Touko Möttönen

PA-3020 -palomuurin käyttöönotto Kajaanin ammattikorkeakoulun tietojärjestelmälaboratoriossa

Tradenomi

Tietojenkäsittely

Kevät 2017

KAJAANIN
AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Tiivistelmä

Tekijä: Möttönen Touko

Työn nimi: PA-3020 -palomuurin käyttöönotto Kajaanin ammattikorkeakoulun tietojärjestelmälaboratoriossa

Tutkintonimike: Tradenomi, tietojenkäsittely

Asiasanat: palomuuri, tietoturva, Palo Alto Networks

Opinnäytetyön tavoitteena oli asentaa Kajaanin ammattikorkeakoulun tietojärjestelmälaboratorion opiskelijoiden hallinnoimaan konesaliympäristöön uusi palomuuri. Aiempi internetyhteys laboratorion konesaliin tuli oppilaitoksen tietohallinnon kautta ja se korvattiin erillisellä valokuituyhteydellä, jotta opiskelijat pääsisivät suorittamaan opintojaan tosielämää vastaavassa ympäristössä.

Perinteinen palomuuri tarkastelee tietoliikennepaketteja ainoastaan niiden IP-osoitteiden ja porttinumeroiden perusteella. Tämän tasoinen tarkastelu ei enää ole riittävää, sillä kehittyneet verkkohyökkäykset voivat naamioida paketteja palomuurisääntöihin sopiviksi ja päästä näin palomuurin ohi. Tässä opinnäytteessä käydään läpi sovelluspalomuurin toimintaa ja sen kykyä torjua jatkuvasti muuttuvia uhkia.

Sovelluspalomuuri pystyy tutkimaan tietoliikennepakettien sisällön ja tunnistamaan käytetyn sovelluksen. Palomuurisääntöjen ei siis tarvitse riippua pelkästään porttinumeroista, vaan sääntöön voidaan liittää palomuurin tuntema sovellus, jolloin palomuuri tunnistaa liikenteen sisällön ja porttien perusteella ja joko hyväksyy tai hylkää sen.

Käytännön osuudessa palomuuri otettiin käyttöön ja sille luotiin suunnitellun mukainen verkkotopologia sekä säännöt. Verkkosuunnitelma ja säännöt luotiin alusta alkaen uudestaan, koska ympäristö muuttui huomattavasti, eikä aikaisempi verkotus vastannut uuden ympäristön tarpeita. Tietojärjestelmälaboratoriossa ei ennestään ollut omaa palomuuria, joten palomuurisäännöt luotiin tarpeiden mukaisesti.

Työn tuloksena tietojärjestelmälaboratorioon saatiin opiskelijoille mahdollisuus tutustua nykyaikaiseen palomuuriin ja samalla mahdollisuus tarjota omia verkkopalveluita internetiin osana opintoja. Tämä on huomattava parannus ja antaa opiskelijoille mahdollisuuden kehittää omaa osaamistaan tosielämää vastaavassa verkkoympäristössä jo opintojen aikana.

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Abstract

Author: Möttönen Touko

Title of the Publication: Installing PA-3020 Firewall to Information Technology Laboratory at Kajaani University of Applied Sciences

Degree Title: Bachelor of Business Administration

Keywords: firewall, information security, Palo Alto Networks

The goal of this Bachelor's thesis was to install a new firewall to the datacenter of the information technology laboratory at Kajaani University of Applied Sciences. The former internet connection to the laboratory came from the university's IT department and it was replaced by a separated connection, that would be equivalent to a real working life environment.

A traditional firewall filters traffic by inspecting only IP-addresses and port numbers from the packets. This kind of inspection is no longer enough, since advanced infiltration methods can disguise a harmful packet in a way that a traditional firewall is unable to identify the threat. This thesis introduces the idea of an application firewall and its ability to intercept continuously developing threats.

An application firewall can inspect the actual content of packets and identify the application that is used. Firewall rules are not solely dependent on port numbers and addresses, but they can also contain a specific application that is known to the firewall. In these situations, the firewall combines the information from port numbers and the content of the package and makes the decision to allow or drop the said packet.

In the practical part of this work, the firewall is installed and configured with planned networking topology and security rules. Network and security rules were created from ground-up, because the environment changed remarkably and the earlier networking topology wasn't suitable for the new environment. The information technology laboratory didn't have a dedicated firewall, so security rules had to be created according to the laboratory's needs.

Students in the information technology laboratory can now carry out hands-on studies in a modern data center infrastructure and are able to offer cloud based services to public internet. This is a remarkable improvement and will allow students to develop their knowledge in real life networking environments during their studies.

Sisällys

1 Johdanto

Palomuuri on yksi tärkeimmistä tietoturvaan vaikuttavista tekijöistä. Yksinkertaistaen sen tehtävänä on rajoittaa liikennöintiä verkkoympäristössä ja estää sekä verkkoon tunkeutuminen, että hallita verkosta ulospäin suuntautuvaa liikennettä. Palomuuri on ensimmäinen laite, joka käsittelee ulkoverkosta tulevaa liikennettä ja sallii tai estää sen.

Palomuurit voidaan luokitella monella eri tavalla, kuten toimintaperiaatteen ja toteutustavan mukaan. Toteutustavan mukaan luokitellut palomuurit jaetaan ohjelmallisiin ja laitepohjaisiin palomuureihin. Ohjelmallisia palomuureja ovat esimerkiksi Windows-käyttöjärjestelmän mukana tuleva palomuuri, ja laitepohjaisia taas erilliset palomuurilaitteet sekä useimmista kuluttajareitittimistä löytyvät palomuurit. Opinnäytetyössäni keskityn palomuurilaitteisiin ja tarkastellaan lyhyesti palomuurien historiaa ja nykyisin käytössä olevia palomuuriratkaisuja.

Opinnäytetyöni teoriaosuudessa tutustun lyhyesti palomuurien historiaan ja toimintaperiaatteisiin. Käytännön osuudessa käyn läpi Palo Alto Networksin valmistaman PA-3020 -palomuurin asennuksen Kajaanin ammattikorkeakoulun(KAMK) tietojärjestelmälaboratorioon. Käyttöönotto on kokonaisuutena huomattavasti laajempi projekti, kuin mitä tämä opinnäytetyö kuvaa. Koko verkkorakenne suunnitellaan alusta alkaen uudestaan helpomman hallittavuuden ja laajennettavuuden saavuttamiseksi. Opinnäytetyö keskittyy kuitenkin kuvaamaan ainoastaan palomuurin käyttöönoton ja käsittelee verkotusta vain pintapuolisesti tuottaakseen lukijalle käsityksen kokonaisuudesta.

2 Tarve palomuurille

Internetin syntyessä, 1980-luvulla verkko suunniteltiin tiedon jakaminen edellä. Käyttäjiä tuolloin oli pienehkö määrä ja se koostui lähinnä tutkijoista ja korkeakouluista. Internetiin pääsy oli rajatulla osalla kansasta ja kotitietokoneet olivat kehittymättömiä, eikä niissä ollut verkko-ominaisuuksia. Tästä syystä tietoturvaan ei ollut tarpeellista kiinnittää huomiota ja sitä pidettiin tarpeettomana. [1, p. 4]

1990-luvun alussa internet alkoi kasvaa kaupallisen kiinnostuksen myötä ja pelkän tiedon jakamisen ohelle tuli tarve suojella omia, esimerkiksi liikesalaisuuksiin, liittyviä dokumentteja. Käyttäjämäärän myötä luonnollisesti myös epärehellisten ja pahantahtoisten osallistujien määrä kasvoi. TCP/IP protokollia ei oltu suunniteltu soveltumaan tietoturvan takaamiseen, vaan tarvittiin uusia keinoja. [1, p. 5]

Yhtenä ratkaisuna otettiin käyttöön palomuurit, jotka suodattivat ulkopuolisesta verkosta tulevaa liikennettä sisäisten sääntöjensä mukaan ja pyrkivät näin estämään ei-toivotut yhteydet. Alkuvaiheessa ei yleensä rajoitettu ulospäin meneviä yhteyksiä. [2, p. 6]

3 Palomuurit

3.1 Ensimmäiset palomuurit

1980-luvun lopulla suurempia lähiverkkoja ryhdyttiin pilkkomaan pienempiin paloihin reitittimien avulla. Tarkoituksena oli ehkäistä laajan verkon aiheuttamia ongelmia, esimerkiksi suurta liikennemäärää ja mahdollisia ongelmia uusien sovellusten käyttöönotossa. Tässä vaiheessa palomuurin tehtävänä ei ollut suojata hyökkäyksiltä vaan ehkäistä tahattomasti aiheutettuja ongelmia. [3]

1990 -luvun alussa otettiin käyttöön ensimmäiset palomuurit tietoturvatarkoituksessa. Palomuurin pohjana toimi reititin, jolle laadittiin säännöt pakettien välitykseen. Säännöt olivat yksinkertaisia, kuten ”Salli kaikki liikenne sisäverkosta ulos” ja ”Estä seuraavia laitteita liikennöimästä sisäverkkoon”. Tällainen toteutus on sinällään tehokas, mutta vaatii jatkuvaa sääntöjen muokkaamista ja on vaikea saada toimimaan virheettömästi. [3]

3.2 Perinteinen palomuuri

Palomuurit voidaan toimintatavan mukaisesti jakaa kolmeen pääryhmään: tilattomiin, tilallisiin ja sovelluspalomuureihin. Palomuurin toiminnan ymmärtämiseksi on tunnettava TCP ja UDP protokollien perusteet ja tietoliikenteen OSI-malli.

UDP-protokolla on yksinkertainen ja kevyt tiedonsiirtomenetelmä, jossa tietokone tai muu verkkolaite voi lähettää toiselle laitteelle viestin ilman ennakkovalmisteluja. UDP ei sisällä varmennusta siitä, onko paketti mennyt perille, eikä myöskään takaa samaan lähetykseen sisältyvien pakettien toimitusjärjestystä. UDP-protokollan yhteydessä lähettäjä ei voi tietää onko paketti mennyt perille, jos vastaanottaja ei erikseen ilmoita paketin saapumisesta. [4, p. 40]

TCP-protokolla on kehittyneempi tiedonsiirtomenetelmä, jossa ennen varsinaisen sisällön lähettämistä viestivät laitteet muodostavat keskenään yhteyden. Yhteydenmuodostuksen ansiosta vastaanottava laite osaa odottaa saapuvaa pakettia ja se kykenee lähettämään kuittauksen lähettäjälle, kun paketti saapuu. Lähettävä laite odottaa varmistuksen edellisen paketin toimituksesta, ennen seuraavan lähettämistä. TCP-protokollaa käyttäessä

paketit saapuvat lähetysjärjestyksessä vastaanottajalle ja lähettävä laite tietää varmasti, että paketti on päätynyt perille. [4, p. 40]

ISO/OSI -malli kuvaa tiedonsiirtoprotokollien yhteistoimintaa. Malli koostuu seitsemästä kerroksesta, joista jokainen tarjoaa palveluja ylemmälle kerrokselle ja käyttää alemman kerroksen palveluja. Perinteinen palomuuri toimii mallin kerroksilla kolme ja neljä, eli verkko- ja kuljetuskerroksilla. Moderni palomuuri kykenee tarkastelemaan ja tarvittaessa puuttumaan myös ylempien kerrosten toimintaan. [5, p. 10, 6, p. 6]

Layer	Function	Example
Application (7)	Services that are used with end user applications	SMTP,
Presentation (6)	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
Session (5)	Establishes/ends connections between two hosts	NetBIOS, PPTP
Transport (4)	Responsible for the transport protocol and error handling	TCP, UDP
Network (3)	Reads the IP address form the packet.	Routers, Layer 3 Switches
Data Link (2)	Reads the MAC address from the data packet	Switches
Physical (1)	Send data on to the physical wire.	Hubs, NICS, Cable

Kuva 1: ISO/OSI-malli. Palomuuri toimii mallin kerroksilla 3 ja 4. Lähde: www.blackmoreops.com

3.2.1 Tilaton palomuuri

Tilaton palomuuri, eli pakettisuodatin, voidaan ajatella reitittimenä, joka tarkastaa kauttaan kulkevan tulevan ja lähtevän liikenteen. Suodatin vertaa tietoliikennepaketin tietoja

määriteltyihin sääntöihin ja tekee sääntöjen perusteella päätöksen välitetäänkö paketti eteepäin vai tuhotaanko se.

