TAMPEREEN
AMMATTIKORKEAKOULU

Aktiivisen IPCop-palomuurin yliheitto

Ilkka Pakkanen

Opinnäytetyö
Joulukuu 2015
Tietojenkäsittely
Tietoverkkopalvelut

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely
Tietoverkkopalvelut

PAKKANEN, ILKKA:
Aktiivisen IPCop-palomuurin yliheitto

Opinnäytetyö 35 sivua
Joulukuu 2015

Opinnäytetyön tarkoituksena oli päivittää Terasoft Oy:n vanha IPCop-palomuuri uuteen versioon ja ottaa se käyttöön uudella palvelinkoneella. Samalla palomuurin tietoturvaa pyrittiin parantamaan ottamalla käyttöön lisäosia, jotka tarkastelevat palomuurin läpi kulkevaa tietoliikennettä. Tavoitteena oli tehdä palomuurin yliheitto vanhalta työasemalta uudelle palvelinkoneelle mahdollisimman pienellä käyttökatkoksella vaarantamatta yrityksen toimintaa. Uusi palomuuri konfiguroitiin käyttäen sisäverkon työasemaa, johon voitiin muodostaa etäyhteys. Yliheitto suoritettiin noudattamalla ennalta laadittuja suunnitelmia.

Palomuurin yliheitto onnistui, ja se otettiin käyttöön ensimmäisellä yrityksellä. Uudella palomuurilla on käytössä vanhalta palomuurilta vain aktiivisessa käytössä olevat osoitteiden- ja porttien muunnokset. Käytöstä poistuneet muunnokset kartoitettiin Terasoft Oy:n yhteistyökumppaneilta ennen palomuurin konfiguroimista. Uudelle palomuurille asennettiin myös Copfilter-lisäosapaketti, joka tarkkailee liikennettä myös OSI-mallin sovelluskerroksella. Copfilterin avulla palomuurin tietoturvaa voitiin kasvattaa normaalia tilallista palomuuria paremmaksi. Terasoft Oy oli tyytyväinen projektiin. Uusi palomuuri tarkkailee liikennettä paremmin kuin vanha palomuuri, ja työ saatiin tehtyä sovitun aikataulun mukaisesti.

Tulevaisuudessa Terasoft Oy:n kannattaa tarkkailla eri Linux-palomuurien kehitystä ja harkita, onko IPCop-palomuurin päivittäminen jatkossa kannattavaa vai pitäisikö ohjelmisto vaihtaa kokonaan toiseen. Työtä tehdessä kävi ilmi, että IPCopin suosio ja kehitys on ollut aktiivisempaa projektin alkuaikoina kuin viimeisten vuosien aikana. Tällä hetkellä IPCop on kuitenkin toimiva palomuuriohjelmisto.

Asiasanat: IPCop, palomuuri, yliheitto

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Network Services

PAKKANEN, ILKKA:
Migration of an Active IPCop Firewall

Bachelor's thesis 35 pages
December 2015

The purpose of this thesis was to update the IPCop firewall of Terasoft Oy to a newer version, and deploy it on a new server. The firewall's security was also aimed to be improved by introducing add-ons that would monitor the traffic that flows through the firewall. The main objective of the project was to carry out the live migration with minimal downtime and without compromising the company's data. The migration and configuration was done using a remote desktop that is in the same subnet with the firewall.

The migration of the firewall was successful and the new firewall was deployed on the first attempt. The new firewall only uses the port forwards that were in active use on the old firewall. Copfilter add-on package was installed on the firewall. It allows the firewall to scan the packets on the application layer of the OSI-model. With the help of Copfilter, the new firewall has better overall security than an average stateful firewall. Terasoft Oy was pleased with the success of the project. The new firewall monitors the traffic more profoundly than the old one, and the whole project was completed in the agreed time frame.

In the future, Terasoft Oy should follow and observe the development of different Linux-based firewalls and consider if updating IPCop is still worthwhile, or whether the whole firewall be replaced with a more promising alternative. During the project it appeared as if the development of IPCop used to be more active in its early years than lately. However, in its current state, IPCop is still a worthy firewall.

Key words: IPCop, firewall, migration

SISÄLLYS

LYHENTEET JA TERMIT

ACK-paketti	Kahden laitteen välillä kulkeva paketti tiedon kuittaamiseen
Active Directory	Microsoft Windowsin käyttäjäkanta ja hakemistopalvelu
DMZ	Demilitarisoitu alue, fyysinen tai looginen aliverkko, joka on yhteydessä epäluotettavaan verkkoon
FTP	File Transfer Protocol, TCP-protokollaa käyttävä tiedonsiirtomenetelmä
ICMP	Internet Control Message Protocol, virheviestien välitykseen käytettävä protokolla verkossa olevien laitteiden välillä
IM	Instant Messaging, pikaviestintä
IP Spoofing	IP-paketti, jonka lähdetietoja on manipuloitu esittämään toista laitetta
lippu	Flag, kertoo TCP-paketissa sen sisällöstä ja määrittelee paketin tarkoituksen
NAT	Network Address Translation, muuntaa osoitteen sisä- ja ulkoverkon välillä
NTP	Network Time Protocol, UDP-pohjainen protokolla aikatiedon välittämiseen
OSI-malli	Open Systems Interconnection Reference Model, tiedonsiirtoprotokollien toimintaa kuvaava seitsenkerroksinen malli
proxy	Välityspalvelin, varastoi väliaikaisesti tietoa suodatus- ja tarkastustoimenpiteenä
SYN flood	Hyökkäysmenetelmä, jossa hyökkääjä kuormittaa palvelinta lähettämällä useita SYN-pyyntöjä lyhyen ajan sisään
UPS-laite	Uninterruptible Power Supply, virransyöttölaite, joka toimii yleensä laitteen ja sen virtalähteen välissä
URL-filter	Uniform Resource Locator, sallittujen verkkosivujen suodattamiseen käytettävä palvelu
VPN	Virtual Private Network, näennäisesti yksityisen verkon luominen julkisen verkon yli.

1 JOHDANTO

Tässä opinnäytetyössä yrityksen aktiivisen IPCop-palomuurin palvelut siirretään vanhasta versiosta uuteen, eli palomuurille suoritetaan yliheitto. Palomuurin uusi versio otetaan käyttöön uudella palvelinkoneella, koska sen toiminta vaatii enemmän suorituskykyä kuin vanha versio. Palomuuri on tietoverkon turvallisuuden kulmakivi, joka täytyy pitää päivitettynä vastaamaan nykyaikaisia tietoturvauhkia (Dempster & Eaton-Lee 2006, 48-49).

Työ on toteutettu Terasoft Oy:lle, joka on palvelin- ja laitetilaa tarjoava tietotekniikkayritys. Työn toimeksiantajana toimii Wild Software Oy. Tärkeää palomuurin yliheitossa on sen tapahtuminen lyhyellä käyttökatkolla, jotta toiminta ei katkeaisi pitkäksi ajaksi. Yrityksen verkko ei saa altistua hyökkäyksille yliheiton missään vaiheessa.

Työn tekemiseen on käytetty konstruktiivisen tutkimuksen toimintamallia. Terasoft Oy:n esittämät vaatimukset lopputuloksesta toimivat pohjana työlle, jonka perusteella palomuuri konfiguroitiin. Työssä palomuurille luotiin portti- ja osoitemuunnoksia, jotka mahdollistavat Terasoft Oy:n asiakkaiden pääsyn heille kuuluviin palveluihin tietoturvallisesti. Palomuurin tietoturvaa haluttiin myös parantaa tutkimalla mahdollisten lisäosien käyttöönottoa.

Lopputuloksena uudelle palomuurille luotiin vanhalla palomuurilla aktiivisessa käytössä olleet portti- ja osoitemuunnokset. Palomuurin turvallisuutta voitiin myös parantaa ottamalla käyttöön Copfilter-lisäosapaketti, minkä avulla palomuurin läpi kulkevien pakettien sisältöä voidaan tutkia mahdollisten hyökkäysyritysten varalta. Sekä toimeksiantaja, että Terasoft Oy olivat tyytyväisiä projektiin ja sen lopputulokseen. Palomuurina toimiva palvelinkone on suorituskyvyltään edeltäjäänsä tehokkaampi. Palomuuri on myös lisäosiensa ansiosta responsiivisempi mahdollisten uhkien varalta.

Tärkeimpänä lähteenä toimii IPCopin oma dokumentaatio, sekä palomuureista kertova kirjallisuus. Vaikka ICT-alalla tapahtuu jatkuvaa muutosta, vanhemmasta kirjallisuudessa voitiin hyödyntää tietoverkkojen ja palomuurien toiminnan perusteita. Verkkojulkaisuja hyödyntäessä niiden sisältämää tietoa vertailtiin IPCopin dokumentaatioon, jonka avulla tiedon luotettavuutta voitiin arvioida.

2 PALOMUURIT

2.1 Palomuurien perusteita

Tietoturvaa ei osattu arvostaa kunnolla, ennen kuin ensimmäinen haittaohjelma, Morris-mato, pääsi leviämään Massachusettsin teknillisestä korkeakoulusta. Vuonna 1988 Robert Tappan Morris halusi todistaa verkon haavoittuvuuden, ja ohjelmoi maailman ensimmäisen madon. (Seeley 1989.) Tämä herätti ihmiset tietoturvan tärkeyteen ja näytti kuinka helposti ja nopeasti yksi mato voi kaataa tärkeitä verkkoja. Vuonna 1989 Jeff Mogul esitteli ratkaisun jonka avulla paketteja voidaan suodattaa, ja päättää saavatko ne kulkea läpi vai ei (Ingham & Forrest 2002). Pakettien suodatus tehtiin lisäämällä reitittimeen sääntöjä, joihin paketin lähdettä ja kohdetta voitiin vertailla. Tämä oli ensimmäinen askel moderneille palomuureille.

