SAVONIA
ammattikorkeakoulu

OPINNÄYTETYÖ - AMMATTIKORKEAKOULUTUTKINTO
TEKNIIKAN JA LIIKENTEEN ALA

SELVITYSTYÖ PALOMUURISÄÄNNÖSTÖN KATSELMOINTI-MALLIKSI – SÄÄNTÖJEN LUOKITTELU SEKÄ RISKIARVIOINTI

TEKIJÄ Miikkamatias Suopajärvi

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Tutkinto-ohjelma Tietotekniikan tutkinto-ohjelma	
Työn tekijä(t) Miikkamatias Suopajärvi	
Työn nimi Selvitystyö palomuurisäännöstön katselmointimalliksi – sääntöjen luokittelu sekä riskiarviointi	
Päiväys 10.5.2022	Sivumäärä/Liitteet 41
Toimeksiantaja/Yhteistyökumppani(t) Kuntien Tiera Oy	

Tiivistelmä

Opinnäytetyön tavoitteena oli saada Kuntien Tieralle luokittelumalli palomuurisäännöille, joiden pohjalta voidaan tehdä riskianalyysi säännöille. Toimeksiantajalla oli tarvetta ohjeelle, jolla tarkastetaan palomuurisääntöjä. Toimeksiantaja voisi käyttää tätä mallia ja ohjetta yleisesti jokaisessa toimipisteessä tulevaisuudessa. Tavoitteena myös oli, että mallia voisi käyttää jokainen palomuurien kanssa toimiva henkilö, jolloin siitä olisi yleistä hyötyä kaikille. Tiivistettynä työn tarkoitus oli nopeuttaa palomuurien tarkastusta ja pohjustaa tulevia saman aihepiirin töitä.

Opinnäytetyö koostuu teoriaosuudesta, jolla pohjustettiin työn toteutuksen teoriaa. Toteutuksen teoriassa sovellettiin teoriaosuutta. Luokittelumallit ja niiden pisteytys kehitettiin teorian pohjalta. Luokittelumallit sisälsivät riskiluokittelun IP-osoitteiden lukumäärille ja riskiluokittelun käytössä olevien protokollien lukumäärille. Näiden yhdistelmästä luotiin riskimatriisi. Riskimatriisin pohjalta tarkastusta alettiin tekemään. Toteutus osiossa riskimatriisia testattiin toimipisteessä mihin työ tehtiinkin.

Opinnäytetyön tuloksena saatiin toimiva riskimatriisi ja ohje tarkastukseen. Toimeksiantaja sai dokumentin, joka oli käytännössä opinnäytetyön raportin tiivistetty versio.Raportista tuli myös osa työtä, koska tavoite oli saada kaikille hyödyllistä tietoa. Toteutuksen aikana ilmeni useampia vaihtoehtoja työn toteuttamiseen, jolloin jatkokehitykseen jää paljon tutkittavaa. Seuraava kehityssuunnitelma olisi tehdä työn pohjalta toimiva sovellus, joka nopeuttaisi tarkastusta merkittävästi.

Avainsanat
Palomuuri, Fortigate, Riskianalyysi, Riskimatriisi

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport	
Degree Programme Degree Programme in Information Technology	
Author(s) Miikkamatias Suopajärvi	
Title of Thesis Study of Firewall Code to Review Model - Classification of rules and risk assessment	
Date 10 May 2022	Pages/Appendices 41
Client Organisation /Partners Kuntien Tiera Oy	

Abstract

The aim of this thesis was to create a classification model of firewall rules for Kuntien Tiera Oy. Based on the model, a risk analysis of the rules could be performed. The customer needed a guide to review firewall rules. The customer would like to use this model and guide at every office in the future. The goal was also that the model could be used by anyone working with firewalls. That would be a general benefit to everyone. In summary, the purpose of the thesis was to speed up the inspection of firewalls and be the basis for further studies on the same topic.

The thesis consists of a theoretical part, which laid the foundation for the theory of actual model. The theoretical part was adapted in the implementation theory. Classification models and their scoring were developed based on the theory. The classification models included a risk classification for the number of IP addresses and a risk classification for the number of protocols in use. A combination of these created a risk matrix. Based on the risk matrix, the audit was started. In the implementation part, the risk matrix was tested at the office where the model was created.

As a result of the thesis, a working risk matrix and guide for the audit were achieved. The customer received a document which was a summary of the thesis. The summary also became part of the thesis, as the aim was to get useful information for everyone. During the implementation, several alternatives for the implementation of the thesis appeared, leaving room for further development. The next step would be to make an application that would speed up the inspection significantly.

Keywords

Firewall, Fortigate, Risk analysis, Risk matrix

SISÄLTÖ

SISÄLLYSLUETTELO

1 JOHDANTO 7
1.1 Kuntien Tiera 7
1.2 Termistö 8
2 TIETOTURVA 8
2.1 Uhkatekijöitä 9
2.2 Hyökkäystyyppejä 9
3 TIETOLIIKENTEEN TEORIA 10
3.1 OSI 11
3.2 TCP/IP-malli 11
3.3 IP 12
3.4 Kuljetustason protokollat 13
3.4.1 TCP 13
3.4.2 UDP 13
3.5 Sovellustason protokollat 14
3.6 Protokollien tunnettuja portteja 15
4 PALOMUURIT 16
4.1 Ensimmäisten sukupolvien palomuurit 16
4.2 Seuraavan sukupolven palomuurit 17
4.3 Seuraavan sukupolven palomuurien teknologioita 17
4.4 Seuraavan sukupolven ja perinteisten palomuurien ero 18
5 RISKIENHALLINTA 18
5.1 Riskien luokittelu 19
5.2 Riskimatriisit 19
5.3 Riskien käsittely 20
6 TOTEUTUKSEN TEORIA 20
6.1 Fortigate 600E 20
6.2 Suojausprofiilit 21
6.3 Lähde- ja osoiteluokkien luokittelu 21
6.4 Lähde- ja osoiteluokkien pisteytys 22
6.5 Protokollien ja suojausprofiilien luokittelu 23

6.6 Protokollien ja suojausprofiilien pisteytys 24
6.7 Yhteiset pisteet 25
7 TOTEUTUS 27
7.1 Excel-ohjeet 27
7.2 Vieraat-palomuuri 28
7.3 Koulut-palomuuri 30
7.4 Yritykset-palomuuri 31
7.5 Laitehallinta-palomuuri 31
7.6 Root-palomuuri 32
7.7 Laboratorio 33
8 YHTEENVETO 35
9 POHDINTA 37
LAINATUT LÄHTEET 39

KUVALUETTELO

Kuva 1. Riskimatriisin esimerkki (Työturvallisuuspakki) 19
Kuva 2. Säännön näkymä (Suopajärvi, 2022) 27
Kuva 3. Lopullisen tuloksen esimerkki (Suopajärvi, 2022) 28
Kuva 4. Ensimmäisen kohdan tilastot (Suopajärvi, 2022) 28
Kuva 5.Toisen kohdan sääntöjen pisteet (Suopajärvi, 2022) 30
Kuva 6. Toisen kohdan tilastot (Suopajärvi, 2022) 30
Kuva 7. Kolmannen kohdan tilastot (Suopajärvi, 2022) 31
Kuva 8. Neljännen kohdan tilastot (Suopajärvi, 2022) 31
Kuva 9. Viidennen kohdan tilastot (Suopajärvi, 2022) 32
Kuva 10. Laboratorion testiympäristön havainnollistaminen (Suopajärvi, 2022) 33
Kuva 11.Testiverkon säännöt (Suopajärvi, 2022) 34
Kuva 12. Testiverkon staattiset reitit (Suopajärvi, 2022) 34
Kuva 13. Root-palomuurin staattiset reitit Testiverkko-palomuurille (Suopajärvi, 2022) 34
Kuva 14. Root-palomuurin säännöt (Suopajärvi, 2022) 35
Kuva 15. Kaikkien sääntöjen tilasto (Suopajärvi, 2022) 35
Kuva 16. Mahdollisen sovelluksen esimerkki (Suopajärvi, 2022) 38

TAULUKKOLUETTELO

Taulukko 1. Uhkatekijät 9
Taulukko 2. OSI-mallin kerrokset (Dostalek & Kabelova, 2006) 11
Taulukko 3. IP-osoitteiden havainnollistamiskuva 12
Taulukko 4. Yleisempiä sovellustason protokolleja 14
Taulukko 5. Tunnettuja protokollien portteja 15
Taulukko 6. Esimerkkejä NGFW-palomuurien ominaisuuksista 17
Taulukko 7. Riskien luokittelu (Lähitapiola, ei pvm) 19
Taulukko 8. Osoitteiden luokittelu 21
Taulukko 9. Osoitteiden pisteytys 22
Taulukko 10. Protokollien ja suojauksien luokittelu 23
Taulukko 11. Protokollien ja suojauksien pisteytys 24
Taulukko 12. Kokonaispisteet 26
Taulukko 13. Excel-taulukon solujen logiikat 27

1 JOHDANTO

Tämän työn aiheena on tutkimustyö, jonka aihe on saatu tilaajalta. Tilaajan puolelta on nähty tarpeelliseksi tehdä tarkistustapa palomuurisäännöille, jota voisi käyttää jokaisessa asiakkaan toimipisteessä. Palomuurien läpikäynti säännöllisesti on todella tärkeää, koska haittaa tekevät tahot kehittävät uusia tapoja, joilla testaan vanhoja tai puutteellisia sääntöjä. Koska sääntöjen tarkastelu on hidasta, (sääntöjä voi olla ja todennäköisesti on satoja) niin käytännössä on tarvetta työlle, joka nopeuttaa ja antaa osviittaa mitä sääntöjä asiantuntijan pitää tutkia tarkemmin.

Työn tarkoituksena on tuottaa riskianalyysi ja samalla luokitella sääntöjä, jotta ne voidaan helposti pisteyttää. Riskianalyysi tulee julkiseen käyttöön, jolloin sitä voi käyttää Tieran muissakin toimipisteissä, mutta myös ympäri Suomea oli yritys tai yksityishenkilö kuka tahansa. Tieran toiveena oli, että työstä tulisi yleishyödyllinen kaikille sitä tarvitseville. Tämän pohjalta saadaan logiikka, jolla prosessia voidaan myös automatisoida, jolloin sääntöjen läpikäynti on nopeampaa. Kun tulokset saadaan selville, niin asiantuntija voi käydä sääntöjä läpi ja muokata niitä tarvittaessa. Tulevaisuudessa riskianalyysia ja luokittelua voidaan käyttää muilla paikkakunnilla

Työ tehdään paikan päällä Tieran yhdessä toimipisteistä. Riskianalyysi kirjoitetaan ohjeeksi ja sen pohjalta tehdään Excel-taulukkoja, joissa sovelletaan pisteytystä. Työssä tullaan myös laboratorio olosuhteissa demonstroimaan, miten erilaiset säännöt toimivat käytännössä. Demonstrointi tulee osoittamaan miten rajauksia tehdään myös sääntöjen ulkopuolella. Luokittelun selvitessä testistä sitä voidaan alkaa käyttämään säännöllisesti. Kuntien Tiera tulee saamaan oman dokumentin käyttöön, mutta se on tiivistetty versio raportista. Raportti on siis myös itse osa työtä, koska se tulee olemaan kaikille saatavilla.

1.1 Kuntien Tiera

Kuntien Tiera Oy on vuonna 2010 perustettu voittoa tavoittelematon inhouse-yhtiö ja Yhteiskunnallinen yritys. Tieralle on ulkoistettu kuntien it-palveluita ja tällä hetkellä Tiera tuottaa palveluita 13 kunnalle ja sillä on 378 kuntaomistajaa. Tieran tehtävänä on parantaa ja kehittää asiakaskuntien it-palveluita.

Kuntien Tiera mahdollisesti saattaa tarjota valmiita opinnäytetyön aiheita opiskelijoille. Yritykselle voi myös itse lähettää omat yhteistietonsa ja mielenkiinnon kohteensa.

(Kuntien Tiera Oy, ei pvm)

1.2 Termistö

All – Termi, jota käytetään tässä työssä, kun kaikki osoitteet tai portit on sallittu.

Any – Termi, jota käytetään tässä työssä, kun suuri luku osoitteita tai portteja on sallittu.

DPI – Deep Packet Inspection. Järjestelmä, joka tutkii perusteellisesti tietoverkossa liikkuvat tietopaketit.

Haktivisti – Hakkeri, jonka motiivi on oman aatteensa levittäminen tai sille

IDS – Intrusion Detection System. Järjestelmä, joka havaitsee ja ilmoittaa hyökkäyksistä verkossa.

IPS - Intrusion Prevention System. Järjestelmä, joka valvoo ja estää uhkia tietoverkossa.

NGFW - Next Generation Firewall, eli seuraavan sukupolven palomuuri.

NTP – Network Time Protocol. Protokolla, joka välittää oikeat aikatiedot tietokoneiden välillä.

Palomuuri – Järjestelmä, joka tutkii ja suodattaa tietoverkoissa kulkevaa liikennettä.

Portti – Numeroituja osoitteita, joista sovellukset kuuntelevat pyyntöjä, numerot ovat väliltä 0-65,536.

SSH – Secure Shell. Protokolla, joka salaa tietoliikennettä esimerkiksi etäyhteyden aikana.

