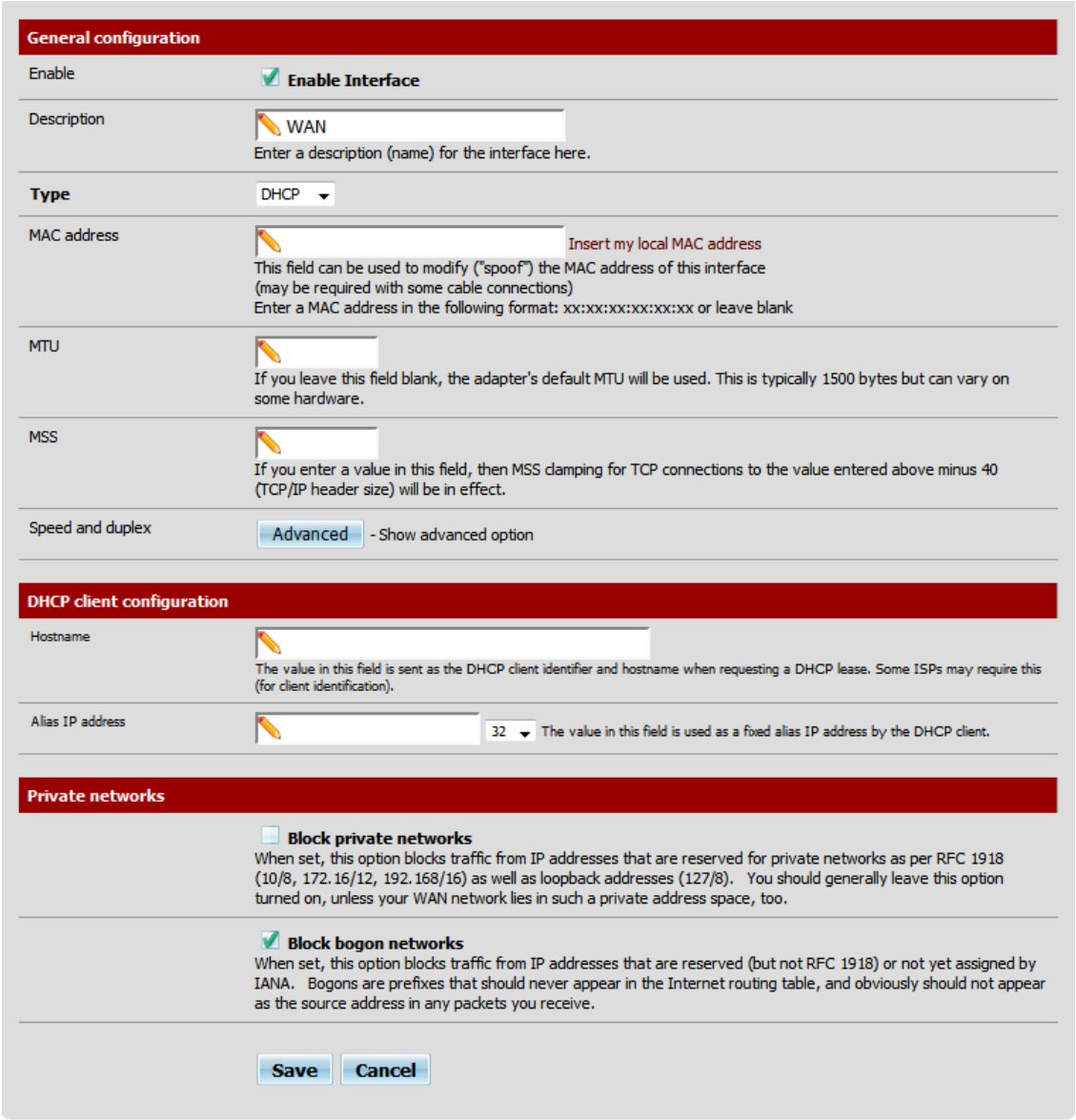


Kuva 11. Dashboard

Heti ensimmäisenä asiana tulee muuttaa kirjautumistunnukset. Pahin virhe on jättää oletustunnus muuttamatta, jolloin siitä muodostuu vakava tietoturvariski. Käyttäjätunnustenhallinta löytyy System-valikon User Manager –kohdasta ja painamalla käyttätunnuksen perässä olevasta edit-napista voidaan muuttaa käyttäjän salasana.

