LAHDEN AMMATTIKORKEAKOULU
Lahti University of Applied Sciences

VIKASIETOINEN PALOMUURI

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietotekniikka
Opinnäytetyö
Kevät 2013
Päivi Viitajoki

Lahden ammattikorkeakoulu

Koulutusohjelma

VIITAJOKI, PÄIVI: Vikasietoinen palomuuri

Tietotekniikan opinnäytetyö, 50 sivua

Kevät 2013

TIIVISTELMÄ

Vuonna 1988 löydettiin ensimmäinen virus Internetistä, minkä jälkeen alettiin kehittää palomuuria. Siitä on tullut tärkein tapa suojata sisäverkkoa ulkopuolisilta tunkeutujilta. Palomuuria voidaan verrata portinvartijaan, joka tietää ketä voidaan päästää sisään ja ketkä tulisi jättää ulos.

Palomuurit omaavat monia ominaisuuksia, joita verkossa voidaan hyödyntää. DHCP vähentää verkkoasetusten manuaalista konfigurointia ja NAT lisää verkon turvallisuutta sekä vähentää IP-osoitteiden tarvetta. Tietoliikennettä priorisoidaan QoS:n avulla. Vikasieto-ominaisuus on olemassa monissa nykyisissä palomuureissa. Sen avulla kaksi palomuuria yhdistetään pariksi, jolloin toisen vikaantuessa toinen on heti käyttövalmiina.

Tässä työssä vertaillaan kolmea palomuuriohjelmistoa, joita ovat pfSense, SmoothWall Express ja Vyatta Core. Vertailun tuloksena päädyttiin valitsemaan opinnäytetyöhön pfSense, koska siinä on helppokäyttöinen WebGUI, vikasieto-ominaisuus ja se on edullinen, koska se on open source-ohjelmisto. Vyatta sekä SmoothWall Express hylättiin sen vuoksi, että Vyattan ilmaisversiossa ei ole käytössä WebGUIta ja SmoothWall Expressistä puuttuu vikasieto-ominaisuus.

Työssä toteutetaan vikasietoinen palomuuripari pfSensellä Mastonet-verkkoa varten. Palomuurissa DHCP jakaa IP:t laitteille ja palomuuri tekee NAT:in. P2P-liikennettä rajoitetaan limiterin avulla, joka on melko yksinkertainen toteuttaa.

Asiasanat: vikasietoinen, palomuuri, DHCP, NAT, kaistanrajoitus, pfSense.

Lahti University of Applied Sciences
Degree Programme in Information technology

VIITAJOKI, PÄIVI: Fault-tolerant firewall

Bachelor's Thesis in Information Technology, 50 pages

Spring 2013

ABSTRACT

The first firewalls were developed when a virus was found in the Internet in year 1988. They have become the most important way to protect a network from outside threat.

There are many features that firewalls include today for example DHCP, NAT and fault-tolerance. Also traffic limiting is possible to do with firewalls.

In this work three different firewalls were compared. These firewalls are pfSense, SmoothWall Express and Vyatta Core. As a result, pfSense was selected, because it is fault-tolerant and it includes an easy to use WebGUI. Also traffic limiting is possible with pfSense.

The fault-tolerant firewall was implemented for Mastonet with pfSense. NAT was configured and DHCP distributes IP addresses to devices. P2P traffic was limited.

Key words: fault-tolerant, firewall, P2P.

SISÄLLYS

ARP	Address Resolution Protocol.
CARP	Common Address Redundancy Protocol.
CIDR	Classless Inter-Domain Routing. Luokaton reititys.
CLI	Command line interface. Komentoliittymä.
CPU	Central Processing Unit. Tietokoneen osa, joka suorittaa tietokoneohjelman sisältämiä konekielisiä käskyjä.
DHCP	Dynamic Host Configuration Protocol.
DMZ	Demilitarized zone. Fyysinen tai looginen aliverkko, joka yhdistää organisaation oman järjestelmän turvattomampaan alueeseen.
DNS	Domain Name System. Internetin nimipalvelujärjestelmä muuntaa verkkotunnuksia IP-osoitteeksi.
DoS	Denial of Service. Palvelunestohyökkäys tarkoittaa tietyn verkkopalvelun lamauttamista siten, että palvelu ei ole käytettävissä.
FIFO	First in/first out.
FTP	File Transfer Protocol.
HSRP	Hot Standby Router Protocol.
HTTP	Hypertext Transfer Protocol.
ICMP	Internet Control Message Protocol.
IDS	Intrusion Detection System. Tunkeilijan havaitsemisjärjestelmä, joka monitoroi vahingollista verkko- tai järjestelmätoimintaa.
IP	Internet Protocol.
LAN	Local Area Network. Lähiverkko.

NAT	Network Address Translation. Osoitteenmuunnos.
OSI-malli	Open Systems Interconnection Reference Model kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa.
PAT	Port Address Translation. PAT kääntää useita eri privaatti osoitteita yhdeksi osoitteksi.
P2P	Peer-to-peer. Vertaisverkko.
PPPoE	Point-to-Point Protocol over Ethernet.
PPTP	Point-to-Point Tunneling Protocol.
QoS	Quality of Service. Tietoliikenteen priorisointi.
RAM	Random access memory. Keskusmuisti.
SSH	Secure Shell. SSH on salattuun tietoliikenteeseen tarkoitettu protokolla.
TCP	Transmission Control Protocol.
UDP	User Datagram Protocol.
VIP	Virtual IP
VLAN	Virtual Local Area Network. Looginen verkko (aliverkko) tai broadcast –alue.
VPN	Virtual Private Network. VPN:llä liikenne tunneloidaan pisteestä A pisteeseen B turvattomien verkkojen, kuten Internetin, läpi.
WAN	Wide Area Network. Laajaverkko.

1 JOHDANTO

Työn tarkoituksena on toteuttaa vikasietoinen palomuuri. Työ toteutetaan virtuaaliympäristössä, jossa on kaksi VMWare-virtuaalikonetta ja kaksi Windows Server 2008 R2 -konetta DMZ-verkossa. ESXi-palvelimelle luodaan virtuaalikoneet, joihin asennetaan palomuuriohjelmisto.

Palomuuri tekee NAT:n ja sisältää DHCP-palvelimen. DHCP-palvelimelta jaetaan IP-osoitteet LAN-verkon laitteille. DHCP-palvelimen lisäksi testataan DHCP relayn toiminta. Työssä testataan staattisen NAT:n ja porttiohjauksen toiminta.

Tavoitteena on toimiva vikasietoinen palomuuripari Mastonet-verkkoa varten. Mastonet on Lahden kaupungin ilmainen langaton, avoin verkko, jota Lahden ammattikorkeakoulu ylläpitää. Palomuuri tekee NAT:in ja sisältää DHCP-palvelimen, jolta IP-osoitteet jaetaan laitteille. Palomuurissa on käytössä kaistanrajoitus.

Työn alkuosassa perehdytään palomuurin toimintaan ja tekniikoihin. Työssä vertaillaan pfSense 2.0.1-ohjelmistoa sekä Smooth Wall Express 3.0-ohjelmistoa että Vyatta Core-ohjelmistoa. Vertailussa käydään kaikkien ohjelmistojen ominaisuudet ja lopuksi esitetään yhteenvetotaulukko tärkeimmistä ominaisuuksista. Tämän jälkeen työssä käydään läpi käytännön toteutus ja viimeisenä yhteenveto työstä.

2 PALOMUURI

2.1 Palomuurien kehitys

Marraskuussa 1988 löydettiin ensimmäinen virus Internetistä. Tämä oli herätys Internetin turvattomuudesta. Alkoi palomuurien kehitystyö, jota on tehty monien kehittäjien toimesta. (Wikipedia 2013.)

Ensimmäisen sukupolven palomuurit perustuvat reitittimeen, joka tutkii vastaanotetun paketin kohdeosoitteen. Vastaanotettaessa paketin otsikko kopioidaan reitittimen CPU:hun ja verrataan reitittimen sääntöihin, jotka perustuvat suodatussääntöihin. Paketti, joka ei sovi sääntöihin, estetään ja sääntöihin sopiva paketti lähetetään eteenpäin. Estettäessä paketti, lähetetään viesti paketin alkuperälaitteelle, jotta lisää paketteja ei lähetetä (reject). Pakettisuodatuspalomuurit toimivat OSI-mallin kolmannella kerroksella. (Wikipedia 2013.)

Toisen sukupolven palomuuri kehitettiin vuosina 1989 – 1990. Toisen sukupolven palomuuri on tilallinen palomuuri, joka estää DoS (Denial of Service)-hyökkäykset. DoS-hyökkäys on nimenomainen yritys saada tietokoneresurssi pois saatavilta tartuttamalla viruksen tai tulvimalla verkko hyödyttömällä liikenteellä. Toisen sukupolven tilalliset palomuurit toimivat OSI-mallin neljännellä kerroksella (kuljetuskerros). Tilallinen palomuuri tutkii onko paketti uuden yhteyden alku, osa olemassa olevaa yhteyttä vai onko paketti osa mitään yhteyttä. (Wikipedia 2013.)

Kolmannensukupolven palomuurit toimivat OSI-mallin sovelluskerroksella. Sovelluspalomuurien etu on se, että palomuuri ymmärtää tiettyjä sovelluksia ja protokollia, kuten File Transfer Protocol (FTP), Domain Name System (DNS) ja Hypertext Transfer Protocol (HTTP). Sovelluspalomuurit toimivat niin, että palomuuri määrittää pitäisikö prosessin sallia annettu yhteys. Sovelluspalomuurit toimivat lähes kuin pakettisuodatus palomuurit. Sovelluspalomuuri asettaa suodatussäännöt/prosessit sen sijaan että se suodattaisi yhteydet/portit. (Wikipedia 2013.)

Nykyisin palomuurit voidaan varustaa IDS:llä (Intrusion Detection System). IDS monitoroi vahingollista verkko- tai järjestelmätoimintaa. Päätehtävä on tunnistaa vahingollinen toiminta, kirjata lokiin vahingollinen toiminta, yrittää estää vahingollinen toiminta ja raportoida kyseisestä toiminnasta. (Wikipedia 2013.)

2.2 Palomuurin toiminta ja tekniikat

Palomuuri on tärkein tapa suojella sisäverkkoa ulkoverkosta tulevilta hyökkäyksiltä ja tunkeutujilta. Palomuuria voidaan verrata portinvartijaksi, joka tietää, ketä tai keitä tulisi päästää sisään ja kuka tulisi jättää ulkopuolelle. Palomuurit ovat järjestelmiä, jotka ovat toteutettu laitteistolla tai ohjelmistolla. Laitepohjainen palomuuri voi olla esimerkiksi tukiasema. Tukiaseman lisäksi tulisi tietokoneessa käyttää ohjelmapohjaista palomuuria. (Oulun kauppaoppilaitos 2004.)

Palomuurin toiminnan perusedellytys on, että kaikki verkkoliikenne sisä- ja ulkoverkon välillä kulkee palomuurin läpi. Palomuurin tulee päästää lävitseen vain liikenne, jonka halutaan läpäisevän palomuurin. Lisäksi palomuurin tulee olla vastustuskykyinen verkko hyökkäyksiä vastaan. (Oulun kauppaoppilaitos 2004.)

Tietoliikenne internetissä kulkee paketeissa. Palomuurilla voidaan blokata tietystä IP-osoitteesta tulevia paketteja, ja se kontrolloi, mihin paketteja päästetään. Paketti joko hyväksytään (accept) tai hylätään (drop) lähettämättä lähettäjälle vastausta. Paketti voidaan myös rejektoida (reject), jolloin lähettäjälle lähetetään ilmoitus siitä, että pakettia ei hyväksytty. (Almgren 2012.)

Palomuuritekniikat voidaan jakaa kahtia: pakettisuodattimeen ja sovelluspalomuureihin kuten luvun alussa on todettu. Pakettisuodattimet voivat olla tilallisia tai tilattomia. Pakettisuodattimeen perustuva palomuuri suodattaa paketteja useiden muuttujien perusteella. Näitä muuttujia ovat muun muassa lähde- ja kohdeosoite, protokolla ja porttinumero. Tällaiseen tekniikkaan perustuvat palomuurit ovat yleensä reitittimiä. Reititinpohjaiset palomuurit ovat helppoja toteuttaa, mutta niissä on toisaalta puutteita, jotka tekevät niistä heikkoja palomuureja. Esimerkiksi palvelunestohyökkäykset ovat reititinpohjaisten

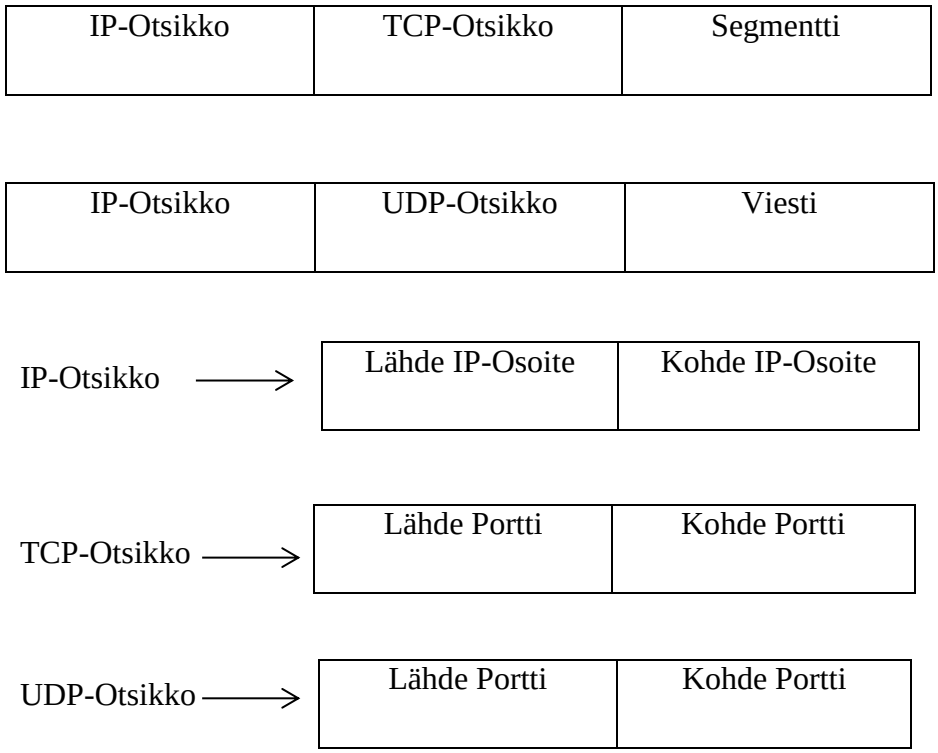
palomuurien heikko kohta, koska niitä ei ole kehitetty käsittelemään tällaisia hyökkäksiä. (Wikipedia 2012.)

Tilattomassa (stateless) palomuurissa pakettia verrataan säännöstöön. Pakettia ei välitetä eteenpäin, jollei paketti ole sallittu. Tilallisessa (statefull) palomuurissa pidetään kirjaa sekä TCP- että UDP-yhteyksistä. Tilallinen palomuuri sallii vain edellä mainittuihin yhteyksiin kuuluvat paketit. TCP-yhteyksien tilasiirtymien tulee myös olla laillisia. (Wikipedia 2012.)

Toisin kuin pakettisuodatin, sovelluspalomuuri tarkkailee paketin sisältämää dataa, ja se toimii OSI-mallin sovelluskerroksella.

2.2.1 TCP/IP-virta

TCP/IP (Transmission Control Protocol / Internet Protocol) -liikenne koostuu paketeista, joissa informaatio sijaitsee. Palomuuri joko hyväksyy tai hylkää liikenteen sen mukaan, mitä paketti pitää sisällään. Kuviossa 1 on kuvattu IP-paketin rakenne, joka rakentuu kolmesta osasta. IP-otsikko sisältää lähde IP-osoitteen ja kohde IP-osoitteen. TCP- tai UDP-otsikko sisältää lähde- ja kohdeportin, jotta voidaan tunnistaa mikä sovellus lähettää ja vastaanottaa liikenteen. TCP-otsikot sisältävät myös lisäinformaatiota kuten sekvenssinumerot, hyväksyntänumerot (acknowledgment) ja keskustelutilan. Kun paketti saavuttaa kohteensa, TCP- ja UDP-kohdeportit määrittävät informaation toimituksen sijainnin palvelimella.