Palomuuri tarkoittaa seinää, joka erittelee kaksi aluetta ja suojaa niitä tulipalon leviämiseltä. Tietotekniikassa käsite on hieman monimutkaisempi, mutta sen toiminnan periaate on kuitenkin sama. Tulipalon sijaan palomuuri estää haittaohjelmien pääsemisen ulkoverkosta sisäverkkoon.

Forrester Researchin (2014) teettämän tutkimuksen mukaan jopa 67% yrityksissä tapahtuneista tietomurroista on tullut yrityksen oman verkon sisältä, eikä ulkoverkosta. Näissä tapauksissa haittaohjelmat ovat voineet kulkea yritysverkkoon esimerkiksi käyttäjien omien laitteiden mukana, jotka ovat saastuneet työpaikan ulkopuolella. Pakettien suodattaminen verkkojen välillä ei siis riitä suojaamaan yritysverkkoa, vaan sisäverkkoa täytyy monitoroida aktiivisesti käyttäen muitakin ohjelmistoja, kuten tunkeilijan havaitsemisjärjestelmää ja virustorjuntaa. Palomuuri on kuitenkin tietoturvan kulmakivi, ja pakollinen osa jokaista tietoverkkoa.

2.2 Erilaiset palomuurit

Erilaisia palomuurityyppejä on paljon ja niitä on joskus vaikea luokitella eri kategorioihin. Yleisiä palomuurityyppejä ovat esimerkiksi pakettisuodatin-, tilalliset ja sovelluspalomuurit (proxy-palomuurit). Sovelluspalomuuri hyödyntää käyttäjän tunnistusta, ja useissa tapauksissa myös pakettien tutkimista. (Stewart 2010, 223-225.)

Hyvä näkökulma palomuurien luokitteluun on tarkastelemalla niiden toimintaa OSI-mallissa. Pakettisuodatinpalomuuri toimii OSI-mallin kolmannella ja neljännellä kerroksella, ja tilallinen palomuuri toimii näiden lisäksi myös viidennellä kerroksella. Sovelluspalomuuri toimii tilallisen palomuurin kerroksien lisäksi myös seitsemännellä, eli sovelluskerroksella. Yleisesti ajatellen palomuuri on sitä parempi mitä useammalla tasolla se toimii. (Magalhaes 2008.) OSI-mallin sovelluskerroksessa toimiminen mahdollistaa uusia tapoja suojata liikennettä hyödyntäen samalla alempien tasojen tekniikoita. Palomuurin valinnassa on monta tekijää joiden perusteella itselle sopiva palomuuri valikoituu. Tekijöitä ovat esimerkiksi liikenteen ja käyttäjien määrä, yrityksen käyttämät sovellukset, koko ja käytössä olevat resurssit. Työssä oletetaan, että lukija tuntee OSI-mallin kerrokset ja niiden sisällön.

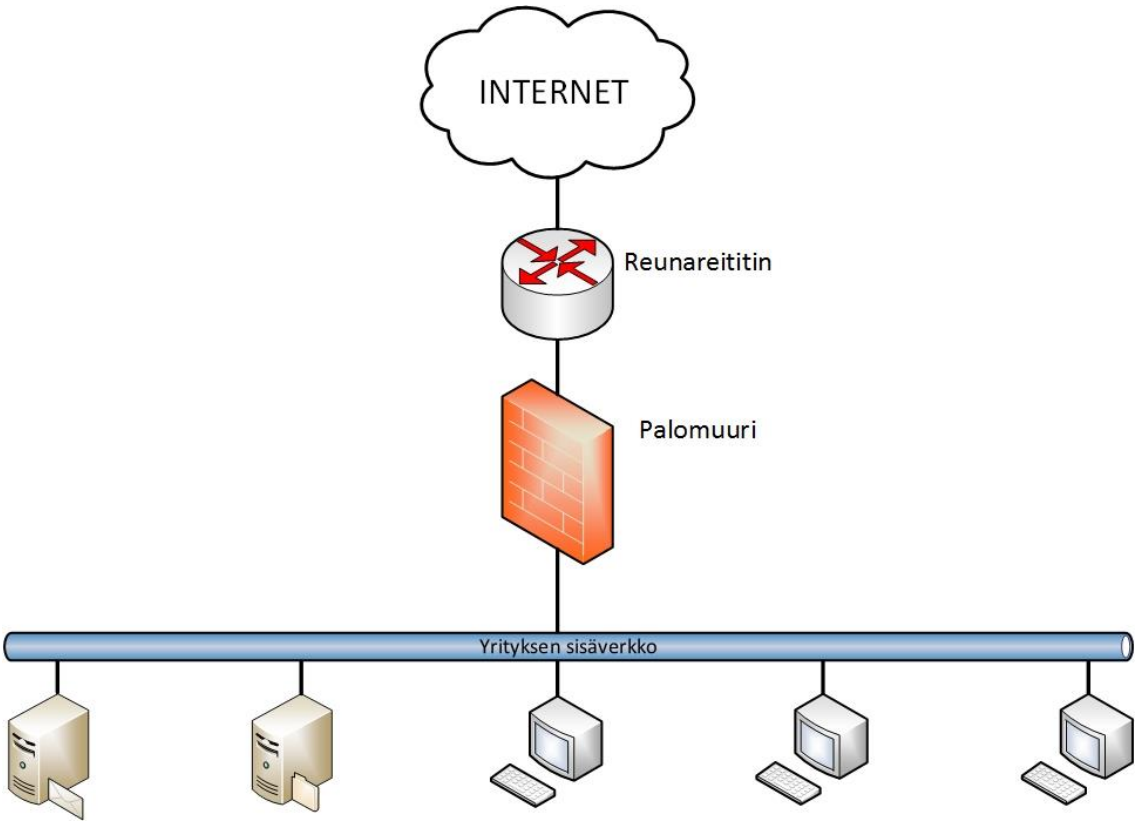
2.2.1 Pakettisuodatinpalomuuri

Ensimmäiset palomuurit tulivat 90-luvun alkupuolella ja ne olivat yksinkertaisia pakettisuodatinpalomuureja. Normaalisti pakettisuodatinpalomuurit toimivat OSI-mallin kolmannella kerroksella, verkkokerroksella. Esimerkkinä pakettisuodatuksesta on reitittimelle tehdyt pääsylistat. Standard-pääsylista voi estää paketin pääsyn lähdeosoitteen perusteella. Jos käyttää extended-pääsylistoja, käyttäjä voi määritellä mistä IP-osoitteesta voi ottaa yhteyden mihinkä osoitteeseen tai osoiteavaruuteen. Samalla voidaan määritellä mitä porttia ja protokollaa se käyttää. Standard-pääsylista toimii OSI-mallin kolmannella kerroksella, ja extended-pääsylista toimii sekä kolmannella että neljännellä kerroksella. (Suehring 2015.)

Pakettisuodatusten tekeminen vaatii paljon aikaa yksittäisten sääntöjen tekemiseen, jotka eivät suojaa käyttäjää kaikelta, kuten TCP SYN flood- ja IP spoofing-hyökkäyksiltä.

Pääsylistojen luomisessa voi käydä myös helposti virhe, jos lisää sallittuja yhteyksiä ja reitittin estää oletuksena kaiken muun. Tällainen tilanne on esimerkiksi, jos paluuliikenne ei ole sallittua vaikka liikenne palomuurilta ulos olisi säännöissä sallittua. Pakettisuodatin ei myöskään osaa tarkastella pakettien sisältöä tarkasti, vaan päästää kaikki paketit läpi jotka läpäisevät kriteerit. Näin paketin sisältö saattaa olla haitallinen ja päästä kulkemaan läpi koska lähde ja kohde vastaavat sääntöä. (Yeo 2003, 51.)

Vaikka pakettisuodatinpalomuuri on nykyajan standardeilla yksinkertainen, eikä toimi yksinään kovin tehokkaana suojana verkolle, sitä voidaan hyödyntää reitittimessä joka toimii sisäverkon ja ulkoverkon rajalla. Kuvassa 1 on esitetty miten reunareititin asettuu topologiaan vahvistamaan verkon tietoturvaa. Alueen reunareitittimelle voi asettaa pääsylistoja joiden avulla suurin osa liikenteestä, jota ei haluta päästä verkkoon, voidaan estää. Tämän jälkeen topologiassa voidaan asettaa tehokkaampi palomuuri, kuten tilallinen palomuuri tai sovelluspalomuuri, ja säästää näin resursseja enemmän prosessointivoimaa tarvitsevalta palomuurilta. (Yeo 2003, 53-54.)



KUVA 1. Esimerkki reunareitittimestä yksinkertaisessa yritysverkossa

2.2.2 Tilallinen palomuuri

Tilallinen palomuuri toimii OSI-mallin kolmannella ja neljännellä kerroksella hyvin samalla tavalla, kuin pakettisuodatinpalomuuri. Tilallisen palomuurin ero näkyy kuitenkin sen toiminnassa viidennellä, eli istuntokerroksella. Pakettisuodatinpalomuurin ongelma on usein paluuliikenteen sallimisessa ja suurien pääsylistamäärien tekemisessä sekä ylläpidossa. Tätä ongelmaa voi helpottaa käyttämällä tilallista palomuuria. (Yeo 2003, 51-52.)

Siinä missä pakettisuodatinpalomuuri ei oletusarvoisesti salli paluuliikennettä, vaan se pitää erikseen sallia pääsylistalla, tilallinen palomuuri muodostaa palvelinten välille yhteyden palomuurisääntöjen sen salliessa. Kun yhteys on sääntöjen mukaan muodostettu, yhteys pysyy ylhäällä niin kauan, kunnes se katkaistaan tai palomuurille määritelty aikakatkaisu katkaisee yhteyden. Jos aktiivista yhteyttä ei löydy, kyseisen säännön mukainen liikenne pudotetaan palomuurilla. Tämä estää hyökkääjiä lähettämästä esimerkiksi ACK-paketteja verkkoon, jotka ovat naamioituja paluuliikenneviestejä. Palomuuri tietää että yhteyttä ei ole muodostettu, eikä se odota paluuliikennettä. (Yeo 2003, 55-57.)

