Onni Korhonen

Fortigate-palomuurin käyttöönotto Kajaanin ammattikorkeakoulun tietojärjestelmälaboratoriossa

Tradenomi

Tietojenkäsittely

Kevät 2023

KAMK • University of Applied Sciences

Tiivistelmä

Tekijä: Korhonen Onni

Työn nimi: Fortigate-palomuurin käyttöönotto Kajaanin ammattikorkeakoulun tietojärjestelmälaboratoriossa

Tutkintonimike: Tradenomi (AMK), tietojenkäsittely

Asiasanat: palomuuri, tietoturva, IPv6, Fortinet

Erilaiset verkon kautta leviävät haittaohjelmat alkoivat yleistymään 1980-luvun lopulla, jolloin ne pystyivät leviämään jo ympäri maailman. Haittaohjelmia vastaan kehitettiin palomuurit, joiden avulla pystyttiin hallinnoimaan ja tarvittaessa estämään verkon läpi liikkuvaa liikennettä. Ensimmäiset palomuurit tarkastivat verkkoliikenteen TCP/IP-paketeista IP-osoitteet ja porttinumerot, joiden avulla ne sallivat tai estivät liikennettä. Myöhemmin kehitettiin sovellustason palomuureja, jotka pystyivät analysoimaan TCP/IP-paketin sisällön ja sen perusteella päättelemään, oliko liikenne haluttua vai ei. Nykyiset palomuurit voivat käyttää näitä tekniikoita yhdessä tarpeen mukaan.

Tämän opinnäytetyön käytännön osuudessa tavoitteena oli vaihtaa Kajaanin ammattikorkeakoulun tietojärjestelmälaboratorioon uusi Fortinetin palomuuri entisen tilalle. Tavoitteena oli säilyttää verkkoympäristössä vähintään samanlaiset toiminnot kuin entisen palomuurin avulla ja mahdollisuuksien mukaan myös lisätä niitä. Lisäksi tavoitteena oli myös selvittää, voisiko laboratorion verkkorakennetta yksinkertaistaa. Kun uusi palomuuri oli toiminnassa, niin työssä perehdyttiin myös IPv6-osoitteiden käyttöön uudessa palomuurissa ja mahdollistettiin laboratorion verkkoliikennöinti myös IPv6-osoitteilla nykyisten IPv4-osoitteiden rinnalla.

Palomuurin käyttöönotto onnistui ja laboratorion verkkoympäristöä saatiin parannettua. Verkkoympäristön rakenne yksinkertaistui ja verkon käyttäjille saatiin mahdollistettua uusia toimintoja. Lisäksi saatiin mahdollistettua IPv6-osoitteilla liikennöinti laboratorion verkkoympäristössä sisä- ja ulkoverkon välillä.

Abstract

Author(s): Korhonen Onni

Title of the Publication: Deployment of Fortigate firewall to the Information Technology Laboratory at Kajaani University of Applied Sciences

Degree Title: Bachelor of Business Administration, Business Information Technology

Keywords: firewall, information security, IPv6, Fortinet

In the late 1980s, malware that spread through the internet started to be more common. Firewalls were developed to control and possibly block the traffic going through the network. The first firewalls could check IP-addresses and port numbers from the TCP/IP-packet of the network traffic and based on those factors it would allow or block the traffic. Later application firewalls were developed and those could analyze the content of the TCP/IP-packet and allow or block the traffic based on that. Modern firewalls can use these techniques together based on need.

The goal of this thesis's practical part was to install a new firewall to the information technology laboratory of Kajaani University of Applied Sciences. The aim was to at least maintain the current features that the old firewall allowed and possibly even enable some new features. One more goal was to figure out if it was possible to simplify the network structure of the laboratory. After the new firewall was up and running it was needed to figure out and made possible to use the network with IPv6-addresses beside IPv4-addresess.

The deployment of the firewall was a success, and the network structure of the laboratory was made better. The network structure was simplified and more features were enabled to the users of the network. It was also made possible to have network connections between internal and external networks with IPv6-addresses.