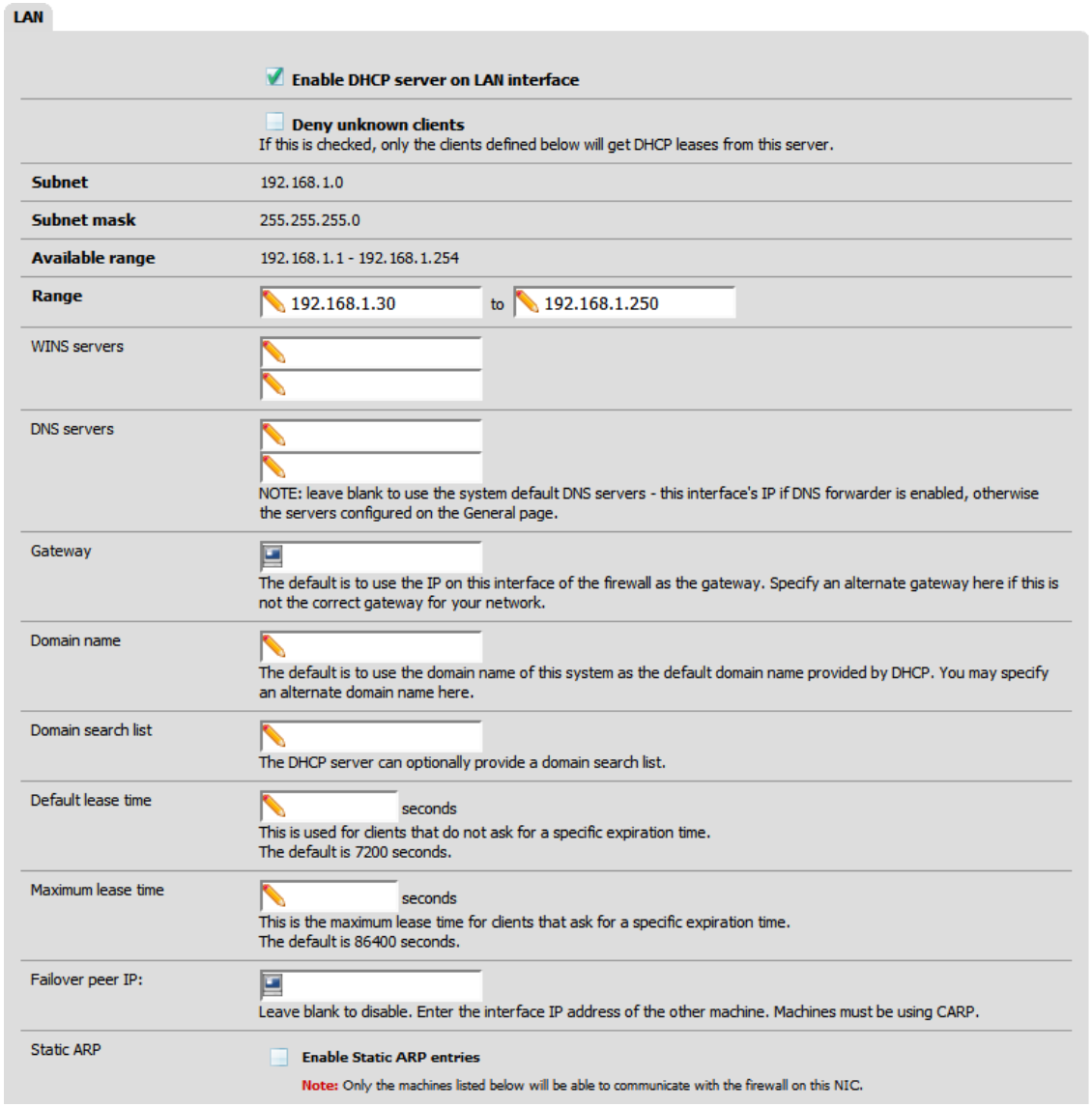
Interface-valikosta löytyvät käytössä olevat verkkokortit. Kuvassa 12 on esitetty WAN-rajapinnan asetusikkuna. Type-kohdan pudotusvalikosta voidaan vaihtaa DHCP-palvelimelta saatava osoite staattiseksi. LAN-rajapinnan asetukset eroavat vain siten, että DHCP client configurationin tilalla on staattiselle IP-osoitteelle kirjoituskenttä.