Kun palvelin lähettää paketin palomuurin läpi, palomuurilla sallittu yhteys muodostuu, ja yhteys menee palomuurin ylläpitämään tilatauluun (state table), jossa se pysyy kunnes yhteys katkeaa. Palomuurille tulee sen jälkeen paluuviestinä TCP-paketti, tai jonkin muun tuetun protokollan paketti. Palomuuri voi lukea tämän paketin otsikkotietoja ja siellä olevia lippuja (flags), joita se vertaa tilatauluun listattuihin yhteyksiin ja joko päästää paketin läpi, tai pudottaa sen (Ogletree 2001, 603). Tilataulu on palomuurille kuitenkin kuormittava tekijä, mikä rajoittaa tilallisen palomuurin käyttöä isoissa yritysverkoissa, tai muissa verkoissa, jossa yhteyksiä on auki paljon samaan aikaan. Pienemmälle yritykselle kuten Terasoftille, jolla on verkossaan rajallisesti käyttäjiä ja työasemia, tilallinen palomuuri on ihan pätevä ja edullinen ratkaisu.

2.2.3 Sovelluspalomuuri

Sovelluspalomuuri toimii OSI-mallin kolmannella, neljännellä ja viidennellä kerroksilla, kuten pakettisuodatin- ja tilallinen palomuuri. Näiden lisäksi sovelluspalomuuri toi-

mii myös sovelluskerroksella, eli OSI-mallin seitsemännellä kerroksella. Sovelluspalomuurin ohjaaminen ja suodatus tapahtuu sovelluskerroksella, mikä mahdollistaa tehokkaamman seurannan ja tarkempien sääntöjen tekemisen kuin aikaisemmin mainituilla palomuurityypeillä. Sovelluskerroksella pakettien sisältö voidaan myös purkaa kokonaan ja sen avulla tehdä päätös siitä annetaanko paketin jatkaa matkaa kohteeseensa. (Magalhaes 2008.)

Sovelluskerros mahdollistaa myös käyttäjien tunnistuksen sisäänkirjautumisella. Kun käyttäjä kirjautuu sisään, hänet oikeutetaan pääsemään ennalta määrätyille palvelimille. Tiedot käyttäjien valtuuksista tallennetaan usein erilliselle palvelimelle, jota voidaan ylläpitää esimerkiksi Active Directoryn avulla. Active Directoryn avulla ylläpitäjä voi helposti luoda valmiita ryhmiä ja lisätä käyttäjiä sinne ilman, että jokaiselle IP-osoitteelle tarvitsee määrätä omat palomuurisäännöt. (Avolio 2015.)

Sovelluspalomuurit vaativat paljon tehoa palomuurilaitteistolta, sekä usein erillisiä palvelimia suorittamaan sisään kirjaukseen ja valvontaan liittyviä tehtäviä. Terasoft Oy toimii palvelimien ja palvelintilan tarjoajana, eikä heidän verkkoon pääse sisään kuin portit ja palveluiden salasanat tietävät henkilöt, joten palomuurilla tunnistautumista ei ole pidetty tarpeellisena ominaisuutena. Yrityksen koko on myös suhteellisen pieni ja palveluita on rajallinen määrä. Tästä johtuen tilallinen palomuuri on hyvä valinta Terasoft Oy:n käyttöön.

2.3 Paikallinen palomuuri

Palomuuri voi olla myös ohjelmisto, joka on asennettu suoraan käyttäjän työasemalle. Hyvä esimerkki tällaisesta palomuurista on esimerkiksi Windowsin palomuuri, joka on tullut kaikkien Windows-käyttöjärjestelmien mukana Windows XP:stä lähtien. Paikallinen palomuuri on erittäin tärkeä osa verkon turvallisuutta, mutta se ei yleensä yksin riitä suojaamaan työasemaa. (Stewart 2010.) Hyvä käytäntö on omata sekä ulkoinen palomuuri että palomuuri joka on asennettuna työasemalle. Näin saadaan useampi kerros suojausta, jotka tukevat toisiaan. Monet kotikäyttäjät eivät välttämättä tiedä, mutta yleensä kodeissa olevat modeemit suorittavat palomuuritoimintoja ja antavat ensimmäisen kerroksen suojautumista ulkoisia vaaroja vastaan.

Koska paikallinen palomuuri on asennettuna työasemalla jota se yrittää suojata, haitalliset ohjelmat ovat jo käytännössä perillä kun paikallinen palomuuri havaitsee ne. Jos haitallinen ohjelma pääsee saastuttamaan työaseman, on myös palomuuri silloin altistunut hyökkäykselle, eikä sen toiminta ole luotettavaa.

3 TEKNIIKAT JA OHJELMISTOT

3.1 IPCop-palomuuri

IPCop on avoimen lähdekoodin ilmainen tilallinen palomuuri, joka sopii kotikäyttöön, sekä pienille ja keskikokoisille yrityksille, kuten Terasoft Oy:lle. IPCop on Linux-jakelu (Linux distribution), eli Linux-pohjainen käyttöjärjestelmä, jota kehitetään GNU GPL:n (GNU General Public License) alla. (Clancey ym. 2015.) GNU GPL-lisensoituja ohjelmia ja niiden lähdekoodia saa käyttää ja muokata vapaasti omaan tarkoitukseensa (Free Software Foundation 2007).

Vuonna 2001 joukko tyytymättömiä kehittäjiä ja käyttäjiä loivat ensimmäisen version IPCop-palomuurista. Markkinoilla oli jo olemassa useita palomuureja, mutta IPCopin kehitysryhmä halusi luoda ilmaisen palomuuriohjelmiston, jonka kehityksessä yhteisö olisi vahvasti mukana. IPCopia alettiin rakentamaan Smoothwallin lähdekoodin pohjalta omana jakelunansa. (Clancey ym. 2015.)

IPCopin hallitseminen ja konfigurointi tapahtuu graafisen käyttöliittymä avulla, mikä tekee siitä helppokäyttöisen myös käyttäjille joille Linux-komennot eivät ole tuttuja. Graafinen käyttöliittymä nopeuttaa ja selkeyttää palomuurisääntöjen tekemistä ja ylläpitoa.

IPCopin ladattava versio on oiva palomuuri sellaisenaan, mutta siitä saataisiin täysi hyöty, tarjolla on paljon erilaisia lisäosia, jotka suorittavat palomuureille tärkeitä tehtäviä. IPCopin kehitysryhmä ei ole vastuussa lisäosien toimivuudesta, ja huonon lisäosan asentaminen tai lisäosan väärinkäyttö voi pahimmassa tapauksessa heikentää palomuurin tietoturvaa (Source Forge 2015).

3.1.1 Verkkosovittimien toimialueet

Palomuurilaitteen verkkosovittimille voidaan antaa yksi neljästä roolista, jotka ovat värikoodattuja riippuen millä alueella ne toimivat; vihreä, punainen, sininen tai oranssi. Tällä on pyritty helpottamaan ylläpitotehtäviä ja selkeyttämään mitä tehtäviä kyseiselle

verkkosovittimelle kuuluu. Vihreä, oranssi ja sininen ovat aina verkkokortteja, mutta punaisen sovittimen roolissa voi vaihtoehtoisesti toimia esimerkiksi modeemilaite (Dempster & Eaton-Lee 2006, 48-49). IPCop vaatii toimiakseen vihreän ja punaisen sovittimen. Oranssi ja sininen verkkosovitin ovat valinnaisia, mutta eivät pakollisia.

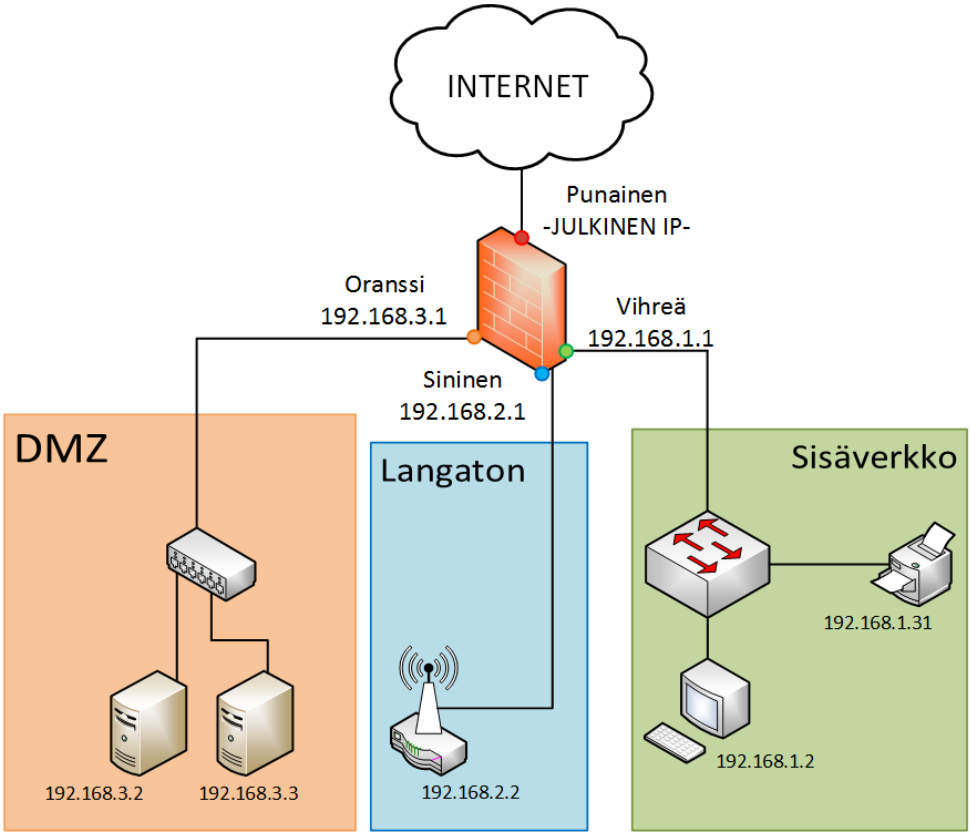
Vihreä sovitin osoittaa sisäverkkoon ja toimii luotettuna osapuolena. Sen IP-osoite asetetaan yleensä sisäverkon IP-osoiteavaruudesta, koska oletusasetuksilla IPCop käsittelee vihreäksi merkattua sovitinta sen mukaisesti, ja käyttää NAT-toimintoja (Network Address Translation) muuttaakseen osoitteen julkiseksi. Vihreä verkkosovitin on verkon topologiasta riippuen tyypillisesti yhteydessä reitittimeen, kytkimeen, keskittimeen, tai jopa suoraan työasemaan. (Dempster & Eaton-Lee 2006, 48.)