Suojausprofiili – Työssä käytetty termi, jolla kuvataan tiettyjä maksullisia UTP-lisenssin palveluita.

Syslog – System Logging Protocol. Protokolla, joka lähettää tapahtumalokeja.

Telnet – Protokolla, jota voidaan käyttää etäyhteyden muodostamiseen tai muuhun vuorovaikutukseen tietokoneiden välillä.

UTP – Fortinetin tarjoama lisenssi palomuureihin, joka mahdollistaa tietoturvallisia lisäpalveluita.

WAF – Web Application Firewall, eli selainpohjainen palomuuri.

2 TIETOTURVA

Tietoturva on nimitys menettelyille ja toimintatavoille, joilla turvataan yrityksen tai organisaation hallussa olevia tietoja. Syyt voivat olla esimerkiksi taloudellisia tai lain vaatimia, kuten yleensä on henkilötietojen kanssa. Kolme tärkeintä seikkaa ovat luottamuksellisuus, eheys ja saatavuus. Luottamuksellisuus tarkoittaa, että kyseessä olevaan tietoon pääsee vain ne henkilöt, joiden tarvitsee päästä käsiksi tietoihin ja jotka omaavat oikeudet. Eheys tarkoittaa, että tietoa pystyvät muokkaamaan vain henkilöt, joilla on oikeus. Eheys pitää myös pysyä silloin kun tieto liikkuu esimerkiksi tietoverkossa. Saatavuus tarkoittaa, että tiedot ovat helposti tai jatkuvasti saatavilla niille henkilöille, joilla on tarvetta ja oikeus päästä niihin käsiksi. (Traficom, 2020; Laakso, 2022)

2.1 Uhkatekijöitä

Uhkien luojia voidaan taulukoida viiteen kategoriaan:

Taulukko 1. Uhkatekijät

Harrastelijat
Haktivisti
Tietoverkkorikolliset
Kyberterroristit
Valtiollinen tiedustelu

Kaikki ryhmät voivat olla yhtä vaarallisia vahingon puolesta, mutta valtioilla on luonnollisesti enemmän resursseja. Harrastelijat eivät välttämättä ajattele liikaa mitä tekevät ja taidot vaihtelevat paljon. Harrastelijan motiivi kokeiluun on monesti vain mielenkiinto ja vahingon arvoa ei aina ymmärretä. Valtiollinen toimija taasen haluaa pysyä näkymättömänä huolehtiakseen omista eduistaan. Nämä ovat toimijoita, jotka eivät tarkoituksellisesti halua aiheuttaa vahinkoa tai haluavat pysyä näkymättöminä, valtiokin yleensä sabotoi toisen valtion etuja mutta harvoin oman maansa. (Järvinen & Rousku, 2017, ss. 33-37)

Haktivisti ja kyberterroristit hakevat tarkoituksenmukaisesti vahinkoa ja huomiota. Haktivistit toimivat enemmän harmaalla alueella, koska motiivina on enemmän aatteen tuominen esille, jolloin suuri vahinko ei edistä sitä. Haktivistit saattavat välillä myös tehdä suoria rikollisia hyökkäyksiä. Kyberterroristit ovat muuten samanlaisia kuin tavalliset terroristit, mutta luonnollisesti toimivat virtuaalisessa maailmassa. Kohteena on yleensä yhteiskuntaa ylläpitävät infrastruktuurit kuten esimerkiksi sähköverkko. Tällä hetkellä ei ole kovin suuri vaikuttaja, mutta tulevaisuudessa aivan varmasti kasvava uhkatekijä. (Järvinen & Rousku, 2017, ss. 34-37)

Tietoverkkorikollisten suurin motivaatio on raha. Siksi suurin osa tietoverkkorikollisten hyökkäyksistä on sellaisia, joilla voisi tienata rahaa, kuten esimerkiksi lunnashaitaohjelma, joka lukitsee koneen tai sen tiedostoja ja avaamiksesi pitää maksaa lunnas. (Järvinen & Rousku, 2017, ss. 35-36)

Kategorian ulkopuolella on vahingossa tapahtuvat tietoturvapoikkeamat. Motivaatiota ei ole, jolloin tämä uhkatekijä on täysin sattumanvarainen ja voi tapahtua melkein, milloin vain. Vahinkojenkin taustalla voi olla aiemmin mainitut uhkatekijät, jotka niin sanotusti laittavat kaiken liikkeelle tarkoituksellisesti tai myös heidän puolestaan vahingossa. (Järvinen & Rousku, 2017, ss. 39-40)

2.2 Hyökkäystyyppejä

Uhkien tekijöillä on lukemattomia keinoja yrittää hyökkäyksiä. Seuraavaksi kerrotaan muutamasta hyökkäystyypistä, joita hakkerit yleisesti käyttävät.

Haittaohjelma (malware): Ohjelma, jonka tehtävänä on saada hakkeri sisään järjestelmään. Ohjelman tarkoituksena on saada tietoa koneelta tai aiheuttaa vahinkoa. Haittaohjelma monesti hidastaa tietokonetta, joka normaalisti suoriutuisi nopeasti, kone voi myös kaatua useammin. Selaimessa tai näytöllä voi olla myös ylimääräistä tavaraa kuten mainoksia tai laajennuksia. (Fortinet, ei pvm)

Yrityksen ollessa kohteena alkaa rikollisten haittaohjelma kryptamaan tietoa ja tiedon vapauttamisesta vaaditaan lunnaita. Tällöin kyseessä on kiristysohjelma (ransomware). Yleensä myös arkaluontoinen tieto uhataan julkistaa yleisesti esimerkiksi pimeässä verkossa. Pimeä verkko on paikka, jossa käyttäjän henkilöllisyys on helppo pitää salaisena. Nämä haittaohjelmat huomataan viimeistään silloin kun kryptaus alkaa, mutta vahinkoa on jo ehtinyt tapahtua. (Järvinen & Rousku, 2017, ss. 93-94; Fortinet, ei pvm)

Nollapäivähaavoittuvuus (Zero Day Vulnerability): Nollapäivähaavoittuvuus on haavoittuvuus ja riski sovelluksessa, josta kehittäjällä ei ole mitään tietoa. Haavoittuvuus on todella vakava, koska yrityksillä ei ole keinoja huomata tai estää niitä, hyökkäysten onnistumisprosentti on myös korkea. (Fortinet, ei pvm)

Väliintulohyökkäys (Man-in-the-middle): Hakkeri soluttautuu käyttäjän ja palvelimen väliin. Käyttäjä ei ole tietoinen, että hakkeri näkee esimerkiksi sähköpostiviestit tai osallistuu videopuheluun. On myös mahdollista, että hakkeri luo botteja, jotka taasen luovat aidontuntuisia viestejä käyttäjälle. (Fortinet, ei pvm)

Verkkourkinta (Phishing): Verkkourkinnassa käyttäjiltä suoraan yritetään saada tietoa esimerkiksi sähköpostiviesteillä. Sähköpostien mukana olevat liitteet ovat suosittuja, koska niihin voi piilottaa haittaohjelmia. Verkkosivu voi olla myös tekaistu ja mahdollisesti yrittää esittää jotain oikeaa organisaatiota. Käyttäjä voi vaikka syöttää verkkopankkitunnukset, jolloin ne päätyvät oikeasti rikollisten käsiin. Verkkourkinnassa käyttäjän pitää olla aktiivinen. Tämä tarkoittaa, että koulutettu ja tarkkaavainen käyttäjä pystyy torjumaan suurimman osan urkinnasta itse. (Klusaité, 2020)

3 TIETOLIIKENTEEN TEORIA

Suomalainen tietoliikenne yritys Elisa (Elisa, ei pvm) määrittelee tietoliikenteen seuraavasti:

> Tietoliikenne on langallisten tai langattomien siirtoteiden kautta tapahtuvaa määrämuotoista tiedonvälitystä viestivien osapuolien kesken. Osapuolina voivat toimia ihmiset tai laitteet. Määrämuotoinen tieto sisältää tekstiä, ääntä tai kuvia. Langallinen siirtotie toteutetaan kupari- tai valokuitukaapeleiden päällä erilaisilla tekniikoilla, esimerkiksi Ethernet, MPLS tai IP. Langaton siirtotie hyödyntää yleisimmin radiotaajuuksia esimerkiksi WLAN- tai mobiilitekniikoiden avulla.

Tässä osiossa tullaan kertomaan tietoliikenteestä ja tarkemmin vielä siihen liittyvistä protokolleista.

3.1 OSI

Open Systems Interconnections (OSI) on ISO-organisaation luoma toimintamalli tietoliikenteelle. OSI tarkoitus on ratkaista hajautettujen järjestelmien ongelma eli miten yhdistää tietokoneita niissä. Se auttaa hahmottamaan tietoverkon toimintaa käyttäjälle. Se koostuu seitsemästä kerroksesta lähtien fyysisestä laitteesta ja päätyen sovellukseen mitä käyttäjä käyttää. Siitä on myös hyötyä, kun ongelmia korjataan, koska ongelma voidaan paikantaa tiettyyn kerrokseen. (Norris, 2021)

Alapuolella oleva taulukko 2 esittelee eri kerrokset ja lyhyesti selittää niiden tehtävät. Laite, joka lähettää tiedon kulkee taulukkoa alaspäin ylhäältä asti, taasen laite, joka vastaanottaa, käy kerroksia alimmasta kerroksesta ylöspäin korkeimpaan.

Taulukko 2. OSI-mallin kerrokset (Dostalek & Kabelova, 2006)

7	Sovelluskerros	Tehtävänä ylläpitää yhteyksiä sovelluksien kesken. Kaikille muille kerroksille ikään kuin pomo, muut tekevät työtä tälle kerrokselle.
6	Esittelytapakerros	Tehtävänä varmistaa, että vastaanottava laite ymmärtää kieltä millä tieto tulee.
5	Istuntokerros	Tehtävänä aloittaa sessioita eli yhteyksiä, ylläpitää niitä ja lopettaa yhteyden tarvittaessa.
4	Kuljetuskerros	Tehtävänä varmistaa, että paketti kulkee kahden laitteen välillä.
3	Verkkokerros	Tehtävänä reitittää paketti oikeaan osoitteeseen tietoverkkojen yli.
2	Siirtoyhteyskerros	Tehtävänä määrittää yhteydenpidot samassa tietoverkossa olevien laitteiden välillä.
1	Fyysinen kerros	Tehtävänä määrittää tiedonsiirron fyysisen kulkutavan kuten esimerkiksi valokuidun avulla.

3.2 TCP/IP-malli

TCP/IP on verkottumisprotokollamalli, jota voi käyttää käytännössä. Se on paranneltu malli OSI-mallista. TCP/IP sisältää viisi tasoa. Ne ovat verkkokäyttökerros, Internet-kerros, kuljetuskerros ja sovelluskerros. Tässä työssä protokollien kannalta tärkeimmät ovat kaksi viimeistä ja osoitteiden kannalta ensimmäiset kaksi kerrosta. (Krimaka.net, ei pvm)

3.3 IP

IP eli Internet Protocol on protokolla, jonka tehtävä on yhdistää tietokoneita, tarkemmin verkkokortteita, ja luoda niiden välille yhteyden, jolloin ne voivat käyttää muita protokolleja laajemman tiedon siirtämiseen. (Blank, 2004; Dostalek & Kabelova, 2006)

IP-osoite koostuu neljästä oktetista, jotka sisältävät kahdeksan binäärilukua eli luku on nolla tai yksi. Näistä saadaan lopulta luku, joka on 0 ja 255 välillä, näitä lukuja tulee neljä ja ne erotetaan pisteellä. IP-osoitteet voidaan tämän pohjalta luokitella luokkiin A, B, C, D ja E. D ja E eivät ole yleisesti käytössä ja A on myös harvinaisempi. B-luokan aliverkon maski on /16 ja ylöspäin. C-luokan aliverkon maski on /24 ja ylöspäin. (Blank, 2004; Computer Hope, 2020)

Taulukko 3 alapuolella havainnollistaa miltä IP-osoite näyttää. 255.255.255.0 maski esitetään monesti myös /24 muodossa ja 255.255.0.0 maski /16 muodossa.

Taulukko 3. IP-osoitteiden havainnollistamiskuva

Luokka	IP-osoitteiden osoiteväli	Verkon maski
A	10.0.0.0–10.255.255.255	255.0.0.0
B	172.16.0.0–172.16.31.255	255.255.0.0
C	192.168.0.0–192.168.255.255	255.255.255.0

3.4 Kuljetustason protokollat

Kuljetuskerros päättää muodostavatko lähettäjä ja vastaanottaja yhteyden ja kuinka tiheästi tarkastavat tämän yhteyden ylläpitämisen toistensa välillä.