Käytettäessä staattista IP-osoitetta WAN-rajapinnassa, tulee muistaa laittaa manuaalisesti DNS-palvelimien IP-osoitteet. DNS-palvelimien osoitteet pystyy muuttamaan System-valikon kohdasta General Setup.



Kuva 12. WAN-rajapinnan asetukset

DHCP-palvelimen asetukset löytyvät Services-valikosta. Palvelimen asetusten muokkaus sivu on esitetty kuvassa 13. Palvelin aktivoidaan rastittamalla valintalaatikko ”Enable DHCP-server on LAN interface” kohdasta. Käytettävä IP-alue muutetaan kappaleessa 1 määritetyn IP-suunnitelman mukaan. Palvelimen myöntämien IP-osoitteiden lista löytyy Status-valikon DHCP leases –kohdasta.



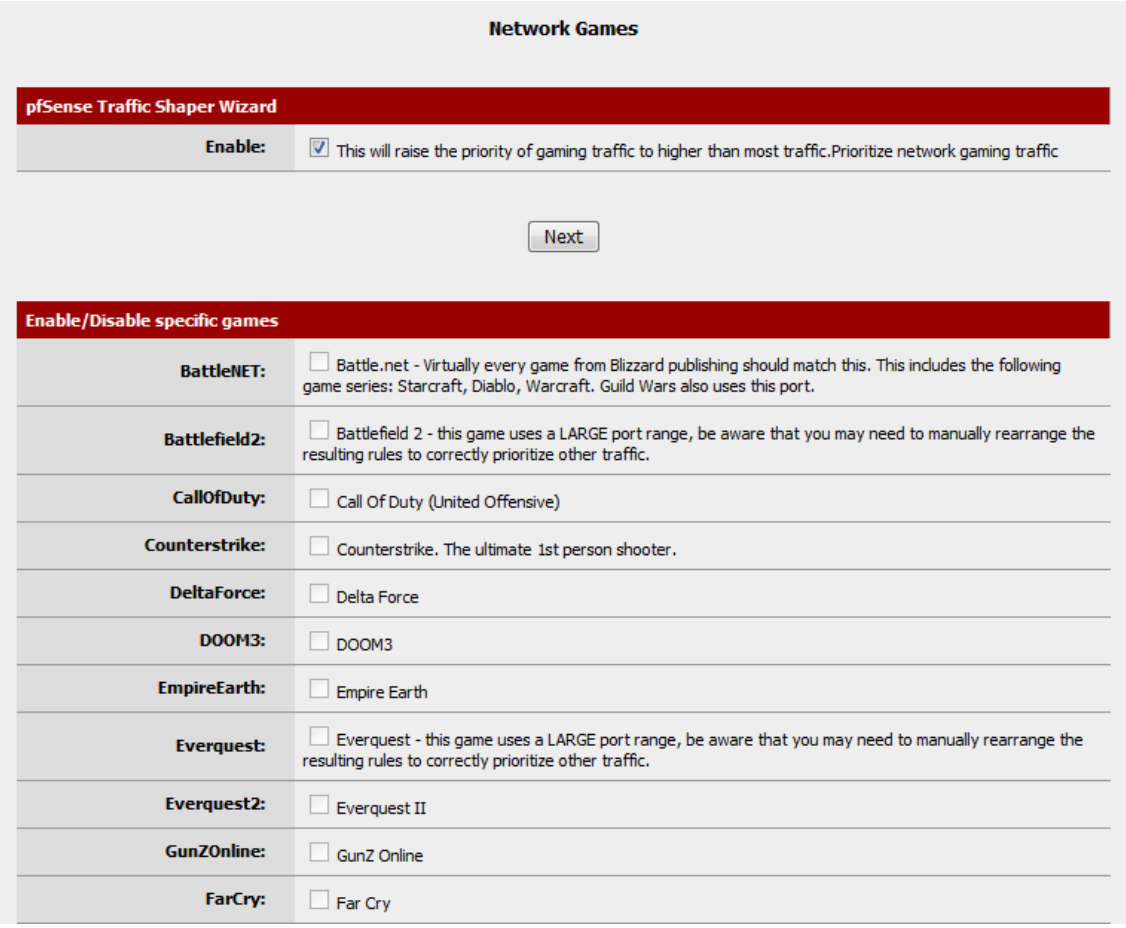
Kuva 13. pfSensen DHCP-palvelin

5.3 Pakettien hallinta

pfSense ei vie paljoa kovalevytilaa, koska osa sen ominaisuuksista pitää ladata internetistä. Näiden pakettien asentaminen ja poistaminen tapahtuu System-valikon Packages-kohdasta.
Saatavilla olevia paketteja on todella monta ja suurinosa niistä asentaa uuden ominaisuuden. Asentamisen suhteen kannattaa olla varovainen, koska suurinosa paketeista on vasta