Punainen verkkosovitin on kiinni epäluotettavassa verkossa. Yleensä tämä epäluotettava verkko on Internet, mutta jos kyseinen palomuuri on keskellä suurta topologiaa, voi punainen verkkokortti osoittaa mihinkä tahansa epäluotettavaan osaan verkkoa. Punaiselle sovittimelle asetetaan tyypillisesti osoite julkisesta verkosta. Suurin osa palomuurin suodatuksesta tapahtuu punaisella sovittimella, jonka tarkoituksena on suojata muita verkkoja ja päästää vain sallitut yhteydet läpi. (Dempster & Eaton-Lee 2006, 49-52.)

Sinisen sovittimen taakse pystyy luomaan ylimääräisen sisäverkon, jota voi käyttää useaan tarkoitukseen. Tässä verkossa voi toimia esimerkiksi langaton tukiasema tai lisää langallisia työasemia. Sinisestä verkosta ei kuitenkaan kulje suoraan liikennettä vihreään verkkoon, paitsi erikseen tehtyjen palomuuriavauksien tai VPN-putken (Virtual Private Network) läpi. Yksi esimerkki sinisen verkon käytöstä olisi normaalien työasemien ja IT-tuen työasemien sijoittaminen eri verkkoihin. IT-tuen käyttämästä vihreästä verkosta pääsisi käsiksi kaikkeen yrityksen dataan, mutta sinisen verkon normaaleilta työasemilta olisi vain pääsy tarkemmin säädeltyihin resursseihin. (Dempster & Eaton-Lee 2006, 53.)

Oranssi verkkosovitin toimii yhdyskäytävänä DMZ-verkolle (DeMilitarized Zone). DMZ-verkossa ovat yleensä palvelimet, jotka ovat suoraan kanssakäymisessä ulkoverkon kanssa, kuten sähköposti- tai WWW-palvelimet. DMZ-verkko ei ole luotettava, mistä johtuen sieltä ei ole suoraan yhteyttä vihreään tai siniseen verkkoon. Palomuurille on tehtävä avauksia sinisen verkon tapaan, jotta keskustelu laitteiden välillä sisäverkosta DMZ-verkkoon on mahdollista. (Dempster & Eaton-Lee 2006, 52-53.)

Kuvassa 2 on esimerkki yrityksen topologiasta, jossa on hyödynnetty jokaista neljää verkon toimialuetta. Topologiaan on myös sijoitettu eri verkkolaitteita havainnollistamaan mitä kyseisillä alueilla voisi olla.



KUVA 2. Esimerkki IPCop-palomuurin toimialueista

3.1.2 Osoite- ja porttimuunnokset

Pääsy sisäverkon laitteille tapahtuu IPCop-palomuurin ulkoisen, eli punaisen osoitteen kautta. Liikenteen ohjaus tapahtuu valitun portin mukaan, eli kaikkiin työasemiin otetaan yhteys samalla IP-osoitteella, mutta käytettävä portti määrää minne työasemalle tai palvelimelle liikenne ohjataan ja mitä palvelua sillä voidaan käyttää. Tämän takia Terasoft Oy:n yhden IPCop-palomuurin takana voi toimia vain yksi osoite tunnetuilla oletusporteilla, kuten http-verkkosivu portin 80 takana.

Palomuurille tehdyissä säännöissä voidaan erikseen määritellä miltä osoitteilta on pääsy eri sisäverkon työasemille. Jos palveluna toimii web-palvelin, sinne voidaan sallia pääsy kaikista osoitteista. Enemmän tietoturvaa vaativille palveluille määritellään tietyt staattiset osoitteet jotta vain tietyt henkilöt saavat pääsyn kyseiselle palvelulle. Tämä vaatii

sen, että asiakkaat ovat hankkineet itselleen staattisen osoitteen palveluntarjoajaltansa tai he käyttävät VPN-tunnelia.

3.1.3 Lokit ja suorituskykymittarit

IPCop tarjoaa laajasti erilaisia lokeja, mittareita ja tauluja joiden avulla ylläpitäjä pystyy seuraamaan palomuurin tilaa. Näiden lisäksi erilaisilla lisäosilla kuten Copfilterin monit-lisäosalla voidaan ottaa käyttöön vielä muita tarkempia palomuurin tarkkailun apuvälineitä.

Kaikki käytössä olevat IPCopin omat palvelut ovat listattuna yhdelle sivulle, josta näkee mitkä niistä ovat käytössä, ja mitkä eivät. Näihin palveluihin kuuluvat esimerkiksi DHCP-, NTP- ja lokipalvelin, url-filter ja OpenVPN server. Samassa taulussa kerrotaan myös kuinka paljon ne käyttävät järjestelmän muistia.

Palomuurina toimivan tietokoneen sisällä olevista komponenteista on olemassa laaja lista, josta saa kaikki tarvittavat tiedot esimerkiksi prosessorista, USB- ja PCI-laitteista, verkkokorteista, RAM-muistista ja kovalevystä. Kyseisten laitteiden kuormituksesta on saatavilla tietoa sekä absoluuttisesti että prosentuaalisesti. Graafiset käyrät esittävät verkkoliikenteen määrää tietyltä aikajaksolta, sekä RAM-muistin käyttöhistoriaa. Vapaana olevan muistin määrä ja sen käyttö eri tarkoituksiin on myös tarkasti esitetty.

Verkkoliitynnöistä on olemassa oma alasivunsa, jossa on merkittynä eri verkkoliittymien osoitteet ja niiden läpi kulkeneen liikenteen tiedot. Tiedoista näkee läpi kulkeneiden pakettien määrän numeraalisesti sekä megabitteinä, virheilmoitukset ja pudotettujen pakettien määrän.

Tilalliselle palomuurille ominainen tilataulu on mahdollista nähdä palomuurilta. Tilataulusta näkee avoinna olevat yhteydet sisäverkon laitteille sekä palomuurille. Aikaisemmin tutuksi tullutta värikoodausta on hyödynnetty tilataulussa, minkä avulla on helppo tarkastella mistä alueelta on yhteys auki minne osoitteeseen.

3.1.4 IPCopin muut palvelut

IPCop tarjoaa paljon palveluita joita Terasoft Oy ei toimintamallinsa vuoksi pääse täysin hyödyntämään. Näitä palveluita ovat esimerkiksi VPN-tunnelit ja DHCP-palvelu. Terasoft Oy:n tarve VPN-tunneleille on yleensä satunnaista. VPN-tunnelia käytetään vain jos ohjelmistokehityksessä tarvitsee suorittaa testi palvelimelta toiselle Internetin ylitse. Koska Terasoft Oy:lla ei ole kahta aliverkkoa, jotka pitäisi yhdistää VPN-tunnelilla, eikä tarvetta testiä varten ole työn tekemisen hetkellä, VPN-tunnelia ei konfiguroida.

Sisäverkon laitteet toimivat staattisilla osoitteilla ja suorittavat erilaisia tehtäviä kuten tietokantapalveluita. Yrityksen yhteistyökumppaneille on jaettu osoitteita joita he voivat käyttää omille työasemilleen tarpeen mukaan. Tämän takia DHCP-palvelusta ei ole samanlaista hyötyä mitä siitä olisi yritykselle, joka lisää jatkuvasti vakioituja työasemia työntekijöilleen tai kotiverkossa missä on normaalikäytössä olevia verkkolaitteita.

IPCopilta voi avata VPN-tunnelin toiselle IPCop-palvelimelle, tai toiselle VPN:ää tukevalle laitteelle. VPN-tunnelin voi avata joko Net-to-Net tai Host-to-Net tyyppisenä, eli joko toiseen verkkoon tai suoraan yhdelle isännälle. Net-to-Net VPN on ratkaisu jota voisi käyttää jos Terasoft Oy:lla olisi toinen sisäverkko jonne haluttaisiin avata pääsy tältä IPCop palomuurilta. Host-to-Net VPN:llä voidaan avata VPN-tunneli IPCop-palomuurilta suoraan käyttäjälle, jolla olisi esimerkiksi käytössään dynaaminen IP-osoite suoraan palveluntarjoajalta. Näin käyttäjä voidaan todentaa, eikä staattista osoitetta tarvitsisi olla, ja käyttäjä pääsisi käsiksi palomuurille mistä tahansa osoitteesta, eikä olisi sidottuna toimimaan vaan yhdestä paikasta.

3.2 Palomuurin lisäohjelmistot

IPCop-palomuurille pystyy asentamaan yhteisön tekemiä lisäosia käyttäjän tarpeiden mukaisesti. Useista tietoturvaa parantavista lisäosista tarkastelen lyhyesti Snort IDS-järjestelmää, sekä Copfilter-lisäosapaketin palveluita. Lisäosia ei kannata ottaa käyttöön kuormittamaan palomuuria, jos niitä ei hyödynnä. Koska Terasoft Oy:n IPCop-palomuuri tulee suurimmaksi osaksi aikaa pyörimään ilman jatkuvaa tarkkailua, pitää mahdolliset lisäosat valita sen mukaisesti.

3.2.1 Snort IDS

Snort on yksi suosituimmista avoimen lähdekoodin IDS-järjestelmistä (Intrusion Detection System). IPCop-palomuuria varten tehdyllä Snort-lisäosalla palomuurin turvallisuutta voidaan kasvattaa OSI-mallin sovelluskerroksen tasolle. Martin Roesch kehitti Snortin vuonna 1998 (Roesch & Green 2015). Snort kuului osana vanhaa IPCopin versiota yksi, mutta nykyään IPCop-palomuurilla ei ole oletuksena mitään pakettien tarkkailua suorittavaa palvelua, vaan sellainen pitää asentaa jälkikäteen lisäosan muodossa (Clancey ym. 2015).