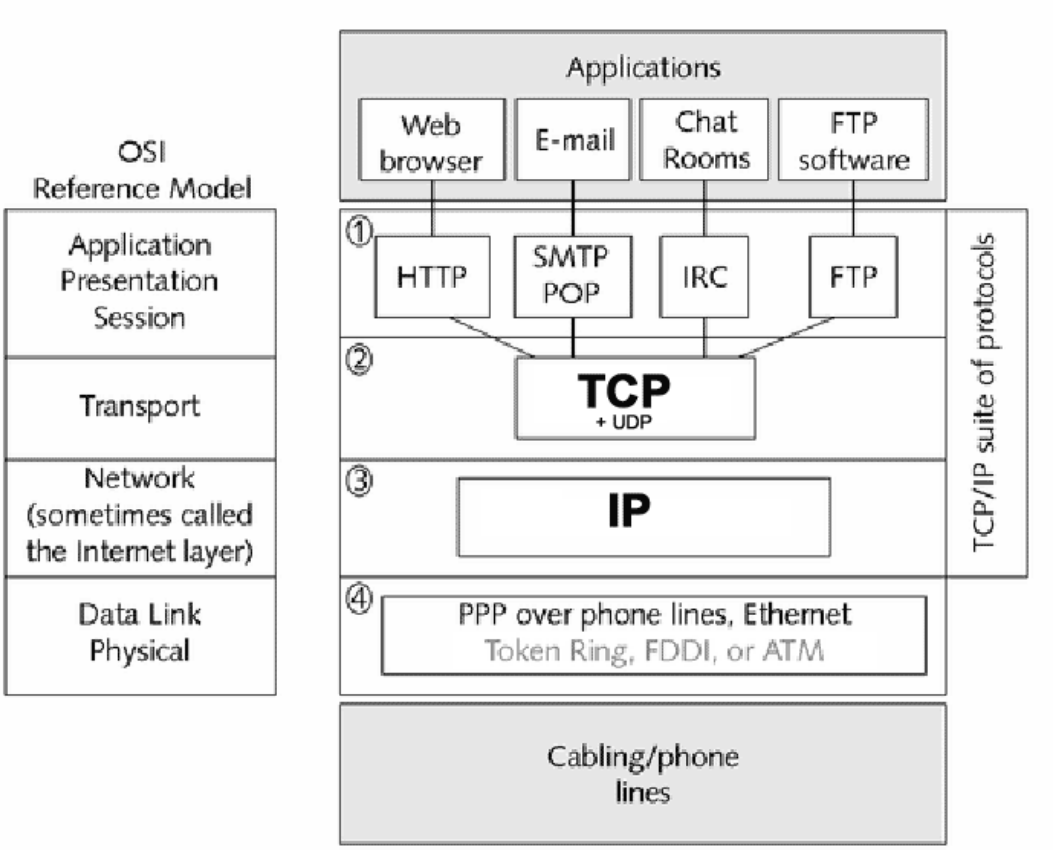


KUVIO 1. IP-paketin otsikko on hyödyllinen palomuurille.

Esimerkiksi kun web-selain lähettää HTTP-pyynnön Web-palvelimelle, pyyntö sisältää lähdeosoitteen ja -portin, josta pyyntö lähetettiin. Lähdeportti tunnistaa sovelluksen, joka lähetti pyynnön. Vastauksessaan Web-palvelin käyttää lähdeporttia kohdeporttina. Kohteen käyttöjärjestelmä tunnistaa porttinumeron kuuluvan selainsovelluksen aloittamalle istunnolle, jolloin käyttöjärjestelmä antaa informaation selaimelle.

2.2.2 Pakettisuodatus

Palomuurin päätehtävä on suodattaa liikennettä. Kuten aiemmin kuvattiin, palomuuri joko hyväksyy tai hylkää paketit perustuen ylläpitäjän arvosteluperusteisiin. Palomuurissa kaikki liikenne estetään, jos liikennettä ei ole nimenomaan sallittu. Pakettisuodatus palomuuri suodattaa paketit niiden TCP- ja IP-otsikon sisältämän informaation perusteella. Yleensä paketit hylätään tai hyväksytään niiden lähde- ja kohdeosoitteen, sovelluksen tai protokollan ja lähde- ja kohdeportin numeroiden mukaan. Pakettisuodatus palomuuri toimii ainoastaan OSI-mallin verkkokerroksella (Network layer). (Northrup 2013.)



KUVIO 2. OSI-malli (Fitzroy 2009).

Kuviossa 2 on esitetty OSI-mallin rakenne. Siinä on seitsemän kerrosta, alhaalta lukien Fyysinen-, Datayhteys-, Verkko-, Kuljetus-, Istunto eli yhteysjakso-, Esitystapa- ja Sovelluskerros. Verkkokerroksella, jossa pakettisuodatus palomuuri toimii, määritetään, millä tavalla informaatio lähetetään vastaanottavalle laitteelle. Verkkokerros siis hallitsee verkon kautta tapahtuvia yhteyksiä ja eristää ylempien kerrosten protokollat alla olevan verkon yksityiskohdista. IP eristää ylemmät kerrokset alla olevasta verkosta ja hoitaa osoitteistuksen sekä informaation lähetyksen. Verkkokerrosta kutsutaan tavallisesti TCP/IP:n verkkokerrokseksi.

2.2.3 Sääntöjen asettaminen

Tässä kappaleessa tarkastellaan esimerkkinä DMZ-liitynnän sisältävää palomuuria, jossa DMZ-verkossa on Internetiin näkyvät palvelimet. DMZ-verkossa estetään aina DMZ-verkosta kaikki liikenne LAN:iin, mutta sallitaan

kaikki liikenne Internetiin. Määritetään ensin liikenteen esto LAN-verkkoon. Valikosta *Firewall* valitaan *Rules* ja *Edit*. *Action*-kenttään valitaan *Block*, *Disabled*-kenttä jätetään tyhjäksi, liitynnäksi valitaan DMZ, protokollaksi valitaan TCP ja lähteeksi valitaan any. Tämä estää kaikki järjestelmät, jotka ottavat yhteyden DMZ-liitynnän kautta. Kohteeksi valitaan LAN ja kohdeportti alueeksi asetetaan *any* molempiin, sekä mistä-kenttään että mihin-kenttään. Kuvaus-kenttään kirjoitetaan säännön kuvaus. Tämän jälkeen voidaan sallia kaikki liikenne DMZ-verkosta Internetiin. Asetetaan samat asetukset kuten edellä, mutta toiminta-kenttään valitaan *pass* ja kohteeksi valitaan LAN, mutta valitaan ***not*** aktiiviseksi, jolloin liikenne sallitaan kaikkialle muualle paitsi LAN:iin. Lisäksi sallitaan ulkoverkosta web-liikenne (TCP 80/443) DMZ-verkon web-palvelimelle sekä sallitaan ssh-liikenne (TCP 21) ja Telnet (TCP 23) DMZ-verkon palvelimelle. Sääntö-esimerkit selviävät taulukosta 1.

TAULUKKO 1. DMZ-verkon palomuurisäännöt.

Toiminto	Protokolla	Lähde	Port-ti	Kohde	Port-ti	GW	Kuvaus
Salli	*	DMZ-verkko	*	! LAN-verkko	*	*	Sallitaan kaikki liikenne DMZ-verkosta Internetiin
Salli	TCP	*	80/ 443	172.31.31.10 (DMZ-verkon palvelin)	80/443	*	Web-liikenne ulkoverkosta web-palvelimelle
Salli	TCP	*	21	172.31.31.10 (DMZ-verkon	21	*	SSH ulkoverkosta DMZ:n

				palvelin)			palvelimelle
Salli	TCP	*	23	172.31.31.20 (DMZ-verkon palvelin)	23	*	Telnet DMZ-verkon palvelimelle
Estä	*	DMZ-verkko	*	LAN-verkko	*	*	Estä kaikki liikenne DMZ-verkosta LAN-verkkoon

2.3 Palomuurien ominaisuudet

Palomuurit omaavat useita ominaisuuksia, joita voidaan hyödyntää verkossa. Muun muassa DHCP (Dynamic Host Configuration Protocol) vähentää huomattavasti verkkoasetusten manuaalista konfigurointia ja NAT (Network Address Translation) lisää verkon turvallisuutta sekä vähentää IP-osoitteiden tarvetta.

2.3.1 DHCP ja DHCP Relay

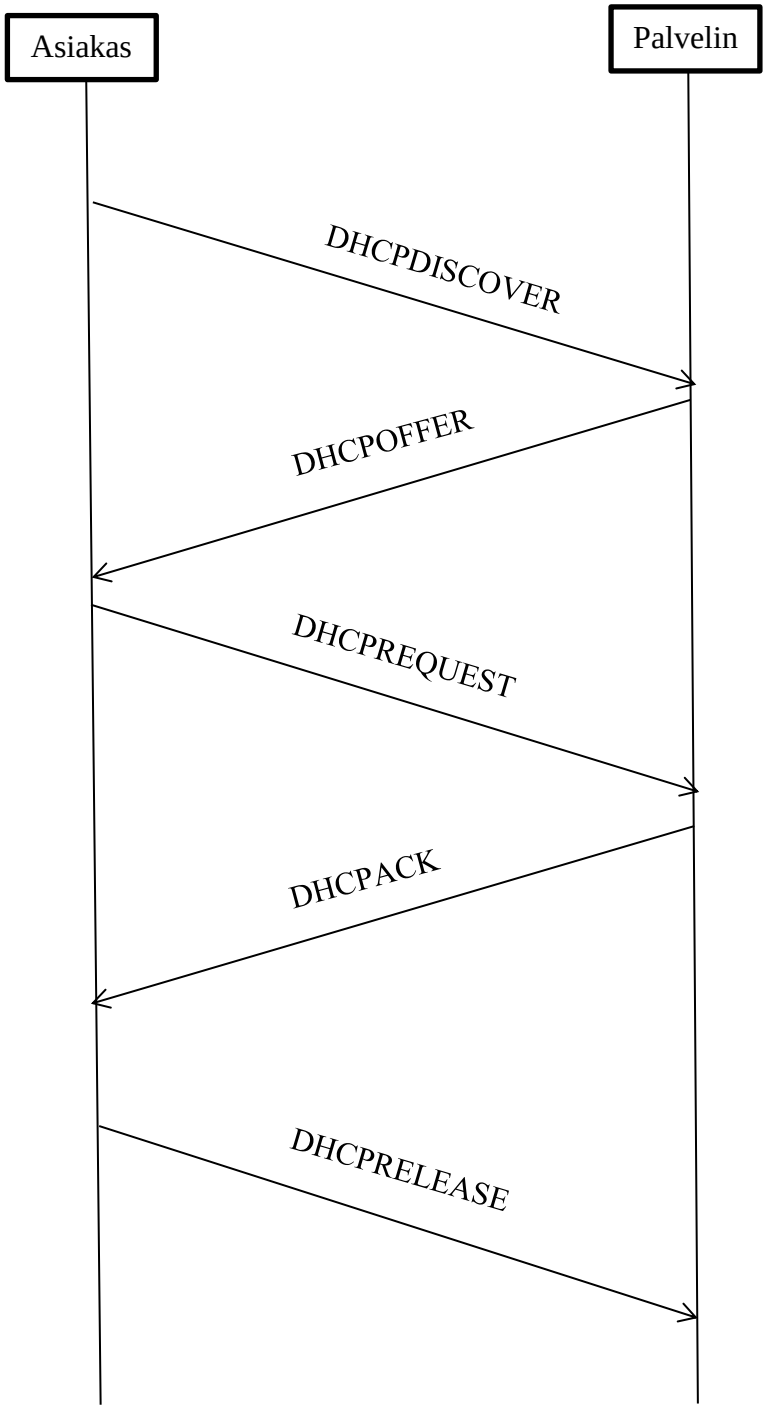
Laitekannan ollessa suuri voi verkkoasetusten asettaminen olla suuri ponnistus laitteita käynnistettäessä. Tällöin voidaan ottaa käyttöön DHCP, joka jakaa automaattisesti osoitteet laitteille.

IP-osoite, aliverkonpeite ja reitittimen osoite voidaan siis määrittää automaattisesti DHCP:n avulla. DHCP-palvelin on verkko-osoitteiden keskitetty hallintapaikka. Esimerkiksi verkon nimipalvelimen muuttuessa, voidaan DHCP-palvelimella muokata kyseistä asetusta keskitetysti, jolloin asetusta ei tarvitse muuttaa

jokaisella laitteella erikseen. Tämä vähentää verkon ylläpitäjän tehtäviä huomattavasti. (Pesonen 2005.)

Asiakas-palvelin arkkitehtuurin lisäksi, joka on DHCP:n perusta, voidaan käyttää DHCP-välityspalvelinta (relay). DHCP Relay mahdollistaa palvelimen toiminnan aliverkon ulkopuolella. DHCP Relay määritetään reitittävän laitteen konfiguraatioon. DHCP toimii normaalisti omassa aliverkossaan. DHCP pitää huolen, että samaa osoitetta ei ole kuin yhdellä asiakkaalla yhtä aikaa. (Pesonen 2005.)

IP-osoitteen saaminen vaatii useita viestejä palvelimen ja asiakkaan välillä. Kuviossa 3 on esitetty kuinka DHCP-asiakas lähettää broadcast-viestin omaan aliverkkoonsa. Tämä on DHCPDISCOVER-viesti, johon palvelin vastaa tarjoamalla osoitetta asiakkaalle viestillä DHCPOFFER. Tämän jälkeen asiakas pyytää osoitetta käyttöönsä viestillä DHCPREQUEST. Palvelin hyväksyy pyynnön viestillä DHCPACK. DHCPRELEASE-viestillä asiakas luopuu osoitteesta sitten, kun ei enää tarvitse osoitetta. (Droms 1997.)



KUVIO 3. Viestien lähetys asiakkaan ja DHCP-palvelimen välillä uutta osoitetta liisatessa.

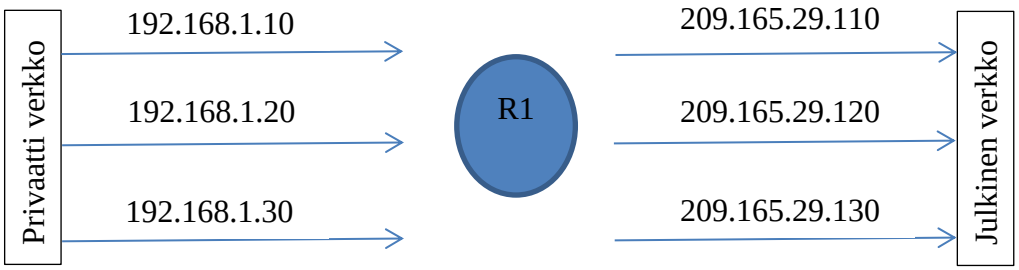
2.3.2 NAT (Network Address Translation), osoittenmuunnos

NAT lisää tietoturvaa ja säästää IP-osoitteita. Estämällä sisäverkon osoitteita näkymästä ulospäin NAT suojaa sisäverkkoa. NAT:in ansiosta kaikki liikenne näyttää kulkevan yhden osoitteen kautta, jolloin sisäverkon rakenne ei paljastu ulkopuolisille. Seuraavaksi esitetään esimerkki, joka havainnollistaa NAT:in toimintaperiaatettaa.

NAT:ia voidaan kuvata verrainnollisesti reseptionistiin, joka huolehtii siitä kuka pääsee puhelimella läpi yrityksen sisäiselle henkilölle. Reseptionistille on annettu ohjeet, että puheluita ei saa yhdistää ellei anneta uusia ohjeita. Yrityksen henkilö myöhemmin soittaa asiakkaalle ja jättää tälle soittopyynnön. Nyt reseptionisti saa ohjeet yhdistää kyseinen asiakas yrityshenkilölle. Asiakas soittaa yrityksen keskusnumeroon, joka on ainoa numero hänen tiedossaan. Reseptionisti yhdistää asiakkaan yrityshenkilölle, jonka numeron hän on tarkistanut puhelinlistalta, jossa on jokaisen yrityshenkilön numeropääte. Reseptionisti yhdistää puhelun, koska hän tietää yrityshenkilön odottavan puhelua tältä asiakkaalta. (Cisco 2011.)

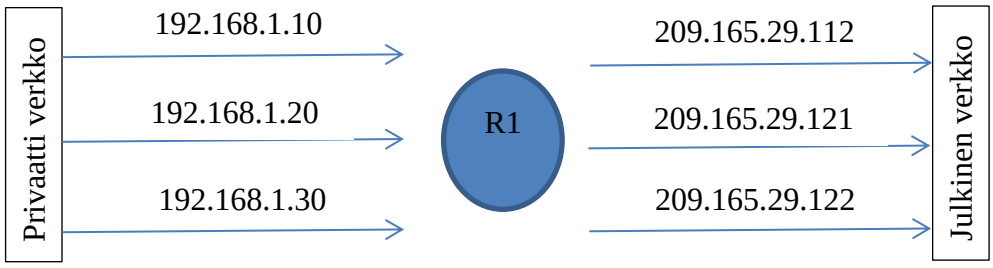
NAT:ia voidaan käyttää palomuurissa, reitittimessä tai tietokoneessa, joka on sisä- ja ulkoverkon välissä. NAT toimii OSI-mallin kolmannella kerroksella, jossa myös reititin toimii. OSI-malli on esitetty kuviossa 2. NAT voidaan toteuttaa monella eri tavalla, josta kerrotaan seuraavaksi.

Staattista (1:1) NAT:ia käytetään tilanteissa, joissa laite täytyy olla saavutettavissa ulkoapäin. Staattisessa NAT:ssa tietty osoite käännetään aina samaan osoitteeseen. Kuviossa 4 on esimerkki, kuinka staattinen NAT toimii. (Cisco 2011.)



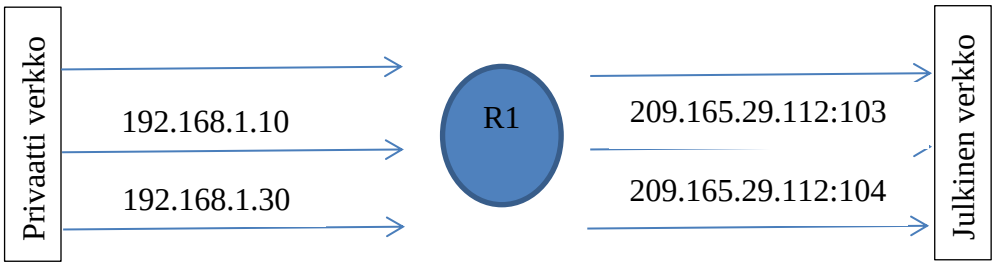
KUVIO 4. Staattisen NAT:in toimintaperiaate. Ympyrä keskellä kuvaa reititintä. (Cisco 2011.)

Dynaaminen NAT kääntää osoitteen ensimmäiseen vapaaseen osoitteeseen poolista, joka tässä esimerkissä on 209.165.29.111 – 209.165.29.161. Kuviossa 5 on esitetty dynaaminen NAT.



KUVIO 5. Dynaamisen NAT:in toimintaperiaate.