beta-vaiheessa. Pahimmassa tapauksessa asennettu ominaisuus voi sekoittaa järjestelmän kokonaan, jolloin koko käyttöjärjestelmän joutuu asentamaan uudestaan. Suositeltavaa on tutustua pakettien tietoihin ja dokumentteihin ennen asennusta.

5.4 QoS-palvelu pfSensessä

Traffic Shaper on pfSensen oma Quality of Service –palvelu, jolla pystytään määrittämään liikenteen priorisointia hyvin tarkasti. Lisäksi sillä voidaan nostaa verkkopelien prioriteetti korkealle (kuva 14), joka on tapahtuman kannalta erittäin hyödyllinen ominaisuus. Käytännössä se nostaa tiettyihin portteihin kulkevien pakettien prioriteettiä. Traffic Shaper löytyy pfSensestä Firewall-valikon alta. Konfiguraatioiden tekemiseen käytetään wizard-toimintoa, koska se on nopein ja yksinkertaisin tapa. Valmiista pohjista valitaan vaihtoehto ”one-wan-multi-lan” eli yksi ulkoverkko ja monta lähiverkkoa.



Kuva 14. Verkkopelien QoS

5.5 Squid-välityspalvelin

Tapahtuman kannalta pfSensen yksi tärkeimmistä toiminnoista on välityspalvelin Squid. Se, mikä tästä ohjelmasta tekee erikoisen ja tärkeän, on web cache –toiminto.