IP tukee kuljetuskerroksessa monia kymmeniä protokolleja, mutta useimmin käytössä ovat TCP ja UDP. Muut ovat harvinaisempia, mutta joitakin myös käytetään säännöllisesti. Seuraavissa kappaleissa kumminkin keskitytään kahteen aiemmin nimettyyn kuljetusprotokollaan ja muihin protokolliin, jotka toimivat sovelluskerroksessa mutta kuljetuksen aikana on käytössä joko TCP tai UDP. (McAfee, 2018)

3.4.1 TCP

Kun IP välittää tietoa kahden koneen välillä, niin TCP:n tehtävä on välittää tietoa kahden sovelluksen välillä. TCP luo yhteyden, jolloin kaksi sovellusta keskustelee ja jos jokin paketti ei saavu perille, niin sitä pyydetään uudestaan. Protokolla ei osaa selvittää, jos pakettia on muokattu, vaan sille on tärkeintä, että se saapuu paikalle ja tarkastukset ovat oikein, nekin hakkeri voi muokata oikeiksi. TCP on kahdesta kuljetusprotokollista hitaampi mutta se varmistaa, että tieto pääsee perille. (Dostalek & Kabelova, 2006)

3.4.2 UDP

UDP on toinen kuljetusprotokolla, joka on suunniteltu olemaan nopea. Tiedon vastaanottamista ei ilmoiteta mitenkään, koska vuoropuheluun ei ole aikaa. Sitä käytetään yleensä videon tai äänen lähettämiseen, esimerkiksi striimauksessa tai se on laajasti videopuhelussa käytetty. Paketteja voi välillä olla saapumatta kohteeseen, jolloin esimerkiksi ääni voi kadota. (Loshin, 2003)

UDP on siis TCP yksinkertaisempi versio. Sen rakenne on yksinkertaisempi, jolloin UDP-paketteja voidaan lähettää nopeammin peräkkäin verrattuna TCP hitauteen varmistettaessa, että paketit pääsevät perille. (Dostalek & Kabelova, 2006)

3.5 Sovellustason protokollat

Taulukko 4 listaa muutamia yleisempiä sovellustasossa toimivia protokolleja. Taulukossa on myös lyhyesti selitetty mitä protokolla tekee.

Taulukko 4. Yleisempiä sovellustason protokolleja

DNS	DNS eli Domain Name System on protokolla, joka muuttaa verkkonimet (domain) IP-osoitteeksi. Käyttäjälle on paljon helpompi muistaa osoitteen nimi kuin sen IP-osoite (x.x.x.x). DNS käyttää kumpaakin kuljetusprotokollaa. (Goralski, 2017)
DHCP	DHCP eli Dynamic Host Configuration Protocol on protokolla, joka jakaa automaattisesti IP-osoitteita laitteille. Yrityksissä tämä tapahtuu DHCP-serverin kautta ja kotioloissa reititin hoitaa asian. Työntekijöiden laitteissa (kuten kannettavassa tietokoneessa) hyödyllinen, koska staattinen IP-osoite ei ole käytännöllinen mutta laitteissa, jotka tarvitsevat tietyn IP-osoitteen tämä protokolla on yleensä pois päältä. (Bluecat, ei pvm)
FTP	FTP eli File Transfer Protocol on protokolla, jonka tehtävä on suorittaa tiedostojen siirto kahden isännän välillä. Kysyvästä isännästä tulee asiakas ja toisesta isännästä tulee serveri. Serveri käsittelee pyynnön ja lähettää mahdolliset pyydetyt tiedostot. Yleensä tähän osoitettu oma FTP-serveri, johon palomuuri vahtii yhteyksiä ja pyyntöjä. Käyttää kuljetustasolla TCP-protokollia. (Blank, 2004)
HTTP	Hypertext Transfer Protocol eli HTTP on protokolla, jonka tehtävä on suorittaa tiedostojen siirtoa ja näyttämistä internetissä selaimen avulla. HTTPS on tietoturvallisempi versio, jossa s-kirjain tarkoittaa SSL-salaus. SSL (Security Sockets Layer) on salaus, joka suojaa käyttäjän selaimen ja käytettävän sivun palvelimen yhteistä liikennettä. HTTP käyttää kuljetustasolla TCP-protokollia. (Kataja, 2017; Vanhatapio, 2020)
SMTP	SMTP eli Simple Mail Transfer Protocol on protokolla, joka mahdollistaa sähköisen postin internetin yli, joka voi olla tekstiä, ääntä tai videota. Voidaan käyttää myös sisäverkossa. (Javatpoint, ei pvm)

3.6 Protokollien tunnettuja portteja

Kun paketti kulkee kohti sovellusta, niin kuljetuskerros osoittaa sille oikean portin. Portti on numero, jota sovellus käyttää lähettämisen ja vastaanottamisen osoitteena. Portti on kuin rivi ihmisiä ja sovellukselle osoitetaan tietty ihminen, joka kertoo asiansa sovellukselle. TCP ja UDP voivat käyttää portteja väliltä 0–65,536. Portteja pitäisi olla mahdollisimman vähän käytössä/vapaana, koska hakkerit yrittävät päästä järjestelmään sisään porttien kautta, jotka eivät ole käytössä. (Blank, 2004)

Hyökkääjät yleensä yrittävät portteja, joiden numero on alle 1023, koska näissä porteissa on yleisimmät protokollat, tästä johtuen niitä kutsutaan hyvin tunnetuiksi porteiksi. Näistä suosituimmat ovat 22 (SSH), 80 (HTTP) ja 443 (HTTPS). Näiden porttien on oltava päällä jatkuvasti. Siksi ne muodostavat 65 % hyökkäysyrityksistä, SSH yksinään jo 35 % vuonna 2019. (Ilascu, 2019)

Hyökkääjät voivat myös satunnaisesti kokeilla suurempia portteja, jos jokin niistä olisi jäänyt auki vahingossa. Kokeilut ovat harvinaisempia yrityksiä kohtaan, koska tämä tekniikka onnistuu paremmin kokemattomien henkilöiden kanssa. Asiantuntijakin tekee kumminkin virheitä, jolloin isommatkin portit kannattaa kokeilla. (Pinzon & Nachreiner, ei pvm)

Tunnettuja portteja on paljon enemmän, mutta alapuolella olevassa taulukossa 5 on joitain tärkeimpiä ja erityisen yleisiä tunnettuja portteja listattuna ja niihin liitettyjä protokolleja.

Taulukko 5. Tunnettuja protokollien portteja

FTP	20–21
SSH	22
Telnet	23
SMTP	25
DNS	53
HTTP	80
NTP	123
HTTPS	443
Syslog	514
FTPS	989–990

4 PALOMUURIT

Palomuurien tarve korostuu vuosittain merkittävästi. Tietoturvaan panostetaan vuosittain enemmän rahaa ja palomuurit ovat yksi osa tätä. Lisäksi nettirikollisten määrä ja hyökkäykset lisääntyvät jatkuvasti, kun enemmän ja enemmän tietoa siirtyy digitaaliseksi. (TrustRadius, 2021)

Palomuurin tehtävänä on suojella laitteita internetistä tulevia uhkia vastaan. Turvallisuutta on helpompi hallita, kun suurin osa uhkista saadaan yhdelle alueelle, jossa ne voidaan hoidella. Palomuuri on vain yksi osa tietoturvaa, mutta se on puolustuksen ensimmäinen linja. (Stallings & Brown, 2018, ss. 311-312)

Palomuuri ei pysty tekemään mitään sen jälkeen, kun hyökkäys on ohittanut sen. Myöskään palomuuri ei voi tehdä sisäiselle mitään ongelmalle, joka johtuu esim. työntekijästä tai ulkopuolelta tulevasta usb-laitteesta. (Stallings & Brown, 2018, s. 313)

4.1 Ensimmäisten sukupolvien palomuurit

Palomuuri tyypillisesti suodattaa liikennettä lähde- ja kohdeosoitteiden ja protokollien avulla. IP-osoitteina voi olla yksittäisiä tai kokonaisia verkkoja. Protokollien kohdalla määritetään myös portti, mitä kautta liikenne kulkee. Tätä palomuurityyppiä kutsutaan pakettisuodattamiseksi. Yksinkertaista pakettisuodattamista pidetään ensimmäisen sukupolven palomuurina. (Juniper Networks, 2014; Stallings & Brown, 2018)

Toisen sukupolven palomuurina pidetään tilallista palomuuria, joka on tilattoman palomuurin parannettu versio. Tilallinen palomuuri toimii samalla tavalla kuin tilaton, mutta se myös tarkkailee yhteyksiä. Tilallinen palomuuri siis tutkii koko paketin, kun tilaton tutkii vain osia siitä. Kummatkin palomuurityypit kumminkin toimivat verkko- ja kuljetuskerroksessa. (Juniper Networks, 2014)

Kolmannen sukupolven palomuurit ovat sovelluspalomuureja. Kaksi edellistä sukupolvea kehitettiin lähekkäin 1980-luvulla. Internetin yleistyessä 1990-luvulla tarvittiin palomuuri, joka toimii OSI-mallissa korkeimmassa kerroksessa. WAF (Web Application Firewall) on nimeen omaan selaimille suunniteltu sovelluspalomuuri. (Juniper Networks, 2014)

4.2 Seuraavan sukupolven palomuurit

Seuraavan sukupolven palomuurit (NGFW) pystyvät estämään moderneja haittaohjelmia ja pystyvät myös tarkkailemaan ja torjumaan hyökkäyksiä sovellustasolla. NGFW-palomuurit pystyvät hyvin älykkääseen toimintaan, koska niihin on rakennusvaiheessa sisällytetty sovelluksien hallinnointia, IPS (Intrusion Prevention System) ja DPI (Deep Packet Inspection). (Nirav, 2021)

Seuraavan sukupolven palomuuri voi myös sisältää muitakin teknologioita. Taulukko 6 seuraavassa osiossa kertoo jo mainituista teknologioista ja muutamasta yleisimmästä teknologiasta uuden sukupolven palomuureissa. Kaikkia teknologioita ei välttämättä käytetä, koska se aiheuttaa palomuureille lisää työtä ja saattaa hidastaa yhteyksiä.

4.3 Seuraavan sukupolven palomuurien teknologioita

Taulukko 6. Esimerkkejä NGFW-palomuurien ominaisuuksista

IPS	IPS eli Intrusion Prevention System tutkii ja selvittää haitallista liikennettä ja aktiivisesti estää sen pääsyä tietoverkkoon. IPS laitetaan tutkimaan liikennettä ja huomattuaan sääntöjen vastaista toimintaa, se toimii sille annettujen ohjeiden mukaan. IPS on suunniteltu esimerkiksi huomaamaan viruksia ja palvelunestohyökkäyksiä verkkoliikenteestä. Se voi eristää käyttäjiä tai estää liikenteen ulkoiselle nettisivulle. (Fortinet, ei pvm; Forcepoint, ei pvm)
IDS	IDS eli Intrusion Detection System on yksinkertaisempi version IPS:stä. IDS huomaa epäasiallisen liikenteen verkossa ja ilmoittaa siitä. Se ei kumminkaan tee itse asialle mitään. Sille on kumminkin käyttöä, jos halutaan, että liikenteeseen koskee vain ylläpitäjä. NIDS ja HIDS ovat IDS yleisiä tarkennuksia. NIDS tutkii tulevaa verkkoliikennettä ja HIDS valvoo tärkeitä kansioita. (Barracuda Networks, ei pvm)
DPI	DPI eli Deep Packet Inspection nimensä mukaan tutkii verkkopaketteja perusteellisesti. Tavalliset palomuurit tutkivat verkkopaketeista vain otsikot. DPI pystyy täten tutkimaan paketin datan, jos data on kyseenalaista, niin paketti estetään. DPI voi myös päästää tärkeät paketit jonon ohitse eli se myös parantaa verkon toimintaa. (Awati & Scarpati, 2021)
UTM	UTM eli Unified Threat Management on 2000-luvun alussa tullut palomuuri. Se kehitettiin, kun oli tarvetta monipuoliseen verkon ja laitteiden suojaamiseen. Nykyään raja on häilyvä ja UTM ei välttämättä ole oma palomuurinsa. Jotkin NGFW-palomuurit sisältävät myös teknologioita, joita esiintyy UTM-palomuureissa. Nykyään ne molemmat mielletään samaksi asiaksi. (Firewalls.com, ei pvm)

4.4 Seuraavan sukupolven ja perinteisten palomuurien ero

NGFW on huomattavasti älykkäämpi ja pystyy monipuolisempaan uhkien torjuntaan kuin perinteinen palomuuri. Suurimman eron tekee sovellustaso, jonka liikenne on kehittynyt huimasti, hakkerit ovat onnistuneet piilottamaan haittaohjelmia myös sovelluksien liikenteeseen. Perinteinen palomuuri jää auttamattomasti jälkeen, koska se tutkii vain paketteja, osoitteita ja portteja. Uusin palomuuriin myös saatu lisättyä toimintoja, joilla saadaan torjuttua haittaohjelmia. NGFW-palomuurit ovat siis selvästi monimutkaisempia kuin perinteiset palomuurit, se onkin niiden heikkous.

Perinteiset palomuurit ovat luonnollisesti halvempia, kuluttavat vähemmän energiaa ja ovat yksinkertaisempia kuin seuraavan sukupolven palomuurit. Seuraavan sukupolven palomuureja voidaan silti säätää niin, että ne eivät ole niin monimutkaisia tai kuluta energiaa, jos käyttäjä tarvitsee silti lisättyjä turvatoimia.