NAT Overloading eli PAT (Port Address Translation) kääntää useita eri privaatti osoitteita yhdeksi osoitteksi, johon on lisätty yksilöivä porttinumero. Kuviossa 6 on esimerkki PAT:sta.



KUVIO 6. PAT:in toimintaperiaate.

2.3.3 QoS

QoS (Quality of Service) on tietoliikenteen priorisointia. Sen avulla voidaan tiettyä liikennettä, esimerkiksi P2P-liikennettä hidastaa tai pudottaa kokonaan pois. Priorisoitu liikenne lähetetään ennen muuta liikennettä.

Ilman priorisointia paketit käsitellään palomuurissa FIFO-menetelmällä (first in/first out). QoS priorisoi erilaista liikennettä ja varmistaa korkeamman priorisoinnin omaavan palvelun saavan tarvitsemansa kaistanleveyden.

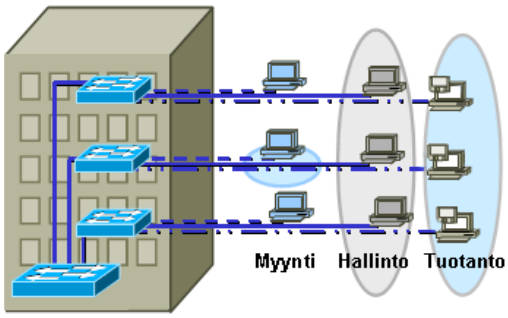
QoS:ä voidaan verrata tässäkin tapauksessa portsariin klubilla. VIP:it (”Very Important Packets”) pääsevät aina ensimmäisinä sisään ilman odotusta. Tavalliset paketit joutuvat odottamaan vuoroaan jonossa ja ns. ei-toivotut paketit pidetään ulkopuolella niin kauan, että parhaat juhlat ovat ohi. Koko ajan klubi pidetään kapasiteetin rajoissa eikä koskaan ylikuormiteta sitä. Jos myöhemmin tulee lisää VIP:jä, niin tavallisia paketteja voidaan heittää ulos, jotta klubi ei ylikuormitu. (Buechler & Pingle 2009, 333.)

2.3.4 VLAN (Virtual Local Area Network)

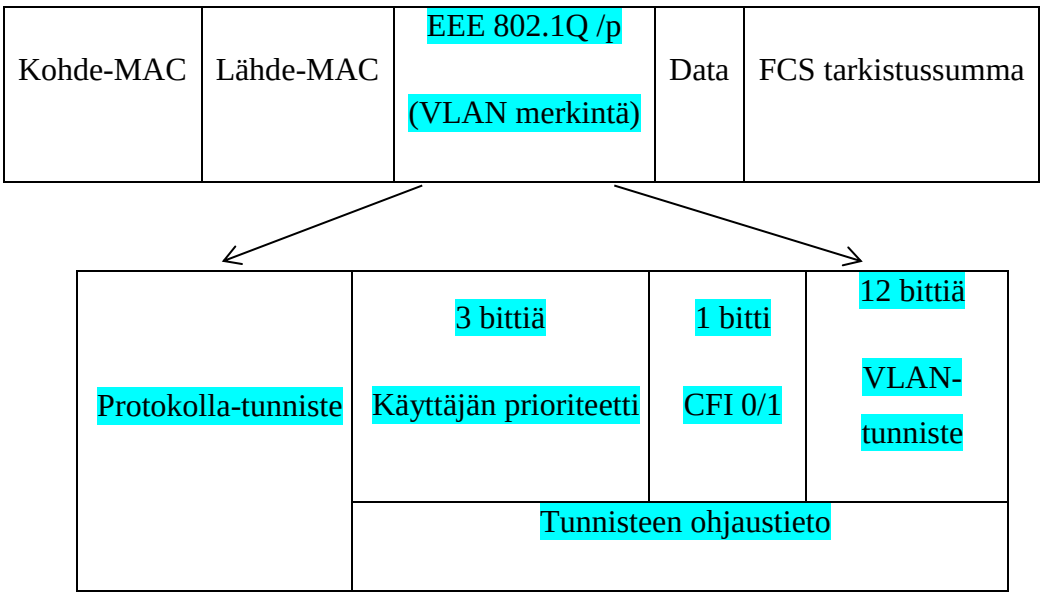
VLAN on looginen verkko (aliverkko) tai broadcast-alue. Usein lähiverkot jaetaan loogisiin käyttäjäryhmiin, joiden jakoperusteena ovat toiminnalliset syyt. Toiminnallisia syitä voivat olla esimerkiksi tuotanto, hallinto ja myynti. Nämä ryhmät halutaan pitää erillisissä verkoissa. Kun fyysisesti yhtenäinen lähiverkko halutaan segmentoida loogisesti täysin erotelluiksi verkoiksi, niin silloin käytetään VLANeja. Kuviossa 5 kaikki saman kerroksen tietokoneet on kytketty samaan kytkimeen, mutta ne voivat liikennöidä vain oman ryhmän jäsenten kanssa.

VLAN:en välinen liikenne täytyy reitittää reitittimen avulla. (Tallinnan Yliopisto 2012.)

Kytkimien on vaihdettava VLAN-tietoja keskenään, minkä vuoksi on otettu käyttöön VLAN-kehystys. Pakettien kuuluminen tiettyyn VLANiin voidaan erotella VLAN-kehysten avulla. Kytkin lisää normaaliin Ethernet-kehykseen VLAN-ID-osan, koska vastaanottavan laitteen tulee tuntea samat VLANit. Kuviossa 6 on esitetty VLAN-kehys. (Tallinnan Yliopisto 2012b.)



KUVIO 5. VLANit myynti, hallinto ja tuotanto. (Tallinnan Yliopisto 2012.)



KUVIO 6. IEEE 802.1Q (dot1.q) -kehys.

Tärkeimmät kentät kehyksessä ovat käyttäjän prioriteetti ja VLAN-tunniste. Kolme bittisellä käyttäjän prioriteetti-kentällä voidaan määritellä 8 prioriteettitasoa (0-7). VLAN-tunniste-kentälle on varattu 12 bittiä eli VLANien suurin määrä on 4096 kappaletta. (Tallinnan Yliopisto 2012b.)

2.3.5 VPN (Virtual Private Network)

VPN:llä liikenne tunneloidaan pisteestä A pisteeseen B turvattomien verkkojen, kuten Internetin, läpi. Tunnelointi toteutetaan salatulla yhteydellä, jolloin ulkopuoliset eivät pääse näkemään tai käsittelemään informaatiota siirron aikana. VPN sisältää kapseloidun, salatun ja autentikoidun yhteyden jaetun tai julkisen verkon läpi.

VPN etäyhteys (VPN remote access) ja reitittimien välinenVPN-yhteys (router-to-router VPN) ovat kaksi tapaa, joilla VPN-yhteys voidaan toteuttaa. VPN etäyhteys on toteutettu siten, että verkossa on erillinen tietokone valvomassa liikennettä. Tietokonkone hoitaa salauksen ennen datan menoa reitittimelle. Reitittimeltä saapuva data myös puretaan tällä tietokoneella.

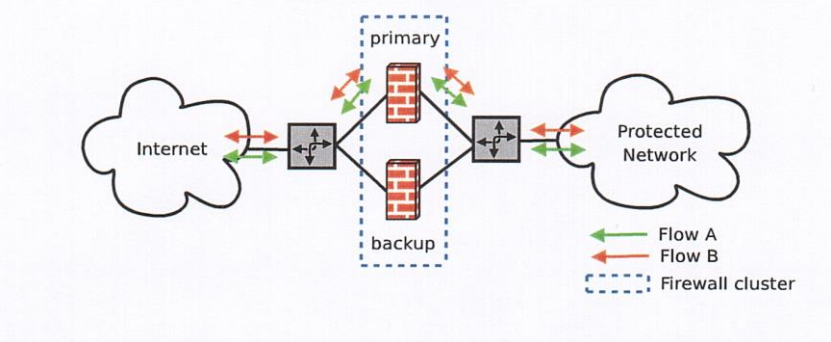
Reitittimien välinen VPN-yhteys on rakennettu suoraan reitittimien väliin. Reitin hoitaa salauksen ja datan purkamisen, jolloin erillistä tietokonetta ei tarvita. Huono puoli tässä tavassa on muun muassa se, että yritys jää yhden reitin valmistajan armoille, koska yhteyttä ei voida luoda erimerkkisten reitittimien välille.

2.3.6 Vikasietoisuus

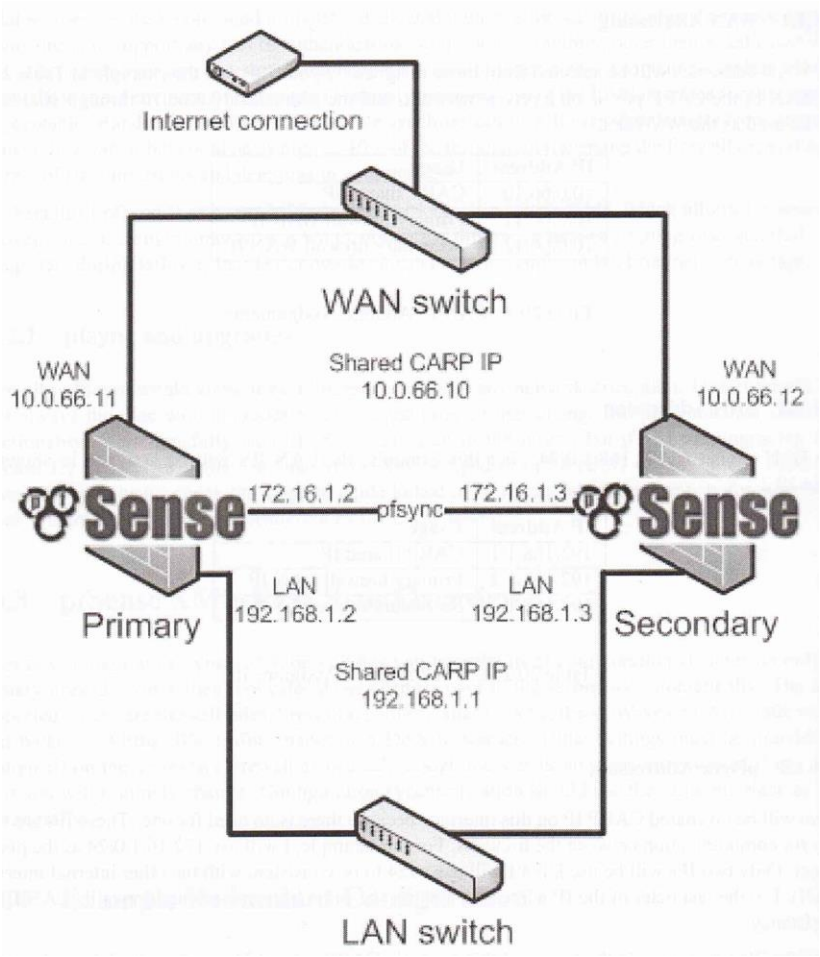
Nykyisin monilla palomuureilla on tarjota vikasieto-ominaisuus. Vikasieto-ominaisuus mahdollistaa kahden palomuurin yhdistäminen pariksi, jossa toinen laite on heti käyttövalmiina toisen vikaantuessa. Muun muassa CheckPoint Firewall-1, StoneGate, Cisco PIX ja Nokia IPSO -palomuureilla on vikasieto-ominaisuus. Avoimen lähdekoodin pfSense tarjoaa myös vikasietoisuuden, joka toteutetaan yhdistämällä CARP (Common Address Redundancy Protocol), pfsync ja pfSensen XML-RPC konfiguraation synkronosointi.

Kummallakin CARP-ryhmän palomuurilla on uniikit IP-osoitteet liittymille sekä yhteisen jaetun CARP VIP:in (Virtual IP). CARP VIP -osoitteet ovat aktiivisia vain silloin, kun palomuuri on master. Jos yhdessäkään liittymässä todetaan vikaa, niin backup palomuuri vaihtaa itsensä masteriksi. Kuviossa 7 on kuvattu yksinkertainen primary-backup palomuuri arkkitehtuuri ja kuviossa 8 on esitetty pfSensellä toteutettu CARP verkkokaavio.

CARP on protokolla, joka sallii useiden isäntien jakaa IP-osoitteryhmän samassa lähiverkossa. CARPin päätarkoitus on tarjota vikasieto-ominaisuus ja CARP on ilmainen, ei-patentoitu vaihtoehto Ciscon HSRP:lle (Hot Standby Router Protocol). CARP on yleensä toteutettu BSD-käyttöjärjestelmissä (Berkeley Software Distribution), jotka ovat Unix-käyttöjärjestelmiä.



KUVIO 7. Yksinkertainen primary-backup -palomuuriarkkitehtuuri.



KUVIO 8. Esimerkki CARP-verkkokaavio. (Buechler & Pingle 2009, 386.)

3 PALOMUURITUOTTEET

3.1 pfSense 2.0.1

PfSense-projekti aloitettiin vuonna 2004. PfSensen kehittäminen aloitettiin 0n0wall:in puutteiden pohjalta. m0n0wall ladataan suoraan RAM-muistiin, joten puutteena nähtiin muun muassa se, että m0n0wall:ia ei voi asentaa normaaliin tiedostojärjestelmään kovalevylle. Tämän seurauksena monet toivottavat toiminnot eivät olleet järkevästi toteutettavissa. PfSense sisältää Unix-pohjaisen käyttöjärjestelmän ja selain käyttöliittymän. Ohjelma on ladattavissa pfSensen verkkosivuilta. (BSD Perimeter LLC 2013a.)

PfSense vaatii vähintään 100 Mhz Pentium-tason tietokoneen, jossa on 128 MB RAM-muistia ja vähintään 1 GB:n kovalevy. Verkkokortteja tulee olla peruskäyttöön kaksi ja laajempaa käyttöä varten kolmesta neljään verkkokorttia. (BSD Perimeter LLC 2013b.)

PfSense-palomuurilla on mahdollista suodattaa TCP- ja UDP-liikennettä lähde- ja kohdeosoitteen, IP-protokollan sekä lähde- ja kohdeportin mukaan. Ohjelmistolla on mahdollista kirjata sääntöön sisältyvää liikennettä lokeihin. Aliakset mahdollistavt IP-osoitteiden, verkkojen ja porttien nimeämisen ja ryhmittelyn. Tämä helpottaa ja selkiyttää palomuurin säännöstön ymmärtämistä varsinkin silloin, kun käytössä on useita julkisia IP-osoitteita ja useita palvelimia. PfSense pystyy siltaamaan liittymiä ja suodattamaan liikennettä niiden välillä. Pakettien normalisointi onnistuu siten, että ei ole monitulkintaisuutta paketin lopullisen kohteen tulkinnassa. Pakettien normalisointi myös kokoaa uudelleen sirpaloituneet paketit, suojaten joitakin käyttöjärjestelmiä tietyn muodon omaavilta hyökkäyksiltä ja hylkää paketit, joilla on väärä lippu yhdistelmä. Tämä ominaisuus on oletuksena päällä, mutta sen voi poistaa käytöstä. Mahdollista asettaa palomuuri puhtaasti reitityskäyttöön disabloimalla suodatuksen. (BSD Perimeter LLC 2013c.)

PfSense on tilallinen palomuuri, ja oletuksena kaikki säännöt ovat tilallisia. Tämä tarkoittaa sitä, että palomuuri seuraa palomuurin läpi kulkevaa verkkoyhteyksien tilaa, kuten TCP virtoja ja UDP tiedonvälitystä. Palomuuri on ohjelmoitu

erottamaan sallitut erityyppisten yhteyksien paketit. Ainoastaan tiettyyn yhteyteen liittyvät paketit sallitaan ja muut hylätään. PfSensellä on paljon ominaisuuksia, joilla tilataulukoita voidaan kontrolloida:

- säädettävissä oleva tilataulukon koko
- säännön perusteella voidaan:
    - rajoittaa yhtäaikaisia asiakas yhteyksiä
    - rajoittaa tiloja/isäntä
    - rajoittaa uusia yhteyksiä/sekunti
    - määrittää tilan aikakatkaisu
    - määrittää tilan tyyppi

PfSense tarjoaa monia vaihtoehtoja tilan hallintaan:

- tilan säilytys - oletuksena kaikille säännöille ja toimii kaikilla protokollilla
- tilan mukauttaminen – toimii vain TCP:llä
- synproxy tila
- none – ei pidä mitään sisääntuloja määrätylle liikenteelle

PfSense tarjoaa neljä vaihtoehtoa tilojen optimointiin:

- normaali – oletus algoritmi
- korkea viive – käytännöllinen esimerkiksi satelliittiyhteyksillä
- aggressiivinen – voi hylätä sallitut yhteydet
- konservatiivinen – yrittää välttää hylkäämästä sallittuja yhteyksiä

PfSensen NAT sisältää porttiohjauksen, joka sisältää useat julkiset IP-osoitteet ja porttialueet. Lisäksi pfSense:ssä on 1:1 NAT yksittäisille IP-osoitteille tai aliverkoille. Outbound (lähtevä) NAT NAT:taa oletusasetuksilla kaiken lähtevän liikenteen WAN IP -osoitteeseen. Advanced Outbound NAT (edistynyt lähtevä NAT) sallii edellä mainitun oletus menettelyn pois päältä kytkemisen, jolloin voidaan tehdä hyvin joustavia NAT-sääntöjä. NAT Reflection (NAT peilikuva/heijastus) on joissakin konfiguraatioissa mahdollinen, jolloin palveluihin päästään julkisella IP-osoitteella sisäisestä verkosta. (BSD Perimeter LLC 2013c.)