Snort tarkkailee paketteja halutuista verkkosovittimista, ja antaa haitallisista paketeista ilmoituksen ja kirjaa sen lokiin. Virusrekisteriin Snort saa verkosta automaattisesti, mutta se vaatii käyttäjän kirjautumisen Snortin verkkosivuille. Kun käyttäjätunnukset ovat tehty, Snort tarjoaa koodin, joka pitää asettaa IPCop-palomuurille. Ilmaisessa versiossa allekirjoituspäivitykset asentuvat 30 päivän välein, ja maksullisessa versiossa päivitykset asentuvat heti kun ne ovat julkaistu. (Roesch & Green 2015.)

Koska tilallisessa palomuurissa ei muuten tapahdu osoitteiden ja porttien suodattamisen lisäksi juurikaan muita turvallisuutta edistäviä toimintoja, IDS-järjestelmä kuten Snort, joka tarkastelee pakettien sisältöä, on tärkeä lisäys (Dempster & Eaton-Lee 2006, 29-30).

3.2.2 Copfilter

Copfilter on lisäosapaketti, joka tarjoaa useita työkaluja IPCop-palomuurin tietoturvan parantamiseen. Sen tarjoamat palvelut mahdollistavat esimerkiksi web-, FTP- ja sähköpostiliikenteen tarkkailun ja skannaamisen. Copfilterin sisältämä ClamAV-virustorjunta ja aikaisemmin mainittu Snort ovat monilla tavoilla samanlaisia, eikä yhdelle IPCop-palomuurille kannata laittaa molempia tekemään päällekkäisiä tehtäviä. Tärkein ominaisuus, minkä molemmat lisäosat tuovat palomuurille on sen ulottuvuuden nostaminen OSI-mallin sovelluskerrokselle.

Lisäosana Copfilter sopii pienelle yritykselle, jolla on paljon erilaista liikennettä, jota täytyy tarkkailla. Vaikka Copfilter tarjoaa paketissaan 12 lisäosaa, kaikkia niistä ei ole pakko ottaa käyttöön, vaan osan voi jättää pois päältä ja ottaa käyttöön myöhemmin tarpeen mukaan. Taulukossa 1 on listattuna kaikki Copfilter-paketin mukana tulevat lisäosat ja niiden toimintatarkoitus. (Madlener 2015.)

TAULUKKO 1. Copfilter-lisäosapaketin sisältämät lisäosat

Nimi	Käyttötarkoitus
monit	Lisäosien monitorointityökalu
P3Scan	POP3-proxy
ProxSMTP	SMTP-proxy
HAVP	HTTP-proxy
Privoxy	HTTP-proxy
C-ICAP	HTTP-proxy
frox	FTP-proxy
SpamAssassin	AntiSpam-filtteri
ClamAV	AntiVirus-ohjelma
Imspector	IM-proxy
Renattach	Liitteiden uudelleennimeäjä
SA Rules	AntiSpam sääntölista

3.3 Halintaan ja toteutukseen käytetyt ohjelmistot ja laitteet

Kaikki työ tehdään etähallintana käyttämällä TeamViewer ohjelmistoa ja Keuruulla sijaitsevaa työasemaa, joka on samassa aliverkossa IPCop-palomuurien kanssa. TeamViewerillä suoritetaan tunnistautuminen, jonka avulla työasemille sallitaan pääsy. Työasema, jota käytän välikätenä palomuurien konfiguroimiseen, on toimeksiantaja Wild Software Oy:n omistama ja tähän käyttöön luovutettu. IPCop-palomuuria pääsee konfiguroimaan vain sisäverkon työasemalta, joten jonkinlainen yhteys sisäverkon työasemaan on pakollinen konfiguroinnin mahdollistamiseksi. Palomuurille voi sallia pääsyn myös suoraan etätyöpisteeltä, mutta sitä ei ole katsottu tarpeelliseksi.

Tällä hetkellä IPCop-palomuureille on sallittu pääsy kaikilta sisäverkon työasemilta vihreän osoitteen kautta, mutta vain käyttäjätunnuksen ja salasanan tietävillä henkilöillä on mahdollisuus päästä tutkimaan palomuuria syvällisemmin ja tekemään sinne muutoksia.

4 MUUTOSTYÖN SUUNNITTELU

4.1 Opinnäytetyön tilaaja

Opinnäytetyön tilaaja on Wild Software Oy, joka on tamperelainen yhden henkilön yritys. Wild Software Oy tarjoaa asiakkailleen ohjelmistojen suunnittelua sekä IT-alan konsultointia ja palveluita.

Terasoft Oy on Keuruulla toimiva tietotekniikkayritys, joka tuottaa pienille ja keskisuurille yrityksille lukuisia erilaisia palveluita, kuten verkkosivujen luomisen, palvelimen laitetilan tarjoamisen ja tietoliikenneyhteydet.

Terasoft Oy, Wild Software Oy sekä muutama muu yritys ovat tehneet vuosien varrella paljon alihankintaa ristiin, kuten tässä opinnäytetyön tapauksessa. Terasoft Oy on antanut Wild Software Oy:lle toimeksiannon, jonka toteutan työssäni.

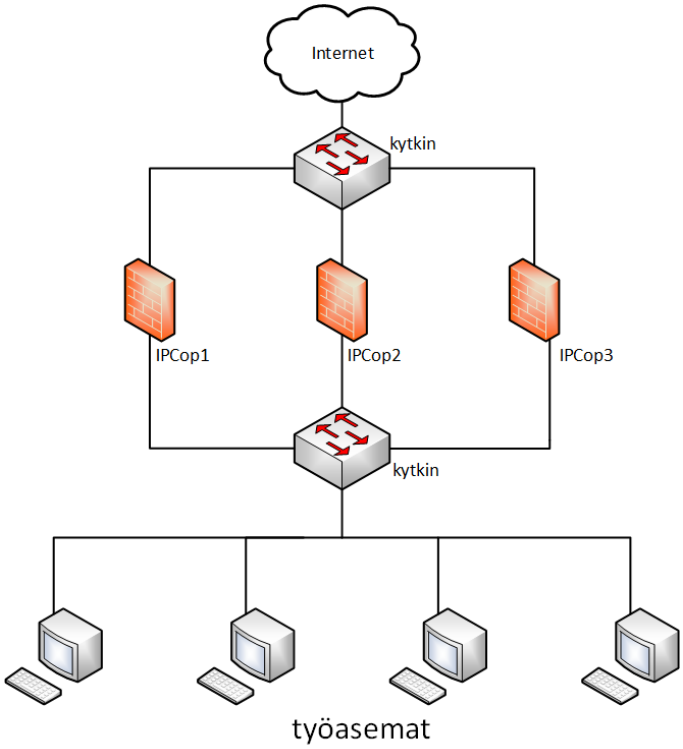
4.2 Tavoite ja tarkoitus

Työssäni on tarkoituksena siirtää vanhan IPCop-palomuurin (IPCop1) osoite- ja porttimuunnokset uudelle palomuurille (IPCop3). Kun aktiivisen laitteen toiminta siirretään toiselle laitteelle, puhutaan termistä yliheitto. Yliheiton yhteydessä vanhat muunnokset, jotka ovat jääneet jo lähteneiltä aikaisemmilta asiakkailta, siivotaan pois tietoturvan parantamiseksi. Myös palomuurin yleistä tietoturvaa tarkastellaan ja pyritään parantamaan ottamalla käyttöön tarpeellisia lisäosia.

Tavoitteena on suorittaa yliheitto mahdollisimman lyhyellä käyttökatkolla. Palomuuri konfiguroidaan valmiiksi testiosoitetta käyttäen ja se otetaan käyttöön täysin toimintavalmiina. Yliheitto suoritetaan päivän hiljaisena hetkenä, jolloin asiakkaat eivät käyttöhistorian perusteella käytä yhtä paljon Terasoft Oy:n isännöimiä laitteitaan. Jotta yliheitto voidaan tehdä turvallisesti, palomuuri otetaan käyttöön osittain testattuna. Työssä noudatetaan testaus- ja paluusuunnitelmia. Näin pyritään takaamaan asiakkaiden tietoturvan säilyminen sekä yrityksen toiminnan jatkuminen mahdollisista vikatilanteista huolimatta.

4.3 Lähtötilanne

Terasoft Oy:n verkon rakenne on suhteellisen yksinkertainen. Verkossa on kytkin, johon on kiinnitetty kaksi IPCop-palomuurina toimivaa työasemaa. Nämä kaksi IPCop-palomuuria ovat kiinni vielä toisessa kytkimessä, jonka takana on X määrä työasemia ja palvelimia. Verkossa ei ole reititintä, vaan reunalla toimiva kytkin on yhteydessä suoraan palveluntarjoajan runkoverkkoon. Liikenne työasemille on jaettu kahden palomuurin välille. Terasoft Oy:n verkon topologia on esitetty graafisesti kuvassa 3.

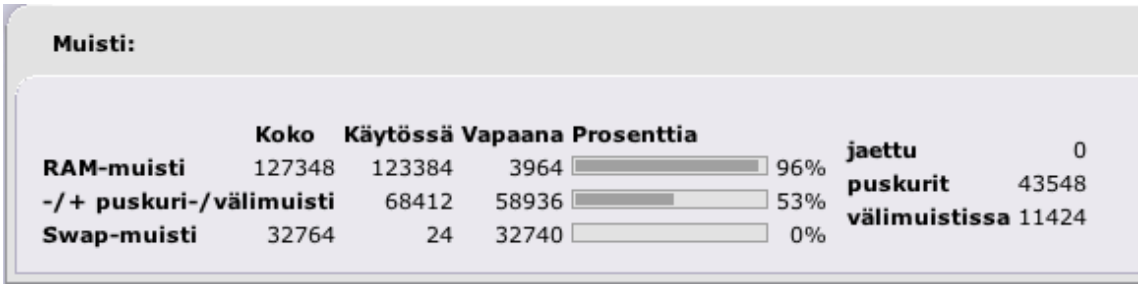


KUVA 3. Terasoft Oy:n verkon topologia

Verkon topologia on työn alussa ja lopussa samanlainen. Lähtötilanteessa verkossa on kaksi aktiivista IPCop-palomuuria; IPCop1 ja IPCop2. Näistä IPCop1-palomuurilla on käytössä vanha IPCopin versio 1.4.16, joka täytyy päivittää uusimpaan versioon 2.1.9. IPCop2 palomuurilla on jo käytössä versio 2. Kyseinen palomuuri ei ole yliheitolle kovin merkityksellinen, joten sen toimintaa ei käydä opinnäytetyössä tarkemmin läpi.