(Nirav, 2021)

5 RISKIENHALLINTA

Palomuurin asennus on ensimmäinen askel, mutta sen ylläpitäminen on olennaista. Hyökkäykset paranevat ja elävät jatkuvasti, jolloin myös palomuurien pitää pysyä perässä ja niiden tarkastus on tärkeässä roolissa. Riskianalyysi auttaa tätä tarkistusta, koska riskianalyysin avulla löydetään riskialttiita sääntöjä. (Pietryga, 2021)

Jarkko Määttänen pohtii ja yhdistelee kandidaattityössään erilaisia riskien määritelmiä. Riski voidaan myös kokea positiivisena, jos määritelmä on poikkeus odotetusta lopputuloksesta. Negatiivinen oletus on kumminkin suurempi, koska niihin varautuminen on myös suurempaa ja positiiviset riskit ovat harvinaisempia. Riskianalyysit myös tehdään yritystä tai organisaatiota uhkaavista asioista, jolloin tässä asiayhteydessä riskit ovat negatiivisia. (Määttänen, 2020)

5.1 Riskien luokittelu

Riskien luokitteluun on niin monta eri tapaa kuin on ihmisiä mutta alla olevaan taulukkoon on listattu neljä pääluokkaa. Riskillä voi olla vaikutuksia kaikkiin, vaikka se luokiteltaisiin vain yhteen. (Lähitapiola, ei pvm)

Taulukko 7. Riskien luokittelu (Lähitapiola, ei pvm)

Strategiset riskit	Liikestrategia Yrityskulttuuri	**Talouden riskit**	Tuottavuus Pääoma ja rahoitus
Operatiiviset riskit	Viestintä Tietojärjestelmät ja -turva	**Vahinkoriskit**	Työtapaturmat Rikollinen toiminta

Riskien luokittelussa pitää myös ottaa huomioon mistä ne tulevat. Riskit voivat olla sisäisiä tai ulkoisia.

Tämän työn osalta operatiiviset riskit ovat aiheellisia. Tietotekniikassa on ylipäätänsä tärkeää seurata uusia teknologioita kuten uusien palomuurien hankkimista tai päivittämistä. Näin vähennetään riskejä, jotka aiheutuvat vanhentuneista järjestelmistä. Nämä voidaan luokitella tietoliikenneturvallisuuteen liittyviksi. Muita luokitteluita voivat olla esimerkiksi ohjelmistoturvallisuus tai tietoaineistoturvallisuus.

(Pro, ei pvm)

5.2 Riskimatriisit

Tapahtuman todennäköisyys	Seurausten vakavuus		
	1. Vähäiset	2. Haitalliset	3. Vakavat
1. Epätodennäköinen	1. Merkityksetön riski	2. Vähäinen riski	3. Kohtalainen riski
2. Mahdollinen	2. Vähäinen riski	3. Kohtalainen riski	4. Merkittävä riski
3. Todennäköinen	3. Kohtalainen riski	4. Merkittävä riski	5. Sietämätön riski

Kuva 1. Riskimatriisin esimerkki (Työturvallisuuspakki)

Riskimatriisi on malli riskienhallinalle. Kuva 1 on esimerkki klassisesta riskimatriisista. Yhdellä akselilla on todennäköisyys riskille ja toisella on riskin vakavuus. Riskiluku tulee sitten kertomalla tai yhteen laskemalla nämä luvut. Väreillä monesti täsmennetään riskin vakavuutta. Punainen yleensä kertoo suurimmista riskeistä, kun rauhallisemmat värit kertovat pienemmistä riskeistä asteittain. Tämä myös kertoo mihin riskiin kannattaa kuluttaa huomiota ja aikaa. (Pelastustieto, 2018)

5.3 Riskien käsittely

Sen jälkeen, kun riskit on matriisin jälkeen löydetty, niin seuraava askel on niiden käsittely. Koska kaikkien läpikäymiseen ei ole aikaa, niin pitää huomioida pahimmat riskit. Riskien käsittelyyn on lukemattomia keinoja ja paras tapa riippuu hyvin paljon käsiteltävästä aiheesta.

Seuraavaksi käsitellään riskejä palomuurien ympäristössä. Näin saadaan hyvä lähtökohta esimerkeille.

Riskejä voidaan pienentää, jolloin niiden vaikutusta tai todennäköisyyttä vähennetään. Palomuurien tapauksessa tämä voisi tarkoittaa sallittujen osoitteiden määrän pienentämistä tai aukinaisten porttien rajausta. Riskin siirtäminen voisi tässä tapauksessa esimerkiksi tarkoittaa, että palomuurin ylläpitäminen siirrettään kyvykkäämmän organisaation tai henkilön käsiin. Kätevin tapa on riskin poistaminen. Esimerkiksi poistamalla palomuurisääntö tai vanhentunut sovellus. Poistaminen ei kumminkaan ole aina mahdollista oli riski minkälainen tahansa, joten pienentäminen on todennäköisin keino käsitellä riskejä. (Määttänen, 2020)

6 TOTEUTUKSEN TEORIA

Sääntöjä on monenlaisia, joten niiden tarkasta luokittelusta tulisi erittäin monimutkainen ja aikaa vievä prosessi. Sääntöjä kumminkin voidaan niputtaa yhteen, jolloin esim. suunnilleen saman määräiset aukinaiset portit tai suunnilleen sama määrä osoitteita päätyvät samaan nippuun. Riski näiden nippujen sisällä ei kauheasti vaihtele, jolloin käytännössä ovat yhtä turvallisia tai turvattomia. Työn alussa päätettiin käyttää 6x6 taulukkoa, jolla saadaan pohja riskianalyysille. 6x6 taulukolla saadaan vähän enemmän pelivaraa ja vaihtoehtoja verrattuna 5x5 taulukkoon. Ensimmäisenä kriteerinä on lähde- ja osoiteluokat ja toisena on protokollat suojausprofiilien kanssa tai ilman.

Riskianalyyseissa ja riskimatriiseissa on yleensä erikseen todennäköisyys, mutta tässä työssä hieman sovelletaan perinteistä mallia ja todennäköisyys ikään kuin sisällytetään osoitteisiin ja protokolliin. Eli se ei ole omana kriteerinään, koska se ei ole nyt pääosassa vaan osa kokonaisuutta.

6.1 Fortigate 600E

Fortigate 600E on Fortinetin kehittämä palomuuri, joka tukee NGFW-toimintoja. Paikkakunnalla mihin työ tehdään, on ollut Fortigate palomuureja kauan käytössä. 600E-sarja on suunniteltu skaalautuvaksi, joka on tarpeellista koska sarja on suunniteltu keski- tai suurikokoisille yrityksille, olivat ne yhdessä maantieteellisessä paikassa tai laajentuneet muualle.

Palomuurissa on käytössä tekoäly, joka torjuu tunnettuja uhkia mutta osaa myös oppia torjumaan ei-tunnettuja uhkia. Tuhansien sovelluksien valitseminen tarkkaan seulontaan kuuluu myös oletuspalveluihin. Laitteen hallinta on myös yksinkertaista helpon hallintakonsolin ansiosta. Laite osaa myös ehdottaa parannuksia turvallisuuteen käyttöönoton aikana. Palomuuri on saanut myös sertifikaatteja puolueettomilta toimijoilta. (Fortinet, 2021)

6.2 Suojausprofiilit

Tutkitussa kohteessa on käytössä UTP-lisenssi (Unified Threat Protection) joka sisältää UTM toimintoja. Näitä toimintoja ei välttämättä ole käytössä jokaisella käyttäjällä tai paikkakunnalla, jolloin tämä pitää ottaa suunnitellussa huomioon. Tähän teknologiaan tullaan tästä edes viittamaan suojausprofiili-sanalla lukemisen helpottamiseksi.

Suojausprofiilit vaikuttavat turvallisuuteen myönteisesti, jolloin niiden käyttäminen pitäisi vaikuttaa pisteytykseen positiivisesti. Riskimatriisin kumminkin pitää pysyä sellaisena, että sitä voi käyttää myös, vaikka ei olisi samoja toimintoja käytössä. Työssä on päädytty ratkaisuun, jossa suojausprofiilien puuttuminen on oletus ja niiden käyttö vaikuttaa pisteytykseen vähennyksenä.

6.3 Lähde- ja osoiteluokkien luokittelu

Käytetään apuna jo valmiiksi olevia määritelmiä tietoverkkojen luokille, eli nyt on käytössä lähinnä C-verkko ja B-verkko. Tässä työssä C-verkossa on 32–350 osoitetta ja sitä pienempi määrä lasketaan yksittäisiksi osoitteiksi. Luvun mentäessä yli 350 luokitukseksi vaihtuu B-verkko ja sitä ylempi on vain any tai all. Eli verkot on luokiteltu:

Taulukko 8. Osoitteiden luokittelu

Osoitteiden määrä
osoite (2 osoitetta)
yksittäiset osoitteet (3–31 osoitetta)
C (32–350 osoitetta)
B (351 -> any osoitetta)
all (kaikki osoitteet)

Lähde- ja osoiteluokille voidaan rajata alarajaksi yhdestä osoitteesta yhteen osoitteeseen, joka tarkoittaa, että vain kaksi osoitetta pääsee läpi. Tätä vähempää osoitteita ei voida päästää läpi, jolloin riski on pienin ja tästä voi luokitella vain ylöspäin.

Seuraavassa askeleessa on useampi osoite käytössä, jolloin riski hieman kasvaa mutta ollaan silti matalissa luvuissa. C-verkossa on jo todennäköisesti reilusti enemmän osoitteita mutta verkko silti tiukasti rajattu. Sama luokittelu käy B-verkossa mutta siinä luvut ovat jo reilusti isompia ja riskikin

kasvaa mukana. Viimeisenä on all, jossa kaikki osoitteet ovat käytössä eli rajausta ei ole ollenkaan, jolloin riski on suurin mahdollinen. Näiden rajojen sisään sääntöjä voidaan sijoittaa. Työn mallissa suurin osoite määrä määrää pisteytyksen. Esimerkiksi jos jommassakummassa on all, niin pienin mahdollinen piste osoitteille on neljä.

Geoblokkaukset ovat suhteellisen harvinaisia poikkeuksia. Geoblokkaukset voi myös olla huomioimatta. Paras tilanne olisi, että käyttäjä tai organisaatio voi itse päättää tämän poikkeustapauksen käsittelemisen itse. Tässä työssä geoblokkaus on all.

6.4 Lähde- ja osoiteluokkien pisteytys

Taulukko 9. Osoitteiden pisteytys

all+all	Suurin mahdollinen yhdistelmä, jolloin suurin mahdollinen riski. Tästä yhdistelmästä tulee 6 pistettä.
b+all b+b	Toiseksi suurimmat mahdolliset yhdistelmät, jolloin hieman rajatumpi. Riskit hieman alhaisempia, mutta silti hyvin riskialtis yhdistelmä. Todennäköisesti internettiin menevää liikennettä suurella määrällä osoitteita. Näistä yhdistelmistä tulee 5 pistettä.
c+all yksittäiset + all b+c b+ yksittäiset	Todennäköisesti internettiin menevää liikennettä suhteellisen pienellä määrällä tai sisäistä liikennettä suurella määrällä. Näistä yhdistelmistä tulee 4 pistettä.
c+c c+ yksittäiset	Osoitteiden määrä on välillä 32–350. Riskien keskivaiheella Näistä yhdistelmistä tulee 3 pistettä.
yksittäiset + yksittäiset	Toiseksi pienin mahdollinen yhdistelmä, jolloin riski kasvaa hieman mutta silti todella rajattu. Tästä yhdistelmästä tulee 2 pistettä.
osoite + osoite	Pienin mahdollinen yhdistelmä, jolloin riski on pienin mahdollinen. Tästä yhdistelmästä tulee 1 piste.

Osoitteet yhteen laskettuina voivat yksittäisistä osoitteista muuttua C-verkoksi tai C-verkko B-verkoksi. Tässä työssä kumminkin enemmän huomioidaan kummassa luokassa, on enemmän osoitteita. Pisteytyksen voisi yksinkertaistaa niin että käytettäisiin aiempaa luokittelutaulua mutta muutaman

kokeilun jälkeen tulokset eivät merkittävästi poikenneet toisistaan. Eli käytännössä lähde – ja osoiteluokka saavat samaan pistemäärän, jossa suurempi määrä määrää.

6.5 Protokollien ja suojausprofiilien luokittelu

Taulukko 10. Protokollien ja suojauksien luokittelu

Protokollat	**Profiilit**
1–2	5
3–6	4
7–11	3
12–20	2
21-any	1
all	0

Profiilit on jaettu kahteen luokkaan. Todennäköisesti profiileita on käytössä internettiin menevässä liikenteessä 3–5 ja sisäverkossa 0–2. Jos suojausprofiileita ei ole ollenkaan käytössä ympäristössä, niin tarkastajan ei tarvitse muistaa kuin 0. Protokollien (porttien) luokittelu menee yksinkertaisesti alussa muutaman luvun lisäyksellä. Viidennessä kohtaa any tarkoittaa käytännössä isoa lukua mutta kaikki portit eivät ole käytössä. Viimeisessä kohtaa on all, jolloin kaikki portit ovat auki.

Protokollien pelkkä lukumäärä ei kerro täysin koko totuutta. Portin numero vaikuttaa myös, mutta ei tarpeeksi merkittävästi, että se olisi käytännöllistä lisätä tähän työhön. Lukumäärä kumminkin luo sen suurimman uhkan. Porttien syvempi pisteytys vaatisi monimutkaisen sovelluksen, että se olisi oikeasti käytännöllistä toteuttaa.