Pakettisuodatin ei tarkastele lainkaan paketin sisältöä, vaan ainoastaan sen tietoja ISO-mallin kolmannella ja neljännellä kerroksella. Näitä ovat lähettäjän ja vastaanottajan IP-osoitteet, käytettävät portit ja protokollat. Pakettisuodattimella voidaan esimerkiksi sallia liikenne ulkoverkosta sisäverkon tietokoneen tiettyyn porttiin. [1, p. 56]

Pakettisuodatuksen suurin etu on nopeus. Koska palomuuri ei tarkasta sisältöä, se kykenee toimimaan lähes yhtä nopeasti kuin tavallinen reititin. Laitteisto on myös yksinkertainen ja hinnaltaan edullinen. Haittapuolena tietoturva on heikompi kuin tilallisen ja sovelluspalomuurin. Pakettisuodatin on erityisen arka lähettäjän IP-osoitteen väärentämiselle. [1, p. 56]

3.2.2 Tilallinen palomuuri

Tilallinen palomuuri on kehittyneempi versio pakettisuodattimesta. Se pitää pakettien osoitteiden tarkastuksen lisäksi kirjaa auki olevista TCP-yhteyksistä ja vertaa saapuvia ja lähteviä paketteja tähän kirjanpitoon. Kun sovellus avaa TCP-yhteyden palomuuri tallentaa yhteyden taulukkoon ja vertaa saapuvia paketteja aiemmin saman yhteyden aikana lähetettyihin paketteihin. Kun yhteys päättyy, palomuuri poistaa sen kirjanpidostaan, eikä enää hyväksy siihen liittyviä paketteja. [1, p. 56]

UDP-protokolla on yhteydetön, eli yhteyteen osallistuvat laitteet eivät suorita kättelyä vaan lähettävät paketteja suoraan toisilleen. Tilallinen palomuuri kykenee kuitenkin seuraamaan UDP-protokollan paketteja. Kun sisäverkon laite ottaa yhteyttä vähemmän turvalliseen verkkoon käyttäen UDP-protokollaa, palomuuri kirjaa tämän ylös ja hyväksyy saapuvat paketit ainoastaan, jos ne täsmäävät lähteneen paketin tietoihin. [1, p. 56]

Tilallinen palomuuri kykenee myös tarpeen mukaan sallimaan paketteja normaalisti suljettuihin portteihin, kuten esimerkiksi FTP-protokollan yhteydessä, jossa yhteys otetaan aluksi oletusporttiin 21, mutta vastausdata saapuu portin 20 kautta. Jos palomuurilla ei ole tietoa FTP-yhteyden alkamisesta, se normaalisti hylkäisi porttiin 20 saapuvan paketin. [1, p. 57]

3.3 Sovelluspalomuuri

Kehittynein tällä hetkellä käytössä oleva palomuurityyppi on sovelluspalomuuri eli seuraavan sukupolven palomuuri (Next-Generation Firewall). Sovelluspalomuurin määritteleminen on hankalampaa kuin perinteisten palomuurien, koska monilla valmistajilla on käytössään omia suojattuja teknologioitaan, jolloin tuotteen eroavat ominaisuuksiensa osalta jonkin verran toisistaan. Konsulttiyhtiö Gartnerin määritelmän mukaan sovelluspalomuurin tulee pystyä havaitsemaan sovelluskohtainen hyökkäys, suodattamaan liikennettä käytetyn sovelluksen perusteella ja purkamaan SSL-salattu liikenne. Sovelluspalomuuri kykenee myös toimimaan perinteisen palomuurin tavoin ja suodattamaan liikennettä ilman pakettien sisällön tarkastelua. [6, p. 15]

Sovelluspalomuuri toimii OSI-mallin kolmannen ja neljännen kerroksen lisäksi kerroksilla viisi, kuusi ja seitsemän. Se siis tarkastelee kokonaisvaltaisesti pakettien sisältöä pelkkien otsikkotietojen lisäksi. Sovelluspalomuuri vertaa paketin varsinaista sisältöä sen käyttämään tiedonsiirtoprotokollaan ja portteihin kyetäkseen selvittämään paketin turvallisuuden. Sovelluspalomuurit voivat myös hyödyntää jatkuvasti päivittyvää tietoa, kuten Palo Alto Networksin käyttämä WildFire-tietokanta, johon kerätään tietoa haitallisista tiedostoista. [6, p. 15, 7]

Sovelluspalomuuri on kehittyneen tekniikkansa takia kallein palomuurivaihtoehto, mutta myös turvallisin. Hankintahinnan lisäksi myös jatkuvasti päivittyvät suojaustietokannat vaativat maksullisen lisenssin, mikä aiheuttaa kustannuksia koko laitteen elinkaaren ajan. Hinnan lisäksi haittapuolena on verkkoliikenteen hidastuminen yksityiskohtaisen tarkastelun seurauksena. [1, p. 57, 2, p. 19]

4 Lähtötilanne

4.1 Toimeksiantajan esittely

Käytännön osuus toteutettiin Kajaanin ammattikorkeakoulun tietojärjestelmälaboratoriossa, joka toimii tietojärjestelmien opiskelijoiden pääasiallisena oppimisympäristönä. Tietojärjestelmälaboratoriossa on 30 Windows-työasemaa ja opiskelijoiden hallinnassa toimiva konesali.

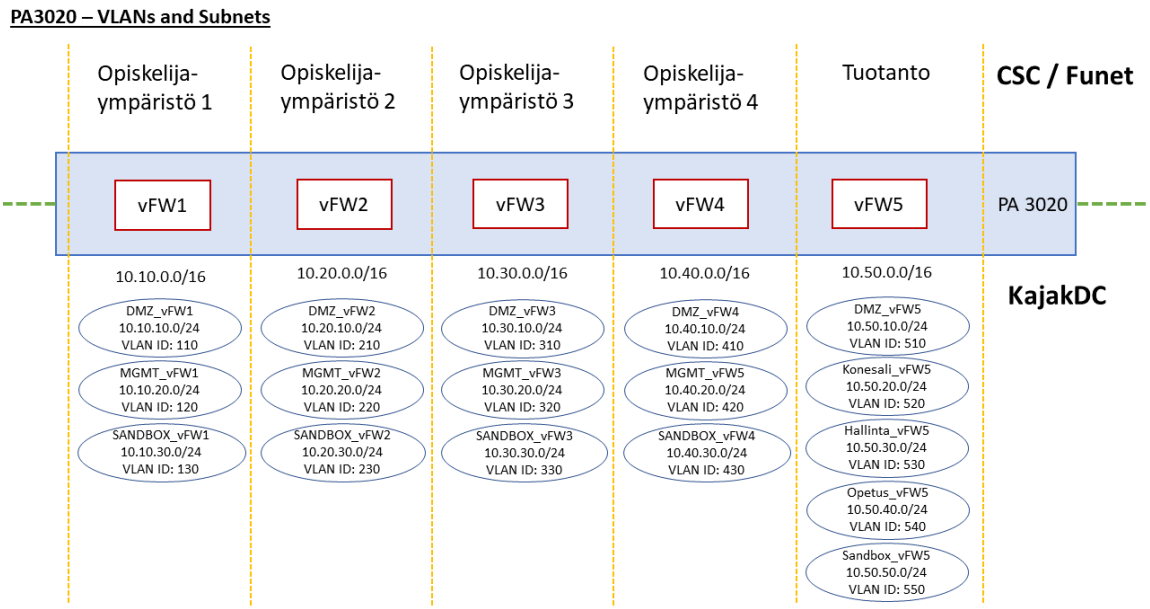
Laboratorion verkkoyhteys toimi aiemmin KAMKin tietohallinnon kautta ja se oli osa koko organisaation yhteistä yhteyttä. Tämä aiheutti rajoituksia opiskelijoiden mahdollisuuksia luoda palveluita julkisesti internetiin saataville. Suuremman organisaation osana oleminen ei myöskään mahdollistanut omien konfiguraatioiden tekoa tai palomuurin lokitietoihin tutustumista.

Syksyllä 2016 tietojärjestelmälaboratorioon päätettiin hankkia oma 1Gbps:n nopeudella toimiva verkkoyhteys CSC:n ylläpitämästä FUNET-verkosta. Samalla KAMK hankki laboratorion käyttöön Palo Alto Networksin PA-3020 -palomuurin.

4.2 Verkko

Palomuurin vaihtamisen yhteydessä myös konesalin ja siihen liittyvän tietojärjestelmälaboratorion tietoverkko suunniteltiin kokonaan uudelleen. Uudessa suunnitelmassa pyrittiin ottamaan huomioon tietoturva, mutta silti sallia opiskelijoille mahdollisuus hyödyntää olemassa olevaa ympäristöä mahdollisimman tehokkaasti.

Verkko koostuu viidestä erillisestä osasta, joista neljä on varattu opiskelijoiden projekteille ja yksi tuotantokäyttöön. Tuotantoympäristö sisältää konesalin ja työasemien kannalta välttämättömät palvelut, kuten palvelinten hallintaosoitteet, Active Directory - ja DHCP-palvelimet sekä työasemat. Opiskelijaympäristöjen käyttö syntyy opiskelijoiden oman tekemisen kautta ja niiden hallinnointi on osa opintoja, joten tässä projektissa keskityttiin tuotantoympäristön toimintaan saattamiseen.



Kuva 2: DC-laboratorion verkkosuunnitelma, laatijat: Koskelo, Mikko ja Möttönen, Touko

Yllä olevassa kuvassa on esitetty yleinen verkkorakenne, jossa keltaisin katkoviivoin erotellut virtuaalipalomuurit jakavat opiskelijaympäristöt ja tuotannon toisistaan erillisiin kokonaisuuksiin. Sinireunaisin soikioin on esitetty palomuurin verkkoalueet ja niihin liittyvät IP-osoitteet sekä VLAN-verkot.

5 Palomuurin käyttöönotto

5.1 Asennus ja testiympäristö

Käyttöönotto aloitettiin asentamalla palomuuri mukana tulleiden kiinnikkeiden avulla paikalleen konesalin palvelinkaappiin. Laitteen paikalleen sijoittamisen jälkeen se käynnistettiin ja otettiin yhteys palomuurin hallintaporttiin kannettavalla tietokoneella. Oletusasetuksena palomuurilla on osoitteenaan 192.168.1.1/24, joten tietokoneen osoite valittiin samasta verkosta ja otettiin selaimella yhteys palomuurin hallintakäyttöliittymään.

Kirjautumisen jälkeen pääkäyttäjän oletussalasana vaihdettiin toiseen. Käyttäjän salasanahallinta löytyy laitteen “Device”-välilehdeltä, kohdasta “Administrators”. Tunnuksen vaihtamisen yhteydessä vaihdettiin myös palomuurin hallintaportin IP-osoite, yhdyskäytävä ja verkon peite, jotta laitetta olisi mahdollista hallita myös konesalin ulkopuolelta samasta sisäverkosta. Hallintaportin asetukset löytyvät “Device”-välilehdeltä, “Setup”-kohdasta otsikolla “Management Interface Settings”. Uudet asetukset otettiin käyttöön painamalla “Commit”-painiketta käyttöliittymässä.

Hallintaportin IP-osoitteen vaihdon myötä palomuurin hallintaportti voitiin kytkeä konetilan kytkimeen ja hoitaa hallinta työasemalta konesalin ulkopuolelta. Alkuvaiheessa oli mahdollisuus tutustua palomuurin toimintoihin ja konfiguroida palomuuria erillään muusta verkosta, joten tässä vaiheessa palomuuri liitettiin ainoastaan ulkoverkkoon ja testikäyttöön otettuun kytkimeen, johon oli edelleen liitetty kolme palvelinta testausympäristöksi.