OpenBSD:n CARP sallii laitteiston vikaantumisen. Vikasieto-ominaisuus mahdollistaa kahden palomuurin yhdistäminen pariksi, jossa toinen laite on heti käyttövalmiina toisen vikaantuessa. Kun ensisijaisen palomuurin liityntä menee alas tai palomuuri jostain syystä siirtyy offline-tilaan, niin toissijainen palomuuri

aktivoituu. Lisäksi pfSense-palomuurissa on asetusten sykronointi kapasiteetti, jolloin ensisijaiseen palomuuriin tehdyt muutokset synkronoituvat toissijaiseen palomuuriin automaattisesti. Tämä pfsync:ksi kutsuttu ominaisuus varmistaa, että palomuurin tilataulukot kopioidaan kaikkiin vikasietopalomuureihin järjestelmässä. Tämä on tärkeä ominaisuus, jotta verkkohäiriöitä ei syntyisi. Olemassa olevat yhteydet pidetään yllä vikaantumisesta huolimatta. Tämä vikasieto-ominaisuus toimii vain käytettäessä staattisia, julkisia IP-osoitteita. (BSD Perimeter LLC 2013c.)

Kuormituksen tasaus on yksi pfSensen ominaisuuksista, ja VPN-yhteyksiä on kolme eri vaihtoehtoa: IPsec (Internet Protocol Security), OpenVPN ja PPTP. IPsec toimii salaten ja kapseloiden IP-paketin IPSec-paketin sisään. Paketin purku tapahtuu tunnelin lopussa, jossa alkuperäisen IP-paketin salaus puretaan ja paketti lähetetään edelleen kohteeseensa. Open VPN on joustava ja tehokas SSL (Transport Layer Security)VPN -ratkaisu, joka tukee useita käyttöjärjestelmiä. SSL VPN voi tunneloida koko verkon liikenteen tai yksittäisen yhteyden. OpenVPN projektissa tunneloidaan koko verkon liikenne. PPTP (Point-to-Point Tunneling Protocol) on suosittu, koska lähes kaikki käyttöjärjestelmät omaavat sisäänrakennetun PPTP-clientin. PfSense PPTP -palvelin voi käytää paikallisen käyttäjäntietokantaa tai RADIUS-palvelimen autentikointia. PfSensessä on myös PPPoE (Point-to-Point Protocol over Ethernet)-palvelin, joka on verkkoprotokolla, jolla kapseloidaan PPP-kehyksiä Ethernet-kehyksen sisään. (BSD Perimeter LLC 2013c.)

RRD-graafit ylläpitävät historiatietoja muun muassa CPU:n käytöstä, kokonaissuoritustehosta, palomuuritiloista, yksittäisestä suoritustehosta jokaisessa liitynnässä ja paketti/sekunti nopeudesta jokaisessa liitynnässä. Tosiaikainen informaatio on jopa tärkempää ja tätä varten pfSensessä on SVG-graafit. SVG-graafi näyttää tosiaikaisen suoritustehon jokaiselle liitynnälle. PfSense:stä löytyy myös dynaaminen DNS, joka sallii julkisen IP-osoitteen rekisteröinnin lukuisalle määrälle DNS palveluiden tarjoajia. PfSense:ssä on myös DHCP-palvelin-ominaisuus ja DHCP Relay-ominaisuus, joista on kerrottu tarkemmin kappaleessa DHCP ja DHCP Relay. (BSD Perimeter LLC 2013c.)

PfSensellä on muun muassa ping- ja traceroute-työkalut, joilla voidaan todentaa yhteyden olemassaolo tiettyyn isäntään (ping), ja traceroutella voidaan selvittää reitityspolku kohteeseen. (BSD Perimeter LLC 2013c.)

PfSenseen on saatavilla lukuisa määrä paketteja (packages), jotka ovat erittäin helppoja asentaa. Turvallisuuteen liittyen muun muassa snort on saatavilla tällaisen paketin muodossa. Verkon hallintaan littyviä paketteja on useita, joista mainittakoon esimerkiksi ntop. Lisäksi saatavilla on pelveluihin ja järjestelmään liittyviä lisäasennuspaketteja. (BSD Perimeter LLC 2013c.)

3.2 SmoothWall Express

SmoothWallin avoimen lähdekoodin kehitysprojekti aloitettiin vuonna 2000. SmoothWall sisältää GNU/Linux-pohjaisen käyttöjärjestelmän ja helppokäyttöisen selain käyttöliittymän. Ohjelma on ladattavissa SmoothWall:in verkkosivuilta. (Smoothwall 2012a.)

SmoothWall Express toimii 200 MHz:n Pentium-tason tietokoneella, jossa on 128 MB RAM-muistia ja vähintään 2 GB:n kovalevy. Tietokoneessa tulee olla kaksi verkkokorttia peruskäyttöön ja kolme tai enemmän, jos järjestelmässä tulee olemaan esimerkiksi DMZ tai langaton verkko. (Smoothwall 2012b.)

SmootWall Express:llä on mahdollista kontrolloida verkkoliikennettä, hallita sisääntulevaa ja uloslähtevää liikennettä, kontrolloida sisäisitä liikennettä sekä pääsyä palveluihin. Tietyn IP-osoitteen estäminen ja ajastetun pääsyn määrittääminen Internetiin on niin ikään mahdollista. Liittymien kanssa työskentely on mahdollista. (Smoothwall Limited 2007, 13.)

SmoothWAll Express estää oletuksena kaiken sisääntulevan liikenteen, joka ei ole uloslähtevän pyynnön tulos. Tästä syystä, kaikilla IP-osoitteilla ja porteilla, joiden liikenne halutaan sallia, täytyy olla porttiohjaussääntö (port forwarding) käytössä. Yleensä porttiohjausta käytetään sallimaan palvelimet DMZ-alueella kommunikoimaan ulkomaailman kanssa Internetissä. Tällöin palvelimien IP-osoitteet, palvelut tai portit eivät paljastu enempää kuin on tarpeellista. Uloslähtevä liikenne voidaan rajoittaa, sallia tai estää pääsy Internetiin perustuen jokaiseen sisäiseen liityntään. Lisäksi voidaan määrittää niin sanottu estolista,

jonka perusteella tietyt IP-osoitteet pääsevät Internetiin. Sisäisen liikenteen hallinta sallii reikien tekemisen esimerkiksi DMZ:n ja LAN:n välille, jotta sisäinen liikenne saa kulkea edellä mainittua väliä. Pääsy palveluihin voidaan sallia IP-osoitteen ja portin perusteella WAN-liittymään, jolloin administraattori pääsee verkon ulkopuolelta palomuuriin käsiksi. SmoothWall Expressiin tai sen takana oleviin koneisiin pääsy voidaan estää valinnaisten ulkopuolisten IP-osoitteiden perusteella. SmoothWall Expresissä on myös QoS-ominaisuus, jolla voidaan priorisoida liikennettä. (Smoothwall Limited 2007, 13 – 18.)

SmoothWall Expressillä voidaan hallita Internet Control Message Protocol:laa (ICMP). WebGUI:lla voidaan myös määrittää liittymien, yhdyskäytävien ja DNS:n asetuksia. SmoothWall Express mahdollistaa IPSec VPN-yhteyksien luomisen toiseen SmoothWall Express järjestelmään tai IPSec:in omaavan asiakkaaseen, jolla on staattinen IP-osoite. SmoothWall Expressin työkaluja ovat Whois, ping ja traceroute. Whois-työkalua voidaan käyttää IP-osoitteen tai domain-nimen omistajuusinformaatiota selvitettäessä. Ping- ja Traceroute-työkalut toimivat samalla tavalla kuin pfSensessä. (Smoothwall Limited 2007, 24 – 36.)

3.3 Vyatta Core

Vyattaa alettiin kehittää avoimen lähdekoodin vaihtoehdoksi perinteisille reitittimille vuonna 2005. Vyatta Core on Debian-pohjainen reititys- ja palomuuriohjelmisto. Tuote on ollut saatavilla vuodesta 2006. Nykisin tuotteesta on saatavilla kolme eri versiota: Vyatta Core, Vyatta Subscription Edition ja Vyatta Plus. Vyatta Core on ilmainen versio, johon on saatavilla kattava dokumentaatio tuotteen käyttöä ja asetuksia varten. Ilmaiseen Core-versioon ei sisälly selain käyttöliittymää. Ohjelma on ladattavissa Vyattan verkkosivuilta. (Wikipedia 2013.)

Järjestelmävaatimuksina Vyatta Corella on yksi ytiminen prosessori, 512 MB RAM-muistia ja suurempi kuin 2 GB:n kovalevy. Prosessorin valinta tehdään ytimien lukumäärän perusteella, kun suoritustehoa halutaan kasvattaa. (Vyatta 2013.)

Vyatta suodattaa liikennettä lähde- ja kohdeosoitteen, lähde- ja kohdeportin, IP-protokollan sekä ICMP-tyypin mukaan. Palomuuri on mahdollista asettaa tilalliseen tai tilattomaan toimintoon. Vyatta sisältää tilallisen vikasieto-ominaisuuden, alue-perustaisen palomuuritoiminnon ja aika-perustaisen palomuuritoiminnon. Oletuksena Vyatta on tilaton palomuuri. Vyatta Corella on mahdollista tehdä NAT, ja Vyatta sisältää DHCP-ominaisuuden ja DHCP Relayn. (Vyatta Inc. 2012a, 2.)

Vyatta-järjestelmän CLI on vuorovaikutuksessa Netfilter Connection Tracking Systemin kanssa, joka tarjoaa yhteyden jäljitystä useille järjestelmän toiminnoille, kuten palomuurille, NAT:lle ja WAN kuorman tasaukselle. Palomuurissa yhteyden jäljitys sallii tilallisen pakettien tarkastelun. (Vyatta Inc. 2012a, 3.)

Palomuurin määrittelyn jälkeen palomuuri voidaan asettaa liittymälle, jossa palomuuri toimii pakettisuodattimena. Taulukosta 2 voidaan katsoa, kuinka palomuuri suodattaa paketteja riippuen, mitä on määritetty:

TAULUKKO 2. Vyattan toimintaperiaate.

Liikenteen suunta	Toiminta
in	Palomuuri suodattaa liittymään tulevat ja Vyatta-järjestelmän kautta ohjatut paketit.
out	Palomuuri suodattaa liittymästä lähtevät paketit. Näitä voivat olla Vyatta-järjestelmän kautta kulkevat paketit tai järjestelmästä lähtöisin olevat paketit.
local	Palomuuri suodattaa Vyatta-järjestelmään tulevat paketit.

Kolme palomuuria voidaan asettaa liittymää kohden: yksi in, yksi out ja yksi local suodatin. Palomuuri on oletuksena auki ja päästää kaiken liikenteen läpi. (Vyatta Inc. 2012a, 4.)

Alueperustaisessa palomuurissa liittymät on ryhmitelty turvallisuusalueiden mukaisesti, joissa jokaisella alueen sisällä olevalla liittymällä on sama turvallisuustaso. Suodatus on käytössä eri turvava-alueiden välillä kulkevalle liikenteelle. (Vyatta Inc. 2012a, 7.)

Vyatta Coressa on kolme eri NAT-tyyppiä, joita ovat SNAT (Source NAT), DNAT (Destination NAT) ja Bidirectional NAT. SNAT on yleisin, ja siinä yksityinen lähde IP-osoite käännetään joksikin julkiseksi IP-osoitteeksi. Masquerade NAT:ssa uloslähetvän paketin lähde IP-osoite vaihdetaan ensisijaiseen lähtevän liikenteen liittymän IP-osoitteeksi, ja palaavien pakettien kohde IP-osoite käännetään takaisin lähde isännän IP-osoitteeksi. DNAT muuntaa kohdeosoitteen, ja sitä käytetään silloin, kun halutaan ulkoverkosta yhteys sisäverkon laitteeseen. Bidirectional NAT:ssa sekä SNAT että DNAT konfiguroidaan samaan aikaan. Sitä käytetään silloin, kun sisäverkon isäntä tarvitsee yhteyden ulkoverkon isännän välille ja samalla ulkoverkon isäntä sisäverkon isännän kanssa. (Vyatta Inc. 2012b, 4.)

Taulukossa 3 on määritelty järjestelmävaatimukset kaikille kolmelle palomuuriohjelmistolle. Taulukosta nähdään, että pfSense voidaan toteuttaa varsin vaatimattomalla laitteistolla ja muistilla verrattuna Vyatta Coreen. Smoothwall puolestaan vaatii hieman pfSenseä tehokkaamman prosessorin.

TAULUKKO 3. PfSensen ja SmoothWall Expressin järjestelmävaatimukset.

Järjestelmä vaatimukset:	**pfSense 2.0.1**	**SmoothWall Express 3.0**	**Vyatta Core**
Prosessori	Pentium 100 MHz	Pentium 200 MHz	1 ytiminen prosessori
Muisti	128 MB	64 MB	512 MB
Kovalevy	1 GB	1 GB	2+ GB

TAULUKKO 4. Yhteenveto pfSEnsen ja SmoothWall Expressin ja Vyattan ominaisuuksista.

Ominaisuus	**pfSense 2.0.1**	**SmoothWall Express 3.0**	**Vyatta Core**
Tilallinen palomuuri ja tilallinen tarkastelu	Kyllä	Kyllä	Kyllä
NAT	Kyllä	Kyllä	Kyllä
Uloslähtevän liikenteen kontrolli	Kyllä	Rajoitettu	Kyllä
P2P-suodatus	Kyllä	Kyllä	Kyllä
IDS (Intrusion Detection System)	Saatavilla	Kyllä	Kyllä
IPSec VPN Open VPN PPTP	Kyllä Kyllä Kyllä	Kyllä Ei Ei	Kyllä Kyllä Kyllä
DHCP DHCP Relay	Kyllä Kyllä	Kyllä Ei	Kyllä
Vikasieto-ominaisuus	Kyllä	Ei	Kyllä
VLAN	Kyllä	Ei	Kyllä
WebGUI	Kyllä	Kyllä	Ei

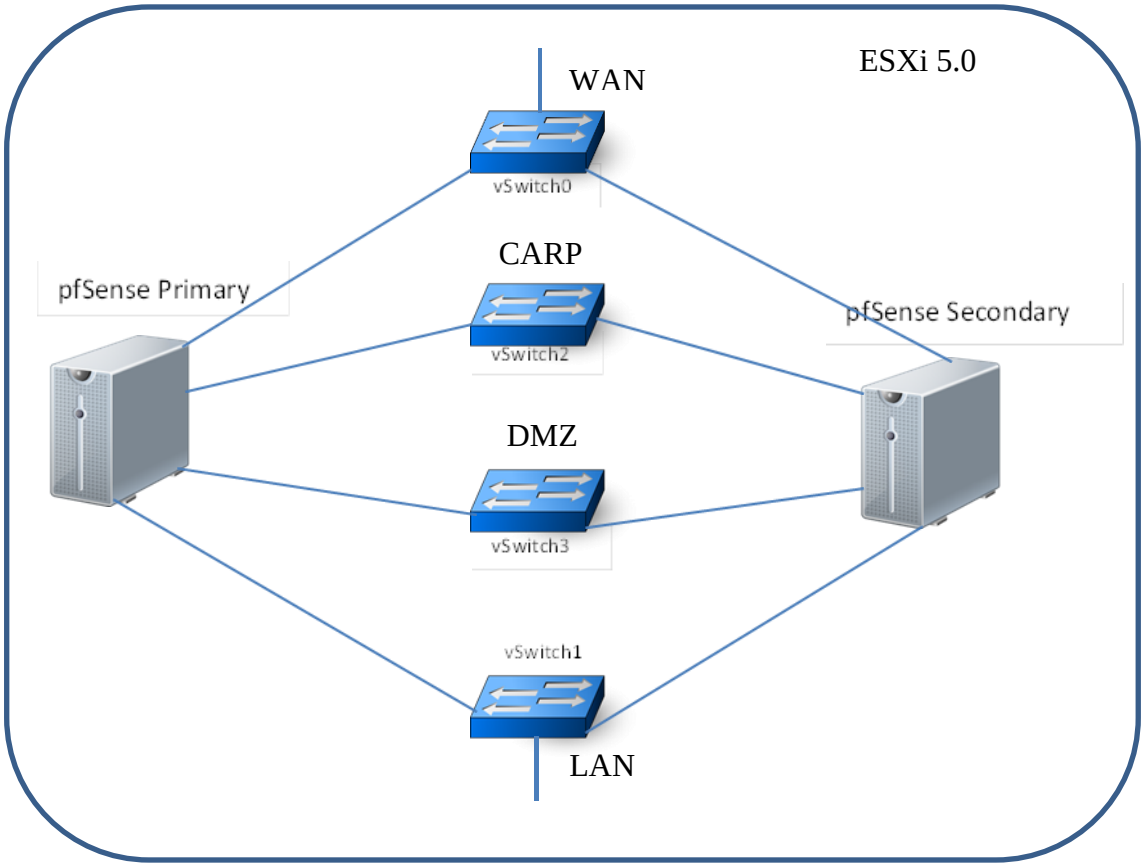
Taulukosta nähdään, että Smootwall Expressissä on rajoitettu uloslähtevän liikenteen kontrolli. Smoothwall Expressillä voidaan joko sallia tai estää pääsy Internettiin, mutta samalla täytyy määrittää ehto, jotta verkko ei olisi kokonaan

auki tai suljettu. Smoothwall Express ei sisällä DHCP Relay-ominaisuutta, vikasieto-ominaisuutta eikä VLAN-ominaisuutta. Vyatassa ei ole käytössä WebGUI:ta ilmaisversiossa, joten sitä on hankala käyttää. Toisaalta Vyattaan saa WebGUI:n, jos ottaa ohjelmasta maksullisen version. Opinnäytetyöhön valitaan pfSense ilmaisuuden ja ominaisuuksien perusteella.