6.6 Protokollien ja suojausprofiilien pisteytys

Taulukko 11. Protokollien ja suojauksien pisteytys

Protokollat	Profiilit
1–2. Todella vähän portteja auki, jolloin riski on pienin mahdollinen. 1 piste.	Jos profiileita on käytössä 0–2 niin tulee 0 pistettä ja jos niitä on käytössä 3–5 niin pisteeksi tulee -1.
3–6. Hieman suurempi määrä portteja auki, mutta riskit ovat vieläkin alhaiset. 2 pistettä.	
7–11. Portteja alkaa olla auki kohtalaisesti ja samalla riskit ovat keskitasoa. 3 pistettä.	
12–20. Portteja on paljon auki mutta selvää rajausta on vielä tehty. 4 pistettä.	
21-any. Any tarkoittaa niin suuria lukuja, että listaaminen ei ole käytännöllistä, mutta kaikki portit eivät ole auki. Käytännössä todennäköisesti mennään sadoissa, ellei tuhansissa aukinaisissa porteissa. 5 pistettä.	
all. Kaikki portit ovat käytössä, jolloin rajausta ei ole yhtään ja riski on suurin. 6 pistettä.	

Lyhyesti selitettynä profiilista tulee joko 0 tai -1. Huomautuksena että pisteytys toimii protokollien kannalta samalla tavalla, oli sääntö sitten sisäverkossa tai ulkoisessa.

Profiilit voisi myös pisteyttää protokollien tapaan, mutta silloin pistetaulukkoa olisi hankala käyttää yleisesti.

Tässä työssä on päätetty, että ilman profiileita oleva palomuuri on oletus ja profiileista saa alennusta. Näin työstä tulee yleismaailmallinen, koska jokaisessa ympäristössä ei välttämättä ole käytössä suojausprofiileita. Vaihtoehtoisesti myös profiilit voisi pisteyttää kuin protokollat, mutta silloin

pistetaulukkoa olisi vaikeampi käyttää yleismaailmallisesti ja kokonaispiste saattaisi vähentyä jopa kolmella pisteellä. Riskimatriisi menisi tässä tilanteessa melkein hyödyttömäksi. Vähintään se menisi vaikeaksi tulkita. Suojausprofiileilla kumminkin on vaikutus, jolloin ne pitää ottaa huomioon.

6.7 Yhteiset pisteet

Kun profiileita on käytössä, niin kokonaispisteestä miinustetaan yksi piste. Profiilien puuttuminen ei vaikuta kokonaispisteeseen. Profiilien vaikutus on hieman suurempi ryppäiden sisälläkin, mutta näin taulukko pysyy paremmin yleismaailmallisena. Tässä työssä myös mahdolliset kuuden pisteen yhdistelmät ja protokollat maalataan punaisiksi. Tämän tarkoitus olisi, että tarkastaja huomaisi myös ne, vaikka kokonaispiste ei menisi punaiselle alueelle.

Taulukosta on siis myös mahdollista saada kokonaispisteeksi yksi, mutta se vain enemmän korostaa kahden pisteen tilannetta, jolloin käytännössä sillä ei ole merkitystä. Sääntö on vain harvinaisen matala riskinen. On myös todennäköistä, että tällaisia sääntöjä ei ole edes luotu vaan jäävät teorian tasolle.

Seuraavan sivun taulukko 12 havainnollistaa miten pisteytys tulee toteuttaa. Osoitteissa on tärkeintä yhdistelmät, jolloin taulukkoon lisätyt muistisäännöt ovat hyödyksi. Protokollat ovat yksinkertaisempia, koska numerot vain tarkoittavat monta porttia on käytössä. Myös profiilien merkintä on muistutettu.

Kokonaispisteet 2–6 ovat vihreällä, jolloin ne menevät Hyvä-luokkaan eli säännöissä ei ole mitään tarkistettavaa. Rajausta on sekä osoitteissa ja protokolleissa. 7–9 kokonaispisteen säännöt menevät ok-luokkaan, jolloin niissä on pieni riski uhkatekijöille. Tarkistaminen on suotavaa, mutta ne eivät silti omaa korkeaa riskitasoa. Porttien tai osoitteiden määrää on rajattu. 10–12 kokonaispisteen omaavat säännöt pitää tarkistaa, koska ne menevät Riski-luokkaan. Protokolleja ja osoitteita on paljon sallittuina ja rajauksia ei ole tehty kumpaakaan päähän. Riskit ovat suurimmillaan näissä säännöissä ja virhe muissa rajauksissa (staattiset reitit) pitää huomata välittömästi.

Luokille voi keksiä sopivammat nimet, jos kokee tarpeelliseksi. Näitä luokkia tullaan käyttämään tässä työssä toteutuksessa.

Taulukko 12. Kokonaispisteet

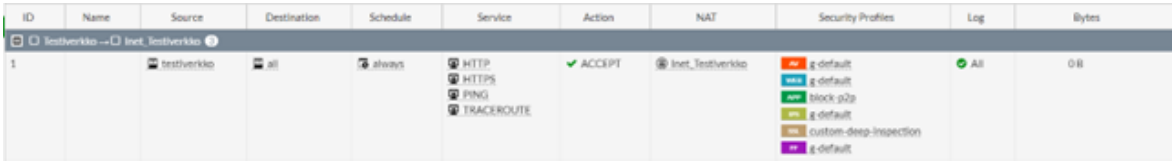
Osoitteiden yhdistelmät ------->

6 pistettä all + all	7	8	9	10	11	12
5 pistettä b + all b + b	6	7	8	9	10	11
4 pistettä c + all yksittäinen + all b + c b + yksittäinen	5	6	7	8	9	10
3 pistettä c+c c + yksittäinen	4	5	6	7	8	9
2 pistettä yksittäiset + yksittäiset	3	4	5	6	7	8
1 pistettä osoite + osoite	2	3	4	5	6	7
+ 0-2 profiilia -> 0 3-5 profiilia -> -1	1 pistettä 1–2	2 pistettä 3–6	3 pistettä 7–11	4 pistettä 12–20	5 pistettä 21->any	6 pistettä all

Aukinaisten porttien määrä ----->

7 TOTEUTUS

Tässä osiossa lähdetään testaamaan riskimatriisia Tieran toimipaikkaan. Testattavia kohteita on viisi. Kolme ensimmäistä kohdetta on suurusjärjestyksessä ja myös viimeinen on suurin. Neljäs kohde erosi luonteeltaan niin paljon ensimmäisistä, jolloin päätöksenä oli ottaa se ennen suurinta kohdetta. Neljäs kohde ei siis soveltunut riskimatriisin testauksen alkuun vaan toimi paremmin loppupäässä. Osion lopussa on myös laboratorio kohta, jossa selvennetään kuinka käytännössä säännöt ovat hieman monimutkaisempia kuin pisteytys voisi antaa ilmi.



Kuva 2. Säännön näkymä (Suopajärvi, 2022)

Kuva 2 selventää mitä säännöstä pitää löytää. Kuvan mukaisesti napataan Source, Destination, Service ja Security Profiles. Security Profiles on siis suojausprofiilit, jolloin tätä ei välttämättä löydy kaikilta. Muu säännöstä on ylimääräistä. Kumminkin kannattaa tarkastaa, että sääntö on läpipäästävä (Accept) eikä estävä (Deny). Deny-säännöillä ei ole mitään riskiluokitusta, jolloin tämän työn soveltaminen niihin olisi tarpeetonta.

7.1 Excel-ohjeet

Kun tiedot on vedetty Excel-muotoon käytössä olevalta sovellukselta, voidaan siitä siistiä turhat sarakkeet pois. Jäljelle pitäisi jäädä viisi kohtaa: A1 kohdalla on ID ja siitä eteenpäin järjestyksessä B1 source, C1 destination, D1 service ja E1 mahdollinen profiles. Näiden soluille ei tarvitse tehdä mitään muuta kuin mahdollinen sääntö, joka maalaa kuutoset punaisiksi mutta se ei ole pakollista. Action-kohdan voi myös jättää (missä tulee ilmi, onko sääntö accept vai deny) koska sen avulla voidaan poistaa estävät säännöt. Action-kohta voidaan laittaa kaiken perään G-sarakkeeseen.

F-sarakkeeseen tulee logiikka. Seuraava taulukko havainnollistaa sen.

Taulukko 13. Excel-taulukon solujen logiikat

Pisteytys (F1)	=JOS.JOUKKO(E2=-1;(B2+C2)/2+D2-1;E2=0;(B2+C2)/2+D2)

Lopputuloksen pitäisi näyttää seuraavan sivun kuvan mukaiselta (Kuva 3). On myös mahdollista värittää pisteytys sarake niin, että väri on tummempi mitä suurempi luku on kyseessä. On mahdollista

myös tehdä värisokeille sopiva malli. Värittömäksi jättäminen ei ole kovin hyvä ratkaisu, koska riskialttiiden sääntöjen huomaaminen on helpompaa värien kanssa.

Kuten alapuolella oleva kuva 3 osoittaa, niin Source- ja Destination-kohtaan tulee sama pistemäärä. Suunnittelun vaihteessa tultiin kokeiltua myös pisteytystä erikseen, mutta se loi vain monimutkaisemman järjestelmän. Se pisteytys ei merkittävästi muuttanut pistetilannetta sääntöjen kohdalla.

Kuva 5 sivulla 30 näyttää suunnittelun eri vaiheen, jossa Excel-malli oli suurempi. Kuva 3 on lopullisen lopputuloksen mukainen. Tämä lopullinen malli ja ohje myös päätyi Tieran saamalle dokumentille. Logiikoita oli alun perin useampia ja Excel oli paljon monimutkaisempi. Loppua kohti Excel kumminkin yksinkertaistui.

Profiles-sarake kannattaa myös jättää, vaikka suojauksia ei olisi käytössä. Näin ei tarvitse alkaa säätämään logiikan kanssa. Profiles-sarakkeeseen voi sitten helposti maalata kaikkiin kohtiin 0. Myös Source-sarakkeen pisteen voi maalata Destination-sarakkeen päälle, kun käyttää yhdistelmiä.

	A	B	C	D	E	F	G
1	ID	Source	Destinatio	Service	Profiles	Pisteytys	Action
2	15	5	5	5	-1	9	ACCEPT
3	18	4	4	6	-1	9	ACCEPT
4	10	4	4	5	-1	8	ACCEPT
5	8	5	5	4	-1	8	ACCEPT
6	21	5	5	5	-1	9	ACCEPT
7	20	5	5	4	-1	8	ACCEPT
8	23	4	4	5	-1	8	ACCEPT
9	12	4	4	2	0	6	ACCEPT
10	17	4	4	6	0	10	ACCEPT
11	19	3	3	6	0	9	ACCEPT
12	14	4	4	2	0	6	ACCEPT
13	16	4	4	1	0	5	ACCEPT
14	22	4	4	6	0	10	ACCEPT
15	25	1	1	6	0	7	ACCEPT

Kuva 3. Lopullisen tuloksen esimerkki (Suopajärvi, 2022)

7.2 Vieraat-palomuuri

2	3	4	5	6	7	8	9	10	11	12
0	0	0	1	2	1	4	4	2	0	0
		Hyvä	ok	Riski	yhteensä					
		3	9	2	14					
		21 %	64 %	14 %						

Kuva 4. Ensimmäisen kohdan tilastot (Suopajärvi, 2022)

Ensimmäinen kohde on sen verran pieni, että kaikki mahtuvat pieneen näytönkaappauskuvaan, kuva 3 toimi sekä esimerkkinä mutta siinä on myös ensimmäisen kohdan säännöt. Kuvan 4 mukaisesti saadut pisteet on laitettu tilastomuotoon, jota tullaan myös käyttämään jokaisessa muussa kohdassa. Hyvä-luokka sisältää 2–6 pisteet, jolloin se on suurin. Nämä säännöt eivät kaipaa sen tarkem-

paa tutkimista vaan ne voidaan sivuttaa. Poikkeuksena voi olla all-sääntö osoitteissa tai protokollissa, jolloin tarkistaminen voi olla järkevää mutta ei pakollista. Suojausprofiilien kanssa kokonaispiste voi tippua Hyvä-luokkaan. Sarakkeessa voi olla silti 6. Siksi näiden värittäminen voisi olla järkevää ja myös niiden tarkistaminen.

Ok-luokka tarkoittaa tässä työssä sääntöjä, jotka ovat saaneet 7–9 pistettä ja ovat vielä matalan riskin sääntöjä, mutta ne olisivat varmuuden vuoksi hyvä tarkastaa, mutta ne eivät sisällä suurta riskiä. Riski-luokka sisältää 10–12 pisteet ja nämä säännöt pitää tarkistaa heti, koska ne sisältävät suuren riskin, jos jotain on konfiguroitu väärin.

Puolet säännöistä koskevat internettiin menevää liikennettä, jolloin suurin osa säännöistä menee ok-luokkaan, mutta riskillisiä sääntöjä on muutama. Profiilien käyttö laskee näiden sääntöjen kokonaispistettä yhdellä. Palomuurilla luonnollisesti oli paljon liikennettä myös internettiin, jolloin profiileita oli paljon käytössä. Jos näissä säännöissä ei olisi ollut profiileita, niin riskiluokka olisi lähempänä kärkeä. Otanta on myös hyvin pieni, mutta antaa hieman suuntaa seuraaviin kohteisiin.