Testiympäristö konfiguroitiin vastaamaan yksittäistä virtuaalipalomuuria varsinaisen ympäristön verkkosuunnitelman mukaisesti, jolloin saatiin mahdollisuus kokeilla sääntöjen luomista ja toimintaa käytännössä. Palomuurin asetusten säätämiseen perehdytään tarkemmin varsinaisen ympäristön käyttöönoton yhteydessä.

Testivaiheessa ei havaittu ongelmia ja palomuurin toiminta tuli tutuksi, mikä helpotti huomattavasti varsinaisen ympäristön asetusten määrittämistä ja käyttöönottoa.

5.2 Palomuurin ohjelmiston ja uhkatietojen päivittäminen

Palomuurin saapuessa siinä oli käytössä PAN-OS -käyttöjärjestelmän vanha 6.1.0 ohjelmistoversio. PAN-OS on Palo Alto Networksin kehittämä käyttöjärjestelmä, jota käytetään yrityksen sovelluspalomuureissa.

Palomuuri lataa päivitykset oletuksena hallintaportin kautta ja tätä porttia käytettiin uusien ohjelmistoversioiden saatavuuden tarkistamiseen. Uusin saatavilla oleva versio oli 7.1.9 ja se ladattiin palomuuriin. Lataamisen lisäksi päivitys tulee vielä erikseen asentaa palomuuriin ja päivittäminen vaatii laitteen uudelleenkäynnistyksen. Palomuurin päivittäminen löytyy “Device”-välilehdeltä kohdasta “Software”. Tämä projektin aikana palomuurille ei tullut uusia ohjelmistoversioita.

Palo Alto tarjoaa käyttöjärjestelmäpäivitysten lisäksi jatkuvasti päivittyviä uhka- ja sovellustunnisteita. Nämä päivitykset on jaettu kategorioihin ja niiden saatavuus riippuu käytössä olevista lisensseistä. Tässä työssä käyttöön otettiin seuraavat:

- **Virustorjunta (Antivirus)**: Päivitykset viruksiksi luokiteltavien ohjelmien tunnistamiseen käytettäviä piirteitä. Virustorjuntatietokanta päivittyy päivittäin, jos uusia viruksia tai tunnettujen virusten uusia versioita havaitaan. [8]

- **Sovellukset ja uhat (Applications and Threats)**: Päivitetyt tiedot liikennöivien sovellusten ja uhkaavan liikenteen tunnistamista varten. Tiedot päivittyvät viikoittain. [8]

- **WildFire**: WildFire on Palo Alton oma, pilvipalveluun perustuva uhkatietokanta, jonka tarkoituksena on pystyä reagoimaan lähes välittömästi uusin turvallisuusuhkiin. WildFire lähettää palomuurille saapuvan, tuntemattoman tiedoston Palo Alton pilvipalveluun tarkempaa analyysiä varten. Pilvipalvelussa tiedosto testataan virtuaalisessa ja fyysisessä ympäristössä ja lisätään tarvittaessa tietokantaan haitalliseksi merkittynä. Uudet WildFire-tunnisteet julkaistaan viiden minuutin välein. [8] [7]

“Device”-välilehden “Dynamic updates”-kohdasta päästiin säätämään palomuurin liikenteen suodatukseen liittyvien tietokantojen päivitystiheyttä. Virustorjunta asetettiin päivittymään tunnin välein, sovellukset ja uhat kerran päivässä ja WildFire-analyysin tulokset 15 minuutin välein.

5.3 Virtuaalipalomuurit

Virtuaalipalomuurit (Virtual Systems) ovat yhden fyysisen palomuurin sisällä toimivia, toisistaan erillisiä loogisia kokonaisuuksia. Virtuaalipalomuurit jakavat fyysisen palomuurin resurssit, kuten laskentatehon ja liitynnät, mutta toimivat toisistaan täysin erillisinä kokonaisuuksina. Virtuaalipalomuureja käyttämällä on mahdollista eritellä esimerkiksi kahden eri organisaation tai osaston liikenne täydellisesti toisistaan ilman tarvetta useammalle fyysiselle palomuurille. Tässä projektissa virtuaalipalomuurien avulla eriteltiin tuotantoympäristö opiskelijoille tarkoitetuista ympäristöistä. [9] [10]

Virtuaalipalomuurit mahdollistavat käyttäjätunnusten helpon hallinnan, sillä tietylle tunnukselle voi antaa oikeudet määrättyihin järjestelmiin. Tässä projektissa tämä on erittäin tärkeää, koska opiskelijoille voidaan antaa täysi hallinta osaan virtuaalijärjestelmistä, mutta samalla voidaan varmistaa että tuotantoympäristöä ei kuka tahansa pysty muuttamaan. Samoin mahdollinen verkkoon tunkeutuminen rajoittuu yhteen virtuaalijärjestelmään.

Virtuaalipalomuurien luominen ja asetusten muuttaminen on “Device”-välilehdellä kohdassa “Virtual Systems”. Uuden virtuaalijärjestelmän luominen onnistuu alareunan “Add” painikkeesta, josta avautuu uusi valikko tarvittavien tietojen syöttämiseksi. Virtuaalipalomuurille tulee antaa kokonaislukuna ID, lisäksi hallinnan helpottamiseksi sille voi myös syöttää kirjaimista ja numeroista koostuvan nimen. Lisäksi on mahdollista valita, mitkä virtuaalijärjestelmät pystyvät viestimään keskenään.

Virtuaalipalomuurille on mahdollista määrittää, kuinka paljon se saa käyttää fyysisen palomuurin resursseja. Tämä mahdollistaa resurssien jakautumisen tasaisesti kaikkien virtuaalijärjestelmien kesken tilanteessa, jossa joku käyttäjä pyrkii viemään kapasiteettia toisilta. Tässä vaiheessa portteja tai virtuaalireitittimiä ei vielä oltu konfiguroitu, joten niitä ei lisätty virtuaalipalomuureihin vaan ainoastaan luotiin tyhjät järjestelmät valmiiksi.

5.4 Liityntöjen konfigurointi

Palomuuriin ryhdyttiin luomaan suunnitelman pohjalta tarvittavat verkot. Laite sisältää 12 ethernet-porttia ja kahdeksan SFP-kuituporttia. SFP (Small Form-factor Pluggable) on valokuituyhteyksien päätelaitteissa käytettävä lähetin-vastaanotin. Se mahdollistaa erilaisten valokuitutyyppien käytön yhdessä laitteessa vain SFP-moduulin vaihtamalla, ilman tarvetta vaihtaa koko piirilevyä. [11]

Funet-yhteys tuli konesaliin valokuidulla, joten se kytkettiin palomuurin kuituporttiin. Palveluntarjoajalta saatiin käyttöön useita julkisia IP-osoitteita, jotka oli ennalta määrätty kuuluvaksi tietylle virtuaalipalomuurille. Erittely eri virtuaalipalomuurien välillä toteutettiin VLAN-merkintöjen avulla.

VLAN (virtual local area network) on verkkoteknologia, joka mahdollistaa fyysisen ja loogisen verkkotopologian erottamisen toisistaan. VLAN teknologiaa käytetään laajemmissa verkoissa pienentämään verkkojen kuormitusta yleislähetyksistä ja rajoittamaan tai sallimaan käyttäjien pääsy tietyille verkkolaitteille. Verkkolaitteessa määritellään portille jokin VLAN-tunniste, jonka jälkeen siihen kytketty laite pystyy lähettämään viestejä ainoastaan laitteille, jotka ovat samassa VLAN-verkossa. Toisiin VLAN-verkkoihin osoitettu liikenne reititetään, tässä projektissa palomuuri toimii myös reitittimenä. [10, p. 433]

Ethernet | VLAN | Loopback | Tunnel

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Virtual System	Security Zone
ethernet1/1	Layer3			none	none	Untagged	none	Opiskelijaymp4	none
ethernet1/1.110	Layer3	Mgmt-ping		10.10.10.1/24	vr-vsys1-opiskelijaymp1	110	none	Opiskelijaymp1	DMZ-vsys1
ethernet1/1.120	Layer3	Mgmt-ping		10.10.20.1/24	vr-vsys1-opiskelijaymp1	120	none	Opiskelijaymp1	MGMT-vsys1
ethernet1/1.130	Layer3	Mgmt-ping		10.10.30.1/24 10.10.31.1/24	vr-vsys1-opiskelijaymp1	130	none	Opiskelijaymp1	Sandbox-vsys1
ethernet1/1.210	Layer3	Mgmt-ping		10.20.10.1/24	vr-vsys2-opiskelijaymp2	210	none	Opiskelijaymp2	DMZ-vsys2
ethernet1/1.220	Layer3	Mgmt-ping		10.20.20.1/24	vr-vsys2-opiskelijaymp2	220	none	Opiskelijaymp2	MGMT-vsys2

Kuva 3: Palomuurin liityntä ja aliliityntöjä

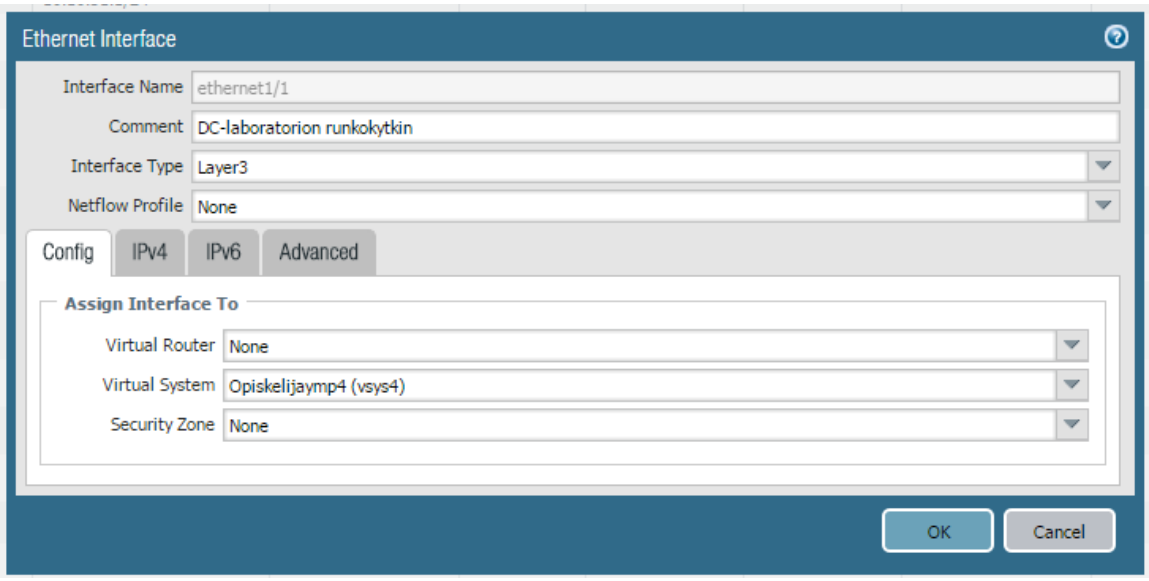
Laitteen liityntöjen konfigurointi onnistuu hallintanäkymän “Network”-välilehdeltä, “Interfaces”-kohdasta. Internettiin yhteydessä olevaan SFP-liityntään konfiguroitiin tyypiksi “Layer3” ja määriteltiin sen kuuluvan laitteen ensimmäiseen virtuaalipalomuuriin. ”Layer 3”-tyyppinen liityntä toimii ISO/OSI-mallin kolmannella, eli verkkokerroksella. Tällainen liityntä hoitaa liikennöinnin IP-osoitteen perusteella ja kykenee reitittämään liikennettä. Muita tietoja liitynnälle ei määritelty, koska yhden fyysisen liitynnän kautta kulkee moneen

eri verkkoon kuuluvaa verkkoliikennettä. Liikenne saadaan eroteltua oikeaan virtuaalipalomuuriin luomalla liitynnän yhteyteen aliliityntä (subinterface).