Kuvassa 4 on kuvankaappaus vanhan IPCop1-palomuurin muistin käytöstä. Koska IPCop1-palomuurina toimivan työaseman komponentit ovat jo nykyajasta pahasti jäljessä, ohjelmistopäivitystä ei suoriteta samalle työasemalle, vaan uusi palomuuri otetaan käyt-

töön uudella palvelinkoneella, jossa on ennen kaikkea enemmän RAM-muistia, sekä tehokkaampi prosessori.



KUVA 4. IPCop1-palomuurin RAM-muistin käyttö

Uusi palvelinkone, mihin IPCop3-palomuuri asennetaan, on huomattavasti paremmin varusteltu (taulukko 2). Ottaen huomioon verkossa olevien työasemien ja verkkoliikenteen määrän, uuden palomuurin komponenttien ei tarvitse olla markkinoiden parhaimmistoa, vaan nykyajan standardeilla hyvin edulliset komponentit riittävät pyörittämään kevyttä Linux-jakelua kuten IPCop. Muistia ja prosessointivoimaa tulee kuitenkin olla tarpeeksi, jotta tarvittavat lisäosat Copfilter-lisäosapaketista voidaan ottaa käyttöön, ja resursseja jää silti käytettäväksi palomuuritoiminnoille kiireisempinäkin hetkinä. Vanhassa IPCop-palomuurissa on RAM-muistia vaivaiset 128 megabittiä, mikä on erittäin kaukana nykyajan muististandardeista. Uutena palomuurina toimivalla palvelinkoneella on kaksi gigatavua RAM-muistia, ja sitä voidaan lisätä enemmän jos testauksessa havaitaan sille tarvetta.

TAULUKKO 2. IPCop3-palomuurin tärkeimmät komponentit

Laite	**Valmistaja ja malli**
Prosessori	Intel Pentium 4, 2.80GHz
RAM-muisti	4 kpl 512MB PC-4200 DDR II ,(2GB)
Kovalevy	Seagate Barracuda 7200.9, 80GB
Verkkokortti 1	Broadcom NetXtreme BCM5721 Gigabit Ethernet
Verkkokortti 2	Realktek RTL8169 Gigabit Ethernet

Työssä minulla on itselläni käytössä järjestelmänvalvojan oikeudet, mutta ei juuritason oikeuksia. Tämän takia pystyn vain tekemään muutoksia palomuureille, mutta asennukset täytyy tilata Terasoft Oy:lta. Tästä johtuen IPCop3-palomuuri oli valmiiksi asennet-

tuna palvelinkoneelle, jotta siihen voidaan konfiguroida oikeat portti- ja osoitemuunnokset. Palomuurille on asetettuna ainoastaan asennuksen yhteydessä tarvittavat tiedot, kuten vihreän ja punaisen verkkokortin osoitteet, aikapalvelimen tiedot, sekä DNS-palvelimien osoitteet. Terasoft Oy:n edustaja asentaa myös tarvittavat lisäosat palvelinkoneelle, mutta niiden konfigurointia ja käyttöönottoa ei ole tehty. IPCop-palomuurin asennus on erittäin suoraa toimintaa, eikä se vaadi asentajalta kuin muutaman tiedon verkosta. Lisäosat palomuureille täytyy siirtää tiedostonsiirto-ohjelman, kuten WinSCP:n avulla. Tämän jälkeen palomuurille otetaan yhteys pääte-emulaattorilla kuten PuTTY:lla, jonka avulla tiedostot voidaan purkaa ja asentaa palomuurille.

4.4 Testaussuunnitelma

Yliheiton, kuten minkä tahansa muunkin käyttöönoton onnistumisen kannalta, hyvä suunnitelma on erittäin tärkeä. Suunnitelmien avulla pyrin luomaan toimintamallin mahdollisten erilaisten ongelmatilanteiden varalta. Tällaisia tilanteita ovat esimerkiksi palomuurin virheellinen toiminta tai henkilökohtaisten esteiden ilmeneminen. Testauksia ja niihin liittyviä suunnitelmia työssäni on kaksi. Ensimmäinen testaus tapahtuu ennen tuotantokäyttöönottoa, ja toinen sen jälkeen.

4.4.1 Käyttöönottotestaus

Ennen palomuurin käyttöönottoa tuotannossa, muurin toimintaa testataan yhdellä työasemalla. Työaseman oletusyhdyskäytäväksi otetaan nykyisen palomuurin IP-osoitteen sijasta IPCop3-palomuurin testikäytössä oleva IP-osoite, missä sitä on konfiguroitu. Tämän jälkeen testataan sekä yhteyttä jonka pitäisi toimia, että yhteyksiä joidenka ei pitäisi toimia.

Tällä testillä pyritään varmistamaan, että portti- ja osoitemuunnokset ovat tehty oikealla tavalla, ja ainakin yksi työasema toimisi tarkoituksen mukaisesti. Vaikka testi kertoo vain pienen osan palomuurista toimivan oikein, sen merkitys on kuitenkin suuri. Testin avulla pystyy varmistamaan ainakin yhden toimivan portinohjauksen, jota voi tuotantokäyttöönotossa ilmenevien ongelmien tullessa käyttää vertailupohjana toimivalle konfiguraatiolle.

4.4.2 Tuotantotestaus

Koska IPCop on tilallinen palomuuri ja niitä on Terasoft Oy:n verkossa kaksi kappaletta, työasemilla pitää olla paluuliikenne asetettuna samalle palomuurille, mistä alkuperäinen yhteys on tullut. Jos paluuliikenne on ohjattu eri palomuurille kuin saapuva liikenne, palomuuri tiputtaa paketit koska yhteyttä ei ole luotu tilatauluun. Tästä syystä on päädytty ratkaisuun, että IPCop3-palomuuri perii osoitteensa IPCop1-palomuurilta. Näin uudella palomuurilla on käytössä palvelut ja osoite, jotka vastaavat sisäverkon työasemien oletusyhdyskäytäviä. Uuden IP-osoitteen käyttäminen olisi vaatinut jokaisen työaseman oletusyhdyskäytävän muuttamisen.

Tuotantokäyttöönotossa testaus alkaa heti, kun IPCop3-palomuuri on saanut uuden IP-osoitteensa. Testauksesta on ilmoitettu asiakkaille, joiden täytyy itse varmistaa palomuurin toimiminen staattisista IP-osoitteistaan, joista yhteydet palomuurilla ovat sallittu. Testaan yhdessä Wild Software Oy:n edustajan kanssa hänen omat työasemat, ja seuraan samalla palomuurin tietoliikenne lokeja, sekä lisäosien toimintaa. Testauksessa pyritään käymään läpi kaikki palomuurilla toimivat portti- ja osoitemuunnokset.

4.5 Paluusuunnitelma

Palomuurin käyttöönotossa on erittäin tärkeätä olla paluusuunnitelma. Paluusuunnitelmalla voidaan taata, että verkon toimintaa voidaan jatkaa, vaikka uusi palomuuri ei toimisikaan odotetusti. Koska uusi palomuuri voidaan todeta toimivaksi vain yhdellä työasemalla aikaisemmin tehdyn testauksen perusteella, paluusuunnitelma täytyy olla olemassa verkon toiminnan turvaamiseksi.

Toimiva palomuuri täytyy olla olemassa jokaisessa työn vaiheessa. Työn aikana vanhalle IPCop1-palomuurille ei tehdä mitään muutoksia. Mikäli uusi IPCop3-palomuuri ei toimi odotetusti, vian kriittisyys täytyy arvioida. Mikäli vika ei ole kriittinen, palomuuria voidaan korjata sen ollessa tuotantokäytössä. Tämänlainen tilanne on esimerkiksi, jos yhteyksiä joiden pitäisi toimia, on estetty. Jos taas tilanne on päinvastainen, eli palomuurin läpi pääsee enemmän yhteyksiä kuin sallittu, palomuuri täytyy ottaa välittömästi pois käytöstä, ja vanha IPCop1-palomuuri otetaan takaisin käyttöön.

Uuden palomuurin käyttöönottoon on varattu aikaa kolme tuntia. Tämän kolmen tunnin aikana uuden palomuurin täytyy olla täysin toimiva, eikä sitä sen jälkeen korjata ilman että se otetaan pois tuotantokäytöstä. Mikäli palomuurin yliheitto on onnistunut, vanha IPCop1-palomuuri voidaan ajaa alas. Sen asetukset pidetään silti ennallaan vielä tulevaisuudessakin, mikäli uusi palomuuri lopettaa toimintansa ennalta-arvaamattomasti.

5 MUUTOSTYÖN TOTEUTUS

5.1 Toteutus

Vanhalle IPCop1-palomuurille oli jäänyt vanhoja porttienohjauksia asiakkailta, jotka eivät enää ole Terasoft Oy:n asiakkaina. Tämän lisäksi myös nykyisille asiakkaille on olemassa joitakin porttimuunnoksia palveluihin, jotka eivät ole enää käytössä. Ylimääräiset porttienavaukset ovat tietoturvariski, joka on syytä ottaa huomioon uutta palomuuria konfiguroidessa. Tästä syystä ennen työn aloittamista, kartoitin Terasoft Oy:n yhteistyökumppaneilta mitkä porttimuunnokset ovat vielä aktiivisessa käytössä, jotta vain tarpeelliset muunnokset tulevat uuden palomuurin käyttöön.