Koska internetin päässä olevia osoitteita on hyvin vaikea rajoittaa, niin osoiteluokkiin tulee melkein automaattisesti vähintään nelonen pisteeksi, jolloin yhteispiste tulee olemaan korkea, vaikka protokolleja olisi vähän. Tässä palomuurissa niitä oli rajattu jolloin 10 pisteitä olisi tullut, ellei profiileita olisi ollut käytössä. Säännöissä 8 ja 10 profiileita oli kaksi vähemmän kuin muissa mutta niistä oli silti tärkeimmät käytössä, jolloin niidenkin yhteispisteet laskivat yhdellä.

Kuten aiemmin mainittu niin otanta on aivan liian pieni, kokoluokka sopii juuri ja juuri karkean riskimatriisin testaamiseen. Tällä kohteella voi hieman hioa matriisia, mutta lopullista versiota sillä ei saa. Saadut tilastot eivät kumminkaan vaikuta liian vääriltä, jos Riski-luokka olisi suurin tai lähempänä 50 prosenttia, niin silloin pitäisi miettiä luokittelut ja pisteytykset uusiksi. Näillä tuloksilla voi rohkeasti lähteä testaamaan vähän suurempaa otantaa.

7.3 Koulut-palomuuri

A	B	C	D	E	F	G	H	I	J	K	L
ID	Source	Destinatic	Service	Security P	Pisteytys					yhteensä	Action
1	4	4	2	-1	5					5	ACCEPT
3	4	4	2	-1	5					5	ACCEPT
7	4	4	1	0	5					5	ACCEPT
9	4	4	2	0	6					6	ACCEPT
10	5	5	2	0	7					7	ACCEPT
36	4	4	2	0	6					6	ACCEPT
14	3	3	2	0	5					5	ACCEPT
40	3	3	2	0	5					5	ACCEPT
41	3	3	2	0	5					5	ACCEPT
16	4	4	6	0	10					10	ACCEPT
17	4	4	2	0	6					6	ACCEPT
22	4	4	6	-1	9					9	ACCEPT
30	4	4	6	-1	9					9	ACCEPT
29	4	4	6	-1	9					9	ACCEPT
27	4	4	6	-1	9					9	ACCEPT
31	4	4	6	-1	9					9	ACCEPT
28	4	4	6	-1	9					9	ACCEPT
32	4	4	6	-1	9					9	ACCEPT
33	4	4	6	-1	9					9	ACCEPT
34	4	4	3	-1	6					6	ACCEPT
26	5	5	6	-1	10					10	ACCEPT
38	5	5	4	-1	8					8	ACCEPT
42	4	4	6	0	10					10	ACCEPT
46	4	4	1	0	5					5	ACCEPT
45	4	4	6	-1	9					9	ACCEPT
47	5	5	4	-1	8					8	ACCEPT
37	4	4	3	-1	6					6	ACCEPT
49	2	2	2	0	4					4	ACCEPT
50	4	4	6	0	10					10	ACCEPT
53	4	4	6	0	10					10	ACCEPT
55	4	4	3	0	7					7	ACCEPT
56	4	4	4	0	8					8	ACCEPT
57	4	4	6	-1	9					9	ACCEPT
58	4	4	6	0	10					10	ACCEPT
59	4	4	6	-1	9					9	ACCEPT

Kuva 5.Toisen kohdan sääntöjen pisteet (Suopajärvi, 2022)

2	3	4	5	6	7	8	9	10	11	12
0	0	1	7	5	2	3	11	6	0	0
		Hyvä	ok	Riski	yhteensä					
		13	16	6	35					
		37 %	46 %	17 %						

Kuva 6. Toisen kohdan tilastot (Suopajärvi, 2022)

Toisessa kohdassa voidaan vielä laittaa säännöt näkyville kuvan 5 mukaisesti, mutta seuraavissa kohteissa on vain kuvan 6 mukaiset tilastot näkyvillä. Sääntöjä tulee olemaan niin paljon, että niiden laittaminen tulisi olemaan epäkäytännöllistä. Kuva 5 myös toimii aiemmin mainittuna esimerkkinä, kuinka Excel kehittyi testaamisen aikana.

Seuraavassa kohteessa on vähän yli kaksinkertainen määrä sääntöjä, jolloin luvut hieman myös tasaantuvat. Liikennettä internettiin on myös suuri määrä, jolloin moni sääntö tippuu ok-luokkaan. Silti riskit pysyvät 17 % paikkeilla. Internettiin menevistä säännöistä myös saataisiin joidenkin pisteitä hieman alas, jos aukinaisten porttien määrää vähän rajoitettaisiin. Punaiset kuutoset osoittavat, että all-sääntö on voimassa.

Ensimmäistä kohdetta lukuun ottamatta tässä kohteessa on vähiten Riski-luokkaan kuuluvia sääntöjä suhteutettuna muihin sääntöihin. Tässäkin näkee suojauksien tehon koska ilman niitä yhdeksän pis-

teen säännöt hyppäisivät kymmeneen ja Riski-luokasta tulisi moninkertaisesti suurempi. Sisäverkossa olevissa säännöissä on myös paljon yksittäisiä osoitteita, koska niiden kanssa on all-sääntö niin se nostaa pistemäärää, mutta vain sen verran että ok-luokasta tulee isoin prosenttimäärä. Ensimmäisen kohdan kanssa paljon yhteistä. Tämä todennäköisesti johtuu palomuurin luonteesta (paljon internettiin päin meneviä sääntöjä) ja sääntöjen vähäisestä määrästä.

Tämä oli jo hyvä testi riskimatriisille sääntöjen lukumäärän avulla. Tällä määrällä sääntöjä matriisia saa hiottua tarkemmaksi, mutta vielä suurempia määriä tarvitaan.

7.4 Yritykset-palomuuri

2	3	4	5	6	7	8	9	10	11	12
4	11	15	16	19	9	13	31	27	1	0
		Hyvä	Ok	Riski	yhteensä					
		65	53	28	146					
		45 %	36 %	19 %						

Kuva 7. Kolmannen kohdan tilastot (Suopajärvi, 2022)

Tässä kohteessa on paljon myös internettiin päin menevää liikennettä mutta joukossa on paljon yksittäisiä osoitteita tai suojaukset ovat käytössä, jolloin Riski-luokka on pieni, vaikka se on suurin tähän mennessä. Ensimmäinen kohta, jossa Hyvä-luokka on muita suurempi, tämä selittyy juuri yksittäisillä osoitteilla tai c-luokan verkoilla. B-luokan verkkoja on hyvin harvassa.

Yritykset-palomuuri on samankaltainen luonteeltaan kuin edelliset palomuurit, mutta suurin ja siksi tarkin. Kun sääntöjen määrä lisääntyy (todennäköisesti sisäverkossa paljon liikennettä myös silloin) niin Hyvä-luokka näyttäisi olevan suurin ja Riski-luokan prosentit asettuvat 20–30 % välille. Tämä on tärkein kohde riskimatriisin kannalta, koska sääntöjen määrä alkaa olla suuri. Edelliset kohteet kun otetaan huomioon, niin todennäköisesti kaikenlaisia sääntöjä on tullut vastaan. Tämän jälkeen hiontaa ei tarvitse tehdä suuresti.

7.5 Laitehallinta-palomuuri

2	3	4	5	6	7	8	9	10	11	12
2	1	11	7	6	6	3	2	10	0	3
		Hyvä	Ok	Riski	yhteensä					
		27	11	13	51					
		53 %	22 %	25 %						

Kuva 8. Neljännen kohdan tilastot (Suopajärvi, 2022)

Laitteet-palomuurilla on laitehallintaan liittyviä sääntöjä, jolloin internetistä tulevaa tai sinne menevää liikennettä ei ole kauheasti. Tämä todennäköisesti vaikuttaa siihen miksi Hyvä-luokka on tähän mennessä suurin. Laitteisiin ei ole tarvetta päästä hallitsemaan suurista verkoista, vaan lähteinä yleensä oli pieni joukko osoitteita.

Kuten kuva 8 näyttää niin Riski-luokan sääntöjä on neljäsosa säännöistä. Ok-luokka on jäänyt pieneksi koska joko osoitteita ei ole paljon ja/tai protokollia on rajattu myös paljon. All-sääntöjä myös löytyy jonkin verran mikä nostaa Riski-luokkaa.

Tilastoihin ei otettu mukaan sääntöjä, joissa lähteinä oli käyttäjiä, koska osoitteiden määrää on vaikea arvioida. Käyttäjä voi käyttää yhtä tai useampaa konetta, all on myös liian raju luokittelu. Tarkan luvun saaminen ei ole siis taattu, sääntöjä on siis hieman enemmän kuin 51. Samoin tehtiin Root-palomuurin tapauksessa seuraavassa kappaleessa, mutta siellä tämän kaltaisia sääntöjä oli huomattavasti vähemmän.

7.6 Root-palomuuri

2	3	4	5	6	7	8	9	10	11	12
13	23	38	57	25	20	17	28	58	8	6
		Hyvä	ok	Riski	yhteensä					
		156	65	72	293					
		53 %	22 %	25 %						

Kuva 9. Viidennen kohdan tilastot (Suopajärvi, 2022)

Root-palomuurilla sääntöjen prosentit ovat täysin samat kuin Laitteet-palomuurilla, vaikka sääntöjä on melkein kuusinkertainen määrä. Kumminkin esimerkiksi 12 pisteen sääntöjä on vain kaksinkertainen määrä. 10 pisteen sääntöjä on eniten Riski-luokasta, joka osoittaa, että korkean riskin omaavia sääntöjä on silti murskaava enemmistö matalassa päädyssä.

Luonnollisesti sääntöjä on paljon koska Root-palomuuri toimii kaikkien palomuurien kanssa yhteistyössä. Root hieman kumminkin erottuu Laitteet-palomuurista koska internettiin päin meneviä sääntöjä on huomattavasti enemmän.

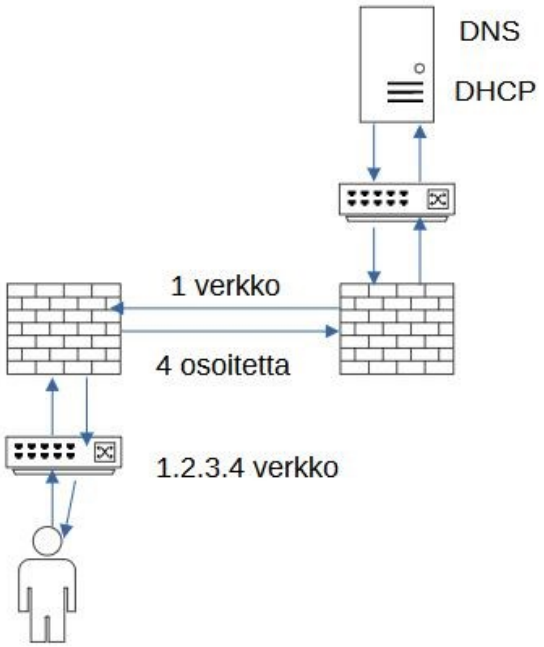
Root-palomuurilla on tasapaino rajoittamisen kanssa koska all-all sääntöjä löytyy paljon, jolloin rajoitus on tehty todennäköisesti kohteena olevassa palomuurissa tai rajoitus on tehty Root-palomuurissa staattisilla reiteillä. Myös yksittäisiä osoitteita tai C-verkkoja on paljon. B-verkkojenkin kanssa on monesti yksittäisiä osoitteita, protokolleissa porttien määrät ovat laidasta laitaan. All-sääntöjä kumminkin on myös paljon, joka nostaa kokonaispistettä keskivälin suuremmalle puolelle.

Suojauksia on jonkin verran mutta nämä säännöt ovat selvästi vähemmistössä. Root-palomuurilla luonnollisesti on paljon liikennettä sisäverkossa.

Tämä oli luonnollisesti kohteena lopullinen testi riskimatriisille. Sääntöjä oli tässä kohteessa yksinään tarpeeksi testaamiseen ja hiomiseen. Kumminkin se myös vaikutti siihen, että lopullinen versio oli

hyvä saada kohtuullisen valmiiksi ennen tätä kohdetta. Tämä johtui siitä, että vaikka kohteen nopealla rytmillä tarkasti päivässä, niin ei sitä kauhean useasti halua tehdä.