Aliliitynnän luominen tapahtuu “Add Subinterface” painikkeesta. Liitynnän tyyppi määräytyy sen pääliitynnän mukaisesti, eli tässä tapauksessa “Layer3”. Aliliitynnälle tulee määrittää lisäksi tunnistenumero, tässä tapauksessa tunnistenumerona käytettiin liityntään kuuluvan VLAN:in numeroa. VLAN-numero merkitään myös “Tag”-kenttään, jotta palomuuri osaa ohjata liikenteen oikeaan paikkaan.

Aliliitynnälle valittiin käyttöön ensimmäinen virtuaalipalomuuri ja määriteltiin IP-osoitteeksi palveluntarjoajan antama kiinteä IP-osoite. Lisäksi “Advanced” välilehdeltä luotiin uusi hallintaprofiili “Management Profile”, jossa sallittiin liitynnälle ping-viesteihin vastaaminen. Muut asetukset jätettiin tässä vaiheessa tyhjiksi tai oletusasetuksille. Sama prosessi toistettiin kaikille virtuaalijärjestelmille, jolloin jokainen niistä kykeni vastaanottamaan sille kuuluvan liikenteen.

Sisäverkkoon palomuuri yhdistettiin runkokytkimen kautta ethernet-kaapelilla. Tämä liityntä määriteltiin edellisen tavoin, eli luotiin aliliityntä kaikille tarvittaville VLAN-verkoille. Kaikki sisäverkkoon suuntautuva liikenne hoidetaan yhden liitynnän kautta runkokytkimelle, joka edelleen kuljettaa paketit oikeaan paikkaan oman konfiguraationsa mukaisesti.



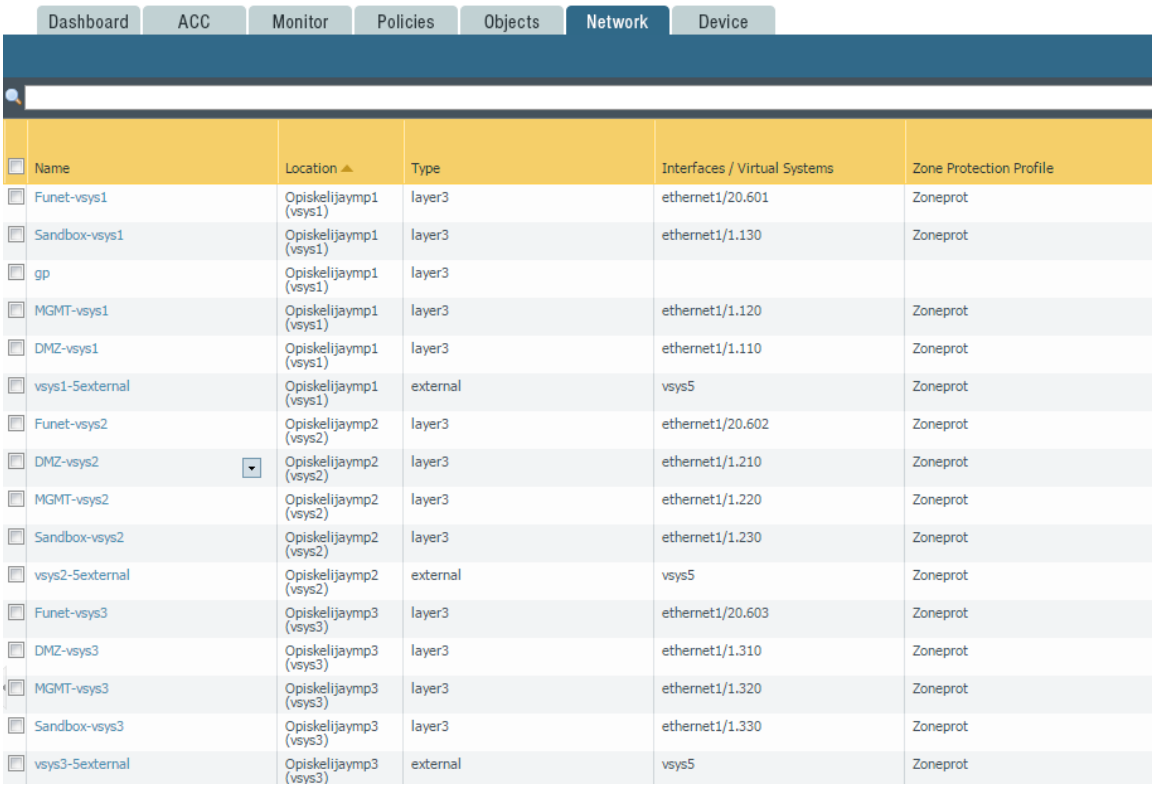
Kuva 4: Liitynnän luominen

Sisäverkossa käytettiin yksityistä 10.0.0.0/8 IP-osoiteavaruutta, jolla pystyttiin luomaan loogisesti jatkuva numerointi verkon eri osien välille. Esimerkiksi ensimmäiseen virtuaalipalomuuriin kuuluvat osoitteet ovat 10.10.0.0/16 ja toiseen 10.20.0.0/16. Verkkoalueet kunkin järjestelmän sisällä määriteltiin kolmannen oktetin avulla, esimerkiksi 10.10.20.0/24. Tällöin jokaiseen alueeseen jäi 254 vapaata IP-osoitetta laitteille ja alueiden väliin jäi reilusti tilaa, johon verkkoja voi tulevaisuudessa laajentaa, jos tarvetta ilmenee. Tässä vaiheessa ei pidetty tarpeellisena tehdä ylisuuria verkkoja ”kaiken varalta”, vaan päädyttiin mieluummin ratkaisuun, joka mahdollistaa helpon verkon muokkaamisen tulevaisuudessa.

Jokaiselle aliliitynnälle määriteltiin VLAN-verkon lisäksi sisäverkon IP-osoite suunnitelman mukaisesti. Nämä aliliityntöjen osoitteet toimivat kyseisen liitynnän oletusyhdyskäytävinä muihin verkkoihin.

5.5 Verkkoalueet

Verkkoalue (Security zone) on yhdestä tai useammasta liitynnästä koostuva looginen kokonaisuus, jonka avulla palomuuri valvoo ja ohjaa verkkoliikennettä. Hyvin suunnitellut verkkoalueet mahdollistavat liikenteen suodattamisen ja tärkeiden palveluiden turvaamisen. Verkkoalueilla on tärkeä rooli palomuurin sääntöjen luomisessa, sillä käytännössä ei ole mahdollista määrittää sääntöjä kaikelle liikenteelle IP-osoitteen tarkkuudella vaan verkko on jaettava kokonaisuuksiin, joille määritellään aluekohtaiset liikennöintisäännöt. [12]

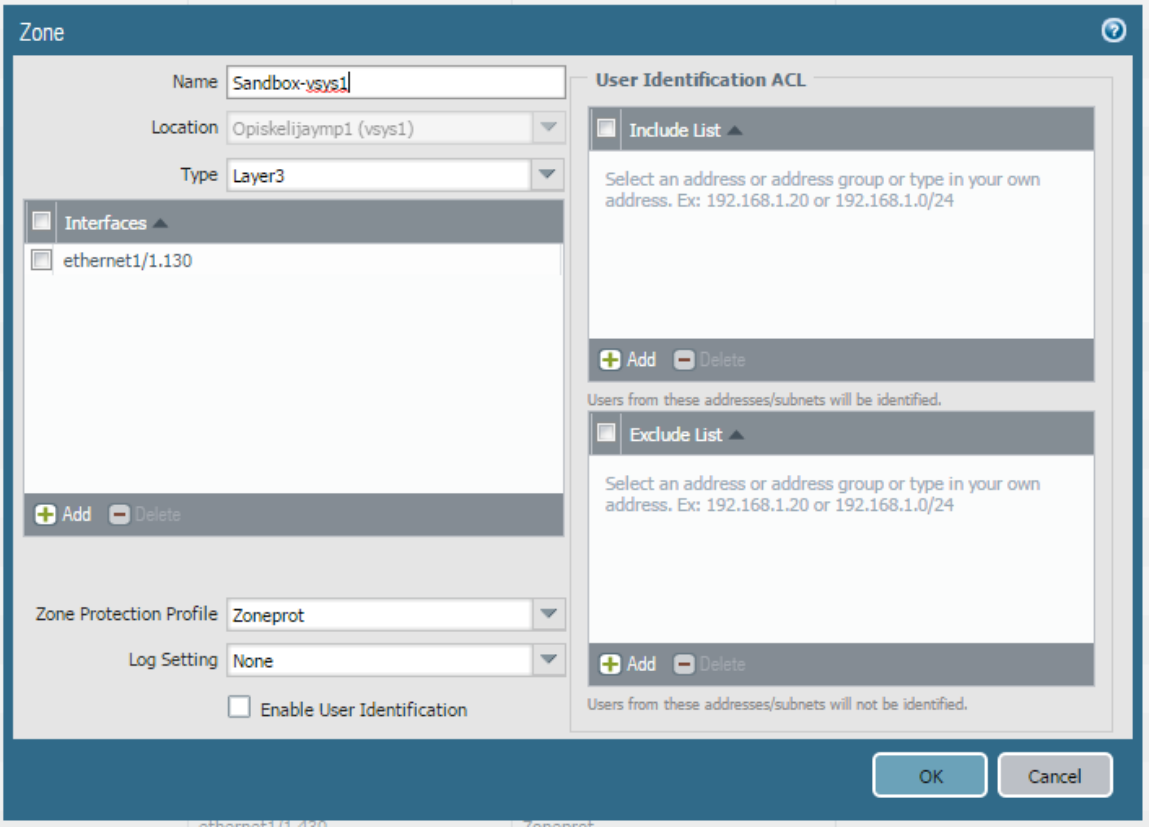


Name	Location	Type	Interfaces / Virtual Systems	Zone Protection Profile
Funet-vsys1	Opiskelijaymp1 (vsys1)	layer3	ethernet1/20.601	Zoneprot
Sandbox-vsys1	Opiskelijaymp1 (vsys1)	layer3	ethernet1/1.130	Zoneprot
gp	Opiskelijaymp1 (vsys1)	layer3		
MGMT-vsys1	Opiskelijaymp1 (vsys1)	layer3	ethernet1/1.120	Zoneprot
DMZ-vsys1	Opiskelijaymp1 (vsys1)	layer3	ethernet1/1.110	Zoneprot
vsys1-5external	Opiskelijaymp1 (vsys1)	external	vsys5	Zoneprot
Funet-vsys2	Opiskelijaymp2 (vsys2)	layer3	ethernet1/20.602	Zoneprot
DMZ-vsys2	Opiskelijaymp2 (vsys2)	layer3	ethernet1/1.210	Zoneprot
MGMT-vsys2	Opiskelijaymp2 (vsys2)	layer3	ethernet1/1.220	Zoneprot
Sandbox-vsys2	Opiskelijaymp2 (vsys2)	layer3	ethernet1/1.230	Zoneprot
vsys2-5external	Opiskelijaymp2 (vsys2)	external	vsys5	Zoneprot
Funet-vsys3	Opiskelijaymp3 (vsys3)	layer3	ethernet1/20.603	Zoneprot
DMZ-vsys3	Opiskelijaymp3 (vsys3)	layer3	ethernet1/1.310	Zoneprot
MGMT-vsys3	Opiskelijaymp3 (vsys3)	layer3	ethernet1/1.320	Zoneprot
Sandbox-vsys3	Opiskelijaymp3 (vsys3)	layer3	ethernet1/1.330	Zoneprot
vsys3-5external	Opiskelijaymp3 (vsys3)	external	vsys5	Zoneprot

Kuva 5: Verkkoaluenäkymä

Verkkoalueet luodaan “Network”-välilehden kohdasta “Zones”. Alueet luodaan alareunan “Add”-painikkeella. Jokaiselle virtuaalipalomuurille luotiin turvaton alue ulkoverkon puoleiseen liityntään ja verkkosuunnitelman mukaiset sisäverkon alueet. Kaikki nyt luodut alueet ovat tyypiltään “Layer3”.