4 KÄYTÄNNÖN TOTEUTUS

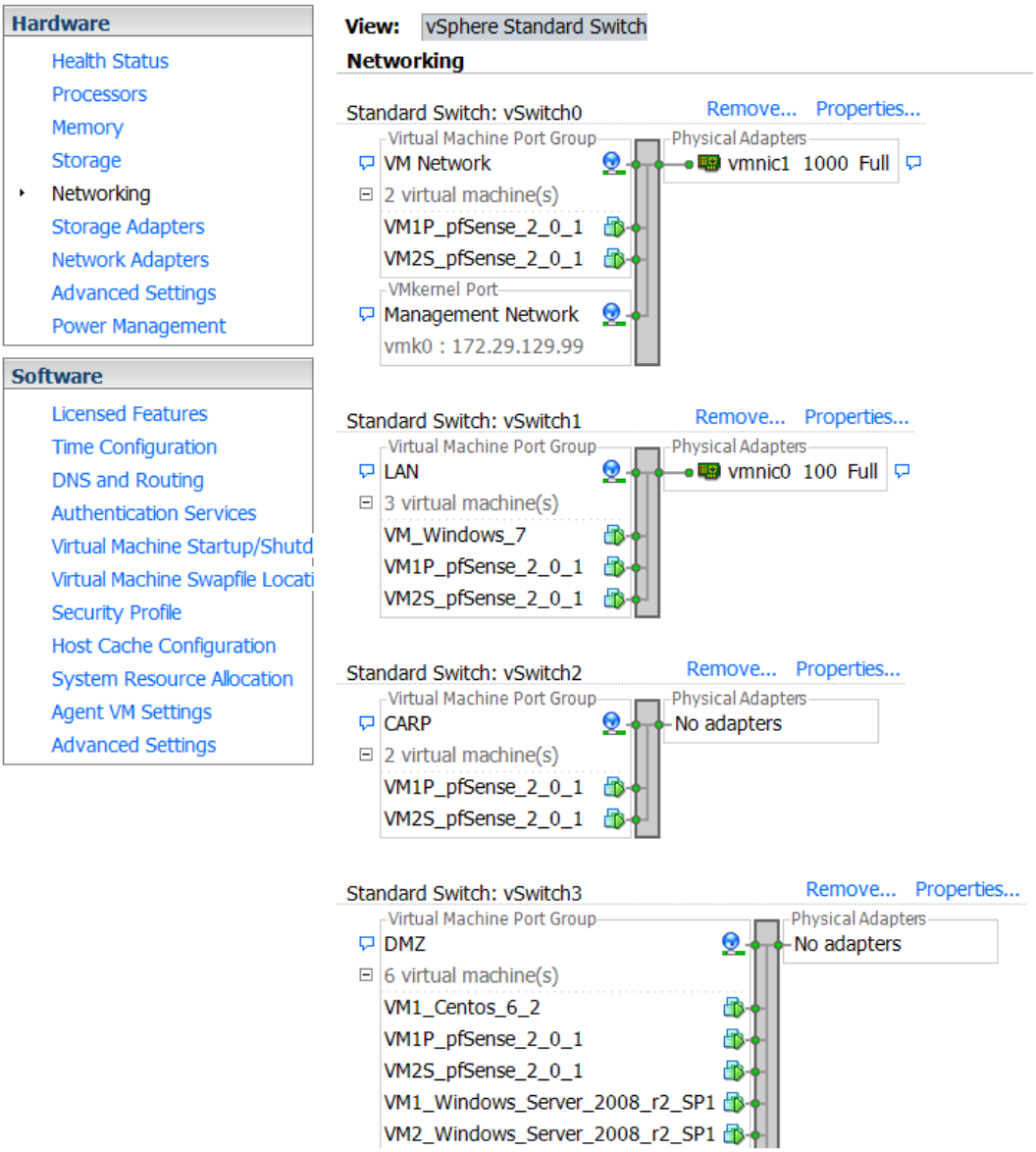
4.1 Testiympäristön kuvaus

Testiympäristö pitää sisällään ESXi-palvelimen, johon on asennettu kaksi VMwaren virtuaalikonetta. Näihin virtuaalikoneisiin asennettiin pfSense 2.0.1-palomuuriohjelmistot. Verkkoon sisältyy myös DMZ-verkko, johon kuuluu kaksi Windows Server 2008 R2 -palvelinta. PfSense -palomuurit yhdistettiin CARP:in avulla. LANista on yhteys Internettiin. Kuviossa 9 on esitetty testiympäristö.



KUVIO 9. Testiympäristö.

Kuviossa 10 on testijärjestelmä ESXi:n näkökulmasta.



KUVIO 10. Kaaviokuva ESXi:n sisältämästä järjestelmästä.

Taulukoissa 5,6,7,8 ja 9 on esitetty IP-osoitevalinnat, joilla työ on toteutettu.

TAULUKKO 5. WAN IP-osoite määritykset.

IP-osoite	Käyttö
172.29.129.149	CARP jaettu IP
172.29.129.147	Ensisijainen palomuuri WAN IP
172.29.129.148	Toissijainen palomuuri WAN IP

TAULUKKO 6. LAN IP -osoite määritykset.

IP-osoite	Käyttö
192.168.1.1	CARP jaettu IP
192.168.1.2	Ensisijainen palomuuri LAN IP
192.168.1.3	Toissijainen palomuuri LAN IP

TAULUKKO 7. Pfsync IP -osoite määritykset.

IP-osoite	Käyttö
172.16.1.2	Ensisijainen palomuuri LAN IP
172.16.1.3	Toissijainen palomuuri LAN IP

TAULUKKO 8. DMZ-verkon IP-osoite määritykset.

IP-osoite	Käyttö
172.31.31.254	Ensisijainen palomuuri LAN IP
172.31.31.253	Toissijainen palomuuri LAN IP

TAULUKKO 9. Windows Server 2008 R2 -koneiden IP-osoitteet.

IP-osoite	Käyttö
172.31.31.10	Windows Server 2008 R2, kone 1
172.31.31.20	Windows Server 2008 R2, kone 2

4.1.1 ESXi 5.0:n asennus ja asetukset

Tässä työssä käyetyn tietokoneen tiedot:

- Intel ® Core ™2 Quad CPU Q6600 @ 2,40 Ghz
- Keskusmuisti 8192 MB

Asentamiseen tarvitaan ESXi:n levykuva, joka löytyy VMwaren verkkosivuilta. Käyttäjän rekisteröidyttyä VMwaren verkkosivuille levykuvan lataaminen on mahdollista. Levykuva poltetaan CD-ROM-levylle käyttämällä jotakin poltto-ohjelmaa tai Windowsin omaa poltto-ominaisuutta. Levykuvan polton jälkeen tietokone käynnistetään uudelleen CD-asemalta, jotta VMware ESXi:n asennus avautuu ESXi:n käynnistämisvalikkoon. Valikosta valitaan ESXi:n asentaminen, jolloin ohjelma lataa tarvittavat modulit ja prosessit. Tämän jälkeen alkaa varsinainen asennus.

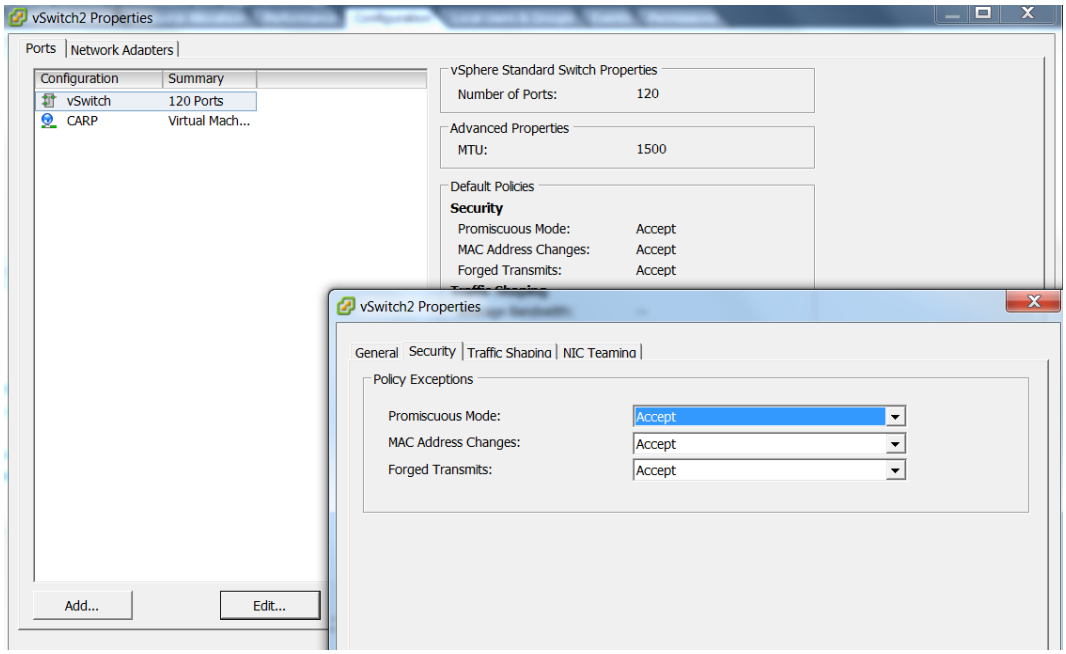
Sitten valitaan levy, jolle ESXi asennetaan. Asennuksen aikana valittu levy formatoidaan, jolloin kaikki levyllä oleva tieto katoaa. Asennuksen onnistuttua

käyttäjälle ilmoitetaan, että asennettu ESXi toimii 60 päivää ilmaisessa kokeilutilassa. Kokeiluajan päätyttyä tuote täytyy rekisteröidä VMwaren verkkosivuilta saatavalla lisenssiavaimella. ESXin etähallintaa varten tarvitaan VIClient. Paikallisesti ESXiä hallitaan DCUIn kautta, josta asetetaan myös perusasetukset. Asennus viimeistellään käynnistämällä tietokone uudelleen.

Tietokoneen uudelleen käynnistyksen jälkeen ESXi:tä voidaan hallita DCUI:lla. Etähallintaa varten täytyy ladata VIClient, joka löytyy kirjoittamalla ESXi:lle annettu IP-osoite web-selaimen osoitekenttään. Tältä web-sivulta voidaan ladata etähallintaohjelma VIClient.

Seuraavaksi asetetaan IP-osoite ja DNS-osoitteet sekä palvelimen käyttämä isäntänimi. Nämä tehdään DCUI:n kautta. Seuraavaksi käynnistetään VIClient ja kirjaudutaan sisään käyttäjänimen, salasanan ja IP-osoitteen avulla.

Virtuaalikytkimissä tulee kytkimen ominaisuuksissa turvallisuus-asetuksissa olla Promiscuous Modessa *Accept*. Tämä mahdollistaa pingauksen CARP-osoitteeseen. Kuviossa 11 on esitetty asetusten määrittäminen.



KUVIO 11. Promiscuous Mode.

4.1.2 PfSensen asennus

PfSensen asentamiseen tarvitaan asennusmedia, joka on ladattavissa pfSensen verkkosivuilta. Virtuaalikone käynnistetään ja CD asetetaan levyasemaan, joka on liitetty virtuaalikoneeseen. Tällöin pfSensen asennusohjelma käynnistyy. Asennusohjelmassa määritetään asennettujen verkkokorttien roolit, jotka tässä kokoonpanossa ovat LAN, WAN, DMZ ja CARP.

Liittymien määritysten jälkeen asennusohjelma etenee valikkoon, josta valitaan pfSensen asennus kovalevylle. Edetessään asennuohjelmassa voidaan valita pika-asennus, jolloin asennus etenee Kernelin valinta vaiheeseen. Valitaan Uniprocessor Kernel (UP), jota käytetään silloin, kun käytössä on yksi prosessori. Asennuksen ollessa valmis, käynnistetään vielä virtuaalikone uudelleen.

4.2 Palomuurin asetukset

Asennuksen jälkeen pfSense on valmis konfiguroitavaksi. Tämä tehdään käyttäen WebGUI:ta (web-pohjainen konfigurointikäyttöliittymä). WebGUI:hin liitytään erilliseltä työasemalta, joka on kytketty samaan kytkimeen palvelimen kanssa. Uuden pfSense systeemin LAN IP on 192.168.1.1 aliverkon peitteellä /24. Otetaan yhteys edellä mainittuun osoitteeseen web-selaimella, jolloin päästään sisäänkirjautumissivulle. Kirjaudutaan sisään käyttäjätunnuksella *admin* ja salasanalla *pfsense*, jolloin asennusvelho käynnistyy automaattisesti. Siirryttäessä seuraava-painikkeella eteenpäin, avautuu näyttö, jossa annetaan yleiset parametrit:

- Hostname = firewall_primary / firewall_secondary
- Domain = viitpaiv.local
- Primary DNS Server = voidaan asettaa, jos on tiedossa
- Secondary DNS Server = voidaan asettaa, jos on tiedossa

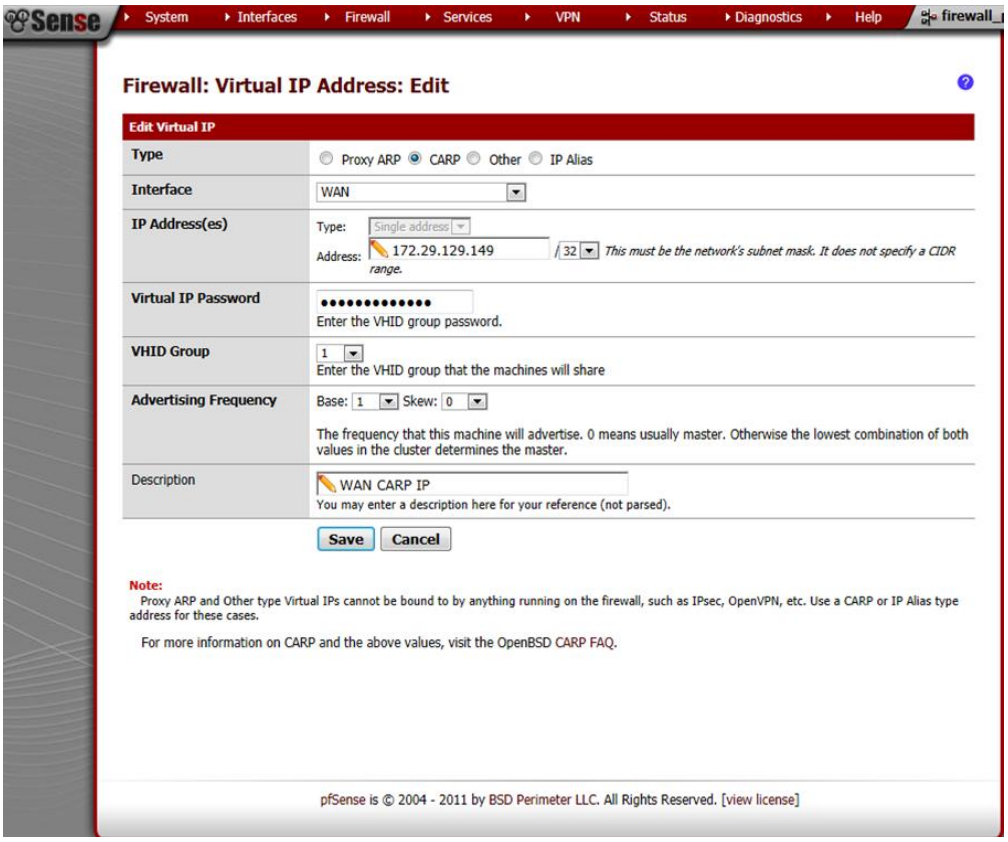
Seuraavaksi konfiguroidaan aikavyöhyke ja Network Time Protocol (NTP) palvelin. Tähän voidaan jättää oletuksena aikapalvelimen isäntänimi *0.pfsense.pool.ntp.org*, joka hakee satunnaisesti palvelimia poolista, jossa on ”hyviksi todettuja” NTP isäntiä. Aikavyöhyke valitaan pfSense systeemin sijainnin mukaan.

Aikavyöhykkeen ja NTP-palvelimen määritysten jälkeen valitaan WAN-tyyppi, joka tässä tapauksessa on staattinen. Mahdolliset vaihtoehdot ovat Staattinen, DHCP, PPPoE (Point-to-Point Protocol over Ethernet) ja PPTP (Point-to-Point Tunneling Protocol). MAC osoite-kenttä voidaan jättää tyhjäksi, kuten myös MTU-kenttä. Joissakin tapauksissa voidaan pienentää MTU-arvoa varmistamaan pakettien asianmukainen koko Internet-yhteydelle. Koska WAN:lle valittiin staattinen tyyppi, täytyy määrittää myös IP osoite, CIDR aliverkon peite ja oletusyhdyskäytävä. DHCP isäntänimen kenttä voidaan jättää tyhjäksi. Viimeiseksi aktivoidaan valinnat *Block RFC1918 Private Networks* ja *Block bogon networks*. Nämä valinnat estävät sekä rekisteröidyt privaatit verkot että liikenteen, joka on peräisin varatusta tai määräämättömästä IP avaruudesta.

Kun WAN-määritykset on tehty, jatketaan LAN-määrityksillä. Asetetaan IP-osoite (Taulukko 2) ja aliverkon peite. Seuraava askel on muuttaa admin salasana, jota käytetään sisäänkirjautuessa WebGUI:hin. Asennusvelho loppuu tähän. Painetaan vielä Reload-painiketta, jolloin WebGUI latautuu uudelleen ja muutokset astuvat voimaan.

4.2.1 CARP VIP ja pfsync

CARP Virtual IP:t määritetään valikossa *Firewall* → *Virtual IPs*, jossa klikataan lisää-painiketta, jolloin avautuu virtuaali IP:n muokkausruutu, joka on esitetty kuviossa 12.



KUVIO 12. Virtuaali IP:n määritys.