5.1.1 Portti- ja osoitemuunnosten luominen

Porttien uudelleenohjauksen tekeminen on tehty erilaiseksi IPCop-palomuurin versiolla 2, kuin mitä se oli versiossa 1. Vanhassa versiossa kaikki tapahtui yhdessä ruudussa, missä syötettiin arvoina lähdeosoite, lähdeportti, kohdeosoite ja kohdeportti. Tämä aiheuttaa vaikeuksia kun mikä tahansa sisäinen tai ulkoinen portti tai osoite muuttuu. Tällöin palomuurin ylläpitäjän täytyy vaihtaa jokainen porttimuunnos erikseen, jossa muuttunut osoite on käytössä. Jotta palomuurin ylläpitäjän työtä voidaan helpottaa, uudessa IPCop-palomuurin versiossa 2 kaikki porttimuunnokset voidaan koostaa osista, joille annetaan nimi ja arvo.

Osat täytyy määritellä kahdessa paikassa; osoitteet ja palvelut. Osoitteisiin pystyy luomaan nimen eri IP-osoitteelle, sekä sisäisille että ulkoisille. Tässä vaiheessa luotiin palaset kaikille sisäverkon työasemille, sekä staattisille ulkoisille osoitteille, joista yhteyksiä muodostetaan sisäverkon koneille.

Palveluissa on suuri lista tunnettuja portteja sekä IPCopin omia portteja, mitkä ovat yhdistetty niiden käyttämiin palveluihin. Nämä kuuluvat IPCopin alkuperäisasennukseen. Näiden oletusporttien lisäksi täytyy luoda muut portit palveluille, joita palomuuri käyttää uudelleenohjauksessa. Tähän lasketaan portit joita käyttäjä käyttää yhdistääkseen, sekä portteja joihin palomuuri ohjaa liikennettä porttimuunnoksen yhteydessä. Palvelui-

den luominen on yksinkertaista. Se vaatii vain palvelulle nimen, protokollan sekä porttinumeron. Palvelulle voi myös määritellä ICMP-tyypin, mutta se ei ole työasemille tehdyissä porttimuunnoksissa tarpeellista. Terasoft Oy:n aliverkossa ei ole laitteistoa, jotka hyötyisivät merkittävästi ICMP-tyyppien määrittelystä.

Kun osoitteet ja palvelut ovat määritelty, porttiohjaukset voidaan koostaa tehdyistä osista. Porttiohjaukselle valitaan osista tarvittaessa lähdeosoite, jos vain tietystä osoitteesta sallitaan pääsy tiettyyn palveluun. Muussa tapauksessa siihen jätetään any, eli kaikista osoitteista voi käyttää palvelua. Kohdeosoite voidaan määritellä manuaalisesti, mutta kuten aikaisemmin todettiin, osoitteet kannattaa valita ennalta määritellyistä osista. Listalta valitaan oikea kohdeosoite, mikä palveluun kuuluu. Lopuksi määritellään lähde- ja kohdeportti, mitä yhteys käyttää. Portti voidaan valita joko ennalta määritettyjen palveluiden listalta, tai erikseen ylläpitäjän määrittelemistä palveluista. Lopuksi voi valita kirjataanko tämän porttimuunnoksen tapahtumat lokiin, ja otetaanko porttimuunnos heti käyttöön vai ei. Uudet porttimuunnokset jätettiin luomisen yhteydessä pois päältä odottamaan testausta ja käyttöönottoa.

5.1.2 Lisäosien käyttöönotto

Lisäosiksi palomuurille Terasoft Oy halusi ottaa käyttöön Copfilterin, joka tarjoaa pakettimuodossa käyttäjälle erilaisia liikenteentarkkailutyökaluja. Terasoft Oy:n sisäverkossa on yrityksen toimintamallin takia vain asiakkaiden työasemia, joten kaikki tarjolla olevat palvelut eivät ole tarpeellisia.

Copfilter-paketin mukana tulee ClamAV niminen viruksentorjuntaohjelma, joka käyttää hyväksi muita Copfilterin palveluita tarkkaillakseen ja analysoidakseen pakettien sisältöä. Tärkeimmäksi palveluiksi nousi http-, smtp- ja pop3-proxyt, sekä monitorointityökalu. Kyseiset proxyt toimivat transparent modessa (läpinäkyvä tila). Tämä tarkoittaa, että käyttäjät eivät tiedä proxyn olemassaolosta mitään, eikä siihen yhdistääkseen tarvitse tehdä käyttäjän osalta minkäänlaista konfiguraatiota. Transparent proxy toimii palomuurissa, ja se tarkistaa liikennettä joka kulkee palomuurin läpi (Andrei 2010). Sana proxy voi aiheuttaa hämmennystä, sillä terminä se yhdistetään yleensä erilliseen osoitteeseen, jonka kautta liikenne kuljetetaan. Transparent proxyn tapauksessa se on käy-

tännössä vain palomuurilla toimiva, käyttäjälle huomaamaton liikenteentarkkailutyökalu.

Jotta http-proxyt saa toimimaan, IPCop-palomuurilla pitää laittaa www-välimuisti päälle. Tämä tarkoittaa, että kaikki http-liikenne kulkee IPCopin oman transparent-proxyn läpi, jossa halutut verkkosivut, osoitteet, portit tai muu sisältö voidaan halutessa suodattaa. Kellonaikoja jolloin www-liikenne sallitaan voi halutessaan myös säätää. Kun www-välimuisti on käytössä, privoxy-lisäosa tarkistaa URL-osoitteen tietokannastaan. Jos osoite sallitaan läpi, se kulkee havp-lisäosalle, joka toimii omana transparent-proxyna. Jotta paketti voidaan analysoida mahdollisten vaarojen varalta, havp-lisäosa käyttää ClamAV-lisäosaa tarkastaakseen paketin sisällön. Mikäli ClamAV ei havaitse paketissa mitään vaarallista, se pääsee kulkemaan kohteeseensa. (Madlener 2005.)

ClamAV:lle voi määritellä kuinka usein se hakee päivityksiä rekisteriinsä, ja tekeekö se niin automaattisesti. ClamAV käyttää OpenAntiVirus-projektin virustietokantaa päivityksiinsä (OpenAntiVirus 2015). Jos ClamAV löytää liikenteestä mielestänsä viruksen tai spam-viestin, kyseinen tiedosto menee karanteeniin. Karanteenista näkee esimerkiksi sähköpostiviestin tiedot, kuten lähettäjän ja kohdeosoitteen, otsikon ja tiedoston nimen. Tämän jälkeen viestin voi joko poistaa, tai lähettää eteenpäin sen alkuperäiseen kohdeosoitteeseen.

Viimeisenä käyttöön otettiin monit joka toimii käyttöönotettujen palveluiden tarkkailijana. Jos jokin proxy esimerkiksi lopettaa toimintansa, monit pyrkii käynnistämään kyseisen palvelun uudestaan, ja ilmoittaa tapahtuneesta viestinä ylläpitäjälle ennaltamääriteltyyn sähköpostiin.

5.2 Toteutuksen testaus

Toteutusta haluttiin testata ennen käyttöönottoa. Testauksen tarkoitus oli varmistaa että vähintään kaksi tehdyistä porttimuunnoksista toimii kuten pitää, jotta palomuuri voidaan ottaa tuotantokäyttöön.

Testattavaksi valittiin yksi Wild Software Oy:n työasemista, joka tällä hetkellä käyttää vanhaa IPCop1-palomuuria oletusyhdyskäytävänä. Tälle työasemalle asetettiin oletus-

yhdyskäytäväksi uuden IPCop3-palomuurin testiosoite. Työasemalle piti kuitenkin varmistaa pääsy kahta reittiä, mikäli portinohjaus ei toimisi, ja lukitsisin itseni siitä ulos epäonnistuneen testin seurauksena. Tämän takia testausta varten käytössä oli myös toinen työasema samasta verkosta, josta voitiin muodostaa etäyhteys kahden sisäverkon laitteen välillä VNC-etäyhteysohjelmistolla.

Testattava palvelu työasemalla oli Helix-tietokantapalvelu. Työasemalla on kahden eri loppuasiakkaan tietokannat, joihin voidaan olla yhteydessä client-ohjelman avulla. Molemmille oli tehty oma portinohjaus, joten niitä voitiin testata erikseen. Yhteys muodostettiin selaimella, johon asetettiin IPCop-palomuurin ulkoinen osoite ja palvelua vastaava TCP-portti.

Ensimmäinen testi tehtiin niin, että palomuurin portin edelleenohjaukset olivat pois päältä. Tarkoituksena oli varmistaa, että liikenne ei kulje läpi, ja palomuuri tiputtaa paketit. Testi meni odotusten mukaisesti, ja yhteyttä ei voitu muodostaa.

Seuraavaksi molempien Helix-palveluiden porttien edelleenohjaukset aktivoitiin testiä varten. Ensimmäinen yhteys muodostui heti, kuten oli tarkoituskin. Toisen palvelun yhteyttä ei voitu muodostaa. Ongelman selvittämiseen meni hieman aikaa, mutta Helix-ohjelmiston uudelleenkäynnistäminen korjasi ongelman. Häiriö aiheutui työasemalle tehdyistä osoitteen muutoksista. Kyseinen ongelmatilanne on tunnettu joissain Helix-versioissa. Palvelu ei osaa ottaa uusia osoitteita käyttöön ilman uudelleenkäynnistämistä. Kun uudelleenkäynnistäminen oli suoritettu, palvelu alkoi toimia normaalisti.

Testaus suoritettiin onnistuneesti, ja uuden palomuurin käyttöönoton kanssa voitiin edetä suunnitellussa aikataulussa.