Yhdellä verkkoalueella voi olla useita verkkoliityntöjä, mutta yksi liityntä ei voi kuulua kuin yhteen alueeseen. Tässä suunnitelmassa jokainen alue sisältää vain yhden verkkoliitynnän ja jokainen alue oli myös erillinen aliverkko ja sillä oli oma VLAN.



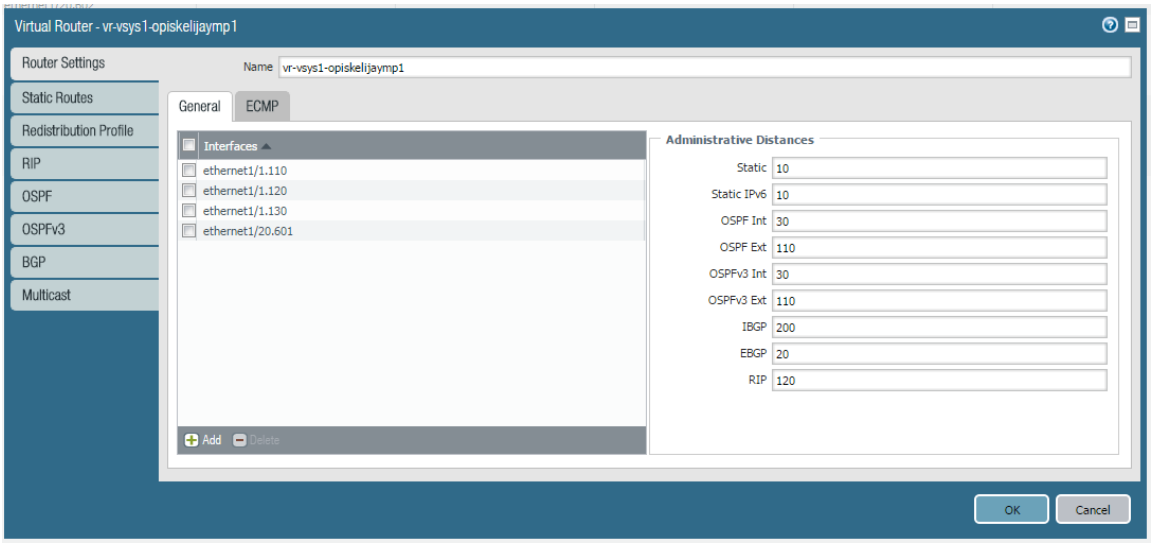
Kuva 6: Verkkoalueen luominen

Virtuaalipalomuurit eivät pysty normaalisti lähettämään paketteja toisilleen vaan kaiken liikenteen tulee kulkea ulkoverkon kautta. Palomuuriin on mahdollista luoda erillinen “External Zone” eli ulkoinen alue, jonka kautta on mahdollista sallia virtuaalipalomuurien välinen liikenne. Ulkopuolista aluetta luotaessa valitaan alueen tyypiksi “External” jolloin käytettävän liitynnän sijasta on mahdollista valita mille virtuaalipalomuureille kyseisen alueen kautta pystyy liikennöimään. Ulkopuoliset alueet luotiin kaikille palomuureille ja näkyvyydet määriteltiin niin, että tuotannon virtuaalipalomuuri pystyy liikennöimään kaikkiin luotuihin virtuaalipalomuureihin, mutta muut ainoastaan tuotannon virtuaalipalomuuriin.

5.6 Virtuaalireitittimet

Jokaiselle virtuaalipalomuurille tarvittiin oma virtuaalireititin hoitamaan pakettien reititystä aliverkkojen, eli tässä tapauksessa samalla myös alueiden välillä. Virtuaalireitittimen luonti onnistuu “Network”-välilehden “Virtual Routers”-kohdasta. Alareunan “Add” painiketta painamalla avautuvaan valikkoon syötetään reitittimen nimi ja valitaan siihen kuuluvat verkkoliitynnät. Kaikkien liityntöjen tulee olla samasta virtuaalijärjestelmästä. Tässä

projektissa käytössä oli vain yksi reititin jokaista virtuaalipalomuuria kohti, siihen kuuluvaksi valittiin kaikki kyseisen virtuaalipalomuurin verkkoliitynnät.



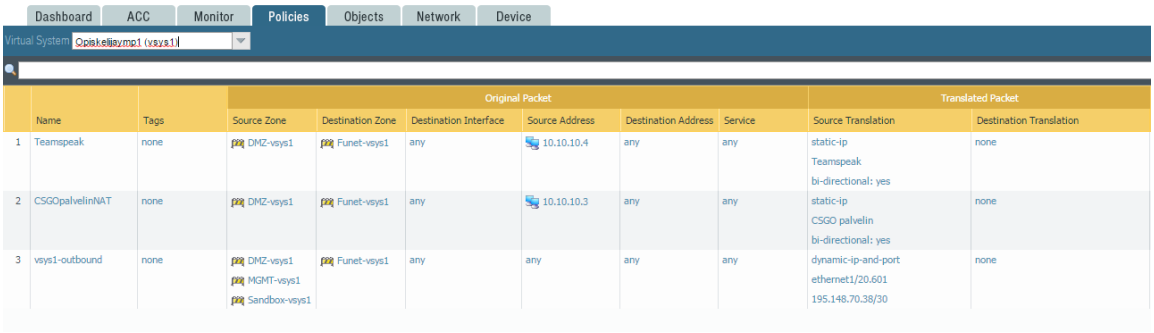
Kuva 7: Virtuaalireitittimen luonti

Virtuaalireititin osaa automaattisesti hoitaa suoraan siihen liittyvien liityntöjen välisen liikenteen reitittämisen, joten erillisiä reittejä ei tarvinnut sitä varten tehdä. Kiinteä reitti (static route) sen sijaan asetettiin ulospäin menevälle liikenteelle, koska virtuaalireititin ei muuten osaisi lähettää internettiin suuntautuvaa pakettia oikealle laitteelle.

Kiinteät reitit määritellään “Static Routes”-kohdassa virtuaalireitintä luotaessa tai ne voi lisätä samasta valikosta myös jälkeenpäin. Oletusreitti, eli reitti paketeille joiden määränpäätä reititin ei suoraan tiedä, määriteltiin antamalla kohdeosoitteeksi kaikki IPv4-osoitteet sisältävä 0.0.0.0/0. Lisäksi valittiin kohdeliityntä, johon paketti lähetetään ja seuraavan reitittimen IP-osoite. Verkkoliitynnäksi valittiin luonnollisesti internettiin yhteydessä oleva liityntä ja seuraavaksi reitittimeksi palveluntarjoajan antama IP-osoite.

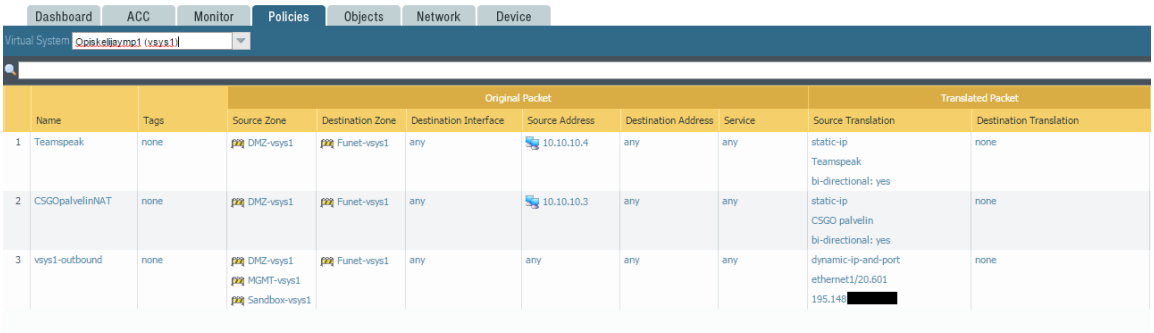
6 Osoitteenmuunnos

Osoitteenmuunnos (NAT, network address translation) on julkisen ja yksityisen verkon rajalla käytettävä menetelmä, jolla sisäverkon laitteet saadaan piilotettua ulkoverkossa olevalta tarkkailijalta. Sisäverkon suojaamisen lisäksi osoitteenmuunnos vähentää julkisten IP-osoitteiden tarvetta, kun useampi sisäverkon laite jakaa saman julkisen IP-osoitteen. [5, p. 101]



Kuva 8: Osoitteenmuunnos

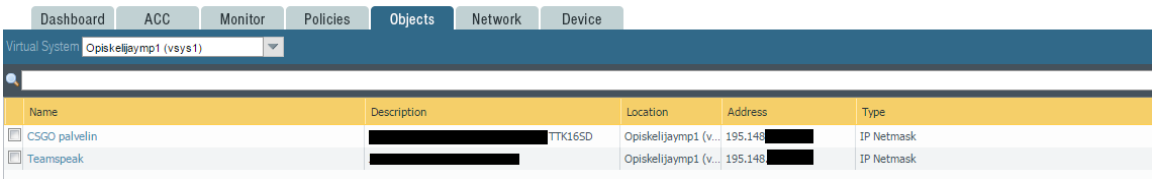
Sisäverkon yksityiset IP-osoitteet, eli tässä projektissa 10.0.0.0/8 avaruus, eivät reitity internetissä, eli niiden avulla voi liikennöidä ainoastaan sisäverkossa olevien laitteiden kesken. Kun sisäverkosta halutaan ottaa yhteyttä internetissä sijaitsevaan palvelimeen, palomuuri vaihtaa lähettäjän yksityisen osoitteen julkiseksi osoitteeksi, eli siksi osoitteeksi, joka sille on määritelty julkisen verkon liitynnässä. Palomuuri tekee myös merkinnän omaan lokiinsa tehdystä osoitteenmuutoksesta, jotta se osaa ohjata vastauksena saapuvan paketin oikealle sisäverkon laitteelle. [5, p. 101]



Kuva 9: Osoitteenmuunnos palomuurissa

Palomuurissa osoitteenmuutos toteutetaan luomalla osoiteobjekti ja liittämällä se NAT-sääntöön. Osoiteobjekti on vain tietty IP-osoite, jolle on annettu nimi. Sen luominen ei ole

välttämätöntä, mutta se helpottaa osoitteiden hallintaa, koska käyttäjä näkee itse määrittämänsä osoitteen nimen pelkän numerosarjan sijaan. Osoiteobjektia käytettäessä osoitteen muuttaminen on helpompaa, koska osoitetta ei tarvitse päivittää useampaan sääntöön, vaan riittää sen muuttaminen osoiteobjektissa. [13]