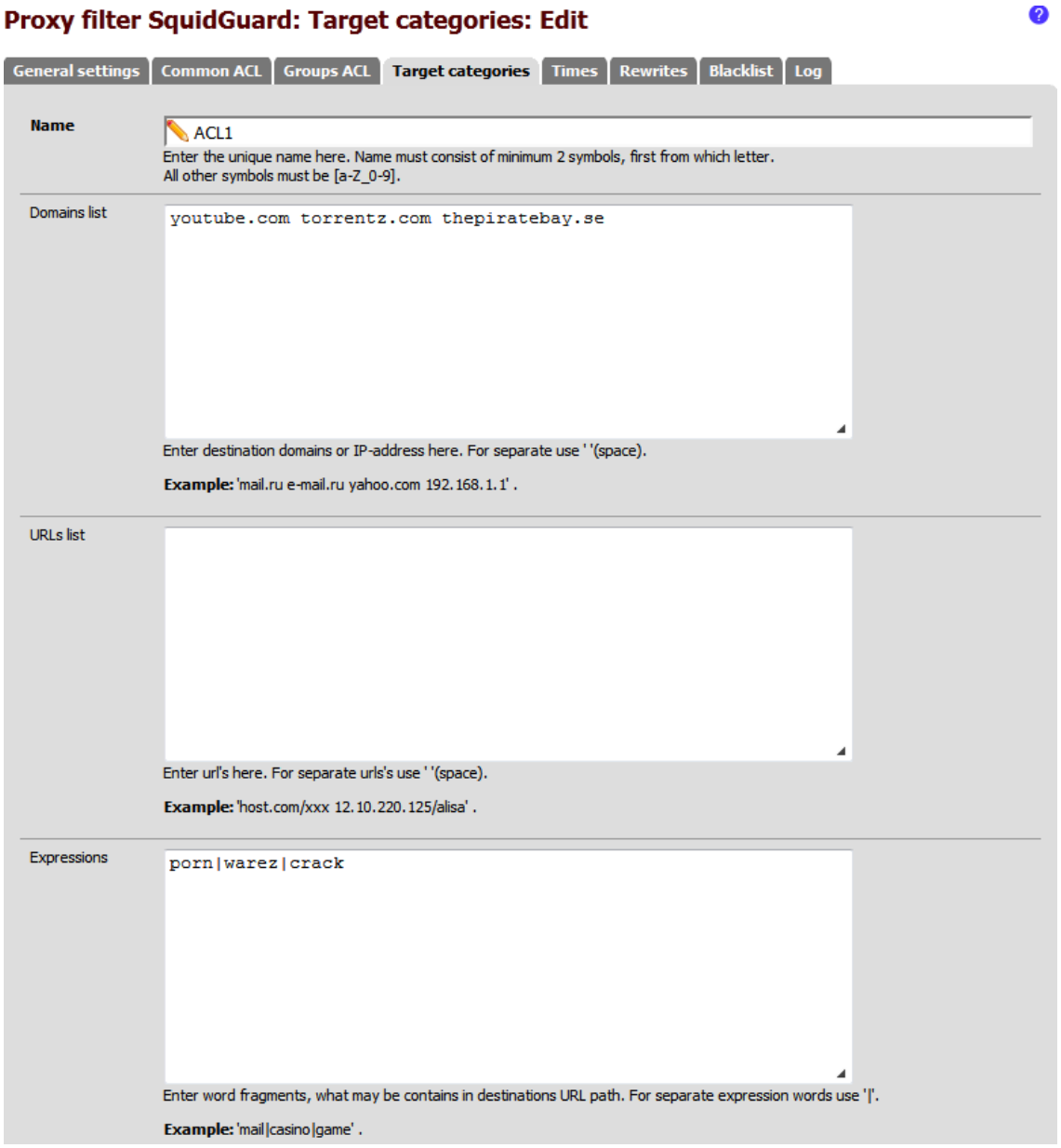
Web cache eli web-välimuisti tallentaa internetistä ladattuja tiedostoja pfSense-tietokoneen kovalevylle. Kun toinen asiakas yrittää ladata saman tiedoston, reititin huomaa tämän ja aloittaakin siirron kovalevyltään. Tämä nopeuttaa valtavasti tiedostojen latausaikoja ja vähentää ulkoverkon kaistankäyttöä, sallien enemmän käyttövaraa muille.

Jos web cachea käytetään suurissa verkoissa, on erittäin tärkeää vaihtaa IDE-kovalevy SATA-kovalevyyn. IDE-tekniikka kykenee siirtämään enimmillään vain 133 MB/s, kun taas SATA kykenee yli 1,5 GB/s:ssa. IDE-kovalevy ei siis pysty siirtämään dataa tarpeeksi nopeasti yli 100 tietokoneen verkossa.

5.6 pfSensen sivustosuodatus

Vanhassa reitittimessä käytettiin Ciscon omaa sivustosuodatinta, jolla suodatettiin pornograafista ja ohjelmistopiratismiin liittyviä sivuja. Squidiin on saatavissa lisäpaketti SquidGuard, joka mahdollistaa sivustosuodatuksen Squid-välityspalvelimen avulla. SquidGuardin asetukset löytyvät service-valikosta Proxy filter -kohdasta.