Virtuaali IP:n tyypiksi valitaan CARP ja liitynnäksi WAN. IP osoitteeksi asetetaan IP-osoite, joka on valittu aikaisemmin tähän tarkoitukseen. Tämä IP-osoite selviää taulukosta 1. Virtuaali IP:n salasana voi olla mikä tahansa, ja sitä ei tarvita tulevaisuudessa, koska se synkronoidaan automaattisesti toissijaiseen palomuuriin. Jokaisella CARP IP:llä palomuuriparissa täytyy olla ainutlaatuinen *VHID group* (Virtual Host ID). Sen täytyy olla eriävä muista aktiivisessa käytössä olevista VHID:eistä, jotka ovat mahdollisesti käytössä muissa palomuureissa samassa verkossa. VHID voidaan aloittaa numerolla 1. *Advertising Frequency* ensisijaisessa palomuurissa asetetaan arvoon 0. Toissijaisessa palomuurissa tämä arvo tulee olla 1 tai enemmän. *Description*-kenttään kirjoitetaan kuvaus ja lopuksi tallennetaan tiedot *Save*-painikkeella.

WAN CARP IP:n määrityksen jälkeen lisätään LAN CARP IP, jolloin tyypiksi asetetaan CARP ja liitynnäksi valitaan LAN. Jaetuksi LAN IP:ksi aseteaan aiemmin valittu IP, joka on esitetty taulukossa 2. *Virtual IP Password* on eri IP ryhmälle, joten sen ei tarvitse olla sama kuin WAN CARP IP:llä, eikä salasanaa tarvitse tietää milloinkaan myöhemmin. VHID arvon tulee olla eri kuin WAN CARP IP:llä. Tavallisesti VHID asetetaan yhtä numeroa isommaksi eli tässä

tapauksessa numeroksi 2. Myös tässä tapauksessa *Advertising Frequency* tulee olla 0. Kuvaukseksi voidaan kirjoittaa LAN CARP IP ja lopuksi tallennetaan asetukset. Tallennuksen jälkeen molemmat virtuaali IP:t näkyvät VIP-listassa ja samalla sivulla klikataan *Apply changes*-painiketta, jolloin molemmat CARP IP:t aktivoituvat.

Seuraava tehtävä on määrittää NAT siten, että verkon asiakkaat käyttävät jaettua WAN IP:tä. Valikosta *Firewall* valitaan *NAT* ja välilehti *Outbound*. Valitaan *Manual Outbound NAT* ja tallennetaan *Save*-painikkeella. Näytölle ilmestyy sääntö, joka NATtaa LAN liikenteen WAN IP:hen. Säädetään tätä sääntöä siten, että se toimii CARP IP:n kanssa. *Edit*-painikkeella päästään tilaan, jossa muutokset voidaan tehdä. *Translation*-osiossa valitaan WAN CARP IP-osoite alasvetovalikosta ja kuvaus-kenttään kirjoitetaan *NAT LAN to the WAN CARP*. Tallennuksen ja muutosten käyttöönoton jälkeen uudet yhteydet WAN:sta käännetään CARP IP:ksi. Tämä voidaan varmistaa esimerkiksi web-sivulla, joka näyttää IP osoitteen josta sivulle on päästy, esimerkiksi *http://www.pfsense.org/ip.php*.

NAT määritysten jälkeen konfiguroidaan *pfsync*-liittymä, joka tässä työssä on nimetty CARP:ksi. CARP-liittymä on kommunikointi linja ensisijaisen- ja toissijaisen palomuurin välillä. Valikossa mennään *Interfaces*-välilehdelle ja valitaan OPT1 ja aktivoidaan sekä nimetään liittymä. Asetetaan staattinen IP ensisijaiselle palomuurille. Tämä IP on aiemmin valittu ja esitetty taulukossa1. Lopuksi tallennetaan muutokset. Pfsync-liittymä tarvitsee myös palomuurisäännön, joka sallii liikenteen toissijaisesta palomuurista. Tämä tapahtuu valikon *Firewall* alla *Rules*-linkin takaa välilehdellä pfsync. Lisätään sääntö, joka sallii minkä tahansa protokollan liikenteen mistä tahansa lähteestä mihin tahansa kohteeseen.

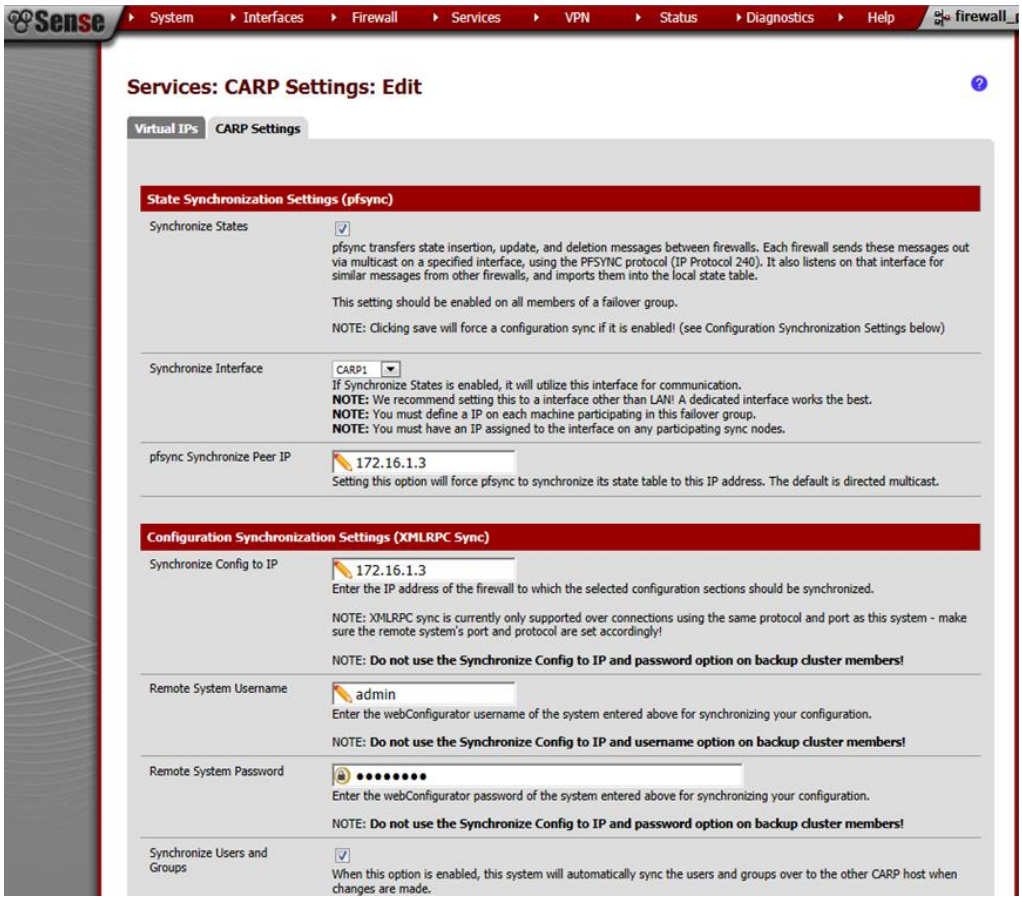
Koska pfSense toimii myös DHCP-palvelimena, täytyy oletusyhteyskäytäväksi määrittää CARP IP. Navigoidaan valikkoon *Services* → *DHCP Server* ja muutetaan *Gateway*-kenttään jaettu LAN CARP IP. Asetetaan *Failover Peer IP*:ksi toissijaisen palomuurin LAN IP. Tämä sallii DHCP palvelun ylläpitää molemissa palomuureissa yhteistä osoitteen liisaus ryhmää. Lopuksi tallennetaan

ja otetaan asetukset käyttöön. Nyt ensisijainen palomuuri on CARP:in osalta kunnossa ja aloitetaan toissijaisen palomuurin asetuksien säätäminen.

Kun toissijainen palomuuri on asennettu ja LAN IP määritetty, asetetaan DHCP-asetukset samoiksi, kuin ensisijaisessa palomuurissa. Kirjaudutaan WebGUI:hin ja käydään läpi asennusvelho. Määritetään WAN IP (Taulukko 1) ja admin salasana samaksi kuin ensisijaisessa palomuurissa. Lisäksi säädetään pfsync liittymän asetukset kuten ensisijaisessa palomuurissa ja valitaan IP-osoitteeksi toissijaiselle palomuurille valittu pfsync-liittymän IP, joka löytyy taulukosta 3. Tarvitaan vielä tilapäinen palomuurisääntö, joka sallii konfigurointi synkronoinnin tapahtua. Lisätään sääntö, joka sallii minkä tahansa protokollan liikenteen mistä tahansa lähteestä mihin tahansa kohteeseen. Lisätään kuvaukseen ”*temp*”, jotta myöhemmin voidaan tarkistaa, että sääntö on korvattu.

Viimeiseksi määritellään synkronointi ensisijaisen- ja toissijaisen palomuurin välillä. Ensisijaisessa palomuurissa navigoidaan *Firewall* → *Virtual IPs* ja valitaan *CARP settings*-välilehti. Aktivoidaan *Synchronize Enabled* ja valitaan CARP1 (pfsync) synkronointi liittymäksi. *Pfsync sync Peer IP*:ksi määritellään toissijaisen palomuurin pfsync-liitynnän IP-osoite taulukosta 3. Aktivoidaan kaikki loput sivulla olevat valintaruudut ja asetetaan toissijaisen palomuurin pfsync-liitynnän IP-osoite taulukosta 3 *Synchronize Config to IP*-kenttään. Lisäksi asetetaan WebGUI admin salasana *Remote System Password*-kenttään ja tallennetaan asetukset, jolloin ensisijaisesta palomuurista kopioidaan asetukset automaattisesti toissijaiseen palomuuriin. DHCP-palvelun asetukset eivät synkronoidu, joten navigoidaan valikkoon *Services* → *DHCP Server* ja muutetaan *Gateway*-kenttään jaettu LAN CARP IP. Asetetaan *Failover Peer IP*:ksi ensisijaisen palomuurin LAN IP. Kun asetukset synkronoituvat toissijaiseen palomuuriin, niin tiedetään, että sync-liittymä toimii niin kuin pitää. Synkronointiasetukset selviävät kuviosta 13.

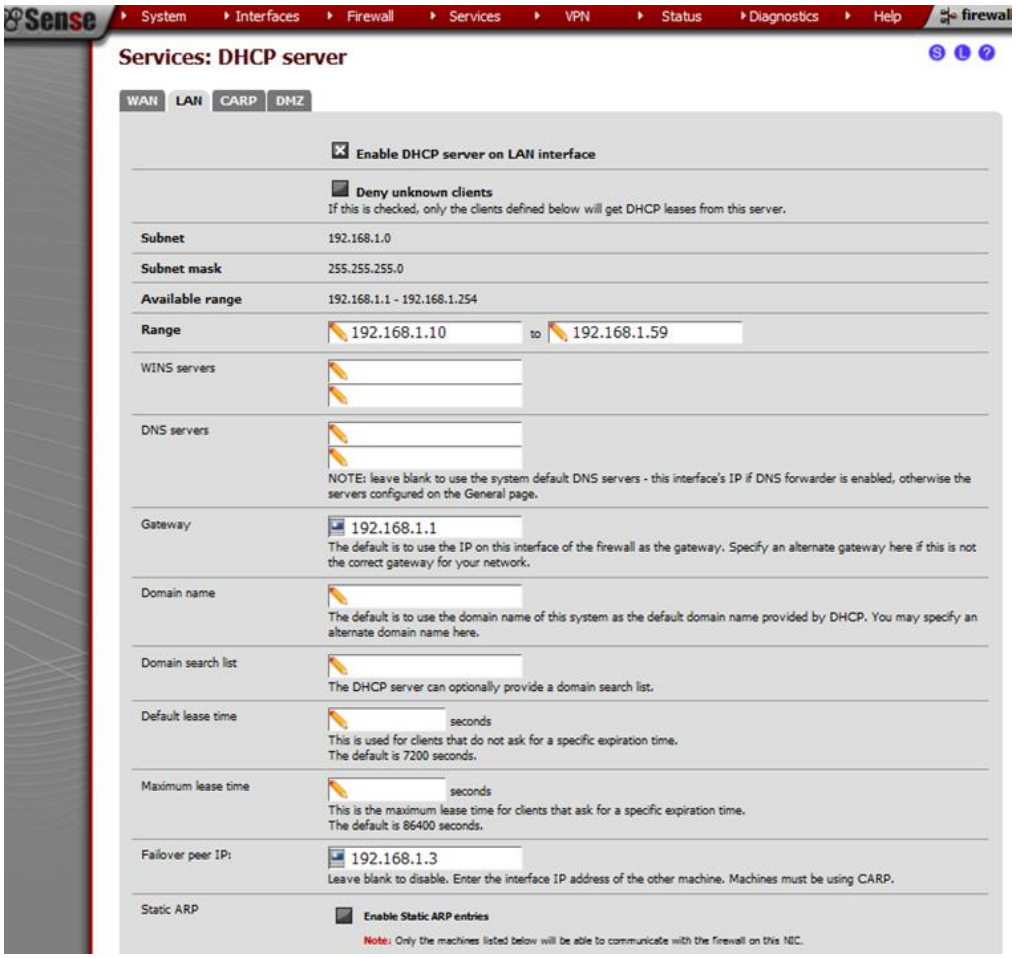
Vikasietoisuus testataan sammuttamalla ensisijainen palomuuri. Tällöin toissijainen palomuuri nousee masteriksi, kun CARP-määritykset ja synkronointiasetukset ovat oikein tehty.



KUVIO 13. Synkronointiasetukset.

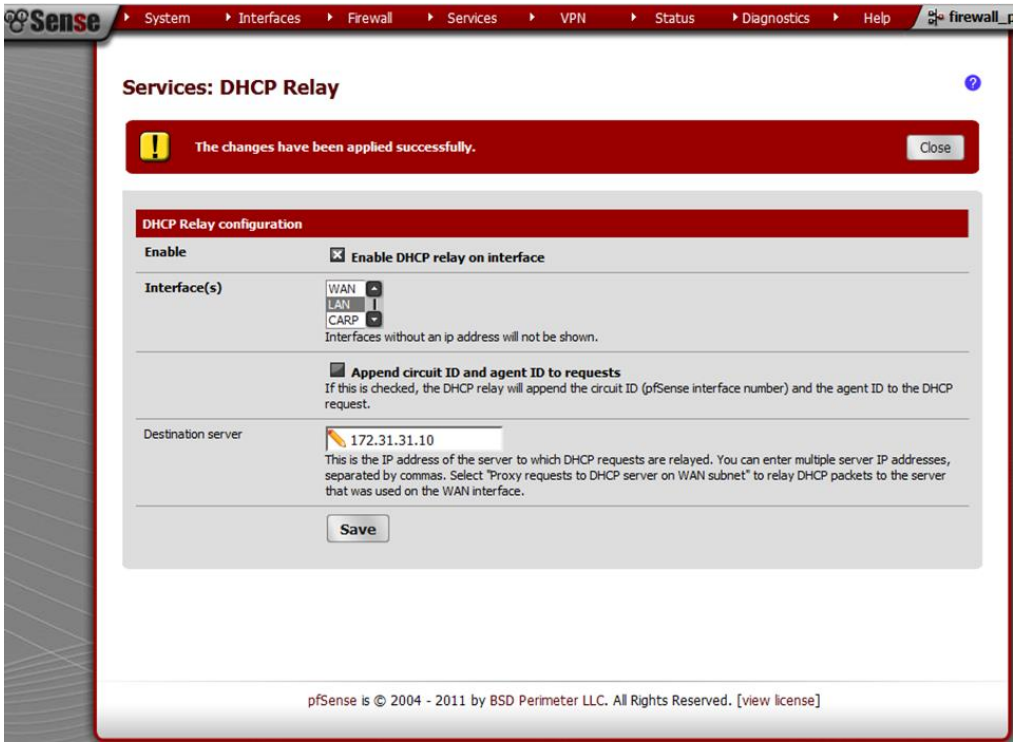
4.2.2 DHCP ja Relay

DHCP määritellään *Services*-valikon *DHCP Server*-linkin alla. Siirrytään *LAN*-välilehdelle ja aktivoidaan valinta: *Enable DHCP Server on LAN interface*. Määritetään kohdassa *Range* IP-osoiteväli, josta DHCP-palvelin jakaa IP-osoitteet. *Gateway*-kohtaan asetetaan IP-osoite, joka toimii oletusyhdyskäytävänä. *Failover Peer IP*:ksi asetetaan toissijaisen palomuurin LAN IP -osoite. Asetukset voidaan nähdä kuviossa 14.



KUVIO 14. DHCP-palvelun asetukset.