Kuva 10: Osoiteobjekteja

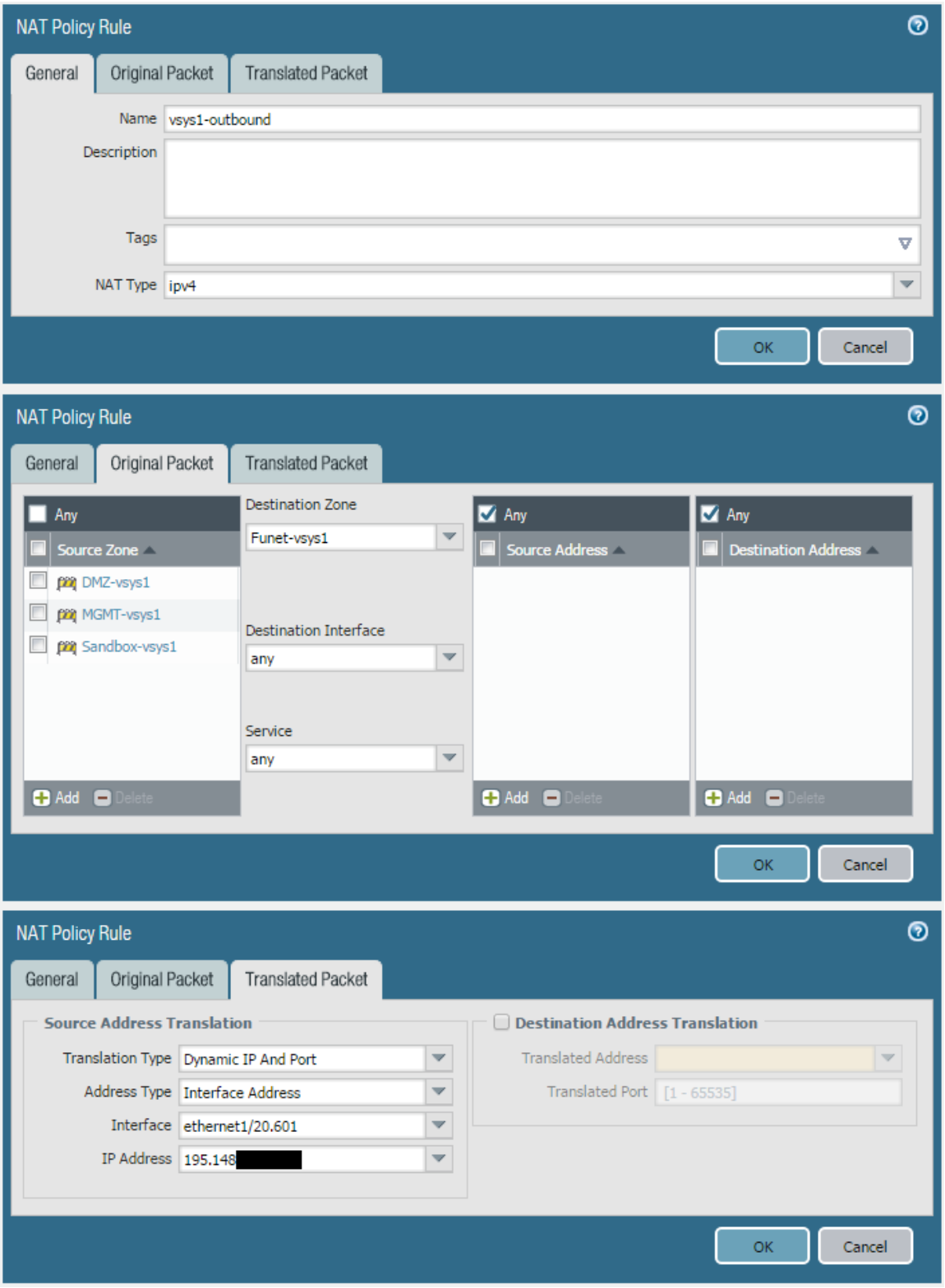
Osoiteobjektin luominen tapahtuu palomuurin ”Objects”-välilehden ”Addresses” valikosta. ”Add”-painikkeesta avautuvaan ikkunaan kirjoitetaan objektin nimi ja haluttaessa kuvaus. Tyypiksi valitaan ”IP Netmask” ja kirjoitetaan haluttu julkinen IP-osoite. Muutokset tallennetaan ”OK”-painikkeella.

Varsinainen NAT-sääntö luodaan ”Policies”-välilehden ”NAT” valikosta ”Add”-painikkeella. Säännölle määritellään haluttu nimi ”General”-välilehdellä ja siirrytään ”Original Packet”-välilehdelle. Ensimmäiseksi luotiin useamman laitteen kesken jaettu osoitteenmuutossääntö, joka on tässä tapauksessa koko verkkoaluetta koskeva. Lähdealueeksi (Source zone) valitaan alue, jota sääntö koskee, sama osoitteenmuunnossääntö voi olla käytössä useammalla alueella, jolloin kaikki tätä osoitetta käyttävät alueet tulee valita. Kohdealue (Destination zone) valitaan pudotusvalikosta, tässä tapauksessa kohdealue on julkinen verkko. Koska sääntö on tarkoitettu koko verkkoalueen käyttöön, annetaan lähdeosoitteena (Source Address) olla mikä tahansa (Any). Samoin kohdeosoite (Destination Address) voi olla mikä tahansa.

”Translated Packet”-välilehdeltä valitaan osoitteenmuunnostyypiksi (Translation Type) ”Dynamic IP and Port” ja valitaan osoitteeksi aiemmin luotu osoiteobjekti. Osoite voidaan tässä kohtaa kirjoittaa suoraan IP-osoitteena, jos osoiteobjektia ei haluta käyttää. Muutokset tallennetaan ”OK”-painikkeella.

Edellä kuvattu osoitteenmuutos sallii sisäverkon laitteiden liikennöidä internettiin. Kun halutaan sallia ulkoverkosta pääsy sisäverkkoon, osoitteenmuunnos määritellään seuraavasti: ”Original Packet”-välilehdelle valitaan verkkoalueiden lisäksi lähdeosoitteeksi sen laitteen sisäverkon osoite, johon halutaan sallia pääsy ulkoverkosta. ”Translated Packet”-välilehdellä valitaan osoitteenmuunnostyypiksi ”Static IP” ja valitaan haluttu osoiteobjekti listalta tai kirjoitetaan haluttu osoite suoraan. Lisäksi valitaan kohtaan ”Bi-directional”

”Yes”, jolloin palomuuri sallii muutoksen ulkoverkosta tuleville paketeille, eli osoitteenmuunnos toimii sekä ulos- että sisäänpäin tuleville yhteyksille.



Kuva 11: Osoitteenmuunnoksen määrittäminen. Kuvassa näkyvät kaikki välilehdet.

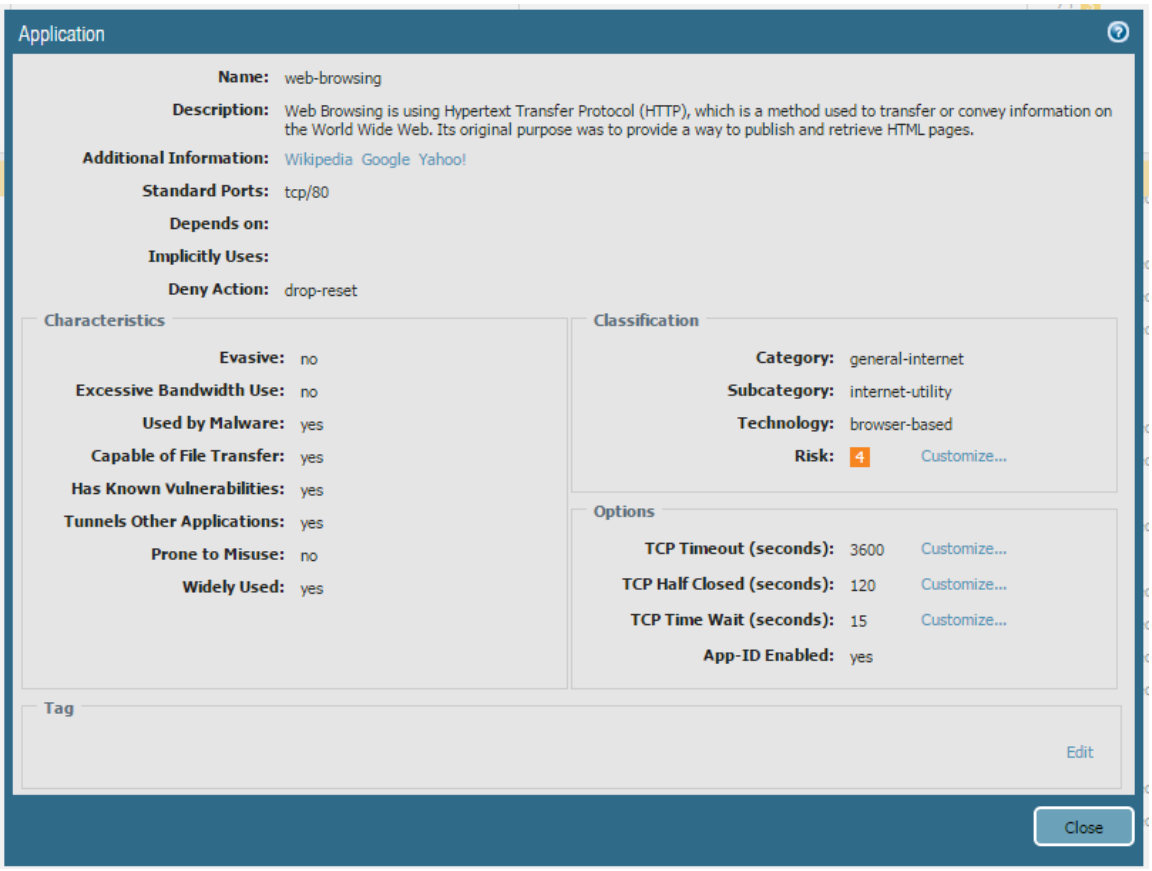
Palomuurissa voi olla lukuisia osoitteenmuunnossääntöjä samalla verkkoalueella, tällöin on tärkeää huolehtia sääntöjen keskinäisestä järjestyksestä. Kun palomuuri suorittaa osoitteenmuutoksen, se käy sääntölistan läpi ylhäältä alkaen, ja ottaa käyttöön ensimmäisen säännön, joka täsmää pakettiin. Tässä on vaarana, että laajempi, esimerkiksi koko verkkoaluetta koskeva, sääntö peittää alleen suppeamman, vain yhtä laitetta koskevan säännön. Tällöin on mahdollista, että liikennöivän laitteen julkinen IP-osoite voi muuttua riippuen liikennöintisuunnasta ja kohdeosoitteesta. Muutoksia käyttöönotettaessa (commit) palomuuri osaa yleensä huomauttaa, jos jokin osoitteenmuunnossääntö peittää jonkin toisen säännön, mutta ylläpitäjän on silti syytä tiedostaa asia.

7 Säännöt

7.1 Sovelluksen tunnistaminen

Käytetty palomuuri kykenee tunnistamaan käytetyn sovelluksen liikenteen perusteella ja tätä ominaisuutta hyödynnetään sääntöjen laatimisessa. Palomuuri sisältää yli 2500 sovelluksen tunnistetietokannan, jota Palo Alto päivittää viikoittain. Käyttäjän on myös mahdollista lisätä omia sovellustunnisteita, jos käytössä olevaa sovellusta ei löydy valmiiksi.

Sovelluslista löytyy laitteen ”Objects”-välilehdeltä ”Applications”-kohdasta. Sovellukset on luokiteltu niiden käyttötarkoituksen perusteella viiteen eri kategoriaan, jotka ovat Yritysjärjestelmät (Business-systems), Yhteistyö (Collaboration), Yleinen internet (General-internet), Media (Media) ja Tietoverkot (Networking). Nämä on jaettu vielä erikseen yhteensä 30 alakategoriaan tarkemman luokittelun vuoksi. Kategorioiden lisäksi sovellukset on luokiteltu niiden käyttämän verkkoteknologian (Technology), riskiluokituksen (Risk) ja sovellukselle tyypillisten piirteiden (Characteristic) mukaan.