SquidGuardilla voidaan suodattaa sivustoja domainin, URL:n ja asiasanojen mukaan (kuva 15). Esimerkkisuodattimelle annetaan nimeksi ACL1 ja sillä estetään youtube-, torrentz- ja thepiratebay-sivustot. Lisäksi suodatetaan URL:ssa esiintyviä sanoja, kuten porn, warez ja crack. Lopuksi voidaan valita, ohjataanko suodattimeen jäävät yritykset virheilmoitus sivulle vai jollekin toiselle sivustolle.



Kuva 15. SquidGuard-suodatin

Tämän jälkeen suodatuslistalle voidaan määrittää aika, jolloin se on käytössä. Esimerkiksi jos työpaikalla halutaan vähentää työntekijöiden Facebookin käyttämistä. Times-välilehteen määritetään tällöin, ettei Facebookia voi käyttää välillä 9.00-12.00 ja 12.30-16.00 kaikkina arkipäivinä.

6 POHDINTA

Verkkopelitapahtumaa järjestäessä, nämä kolme asiaa ovat olleet suureksi avuksi:
Koskaan ei voi olla liian aikaisin. Pahin vihollinen on kiire, josta seuraa stressi. Stressaantuneena ihminen tekee enemmän virheitä.
Muutoksia tehtäessä järjestelmään, kaikki vanhat asetukset tulee ottaa AINA talteen ja mieluusti vielä kahteen eri paikkaan. Jos muutokset eivät anna haluttua tulosta tai pahimmassa tapauksessa sekoittavat koko järjestelmän, on paljon helpompaa etsiä vikaa ja palata toimiviin asetuksiin jos aika ei riitä.
Varasuunnitelmia kannattaa tehdä. Tapahtumaa järjestettäessä menee aina jokin asia pieleen. Varautumalla hyvin, saadaan ongelmat korjattua nopeasti ja osallistujat ovat tyytyväisiä. Hyvin suunniteltu on puoliksi tehty.

Vaihtamalla pfSense reitittimen tilalle ja ottamalla web cache käyttöön, saadaan vähennettyä ulkoverkon kaistan käyttöä huomattava määrä. Graafista vertailua ei voi tehdä, koska Ciscon reitittimessä ei käytetty analyysityökaluja. Ero oli huomattavissa ainoastaan internettiä käyttäessä ja pelatessa verkkopelejä.
Kaistankäyttö viimeisimmässä tapahtumassa (TiTeLAN 1/12) oli noin 75 Mbit/s ruuhkaisimpana aikana. Normaali käytössä se pysyi alle 25 Mbit/s.
Käytettävä kaista oli tilan verkkovastaavan mukaan 100 Mbit/s.

pfSensen-komentorivin kuvankaappaukset on otettu käyttämällä apuna VirtualBoxia. Sillä pfSense toimii suhteellisen hyvin. Valitettavasti käynnistyksessä oli välillä ongelmia, joka luultavasti johtui ulkoisesta USB-kovalevystä, jolle virtuaalikovalevy oli luotu. Lisäksi asennusta ei voitu ajaa USB-muistitikulta, vaan se piti tehdä VirtualBoxin kautta käyttämällä levykuvaa.

LÄHTEET

Donahue, Gary A. 2007. Network Warrior. Everything you need to know that wasn't on the CCNA exam. United States of America: O'Reilly.

Wiesen, G. 2012. What is a DoS attack? WiseGEEK. Luettu 12.5.2012. http://www.wisegeek.com/what-is-a-dos-attack.htm

Koivumäki, K. 2010. Modularisoitu lähiverkostointijärjestelmä. Tietotekniikan koulutusohjelma. Tampereen Ammattikorkeakoulu. Opinnäytetyö. Luettu 6.5.2012. https://publications.theseus.fi/bitstream/handle/10024/22820/Koivumaki_Kalle.pdf?sequence=2

Tatum, Malcolm. 2012. What is MAC flooding? WiseGEEK. Luettu 6.5.2012. http://www.wisegeek.com/what-is-mac-flooding.htm