7.7 Laboratorio

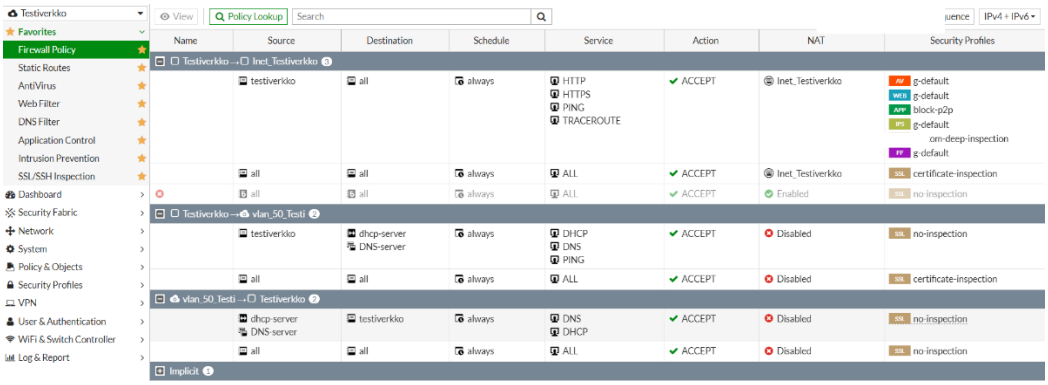


Kuva 10. Laboratorion testiympäristön havainnollistaminen (Suopajärvi, 2022)

Kuva 10 on tarkoitus havainnollistaa Testiverkko-palomuurin ja Root-palomuurin keskinäistä liikennettä. Palvelimet voisivat olla mitä vaan, mutta tähän esimerkkiin on otettu DNS -ja DHCP-palvelimet. Tämä osio keskittyy avaamaan kuvaa enemmän ja käyttämään sitä esimerkkinä. Palomuurisäännöt ovat monimutkaisempia, mitä aluksi voisi luulla.

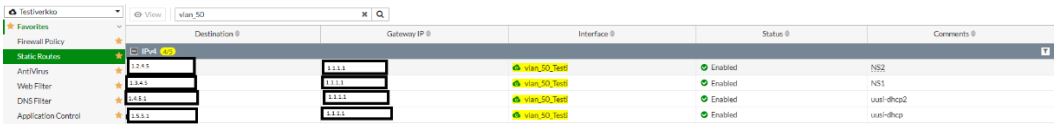
Laboratorio olosuhteisiin on luotu yksinkertaisia sääntöjä, joilla demonstroidaan liikenteen monimutkaisuus. Korkean pisteen omaava sääntö pitää sisällään riskin, mutta käytännössä sitä rajataan staattisilla reiteillä tai protokollia on saatettu rajata toisessa päässä olevassa palomuurissa.

Rajaus jos on jätetty kokonaan pois tai jos rajauksessa on tapahtunut inhimillinen virhe, niin sääntö on oikeasti yhtä riskillinen kuin kokonaispiste antaa ymmärtää. Siksi varsinkin korkean riskin säännöt on hyvä tarkastaa koska voidaan elää turvallisessa kuvitelmassa. Säännön laitossa on voinut tapahtua virhe, koska asentajakin on ihminen. Rajauksen onnistuessa sääntö ei ole käytännössä niin riskialtis kuin kokonaispisteestä voisi olettaa.



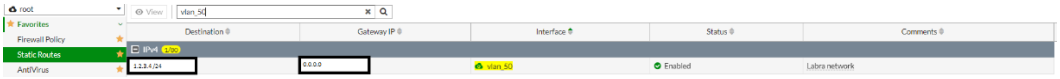
Kuva 11.Testiverkon säännöt (Suopajärvi, 2022)

Kuva 11 on kuvan 10 alkuosa, jossa testiverkko on kuvitteellinen 1.2.3.4 /24 verkko. Kyseessä on siis kaksi alempaa sääntörypästä, ylin on liikenne internettiin päin. Kummassakin alempi sääntö saisi heti 12 pistettä, jolloin ovat suuren riskin sääntöjä. Tarkemmin kun asiaa tutkitaan, niin osoitteita on rajattu staattisilla reiteillä ja samanlainen rajaus on tehty porteille.



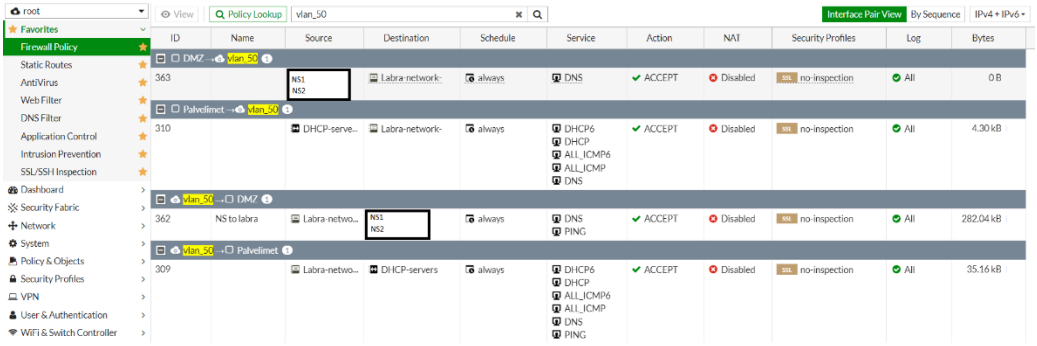
Kuva 12. Testiverkon staattiset reitit (Suopajärvi, 2022)

Kuva 12 näyttää että oikeasti vlan_50-käyttöliittymään kohteeksi on sallittu vain neljä osoitetta, sensuroidut kohdat ovat yksittäisiä kohteita. Eli all-sääntökin muuttuu kohdeluokassa useaksi yksittäiseksi. Testiverkko-palomuurilta ei voi siis vlan_50-käyttöliittymän puolesta päästä muihin osoitteisiin, jollei lisää staattisia reittejä lisää.



Kuva 13. Root-palomuurin staattiset reitit Testiverkko-palomuurille (Suopajärvi, 2022)

Kuva 13 näyttää että Testiverkko-palomuurille on vain yksi staattinen reitti. Vaikka Root-palomuurilla kohteena olisi all, niin oikeasti liikenne menisi vain yhteen c-luokan verkkoon. Lisäämällä lisää staattisia reittejä saataisiin lisää kohteita, mutta tällä hetkellä vlan_50-käyttöliittymään ei voi mennä kuin yksi verkko.



Kuva 14. Root-palomuurin säännöt (Suopajärvi, 2022)

Kuva 14 näyttää säännöt, jotka tulevat tai menevät vlan_50-käyttöliittymään. Kyseessä on siis Testiverkko-palomuuria koskevat säännöt. Säännöissä on jo tehty rajaukset, mutta teoriassa voitaisiin laittaa kohteeksi ja lähteeksi all. Käytännössä tämä tarkoittaisi kumminkin, että lähteenä olisi enimmillään neljä osoitetta ja kohteena yksi C-verkko. Protokollat olisivat kumminkin samat, jolloin näillä säännöillä saadaan niihin erilaiset vaatimukset.

Protokollien osalta voidaan tehdä myös rajausta. Jos Testiverkosta poistetaan protokollien kohdalta viimeinen all-sääntö (Kuva 11) niin palvelimilta päin sallitaan vain kaksi protokollaa. Kuva 14 kumminkin näyttää, että sama DHCP-palvelimelle tehty sääntö (ID 310) sallisi useamman protokollan. All-sääntö kun on voimassa, niin ne menevät läpi, mutta muuten menisi vain kaksi protokollaa läpi.

8 YHTEENVETO

	Kaikki säännöt		
Hyvä	ok	Riski	Yhteensä
264	154	121	539
49 %	29 %	22 %	

Kuva 15. Kaikkien sääntöjen tilasto (Suopajärvi, 2022)

Kuten kuvasta 15 näkee, niin hyvä- ja ok-tasoiset säännöt muodostavat n. 80 % säännöistä ja riskitason säännöille jää se n. 20 %. Yksittäiset kohdat ovat näyttäneet, että riskitason säännöt ovat jatkuvasti pyörineet siinä 20 % paikkeilla ja suurin heitto on ollut muissa luokissa. Luku ei vaikuta liian suurelta tai liian pieneltä vaan juuri siltä, että palomuurissa on luonnollisesti suunnilleen saama määrä korkean riskin sääntöjä. Tämä luku näyttäisi tilastojen mukaan olevan viidesosa säännöistä. Palomuurien sisällöstä voi sitten riippua ovatko säännöt todella turvallisia vai sisältääkö palomuuri matalan riskin sääntöjä paljon, internettiin menevä liikenne vaikuttaa suuresti tähän. Niistä säännöistä harva silti meni suureen riskiluokkaan suojauksien ansiosta, ilman niitä riskiluokka saattaisi kasvaa jopa 30–40 prosenttiin joissain palomuureissa.

Jos haluaisi käyttää pisteytystä osoitteille, jossa kummatkin saavat omat pisteensä niin silloin voisi käyttää taulukon 4 luokittelua pisteytyksen taustana. Tällöin protokolleista pitää vähentää yksi pois, että sitten käytössä olisi 5x5 taulukko. Kumminkin testauksen aikana tämä metodi laski tai nosti kokonaispistettä enimmillään yhdellä, jolloin riskiluokka todennäköisesti silti pysyi samassa. Suurin osa säännöistä siitä huolimatta sai saman pistemäärän, jolloin vain kourallinen muuttui. Ne, jotka muuttuivat, niin olivat todennäköisesti sääntöjä, joissa oli esimerkiksi yksittäinen + all yhdistelmä koska työn pisteytyksellä siitä tulisi 4 mutta taulukon 4 mukaan (5+1) /2 eli 3. Ääripäiden pisteytys olisi siis erilainen luonnollisesti koska pienempi määrä osoitteita hieman ottaa riskiä toisesta päästä pois. Luvut olisivat siis erilaisia hyvä- ja ok-luokissa mutta Riski-luokka pysyisi todennäköisesti suurin piirtein samanlaisena ja se on tärkein kohta tässä työssä.

Työssä käytetty vähän tiukempi linja on silti perusteltua sen kannalta, että riskianalyysin on parempi olla hieman tiukempi kuin liian väljä, sääntö on parempi tarkistaa, jos ei ole varma kuin antaa sen mennä seulan läpi. Ero kumminkin ei ole niin suuri, että muutosta kannattaisi lähteä toteuttamaan koska työssä käytetyllä metodilla saadaan myös käyttökelpoista materiaalia, mutta ehkä seuraavissa versioissa sitä voitaisiin testata uudelleen. Tällä hetkellä enemmän makuasia kumpaa tekniikkaa haluaa suosia.

Saatujen tilastojen perusteella asiantuntija voi sivuuttaa 49 prosenttia säännöistä. Tämä huomattavasti vähentää tarkistettavia sääntöjä ja tarkastusaikaa. Tilanne, jossa vain suuren riskin säännöt halutaan ottaa huomioon, niin säännöistä tarvitsisi tällöin tarkistaa vain 22 prosenttia. Tämä ei ehkä ole kumminkaan suotavaa. Tietenkin kokonaispisteiden arvostelua voi tarkastaja soveltaa mielensä mukaan. Kokonaispistettä voi esimerkiksi soveltaa niin että korkeaan riski luokkaan lisää yhdeksän pisteen säännöt. Tämä hieman nostaa prosentteja tarkistettavien osalta mutta tarkastusaika ei merkittävästi nouse. Tämä on esimerkiksi mahdollista, jos kokee että seitsemän tai kahdeksan pisteen säännöt eivät vaadi tarkastusta.

Laboratorio-osio osoittaa miksi tarkastaminen on tärkeää. Vaikka sääntö omaisi korkean riskin pisteet niin todennäköisesti rajausta on kumminkin tehty. Tämä rajaus pitää tosin tarkistaa inhimillisen tai muun syyn takia. Sääntö voi olla myös vanhentunut ja jäänyt roikkumaan, jolloin se pitää yksinkertaisesti päivittää tai poistaa.

Tarkastamisen nopeus oli hyvä, Excel-kaavio oli saatu kuntoon. Arvio olisi, että kahdeksassa tunnissa hieman hitaallakin vauhdilla saisi 300 sääntöä tarkastettua. Nopealla tahdilla tämän voisi tehdä kuudessa tunnissa.

9 POHDINTA

Työn alussa olleet tavoitteet saavutettiin. Ainoastaan Tieran omien testien tulokset olisi ollut mukava vielä ehtiä saada tähän raporttiin, mutta siinä tuli kiireinen aikataulu vastaan. Työssä kumminkin tuli opittua paljon uutta sekä käytännössä että teorian puolelta. En ihmettelisi, jos tulen käyttämään työn lopputulosta itsekin tulevaisuudessa.

Työn tulos toimii hyvin näinkin, mutta työn edetessä ja varsinkin lopussa selkeni enemmän, kuinka sovellus olisi seuraava askel. Riippuen sovelluksesta se olisi myös nopeampi ja ehkä myös selkeämpi. Se olisi kumminkin seuraava kehityssuunta eikä se muuten vähennä tämän työn arvoa. Tämä työ toimii itsenäisesti oikein hyvin ja vielä paremmin pohjana tulevaisuuden töille.