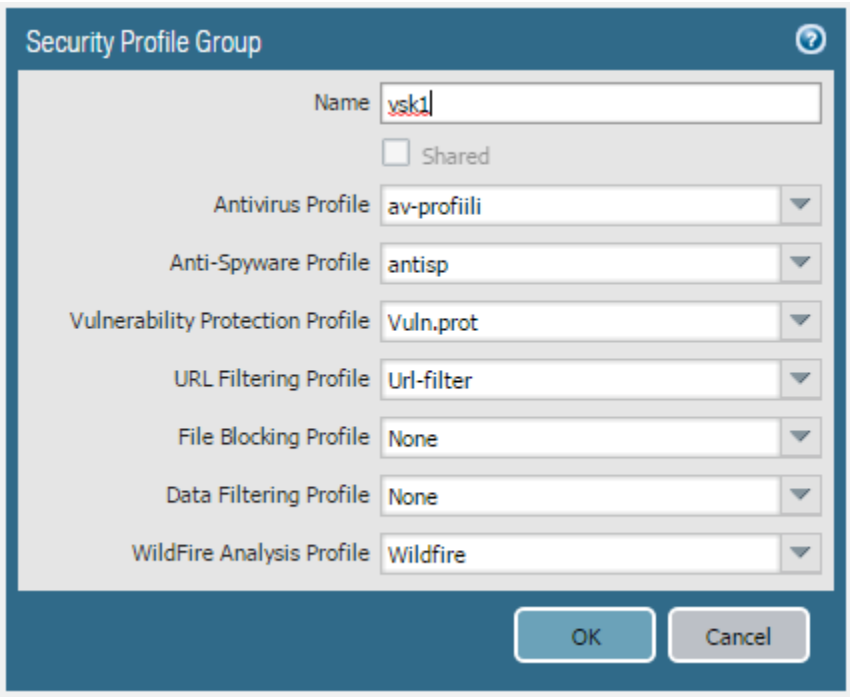
Kuva 12: Web-browsing -sovelluksen tarkemmat tiedot

7.2 Suojausprofiilit

Suojausprofiilit (Security profiles) ovat sääntöihin liitettäviä toimenpidelistoja, joiden palomuuri toimii havaitessaan määritelmän täyttävää liikennettä. Ne tarjoavat lisäsuojaa suorittamalla analyysin sen jälkeen, kun liikenne on jonkin säännön mukaan sallittu. Suojausprofiilit liitetään aina palomuurisääntöön ja niitä sovelletaan sääntökohtaisesti. Suojausprofiileja pääsee luomaan ja muokkaamaan ”Objects”-välilehden ”Security Profiles”-kohdasta. Ne on jaettu kahdeksaan erilliseen luokkaan, joista on mahdollista koostaa suojausprofiiliryhmä, joka sisältää yhden profiilin jokaisesta ryhmästä. [14]

Suojausprofiililuokat:

- Virustorjunta (Antivirus)
- Vakoiluohjelmien torjunta (Anti-Spyware)
- Haavoittuvuuksien suojaaminen (Vulnerability protection)
- URL-suodatus (URL Filtering)
- Tiedostojen esto (File blocking)
- WildFire analyysi (WildFire Analysis)
- Tiedon suodattaminen (Data filtering)
- Palvelunestohyökkäykseltä suojautuminen (DoS Protection)



Kuva 13: Suojausprofiiliryhmä

7.3 Oletussäännöt

Palomuuri sisältää oletuksena jokaisessa virtuaalipalomuurissa kaksi valmista sääntöä, jotka ovat alueen sisäistä ja alueiden välistä liikennettä varten (intrazone-default ja interzone-default). Nämä säännöt eroavat käyttäjän luomista säännöistä huomattavasti, sillä niiden muokkaamista on rajoitettu huomattavasti. Mahdollisia muutoksia ovat liikenteen salliminen tai estäminen, suojausprofiili ja lokiasetukset. Oletussäännöt ovat myös suoritusjärjestyksessä aina viimeisenä, eli palomuuri käyttää niitä, jos mikään muu sääntö ei sovellu tarkastettavalle paketille.

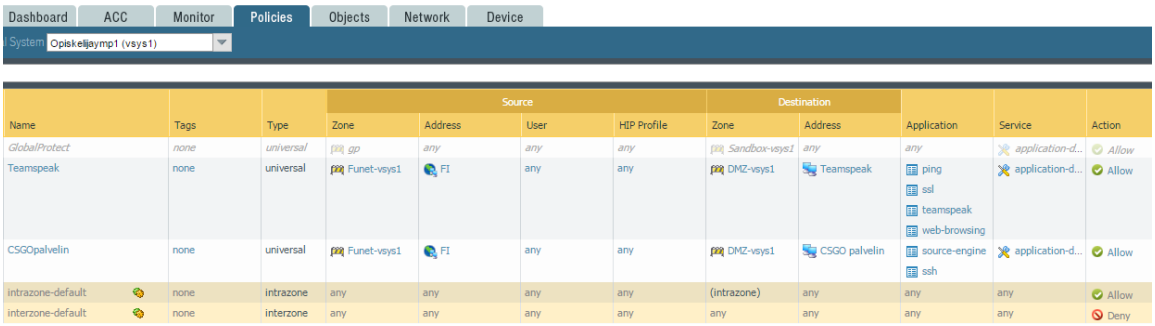
Oletuksena alueen sisäinen liikenne on sallittu ja alueiden välinen liikenne on estetty. Lokin kerääminen kytkettiin päälle, mutta muutoin säännöt jätettiin ennalleen. Tässä projektissa alueen sisäistä liikennettä määrittävällä säännöllä ei ole käytännössä merkitystä, koska alueen sisäinen liikenne kulkee kytkinverkossa, eikä käy lainkaan palomuurilla. Palomuuri ei siis pysty estämään liikennettä alueen sisäistä liikennettä koskeva sääntö rajoittaisikin sitä.

Oletussäännöistä kerätty loki helpottaa ongelmatilanteiden selvittämistä alueiden välisessä liikenteessä. Oletuksena lokin ollessa pois päältä oletussäännöllä kielletty liikenne ei näy palomuurin hallinnassa lainkaan ja ylläpitäjän on vaikeampi tietää, onko ongelma palomuurissa vai jossain muualla. Lokin ollessa käytössä ylläpitäjä näkee, jos palomuuri estää paketin ja osaa joko korjata olemassa olevan säännön tai luoda uuden. Jos palomuurin lokissa ei näy estettyä pakettia, voidaan todeta ongelman olevan jossain muussa verkon osassa.

7.4 Sääntöjen luominen

Säännöt ovat tärkein palomuurin turvallisuuteen vaikuttava tekijä. Edellä kuvatut palomuurin konfiguraatiot eivät tee mitään, jos ei niiden lisäksi määritellä sääntöjä, jotka sallivat pakettien liikkumisen. Periaate palomuurin toiminnassa on, että liikenne estetään, jos mikään sääntö ei sitä salli. Palomuuri tarkastaa sille saapuvan paketin verraten paketin tietoja sääntölistaan. Listan järjestyksellä on väliä, sillä palomuuri aloittaa tarkastelun listan ylimmästä säännöstä ja lopettaa sääntöjen tarkastamisen heti löydettyään sopivan säännön. Samoin kuin osoitteenmuunnoksessa, laajempi sääntö voi siis peittää alleen tarkemmin rajatun säännön ja aiheuttaa odottamattoman lopputuloksen. Tässäkin palomuuri osaa sääntöjen käyttöönoton yhteydessä huomauttaa mahdollisesta ongelmasta.

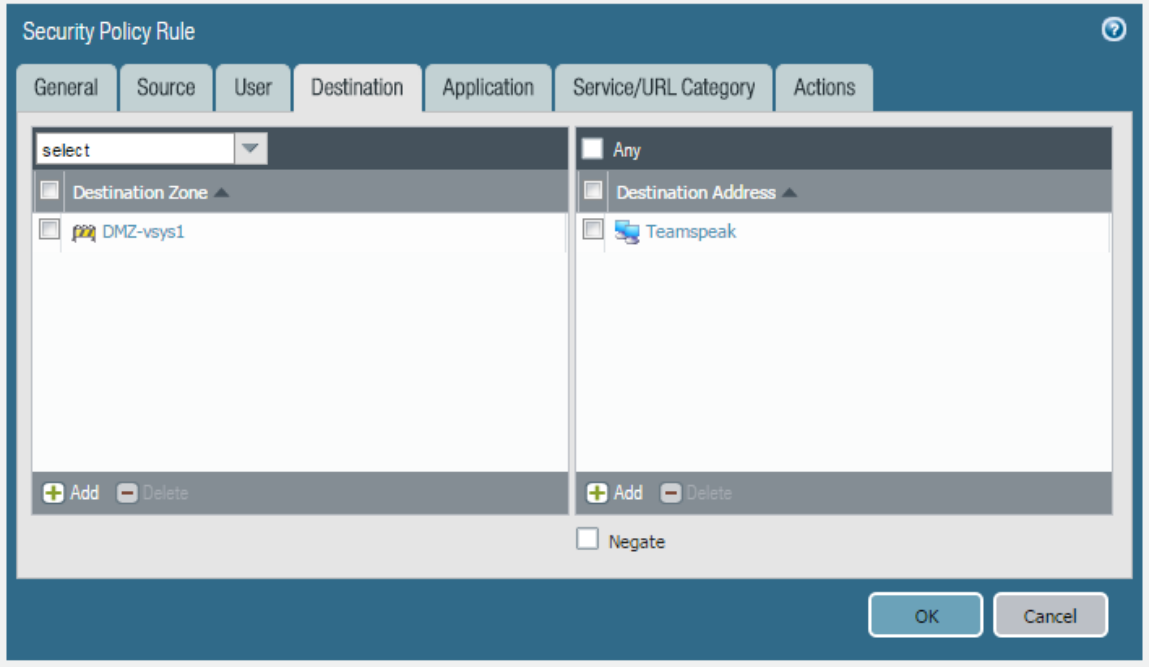
Säännöt luodaan ”Policies”-välilehdeltä ”Security”-kohdasta ”Add”-napilla. Avautuvaan ikkunaan kirjoitetaan säännön nimi ja halutessa tarkempi kuvaus sekä tunniste. Tunnisteiden avulla on mahdollista valita näytettäväksi vain tietyllä tunnisteella merkityt säännöt, jolloin on helpompi muodostaa kokonaiskuva tiettyyn asiaan vaikuttavista tekijöistä.



Kuva 14: Palomuurisääntöjä

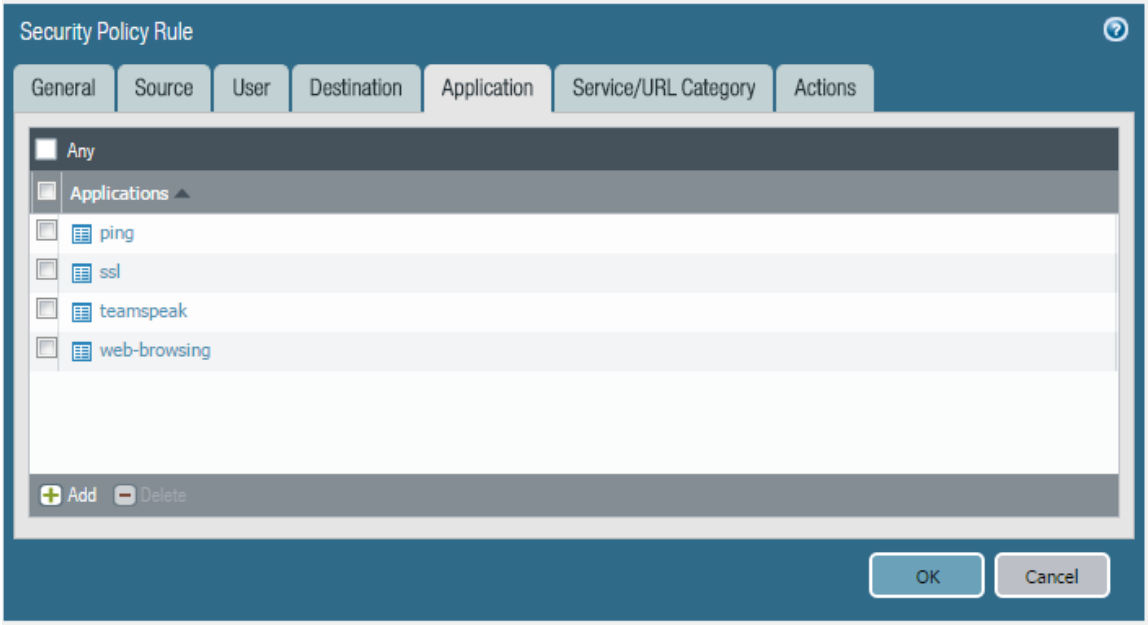
Säännön tyyppi (Rule Type) määrää, mitä liikennettä sääntö koskee. Oletuksena valittuna on yleinen (universal), jolloin sääntöä sovelletaan kaikkeen liikenteeseen. Muut vaihtoehdot ovat verkkoalueen sisäinen (intrazone) ja verkkoalueiden välinen (interzone). Kuten edellä todettiin, tässä projektissa alueen sisäinen liikenne välitetään täysin kytkinverkossa, joten palomuurilla ei ole mahdollisuutta vaikuttaa alueen sisäiseen liikenteeseen. Tästä seuraa myös, että tässä tapauksessa sääntötyypit yleinen ja verkkoalueiden välinen ovat käytännössä toiminnaltaan samat.