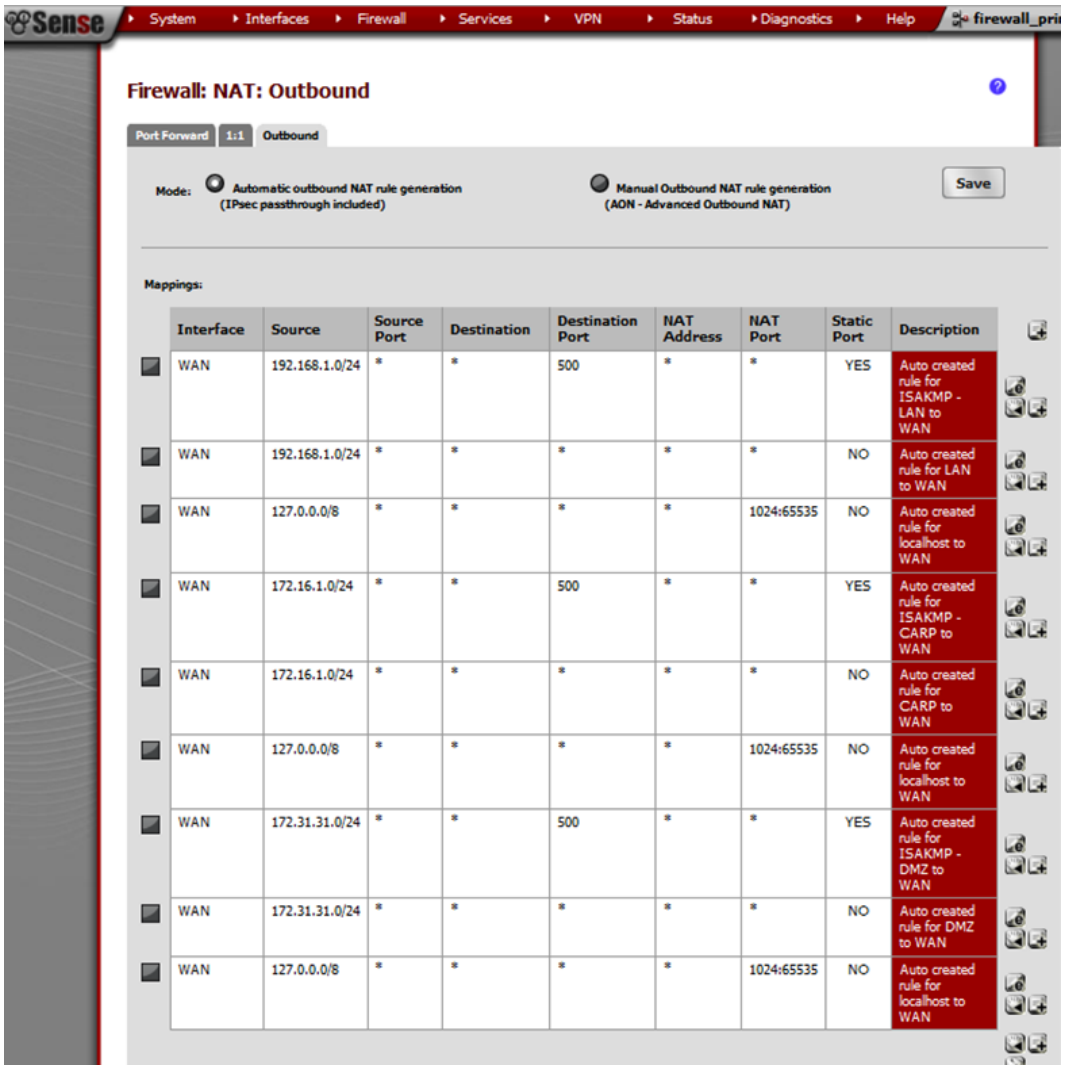
Toinen vaihtoehto on käyttää *DHCP Relay*:ta, jossa *DHCP Relay*:ta käytetään välittämään osoitepyynnöt määritetylle palvelimelle, joka on toisessa segmentissä, eli tässä tapauksessa DMZ-alueella. *Services*-valikosta valitaan *DHCP Relay* ja valitaan liityntä, jossa DHCP Relay:n halutaan toimivan. Tämän jälkeen aktivoidaan *Enable DHCP Relay*. Lisätään DHCP-palvelimen IP-osoite, johon IP-osoitepyynnöt lähetetään. DHCP Relay-määritykset näkyvät kuviossa 15.



KUVIO 15. DHCP Relay-asetukset.

4.2.3 NAT

PfSense generoi automaattisesti yleisimmin sopivimman NAT-konfiguraation. Kuviossa 16 on esitetty automaattisesti luodut NAT-määritykset testiympäristössä. Oletus NAT-konfiguraatio pfSensessä automaattisesti kääntää Internetiin menevän liikenteen WAN IP-osoitteeseen. Monen WAN-liitynnän ollessa kysessä, WAN:sta lähtevä liikenne käännetään automaattisesti WAN-liittymään, joka on käytössä.

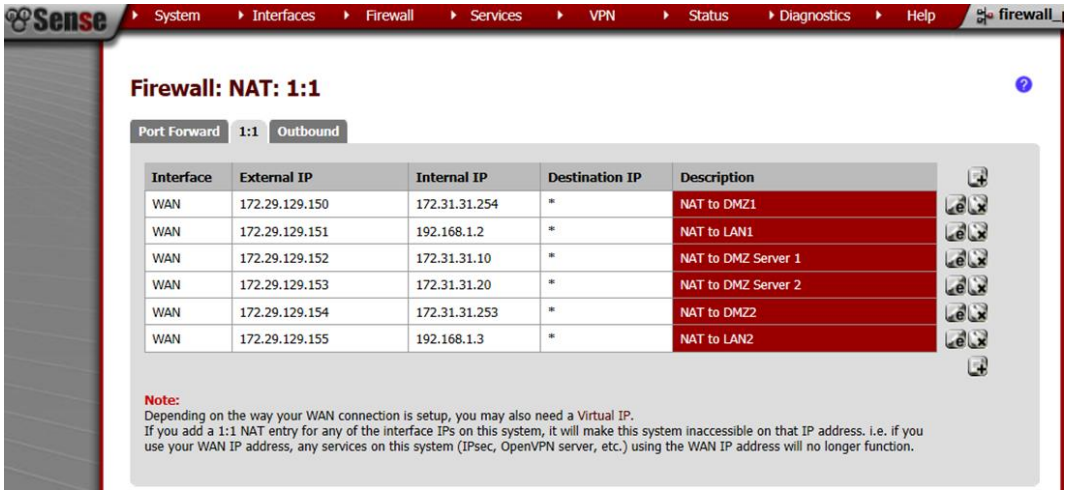


KUVIO 16. Oletuksena luodut automaattiset lähtevät NAT säännöt.

Oletuksena sisääntuleva liikenne Internetistä estetään. Jos halutaan, että liikenne Internetistä sisäverkon isännälle sallitaan, täytyy määrittää staattinen (1:1) NAT tai konfiguroida porttiohajus.

1:1 NAT kääntää yhden julkisen IP-osoiteen yhdeksi privaatiksi IP-osoitteeksi. Kaikki liikenne edellä mainitusta privaatista IP-osoitteesta Internetiin käännetään julkiseeen IP-osoitteeseen, joka on määritetty 1:1 NAT:ssa. Lähtevän(Outbound) NAT:in määritykset ylikirjoitetaan tässä tapauksessa. Internetistä lähtevä liikenne, joka päätyy määritettyyn julkiseen IP-osoitteeseen, käännetään privaatiksi IP-osoitteksi. Liikenne arvioidaan WAN palomuurisääntöjen perusteella ja jos palomuurisäännöt hyväksyvät liikenteen, niin liikenne päästetään sisäverkon isännälle. Kuviossa 17 on esitetty 1:1 NAT:n asetukset. Kuviossa External IP-

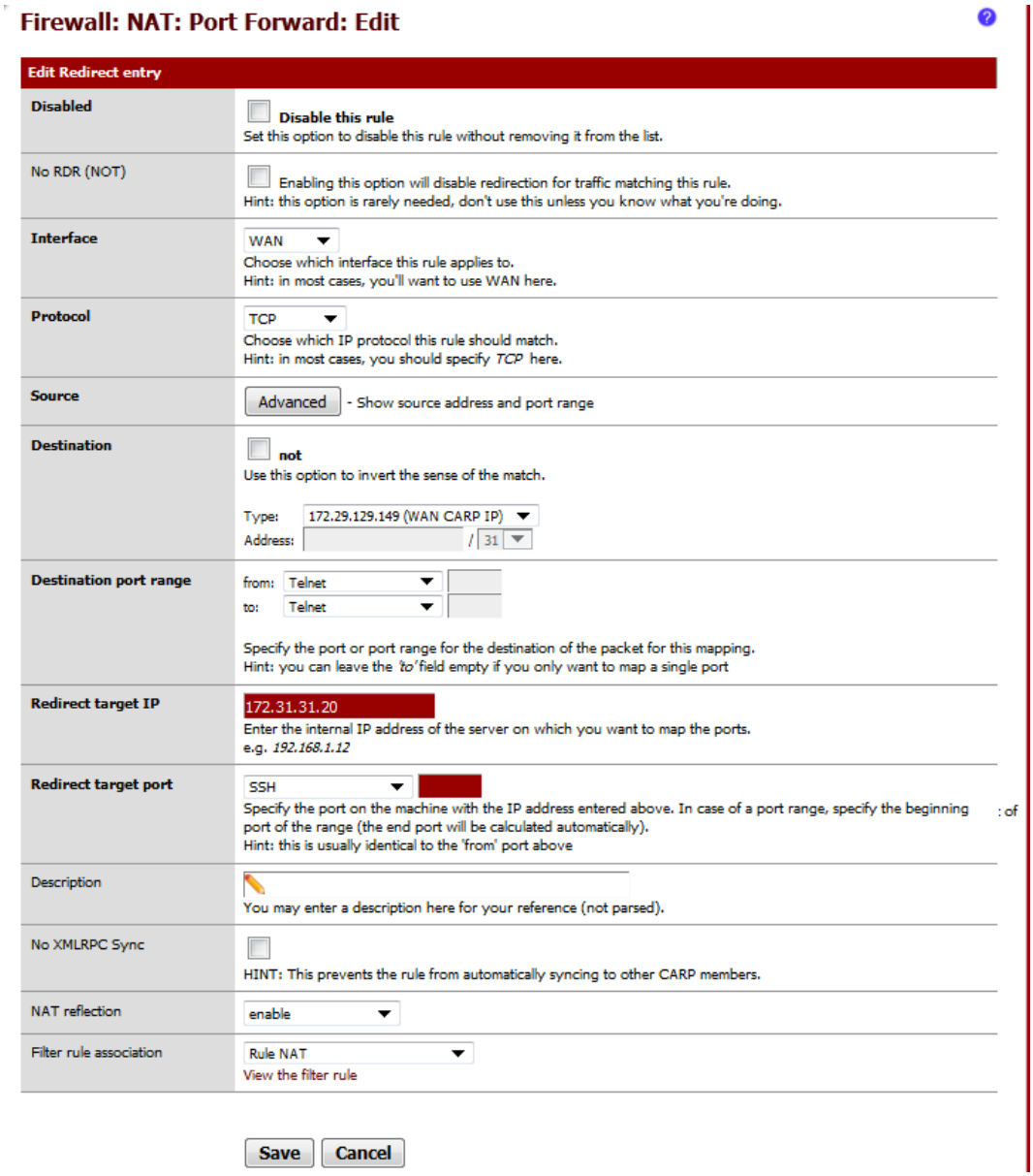
osoite on virtuaali IP, joka on määritetty vastaamaan jokaista sisäverkon liitynnän osoitetta. Näiden virtuaali IP-osoitteiden typpi on Proxy ARP (Address Resolution Protocol). Proxy ARP toimii OSI-mallin 2-kerroksella ja tarjoaa ARP vastauksia määritetylle IP-osoitteelle tai IP-osoitteiden CIDR-alueelle. Tämä sallii pfSensen välittää liikenteen, jonka kohde on määritetty sisäverkon osoite NAT-konfiguraatioiden mukaisesti. Julkisia lisä IP-osoitteita tulisi käyttää vain NAT tarkoituksiin, koska virtuaali IP, Proxy ARP, ei ole määrätty millekään liitynnälle pfSensessä. Tämän johdosta mikään palvelu pfSensessä ei voi vastata näihin IP-osoitteisiin.



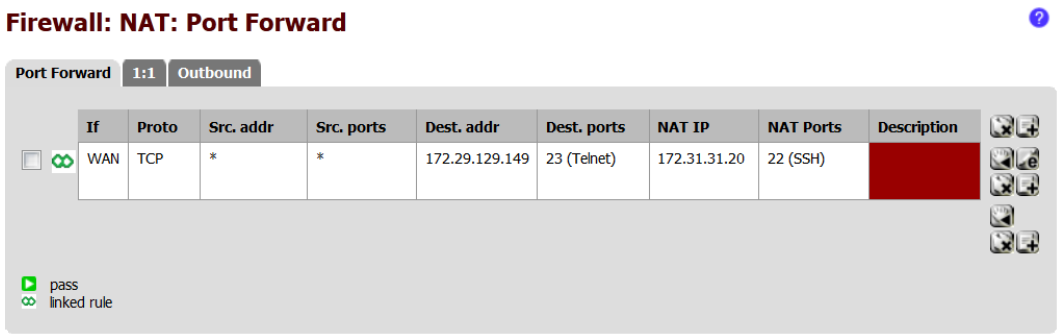
KUVIO 17. Sataattisen NAT:n asetuset.

1:1 NAT:n testaus toteutetaan siten, että asiakastietokoneeseen asetetaan IP-osoite 172.29.129.156 aliverkonpeitteellä 255.255.0.0 ja oletusyhdyskäytäväksi asetetaan 172.29.129.1. Selaimeen kirjoitetaan osoitteeksi https://172.29.129.151, joka on Proxy ARP-osoite. Tämä osoite vastaa ensisijaisen palomuurin LAN-osoitetta 192.168.1.2. Tuloksena aukeaa ensisijaisen palomuurin kirjautumissivu, joten voidaan sanoa, että 1:1 NAT toimii kuten suunniteltu. Ennen testausta on tehty tarvittavat palomuurisäännöt, joista enemmän seuraavassa kappaleessa.

Porttiohjaus määritykset tehdään kuvion 18 osoittamalla tavalla. Valikossa Firewall → NAT ja välilehdellä Port forward, voidaan tehdä porttiohjauksen asetukset. Kuviossa 19 voidaan nähdä, miltä valmis porttiohjaussääntö näyttää.



KUVIO 18. Kuviossa näkyy porttiohjauksen asetukset ja niiden muokkaustila.



KUVIO 19. Valmis porttiohjaussääntö.

Porttiohjaus testataan ottamalla SSH-yhteys Putty-ohjelmalla LAN-verkosta CARP-osoitteeseen 172.29.129.149 porttiin 23 (Telnet). Porttiohjaus muuttaa portin 23 portiksi 22 (SSH). Asiakaskoneen IP-osoite on DHCP:llä saatu osoite 192.168.1.11, aliverkonpeite on 255.255.255.0 ja oletusyhdyskäytävä on 192.168.1.1 testin aikana. Todetaan, että ensisijainen palomuuri on alhaalla ja toissijainen palomuuri on käytössä, sekä porttiohjaus toimii, koska näytölle avautuu sisäänkirjautumissivu.

4.2.4 Palomuurisäännöt

Taulukossa 1 on esitetty DMZ-verkkoon liittyvät palomuurisäännöt. WAN-liitynnässä Windows Server 2008 R2-koneisiin, ensi- ja toissijaiseen palomuuriin sekä DMZ-verkkoon sallitaan TCP-liikenne ja ICMP-kyselyt ja -vastaukset. LAN-liitynnässä sallitaan web-liikenne ja ssh-liikenne ulkoverkkoon.

Palomuurisääntö porttiohjausta varten on nähtävissä kuviosta 21. Säännössä sallitaan TCP-liikenne DMZ-verkon palvelimeen porttiin 22 (SSH).

KUVIO 21. Porttiohjauksen palomuurisääntö.

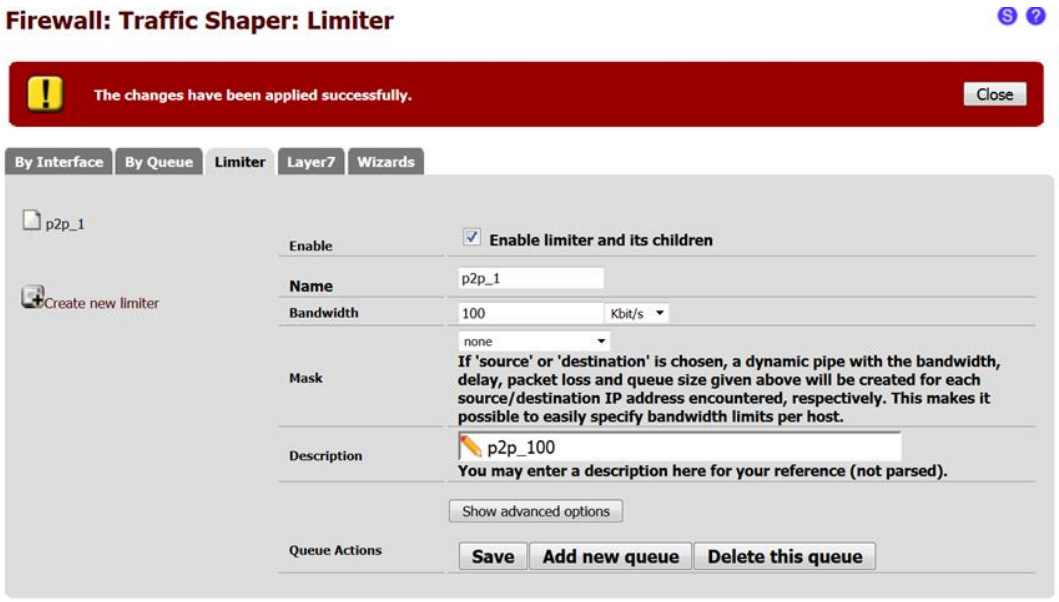
4.2.5 QoS / Traffic Shaper (Kaistanrajoitus)

QoS tai Traffic Shaper ovat työkalu liikenteen priorisointiin pfSensessä. Ilman priorisointia paketit käsitellään FIFO (first in/first out)-menetelmällä. QoS:n avulla voidaan laittaa erilaista liikennettä tärkeysjärjestykseen. Tällöin voidaan varmistaa tärkeimmän palvelun saavan tarvitsemansa kaistan ennen vähemmän tärkeää palvelua. PfSensessä on traffic shaper-velho, jonka avulla on nopeaa ja helppoa priorisoida liikennettä pfSense-palomuurissa.