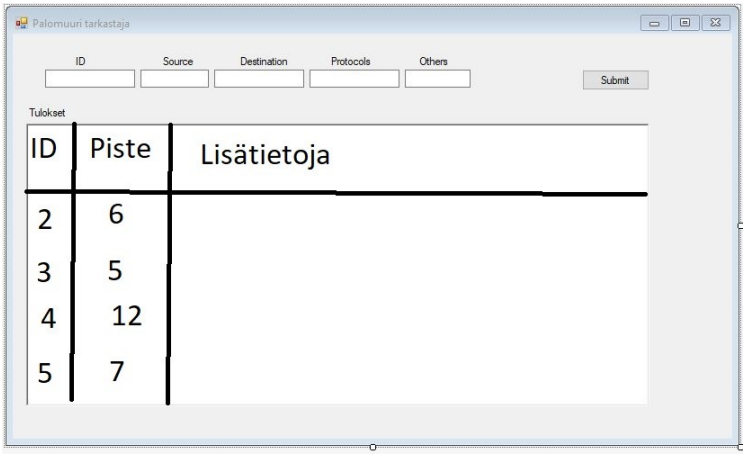
Tarkoitus oli myös tehdä kaikille hyödyllinen opinnäytetyö ja siinäkin minusta onnistuttiin. Kuntien Tiera sai oman dokumenttinsa, joka on käytännössä vain tiivistetty versio tästä raportista. Kaikki tieto ja hyöty on siis kaikkien saatavilla. On mahdollista, että tästä voisi kehittyä jollekin opiskelijalle uusi opinnäytetyö joko mainitun sovelluksen osalta tai muunlaisen jatkokehityksen kautta. Sovelluksesta ei todennäköisesti tulisi julkiseen jakoon kuka sen päättäisi tehdäkään.

Osoitteiden pisteytystä olisi voinut vielä vähän hioa loogisemmaksi, mutta se ei kauheasti vaikuttaisi työn lopputulokseen. Hieman vain jää vaivaamaan tekijää. Tämä kumminkin oli ainoa negatiivinen asia työstä, joka tuli ilmi, jolloin mielestäni työssä on onnistuttu hyvin.

Sekin olisi toinen kehityssuunta, että riskimatriisia sovellettaisiin niin, että se ei käyttäisi yhdistelmiä. Osoitteiden luokitteluun tehtäisiin yksi pykälä lisää. Lähde- ja kohdeosoitteet saavat omat pisteensä. Työn aikana tuli hieman testattua tätä ratkaisua ja lopputulos oli, että se ei merkittävästi muuta pisteitä. Testaus oli kumminkin niin vähäistä, että varmaksi sitä ei voi sanoa. Lähtökohtana voi kumminkin sanoa, että tällä hetkellä on kaksi vaihtoehtoa, miten edetä riskimatriisin kanssa. Kummatkin antavat suunnilleen samankaltaiset pisteet.

Aihe oli omalla tavallaan uusi. Riskimatriiseja ja ohjeita palomuurien tarkastukseen löytyy luonnollisesti paljon, mutta ei suoraan työn lopputuloksen näköistä. Ohjeetkin mitkä tulevat haun jälkeen, ovat epämääräisiä eivätkä ole kovin syvällisiä. Ohjeet ovat siis liiankin yleismaailmallisia. Työ tuo siis uutta näkökulmaa ilmi ja hieman konkreettisemman ohjeen palomuurien tarkastukseen.

Seuraavalla sivulla on hieman enemmän pohdintaa aiemmin mainitusta mahdollisesta sovelluksesta.



Kuva 16. Mahdollisen sovelluksen esimerkki (Suopajärvi, 2022)

Sovelluksen ei tarvitse ulkoisesti olla kovin monimutkainen. Riittää että siihen saa syötettyä tarvittavat tiedot ja kaikki laskeminen luonnollisesti tapahtuu taustalla. Sen tarvitsi vain tulostaa kokonaispiste annetulle säännölle. Sovellus ehkä osaisi hienosäätää pisteytystä, jos sille annetaan jokin tietty riskialtis protokolla tai portti. Tiedot voitaisiin siis antaa porttien kokonaismäärällä tai/ja tietyn protokollan nimellä. Kuva 16 on karkea havainnointi miltä tietojen syöttäminen voisi näyttää. Se nopeuttaisi sääntöjen pisteytystä huomattavasti, mutta teoriassa on parempikin ratkaisu.

Kuvan 16 mukaisesti se voisi ottaa joitain tietoja ylös ja kirjoittaa ne kokonaispisteen perään. Tämä edellyttäisi, että sovellus osaisi itse lukea selaimesta tiedot sivulta. Helpoin ja ehkä tietoturvallisempi ratkaisu olisi, että käyttäjä syöttäisi sovellukselle palomuurista saadun Excel-tiedoston. Sovellus osaisi siitä lukea itse kaiken tarvittavan ja se tulostaisi pisteytyksen Excel-tiedoston pohjalta. Mahdollisesti sovellus osaisi myös tulostaa ylimääräistä tietoa esimerkiksi tietyistä osoitteista tai porteista. Kaikki osoitteet ja portit eivät välttämättä ole aivan tasa-arvoisia.

Tärkeintä kumminkin olisi, että sovellus tekisi mahdollisimman paljon käyttäjän puolesta. Ihannetilanteessa käyttäjän tarvitsee vain syöttää tiedosto tai sivu.

LAINATUT LÄHTEET

Awati, R.;& Scarpati, J. (9. 2021). *Deep packet inspection (DPI)*. Haettu 16. 4. 2022 osoitteesta Techtarget: https://www.techtarget.com/searchnetworking/definition/deep-packet-inspection-DPI

Barracuda Networks. (ei pvm). *What is a Intrusion Detection System?* Haettu 6. 4. 2022 osoitteesta barracuda: https://www.barracuda.com/glossary/intrusion-detection-system

Blank, A. (2004). *TCP/IP Foundations.* Alameda, Kalifornia, USA: John Wiley & Sons, Incorporated. Haettu 3. 3. 2022

Bluecat. (ei pvm). *Glossary: What is DHCP?* Haettu 14. 3. 2022 osoitteesta Bluecatnetworks: https://bluecatnetworks.com/glossary/what-is-dhcp/

Computer Hope. (16. 5. 2020). *IP*. Haettu 24. 2. 2022 osoitteesta Computer Hope: https://www.computerhope.com/jargon/i/ip.htm

Dostalek, L.;& Kabelova, A. (2006). *Understating TCP/IP.* Birmingham, UK: Packt Publishing. Haettu 3. 3. 2022

Elisa. (ei pvm). *Tietoverkot*. Haettu 17. 4. 2020 osoitteesta Yritykielle.elisa: https://yrityksille.elisa.fi/tietoverkot

Firewalls.com. (ei pvm). *What is a utm firewall?* Haettu 16. 4. 2022 osoitteesta Firewalls: https://www.firewalls.com/what_is_utm_firewall

Forcepoint. (ei pvm). *What is an Intrusion Prevention System (IPS)?* Haettu 15. 3. 2022 osoitteesta forcepoint: https://www.forcepoint.com/cyber-edu/intrusion-prevention-system-ips

Fortinet. (2021). FortiGate® 600E Series. *FortiGate 600E Series Data Sheet*. Haettu 21. 3 2022 osoitteesta https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf

Fortinet. (ei pvm). *What is a Cyber Attack?* Haettu 15. 2. 2022 osoitteesta Fortinet: https://www.fortinet.com/resources/cyberglossary/what-is-cyber-attack

Fortinet. (ei pvm). *What Is a Zero Day Attack?* Haettu 18. 2. 2022 osoitteesta Fortinet: https://www.fortinet.com/resources/cyberglossary/zero-day-attack

Fortinet. (ei pvm). *What Is An IPS (Intrusion Prevention System)?* Haettu 21. 2. 2022 osoitteesta Fortinet: https://www.fortinet.com/resources/cyberglossary/what-is-an-ips

Fortinet. (ei pvm). *What is Malware? Types of Malware Attacks*. Haettu 21. 2. 2022 osoitteesta Fortinet: https://www.fortinet.com/resources/cyberglossary/malware

Goralski, W. (2017). *The Illustrated Network : How TCP/IP Works in a Modern Network.* Cambridge, MA, USA: Elsevier Science & Technology. Haettu 7. 3. 2022

Ilascu, I. (17. 9. 2019). *Most Cyber Attacks Focus on Just Three TCP Ports*. Haettu 7. 3. 2022 osoitteesta bleepingcomputer: https://www.bleepingcomputer.com/news/security/most-cyber-attacks-focus-on-just-three-tcp-ports/

Javatpoint. (ei pvm). *SMTP*. Haettu 14. 3. 2022 osoitteesta Javatpoint: https://www.javatpoint.com/simple-mail-transfer-protocol

Juniper Networks. (2014). *Firewall Evolution from Packet Filter to* . Haettu 3. 4. 2022 osoitteesta juniper: https://www.juniper.net/documentation/en_US/learn-about/LA_FIrewallEvolution.pdf

Järvinen, P.;& Rousku, K. (2017). *Työpaikan Tietoturvaopas.* Helsinki, Suomi: Alma Talent. Haettu 21. 2. 2022

Kataja, J. (20. 10. 2017). *SSL-SALAUS: 3 SYYTÄ MIKSI JOKAISEN SIVUSTON TULISI KÄYTTÄÄ SALAUSTA*. Haettu 15. 3. 2022 osoitteesta Zoner: https://www.zoner.fi/tietoturva/ssl-salaus/

Klusaité, L. (15. 9. 2020). *Mitä tarkoittaa phishing eli verkkourkinta?* Haettu 11. 4. 2022 osoitteesta Nordvpn: https://nordvpn.com/fi/blog/verkkourkinta/

Krimaka.net. (ei pvm). *Osi- ja tcp/ip mallit*. Haettu 4. 3. 2022 osoitteesta Krimaka.net: http://www.krimaka.net/tietotekniikka/verkko-ja-ethernet/osi-ja-tcp-ip-mallit.html

Kuntien Tiera Oy. (ei pvm). *Kuntien Tiera Oy*. Haettu 19. 3. 2022 osoitteesta tiera: https://tiera.fi/yritys/

Laakso, M. (2022). *Tietoturvallisuuden peruskäsitteitä*. Haettu 21. 3. 2022 osoitteesta Tietojesiturvaksi: https://tietojesiturvaksi.fi/tietoturvasuunnitelma/tietoturvallisuuden-peruskasitteita

Loshin, P. (2003). *TCP/IP clearly explained.* San Francisco, USA: Morgan Kaufmann Publishers. Haettu 3. 3. 2022

Lähitapiola. (ei pvm). *Riskien kartoitus*. Haettu 21. 3. 2022 osoitteesta lahitapiola: https://www.lahitapiola.fi/asiantuntijapalvelut/riskienhallinta/riskien-kartoitus

McAfee. (16. 1. 2018). *McAfee Enterprise -tuotedokumentaatio*. Haettu 1. 3. 2022 osoitteesta McAfee: https://docs.mcafee.com/fi/bundle/endpoint-security-10.6.0-firewall-product-guide-windows/page/GUID-DFEC962E-2E2F-4BFF-AF9D-5FBA0C167FDC.html

Määttänen, J. (2020). Kandidaattityö. *Riskit ja riskienhallinta vaativissa ohjelmistoprojekteissa*. Espoo, Suomi. Haettu 21. 3. 2022 osoitteesta https://lutpub.lut.fi/bitstream/handle/10024/160895/Kandidaatinty%C3%B6%20-M%C3%A4%C3%A4tt%C3%A4nen%20Jarkko.pdf?sequence=1

Nirav, S. (30. 7. 2021). *Redefining Next-Generation Firewalls*. Haettu 21. 2. 2022 osoitteesta Fortinet: https://www.fortinet.com/blog/business-and-technology/redefining-next-generation-firewalls

Norris, D. (29. 7. 2021). *The OSI Model Explained - 2020 Update*. Haettu 4. 4. 2022 osoitteesta extrahop: https://www.extrahop.com/company/blog/2019/the-osi-model-explained/

Pelastustieto. (8. 2. 2018). *Riskienhallintaa*. Haettu 20. 3. 2022 osoitteesta Pelastustieto: https://pelastustieto.fi/satakunnanpelastuslaitos/2018/02/08/riskienhallintaa/

Pietryga, J. (29. 5. 2021). *Firewall Audit – Why It's Needed & How to Do It Right*. Haettu 24. 2. 2022 osoitteesta xoverture: https://www.xoverture.com/firewall-audit-why-its-needed-how-to-do-it-right-2/

Pinzon, S.;& Nachreiner, C. (ei pvm). *What Is a Port? (and Why Should I Block It?)*. Haettu 7. 3. 2022 osoitteesta Watchguard: https://www.watchguard.com/wgrd-resource-center/security-fundamentals/what-is-a-port

Pro. (ei pvm). *Tietoturvariskit ja niiden arviointi*. Haettu 19. 4. 2022 osoitteesta Tietoturvariskienarviointi: https://www.tietoturvariskienarviointi.fi/

Stallings, W.;& Brown, L. (2018). *Computer Security : principles and practice.* New York, NY, United States: Pearson. Haettu 15. 2. 2022

Suopajärvi, M. (2022).

Traficom. (9. 7. 2020). *Tietoturva*. Haettu 21. 3. 2022 osoitteesta kyberturvallisuuskeskus: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

TrustRadius. (28. 7. 2021). *9 Essential Firewall Statistics for 2021*. Haettu 15. Helmikuu 2022 osoitteesta TrustRadius: https://www.trustradius.com/vendor-blog/firewall-statistics-trends

Työturvallisuuspakki. (ei pvm). *Riskienhallinta.* Haettu 20. 3. 2022 osoitteesta https://xn--tyturvallisuuspakki-r6b.fi/riskienhallinta/

Vanhatapio, J. (24. 1. 2020). *MIKÄ ON HTTP?* Haettu 15. 3. 2022 osoitteesta Zoner: https://www.zoner.fi/tietoturva/http/