”Source”-välilehdeltä valitaan lähdealue (Source Zone) ja halutessa lähdeosoite (Source Address). Lähdealueeksi voidaan määrittää yksi tai useampi alueita tai valita ”Any”-painikkeella lähteeksi mikä tahansa alue. Lähdeosoitteeksi on oletuksena valittu kaikki osoitteet ja käyttäjä voi halutessaan rajoittaa lähdeosoitteita. Lähdeosoite voi olla suoraan kirjoitettu IP-osoite, osoiteobjekti tai osoiteobjekteista luotu osoiteryhmä. Palomuuri sisältää myös valmiita maantieteellisiä osoitelistoja, joiden avulla on mahdollista sallia liikenne esimerkiksi vain suomalaisista osoitteista. ”Negate”-valinnalla voidaan muuttaa valitut osoitteet pois suljetuiksi, eli sääntö koskee kaikkia muita, paitsi valittuja osoitteita. Tämä valinta koskee vain osoitteita, ei verkkoalueita. Kohdealue ja osoite valitaan ”Destination”-välilehdeltä samalla tavalla kuin lähde.



Kuva 15: Kohdealueen ja -osoitteen valinta

”Application”-välilehdeltä voidaan valita mikä sovelluksia sääntö koskee. Sovellukset voi valita yksitellen tai käyttää valmiiksi määriteltyä sovellusryhmää. Jos palomuuri ei tunnista haluttua sovellusta, sen voi lisätä palomuuriin itse tai sallia kaikkien sovellusten liikennöinnin ja rajata sallitut portit. Porttien valinta tehdään ”Service/URL Category”-välilehdeltä. Jos haluttu sovellus löytyy palomuurin listalta ja se käyttää sovellukselle tyypillisiä oletusportteja, jätetään asetukseksi ”application-default” eli sovelluksen oletus portit. Jos portteja halutaan muuttaa, voidaan se tehdä lisäämällä ”Service”-kohtaan haluttu palvelu.



Kuva 16: Sallittujen sovellusten valinta

Palomuuriin ei suoraan pysty syöttämään sääntökohtaista porttinumeroa, vaan ensin on luotava palvelu, johon portit määritellään. Palvelun luonti onnistuu joko säännön luomisen yhteydessä ”New Service”-painikkeella tai ”Objects”-välilehden ”Services”-valikosta. palvelun luominen onnistuu molemmissa samalla tavalla, määritetään palvelulle nimi, käytettävä protokolla, kohdeportti ja halutessa myös lähdeportti.

Palomuuria kokeiltaessa kaikki normaalit internetin palvelut toimivat oletusporttien kautta, eikä erillisiä palveluita tarvinnut tehdä. Opiskelijaprojekteissa oli tarpeen muokata palveluiden kautta sallittuja portteja, jotta harvinaisemmat tai itse luodut sovellukset saatiin toimimaan kunnolla.

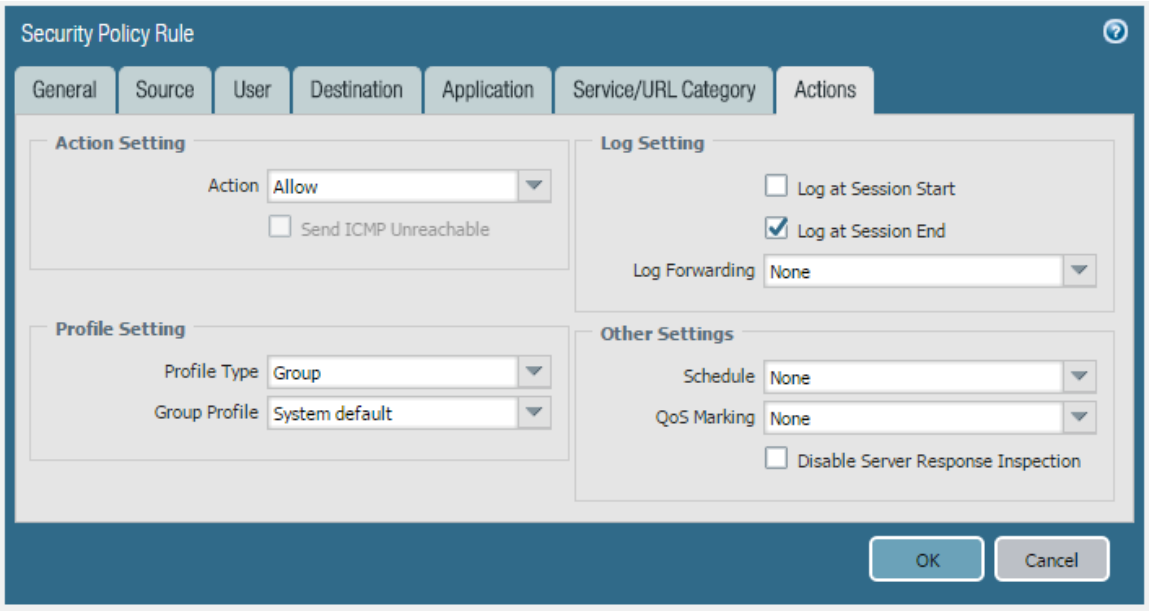
Viimeiseksi määritellään ”Actions”-välilehdeltä sääntöön liittyvä toiminta. Vaihtoehdot ovat: estä (Deny), salli (Allow), pudota (Drop), ja asiakkaan, palvelimen tai molempien TCP-resetointi (Reset client, reset server, Reset both client and server).

Oletuksena on valittuna liikenteen salliminen, jolloin palomuuri päästää säännön mukaisen liikenteen läpi. Estä valinnalla palomuuri estää liikenteen valittuun sovellukseen liittyvän toiminnon mukaisesti. Palomuuri voi siis esimerkiksi lähettää asiakkaalle tiedon ettei palvelin ole saatavilla tai TCP-reset -paketin. Sovelluskohtaisen toiminnan voi tarkastaa ”Objects”-välilehden ”Applications”-kohdan sovelluslistasta.

Paketin pudotus tarkoittaa paketin hävittämistä, ilman liikennöivälle laitteelle ilmoittamista, lisävalintana voidaan vastauksena lähettää ”ICMP unreachable” -paketti, eli kertoa ettei

kohdelaite ole tavoitettavissa. TCP-reset vaihtoehto katkaisee yhteyden lähettämällä erityisen ”TCP-reset”-paketin, joka sulkee avoimen TCP-yhteyden välittömästi. Paketti voidaan määritellä lähetettäväksi joko asiakkaalle, palvelimelle tai molemmille.

Liikenteen sallimisen tai estämisen lisäksi ”Actions”-välilehdeltä voidaan määrittää säännön näkyminen liikennelokissa, asettaa säännölle tietyt voimassaoloajat ja asettaa suojausprofiili. Loki on mahdollista kerätä yhteyden alussa, lopussa tai ei lainkaan. Tässä projektissa loki kerättiin kaikesta liikenteestä yhteyden päättyessä. Yhteyden päättyessä kerätty loki toimii paremmin kuin alussa kerätty, koska yhteyden alussa palomuuri ei vielä kykene tunnistamaan käytettyä sovellusta. Lopuksi kerätty loki siis näyttää enemmän tietoa palomuurin läpi kulkeneesta liikenteestä ja helpottaa ongelmien selvittämistä.



Kuva 17: Toimintojen määrittäminen sääntöön liittyen

DC-laboratorion tuotantoympäristöön luotiin säännöt, jotka sallivat työasemille liikennöinnin ulkoverkkoon suhteellisen vapaasti. Haitallisen sisällön rajoittaminen tehtiin suojausprofiilien avulla sulkemalla haitallinen liikenne ja vaaralliseksi tunnetut sivustot pois.

Tuotantoympäristön alueiden väliseen liikenteeseen laadittiin tarkat säännöt konesaliympäristön turvaamiseksi. Aluksi sallittiin sovellukset, joiden tiedettiin olevan tarpeellisia, kuten VMwaren virtualisointialustan etäyhteys. Sovelluksia lisättiin lokiin kertyneiden merkintöjen perusteella. Tällä tavoin ympäristö saatiin nopeasti toimintaan ja ongelmia ei ole käyttöönoton jälkeen ilmennyt. Uusien palveluiden käyttöönotto vaatii luonnollisesti palomuurisääntöjen päivittämisen käyttöönoton yhteydessä.

8 Yhteenveto

Opinnäytetyön teoriaosuudessa käytiin läpi palomuurien historia ja tarpeen syntyminen yleisellä tasolla. Sen perusteella nykyaikainen palomuuri on monipuolinen laite, joka kykenee suojaamaan verkkoympäristöä jatkuvasti kehittyviltä ja muuttuvilta ulkopuolisilta uhilta. Käytännön osuudessa palomuuri asennettiin paikoilleen ja valmisteltiin käyttöön. Opinnäytetyö keskittyi suurelta osin käytännön osuuteen ja erityisesti nyt käytössä olleeseen palomuurimalliin. Palo Alto Networksin PAN-OS-käyttöjärjestelmä on käytössä kaikissa yrityksen sovelluspalomuureissa, joten tässä esitetyt tiedot pätevät osittain myös muihin palomuurimalleihin.

Palomuuri saatiin toimintaan suunnitellusti ja käyttöympäristö toimii halutulla tavalla. Käytössä ollut palomuuri helpottaa käytön aikaista ylläpitoa automaattisesti päivittyvien uhkatietokantojen ja sovellustunnisteiden kautta, mutta ylläpitäjän on silti suositeltavaa tutustua palomuurin toimintaan ja opetella seuraamaan palomuurin lokiin kertyviä tietoja.

Tietojärjestelmälaboratorion opiskelijoiden näkökulmasta omassa hallinnassa oleva palomuuri tarjoaa hyvän mahdollisuuden tutustua tietoturvaan ja verkon toimintaan todellista ympäristöä mukailevassa oppimisympäristössä. Tästä mahdollisuudesta seuraa luonnollisesti myös vastuu ympäristön tietoturvasta huolehtimisesta.

Lähdeluettelo

[1] C. Amon ja R. J. Shimonski, The Best Damn Firewall Book Period, Syngress, 2003.

[2] A. X. Liu, Computer and Network Security : Firewall Design and Analysis, World Scientific Publishing Company, 2010.

[3] F. Avolio, ”Firewalls and Internet Security - The Internet Protocol Journal - Volume 2, No 2,” [Online]. Available: http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-1/ipj-archive/article09186a00800c85ae.html. [Haettu 1 12 2016].

[4] D. Lowe, Networking All-in-One Desk Reference For Dummies, For Dummies, 2008.

[5] V. Preetham, Internet Security and Firewalls, Course Technology, 2002.

[6] Q. Li ja G. Clark, Security Intelligence, Wiley, 2015.

[7] ”Automatically Prevent Highly Evasive Zero-Day Exploits and Malware,” Palo Alto Networks, [Online]. Available: https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/wildfire. [Haettu 21 4 2017].

[8] ”Dynamic Updates,” Palo Alto Networks, [Online]. Available: https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-dynamic-updates. [Haettu 21 4 2017].

[9] ”Virtual Systems Overview,” Palo Alto Networks, [Online]. Available: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/virtual-systems/virtual-systems-overview#_22320. [Haettu 21 4 2017].

[10] R. Seifert ja J. Edwards, The All-New Switch Book, John Wiley & Sons, Incorporated, 2008.

[11] M. Rouse, ”small form-factor pluggable (SFP),” TechTarget, [Online]. Available: http://searchnetworking.techtarget.com/definition/small-form-factor-pluggable. [Haettu 5 6 2017].

[12] ”Segment Your Network Using Interfaces and Zones,” Palo Alto Networks, [Online]. Available: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/segment-your-network-using-interfaces-and-zones.html. [Haettu 21 4 2017].

[13] ”Configure NAT Policies,” Palo Alto Networks, [Online]. Available: https://www.paloaltonetworks.com/documentation/60/pan-os/pan-os/getting-started/configure-nat-policies#_20684. [Haettu 3 5 2017].

[14] ”Security Profiles,” Palo Alto Networks, [Online]. Available: https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/policy/security-profiles. [Haettu 6 5 2017].