5.3 Käyttöönotto ja testaus tuotannossa

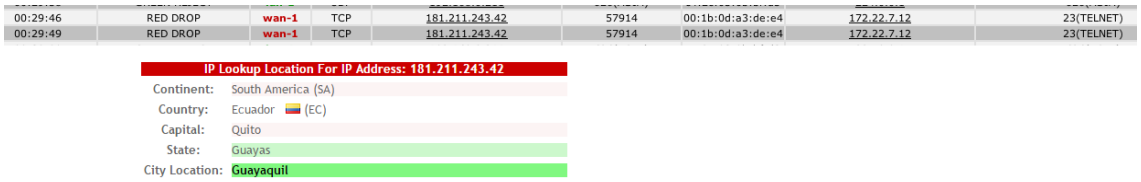
Käyttöönotto tapahtui sovittuun päivänaikaan kello 17.00. Tämä on todettu sopivaksi ajankohdaksi tehdä nopea palomuurin yliheitto. Palomuurin ja palveluiden on tarkoitus olla alhaalla vain muutaman minuutin, joten käyttöönottoa ei todettu tarpeelliseksi tehdä myöhemmin illalla tai yöllä. Palomuurin IP-osoitteiden vaihto tapahtui paikan päällä Keuruulla, koska minulla ei ollut root-tason oikeuksia. Terasoft Oy:n edustaja teki vaih-

don sovittuun kellonaikaan, ja jäi tarkkailemaan tilannetta kunnes ilmoitan palomuurin olevan joko testattu ja toimiva, tai vaihtoehtoisesti vanha palomuuri palautettaisiin käyttöön uuden palomuurin vikatilanteessa.

Ennen palomuurien IP-osoitteiden vaihtoa, palomuuria seurattiin lähettämällä sille ping-kyselyä. Kun osoite ensiksi lopetti ja sitten aloitti pingiin vastaamisen uudestaan, voitiin palomuuria alkaa testaamaan. Wild Software Oy:n edustaja testasi omat palvelunsa, ja samaan aikaan toisen yhteistyöyrityksen henkilö testasi heidän ylläpitämiensä palveluiden toimivuuden. Palomuuri alkoi toimia toivotusti ensimmäisellä yrityksellä, ja yhteydet voitiin heti nähdä tilataulusta.

Kaksi päivää palomuurin käyttöönoton jälkeen Copfilterin monit-lisäosa lähetti sähköpostiviestin, jossa se ilmoitti että palvelu oli käynnistynyt uudelleen. Tämän seurauksena palomuurin tilannetta mentiin katsomaan, ja se oli käynnistynyt uudelleen. Vikaselvityksessä ilmeni, että palomuurin UPS-laite oli mennyt rikki, eikä se toiminut kunnolla. Tämän tapahtuman avulla voitiin todeta, että monitorointi työkalu on responsiivinen, ja ilmoittaa palomuurilla tapahtuneesta häiriöstä.

Palomuurin lokeja selatessa pystyttiin havaitsemaan palomuurin olemassaolon tärkeys. Osoitteista ympäri maailmaa pyritään jatkuvasti erilaisten skannereiden ja manuaalisten yrityksien avulla löytämään heikkouksia. Hyökkääjät etsivät käytössä olevia portteja, ja pyrkivät pääsemään näillä sisään verkkoon. Kuvassa 5 voidaan nähdä, kuinka Ecuadorista yritetään epäonnistuneesti muodostaa Telnet-yhteyttä uudelle palomuurille.



KUVA 5. Telnet-yritykset Ecuadorista

5.4 Lopputulokset

Projektin ollessa päätöksessä Terasoft Oy:lla oli käytössä nyt päivitetty, viimeisin versio IPCop-palomuurista, joka toimii toiveiden mukaisesti. Palomuurin toiminnot ovat tehtävänannon mukaiset, ja turvallisuutta pystyttiin myös lisäämään lisäosien muodossa.

Vanhan palomuurin siivous porttienohjauksista, jotka eivät ole enää käytössä, oli tärkeä asia tehdä. Kaikki ylimääräiset porttienohjaukset ovat vain yksi aukko palomuurissa lisää, mitä hyökkääjät voivat käyttää. Lisäosien käyttöönotolla jossain määrin vaatimaton IPCop-palomuuri voitiin parantaa OSI-mallin verkko, kuljetus- ja istuntokerrokselta toimimaan myös sovelluskerroksella. Palomuurin seurantaa voidaan helpottaa valvontalisäosan avulla, joka ilmoittaa sähköpostiin heti, jos palomuurille on tullut jokin ongelma, kuten virus joka on yrittänyt päästä läpi, tai jos palomuuri tai jokin lisäosa ei jostain syystä enää ole toiminnassa.

6 POHDINTA

Työssä onnistuttiin parantamaan Terasoft Oy:n tietoturvaa päivittämällä vanha palomuuriversio uudempaan, ja samalla ottamalla käyttöön tietoturvaa parantavia lisäosia. Yrityksen toimintamallin takia Terasoft Oy ei pääse täysin hyödyntämään kaikkia Copfilterin tarjoamia lisäosia, minkä takia Snort olisi mielestäni ollut riittävä lisäys. Uusi palomuuri otettiin käyttöön ja siihen tuotiin vanhalta palomuurilta aktiivisessa käytössä olevat porttimuunnokset. Lopputuloksena oli toimiva palomuuri, joka vastasi sekä Wild Software Oy:n että Terasoft Oy:n antamia tavoitteita.

Työ saatiin tehdyksi aikataulussaan, ja uusi palomuuri oli toimintakelpoinen ensimmäisellä yliheittokerralla. Kaikki palvelut alkoivat toimimaan ilman jatkotoimenpiteitä, ja Terasoft Oy:n tietoliikenneyhteydet olivat palomuurin yliheiton aikana poissa toiminnasta vain muutaman minuutin. Toimeksiantajan ja Terasoft Oy:n mielestä projektista suoriuduttiin hyvin, ja he olivat tyytyväisiä lopputulokseen.

Vanha palomuuri käytti jatkuvasti kaiken RAM-muistinsa pelkästään perustoimintaan. Palomuurin vaihto uudelle palvelinkoneelle jossa on parempia komponentteja mahdollistaa uusien lisäosien ja palveluiden lisäämisen jatkossa. Myöskin vaara komponenttien satunnaisesta hajoamisesta on pienempi niiden ollessa uudempia.

Koska IPCop-palomuuria kehittävä yhteisö toimii vapaaehtoisesti, sen jatkokehitys ei ole taattua. Työn aikana tehdyssä taustatyössä huomasin, että IPCop-palomuurin aikaisemmat versiot olivat omana aikanaan suositumpia, kuin sen nykyinen versio. Jos tekisin vastaavaa projektia uudelleen, harkitsisin mahdollisuuksien mukaan kaupallista palomuuria, jolloin sen jatkokehitys olisi taatumpaa. Jos kuitenkin halutaan käyttää ilmaista palomuuria, vaihtoehtoisia palomuureja on useita, joiden kehitysyhteisö on ollut aktiivisempi, kuin IPCopilla on ollut viimevuosina. Kun palomuurin uudelleen päivitys on seuraavan kerran ajankohtainen Terasoft Oy:lla, kehottaisin heitä tarkastelemaan onko IPCop pysynyt kehityksen mukana, ja julkaistaanko siihen aktiivisesti päivityksiä jotka vastaavat sen hetken yleisiä vaatimuksia hyvään tietoturvaan. Vanhassa ja tutussa palomuurissa pysyminen voi tuntua turvalliselta, mutta ominaisuuksien ja päivitysten kriittinen tarkastelu on yrityksen turvallisuuden kannalta tärkeämpää.

LÄHTEET

Andrei, A. 2010. Differences between 3 types of proxy servers: normal, transparent and reverse proxy. Luettu 10.10.2015. http://www.webupd8.org/2010/02/differences-between-3-types-of-proxy.html

Avolio, F. 2015. Firewalls and Internet Security, the Second Hundred (Internet) Years. Luettu 5.9.2015. http://www.cisco.com/web/about/ac123/ac147/ac174/ac200/about_cisco_ipj_archive_article09186a00800c85ae.html

Clancey, C., Goldschmitt, H., Kastner, J., Oberlander, E., Walker, P., Sondermann, M. 2015. IPCop v2.0.0 Administration Manual. Luettu 31.8.2015. http://www.ipcop.org/2.0.0/en/admin/html/

Dempster, B. & Eaton-Lee, J. 2006. Configuring IPCop Firewalls. Birmingham: Packt Publishing Ltd.

Forrester Research 2014. Despite scale of Sony hack, internal breaches most common. Luettu 2.9.2015. https://www.forrester.com/Despite+Scale+Of+Sony+Hack+Internal+Breaches+Most+Common/-/E-PRE7486

Free Software Foundation, Inc. 2007. GNU General Public License. Luettu 15.9.2015. http://www.gnu.org/licenses/gpl-3.0.en.html

Ingham, K., Forrest, S. 2002. A History and Survey of Network Firewalls. Luettu 31.8.2015. http://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf

Madlener, M. 2005. Copfilter An add-on for the IPCop Firewall. Luettu 27.10.2015. http://www.copfilter.org/README.pdf

Magalhaes, R. 2008. The Difference Between Application and Session Layer Firewalls. Luettu 31.8.2015. http://www.windowsecurity.com/articles-tutorials/firewalls_and_VPN/Difference-Between-Application-Session-Layer-Firewalls.html

OpenAntiVirus. 2015. Official OpenAntivirus.org Projects. Luettu 27.10.2015. http://www.openantivirus.org/projects.php

Roesch, M. & Green, C. 2015. Snort Users Manual 2.9.7. Luettu 24.10.2015. http://manual.snort.org/

Seeley, D. 1989. A Tour of the Worm. University of Utah. Luettu 31.8.2015. http://www.cs.unc.edu/~jeffay/courses/nidsS05/attacks/seely-RTMworm-89.html

Source Forge. 2015. IPCop Addons. Luettu 24.10.2015. http://sourceforge.net/p/ipcop/wiki/Addons/

Stewart, J. 2010. Network Security, Firewalls, and VPNs. Mississauga: Jones & Bartlett Publishers

Yeo, S. 2003. Personal Firewalls for Adminstrators and Remote Users. New Jersey: Pearson Education Ltd.