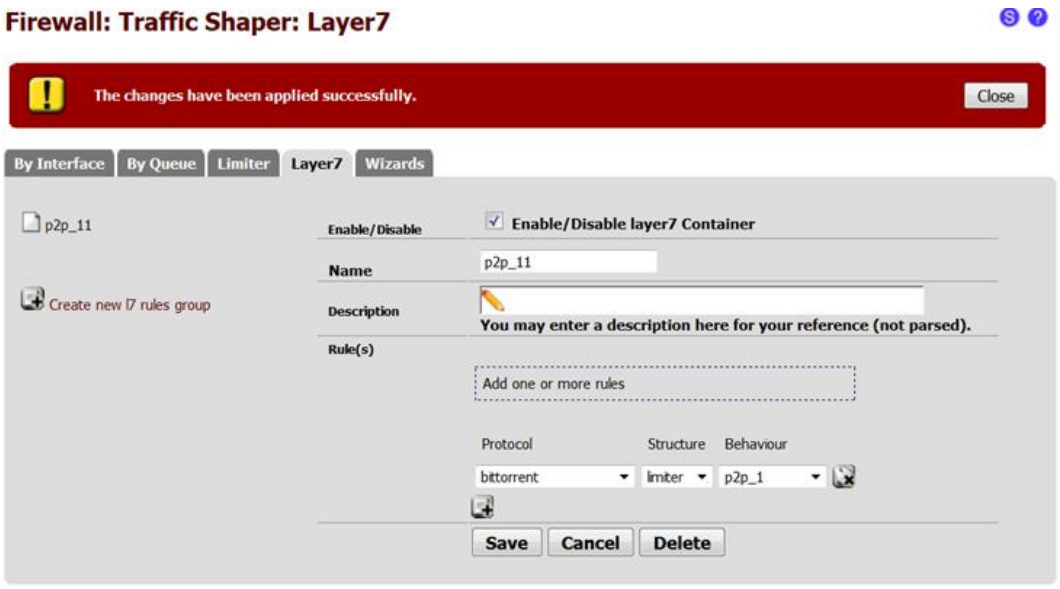
Velhossa voidaan asettaa WAN-liittymälle upload- ja download- nopeudet. Voice over IP (VoIP) -puheluliikenteelle on monia vaihtoehtoja käsitellä VoIP-liikennettä. Penalty Box (rangaistusaitio) ominaisuudella voidaan tietyn tietokoneen saamaa kaistaa säätää. P2P (peer-to-peer) protokollat vievät kaiken

kaistan, jos sitä ei rajoiteta. Verkkopelit tarvitsevat riittävän kaistan, jotta peli olisi nautinto. Joten sitäkin on velhon avulla helppo säätää. Lisäksi on mahdollista säätää jopa 25 erilaista muuta protokollaa, joille voidaan asettaa korkea-, matalampi- tai oletusprioriteetti.

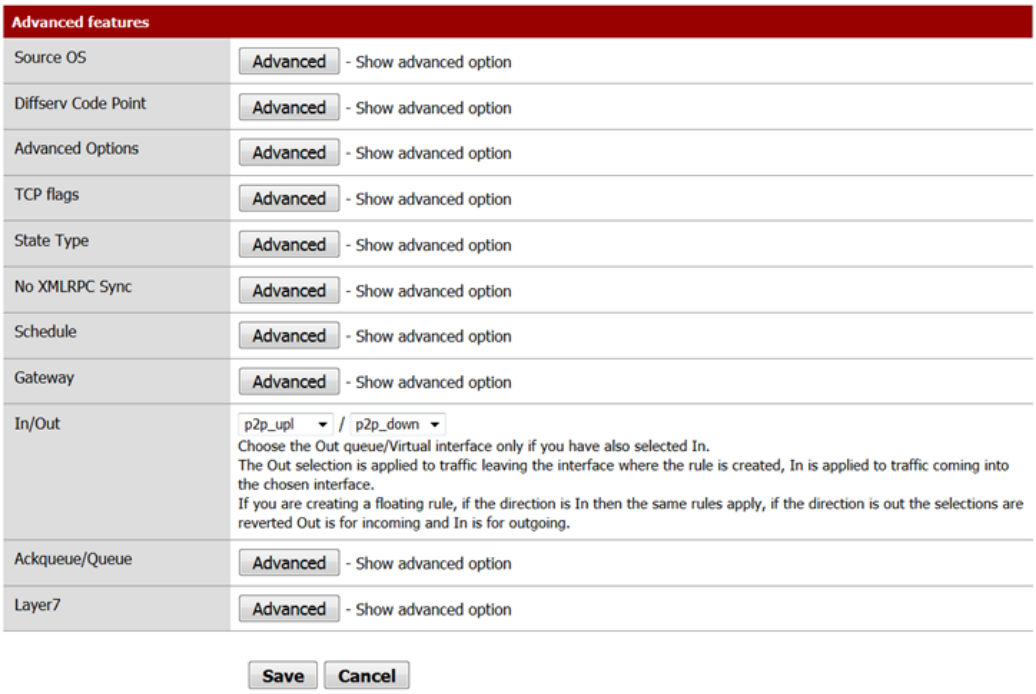
Kaistanrajoitustesti toteutetaan lataamalla P2P-ohjelmalla (peer to peer) tiedosto. Kaistanrajoitus konfiguroidaann Limiter:in avulla, joka löytyy Traffic shaperin alta. Limiteriin määritetään nopeus, joka halutaan asettaa P2P-liikennettä varten, tässä tapauksessa 100 Kbit sekunnissa. Limiter määritellään molemmille lataussuunnille. Tämän lisäksi määritetään Layer 7-välilehdellä sääntö kaistanrajoitukselle. Lopuksi limiter otetaan käyttöön ulkoverkosta sisäverkkoon sallivassa palomuurisäännössä. Tämä tehdään palomuurisäännön alalaidassa lisäasetuksissa kohdassa In/Out. Kuvioissa 22, 23 ja 24 näkyy kaistanrajoitusta varten määritellyt asetukset.



KUVIO 22. Limiter-asetukset.

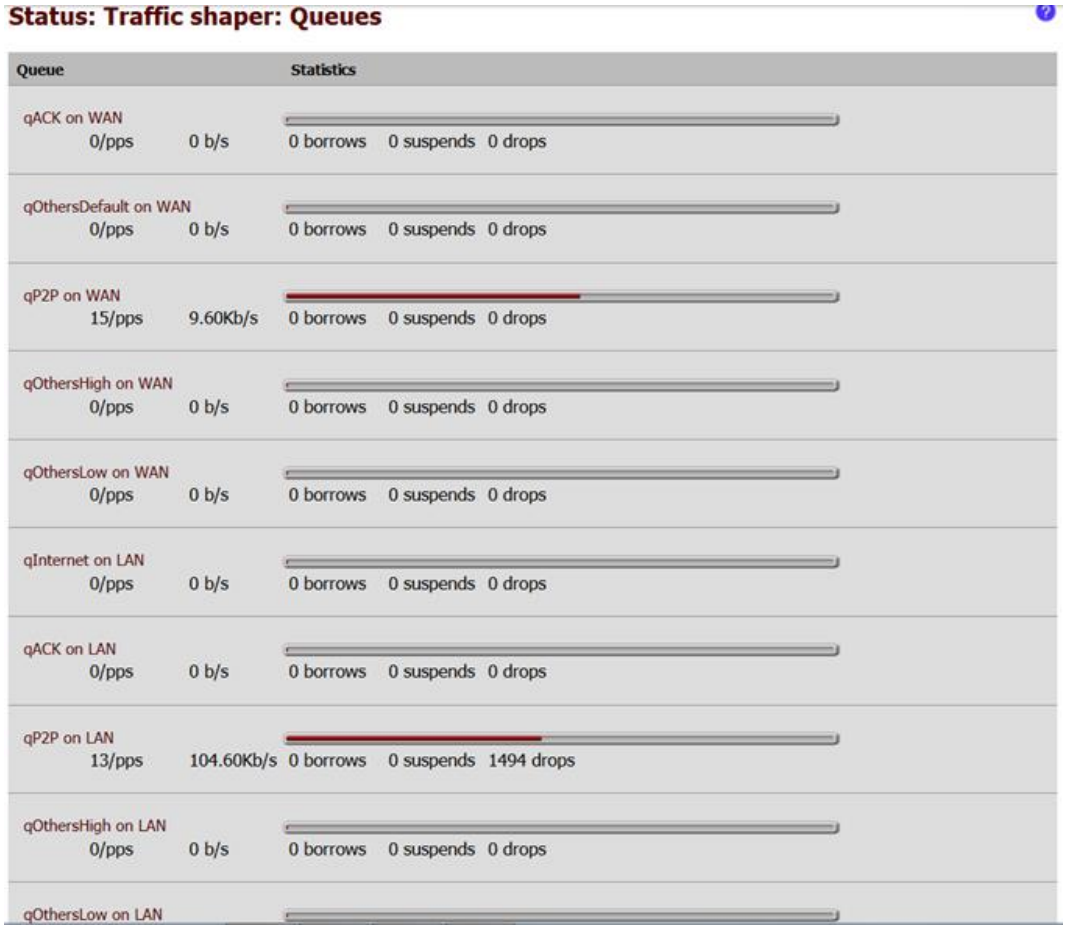


KUVIO 23. Säännön määritys kaistanrajoitusta varten.



KUVIO 24. Palomuurisäännön lisäasetukset.

Kaistanrajoituksen testaus on mahdollista valikossa Status → Queues, kuvio 25. Täällä voi nähdä jokaisen jonon listattuna nimeltä, jonon tämän hetkisen käytön ja joitakin muita jonoon liittyviä statistiikoita. Kuviosta voidaan todeta, että kaista on noin 100 Kbit sekunnissa, kuten kaistaa rajoitettiin.



KUVIO 25. Kaistanrajoitustestin tulos.

Jos huomaa, että velhon asettamat säännöt eivät ole juuri sitä, mitä tarvitaan, voidaan melko helposti muokata tai kopioida säännöt ja luoda itselle mukautettu sääntö. Tämä on mahdollista pfSensessä, jossa pääsee muokkaamaan jonoja. Se voi käytännössä olla monimutkaista.

5 YHTEENVETO

Tässä opinnäytetyössä toteutettiin vikasietoinen palomuuri pfSense-ohjelmistolla. Palomuuri tekee NAT:in ja DHCP-palvelin jakaa IP-osoitteet laitteille. Lisäksi rajoitettiin P2P-liikennettä.

Tietoliikkenne kulkee paketteina verkosssa. Palomuuri voi estää tietystä IP-osoitteesta tulevan paketin. Sen lisäksi palomuuri kontrolloi, mihin paketteja päästetään. Palomuurin päätehtävä on siis suodattaa läpi kulkevaa liikennnettä. Perusedellytys on, että kaikki sisä- ja ulkoverkon välinen liikenne kulkee palomuurin läpi.

Palomuureissa on lukuisia ominaisuuksia, joita voidaan hyödyntää verkossa. DHCP helpottaa verkkoasetusten manuaalista konfigurointia ja NAT sekä lisää verkon turvallisuutta että vähentää IP-osoitteiden tarvetta. QoS:in avulla voidaan priorisoida liikennettä. Priorisoitu liikenne lähetetään ennen muuta liikennettä. Esimerkiksi toiminnallisten syiden perusteella lähiverkko voidaan jakaa loogisiin käyttäjäryhmiin. VLANin avulla nämä ryhmät voidaan pitää erillisissä verkoissa. VPN on liikenteen tunneliointia pisteestä A pisteeseen B. VPN sisältää kapseloidun, salatun ja autentikoidun yhteyden jaetun tai julkisen verkon läpi. Vikasieto-ominaisuus on nykyisin tarjolla monilla palomuureilla. Tämä ominaisuus mahdollistaa kahden palomuurin yhdistäminen pariksi, jossa toinen laite on heti käyttövalmiina toisen vikaantuessa. PfSensessä tämä on toteutettu CARP:in avulla.

Tässä opnnäytetyössä vertailtiin pfSense-ohjelmistoa ja SmoothWall Express-ohjelmistoa sekä Vyatta-ohjelmistoa. SmoothWall Express-ohjelmisto ei sisällä vikasieto-ominaisuutta, joka on suuri puute tämän päivän palomuuriohjelmistoissa. Suuri osa nykypäivän palomuureista sisältää vikasieto-ominaisuuden. Lisäksi SmoothWall Expressissä ei ole mahdollista tehdä staattista NAT:a. Uloslähtevän liikenteen kontrollointi on myös rajoitettua. Vyatan ilmaisversiossa ei ole käytössä WebGUI:ta, joten sen konfiguroiminen on työlästä.

Tässä opinnäytetyössä testiympäristö rakentui virtuaaliympäristöön, jossa palvelimena toimi ESXi 5.0-palvelin. ESXi sisältää kaksi pfSensellä varustettua

virtuaalikonetta ja kaksi DMZ-verkossa toimivaa Windows Server 2008 R2 -virtuaalikonetta. Palomuuripari on vikasietoinen ja tekee NATin sekä DHCP-palvelin jakaa IP-osoitteet laitteille. Limiterillä rajoitettiin P2P-liikenteen saamaa kaistaa.

Palomuuri on tärkein tapa suojautua verkon uhkia vastaan. Ne ovat monien yritysten tietoturvajärjestelyiden tuki ja turva. Sitä voidaan verrata linnakkeen muuriin, joka torjuu ulkopuolelta tulevat hyökkäykset. Ovella portinvartija tietää ketä voidaan laskea sisään ja kuka tulee jättää ulkopuolelle. Palomuurin ansiosta yrityksen verkko voidaan suojata ei halutuilta tunkeutujilta.

LÄHTEET

Almgren, A. 2012. Linux työ, Palomuuri [viitattu 24.3.2012]. Lut. Saatavissa: www2.it.lut.fi/kurssit/04-05/010626000/Palomuuri-Antti_Almgren-raportti.doc

Buechler, C.M, Pingle, J. 2009. pfSense: The Definitive Guide. Reed Media Services.

BSD Perimeter LLC. 2013a. History [viitattu 23.2.2013]. BSD Perimeter LLC. Saatavissa: http://www.pfsense.org/index.php?option=com_content&task=view&id=68&Itemid=76

BSD Perimeter LLC. 2013b. Minimum Hardware Requirements [viitattu 23.2.2013]. BSD Perimeter LLC. Saatavissa: http://www.pfsense.org/index.php?option=com_content&task=view&id=45&Itemid=48

BSD Perimeter LLC. 2013c. Features [viitattu 23.2.2013]. BSD Perimeter LLC. Saatavissa: http://www.pfsense.org/index.php?option=com_content&task=view&id=40&Itemid=43

Cisco. 2011. How NAT works [viitattu 25.3.2012]. Cisco. Saatavissa: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml

Droms, R. 1997. Dynamic Host Configuration Protocol [viitattu 24.3.2012]. Bucknell University. Saatavissa: http://www.ietf.org/rfc/rfc2131.txt

Fitzroy, S. 2009. Class Topics and Reading Assignments [viitattu 23.1.2013]. Fitzroy. Saatavissa: http://neia.seanfitzroy.com/csi110/resources/OSI-internet_model.gif

Northrup, T. 2013. Firewalls [viitattu 24.2.2013]. Microsoft. Saatavissa: http://technet.microsoft.com/en-us/library/cc700820.aspx

Oulun kauppaoppilaitos. 2004. Tietoturvajärjestelmät [viitattu 24.3.2012]. Oulun kauppaoppilaitos. Saatavissa: http://www.okol.org/verkkokurssit/datanomi/tietojarjestelmien_kehittaminen/tietoturvajarjestelmat/palomuurit/palomuurit.htm

Pesonen, L. 2005. DHCP [viitattu 24.3.2012]. Lut. Saatavissa: http://www2.it.lut.fi/kurssit/04-05/010626000/linux-tyot/DHCP-Lasse_Pesonen-raportti.pdf

Smoothwall. 2012a. About [viitattu 24.2.2013]. Smoothwall. Saatavissa: http://www.smoothwall.org/about/

Smoothwall. 2012b. Feature Comparison Chart [viitattu 24.2.2013]. Smoothwall. Saatavissa: http://www.smoothwall.org/about/feature-comparison-chart/

Smoothwall Limited. 2007. Smoothwall Express Administrator's Guide [viitattu 24.2.2013]. Smoothwall Limited. Saatavissa: http://www.smoothwall.org/download/

Tallinnan Yliopisto. 2012a. VLAN-perusteet [viitattu 25.3.2012]. Tlu. Saatavissa: http://www.tlu.ee/~matsak/telecom/lasse/switch2/vlanperusteet.html

Tallinnan Yliopisto. 2012b. VLAN-merkintä [viitattu 30.1.2013] Tlu. Saatavissa: http://www.tlu.ee/~matsak/telecom/lasse/switch2/vlanmerkint.html

Vyatta. 2013. Vyatta Network OS Datasheet [24.2.2013]. Vyatta. Saatavissa: http://www.vyatta.com/sites/vyatta.com/files/pdfs/vyatta_software_datasheet.pdf

Vyatta Inc. 2012a. Vyatta System Firewall [24.2.2013]. Vyatta Inc. Saatavissa: http://www.vyatta.com/download/documentation

Vyatta Inc. 2012b. Vyatta System NAT [viitattu 24.2.2013]. Vyatta Inc. Saatavissa: http://www.vyatta.com/downloads/documentation/VC6.5/Vyatta-NAT_6.5R1_v01.pdf

Wikipedia. 2012. Palomuuri [viitattu 25.3.2012]. Wikipedia. Saatavissa: http://fi.wikipedia.org/wiki/Palomuuri

Wikipedia. 2013a. Firewall (computing) [viitattu 23.2.2013]. Wikipedia. Saatavissa: http://en.wikipedia.org/wiki/Firewall_(computing)

Wikipedia. 2013b. Vyatta [viitattu 24.2.2013]. Wikipedia. Saatavissa: http://en.wikipedia.org/wiki/Vyatta