Sisällys

1 Johdanto

Palomuureilla on nykypäivän verkkoympäristöissä hyvin merkittävä rooli. Niiden avulla voidaan hallita ja monitoroida verkon liikennettä hyvin monipuolisesti ja näin mahdollistaa verkon turvallisuus. Organisaatioiden on entistä tärkeämpää ottaa nämä asiat huomioon, koska verkkoliikenteen määrän jatkaa voimakasta kasvuaan tuoden samalla lisää uusia uhkia ja mahdollisuuksia verkon väärinkäytölle.

Kajaanin ammattikorkeakoulun tietojärjestelmälaboratorio mahdollistaa nykyaikaisen verkkoympäristön hallinnoinnin ja kehittämistyön opiskelijoille. Tietojärjestelmälaboratorion palomuuri täytyi vaihtaa uuteen. Kyseinen työ suoritettiin opiskelijoiden ja laboratorion ylläpitäjien yhteistyössä. Tämän opinnäytetyön projektiosuus kattaa tuon uuden palomuurin käyttöönoton. Aihe on rajattu koskemaan juuri tietojärjestelmälaboratorion tarpeisiin tehtäviä määrityksiä palomuurissa. Teoriaosuudessa avataan palomuurien eri toimintaperiaatteita sekä palomuurin merkitystä entisissä ja nykyisissä verkkoympäristöissä.

2 Teoriataustan esittely

Opinnäytetyön teoriaosuudessa käydään läpi palomuurin merkitystä ja haittaohjelmien toimintaa sekä nykyisissä että entisissä verkkoympäristöissä. Teoriaosuuden tehtävä on auttaa lukijaa ymmärtämään syyt, minkä takia palomuuri on oleellinen osa verkkoympäristöä.

Projektin käytännön tehtävien onnistumiseen tarvitaan kirjallisuutta lähinnä vain palomuurivalmistajan omista dokumentaatioista. Näihin valmistajan materiaaleihin tukeudutaan vahvasti projektin aikana ja asioita tullaan opiskelemaan tarvittaessa, kun ne tulevat eteen.

2.1 Haittaohjelmien leviäminen

Haittaohjelmat, kuten virukset, madot ja troijalaiset, ovat vaikuttaneet valtavasti tietokoneiden tietoturvaan 1980-luvulta lähtien. Haittaohjelmia oli ollut olemassa aikaisemminkin, mutta ne eivät sen ajan teknologialla pystyneet juuri leviämään ja aiheuttamaan tuhoa. 1980-luvulla syntyivät ensimmäiset haittaohjelmat, jotka levisivät laajasti jopa ympäri maailmaa. [1, s. 52.]

Aluksi haittaohjelmat levisivät lähinnä vain yritysten omissa sisäverkoissa. Haittaohjelmien muualle leviäminen vaati ihmisiltä aktiivista toimea, kuten saastuneen levykkeen kuljettamista toiseen paikkaan tai haitallisen sähköpostin avaamista. 1990-luvulla internet alkoi yleistymään, jolloin haittaohjelmat pystyivät leviämään myös suoraan verkon välityksellä laajasti eri puolille maailmaa. [1, s. 52–53; 62–66.]

2000-luvulla verkon kautta leviävät haittaohjelmat yleistyivät huomattavasti ja nähtiin, kuinka nopeasti ne pystyivät leviämään. Hyvä esimerkki tästä on ensimmäinen UDP-pakettien avulla levinnyt verkkomato nimeltä Slammer. Slammer saastutti Microsoftin SQL-tietokantapalvelimia ja koska se käytti leviämäiseen UDP-paketteja, sen ei tarvinnut odottaa kohdelaitteelta vastausliikennettä. Kun UDP-paketti pääsi sisään haavoittuvaan laitteeseen, laite saastui heti ja alkoi levittämään haittaohjelmaa myös itse. Slammer lähti liikkeelle 24. tammikuuta 2003 ja vain 14 minuutissa se ehti saastuttaa kaikki mahdolliset kohteet, jotka se pystyi saastuttamaan. Kaikkiaan saastuneita palvelimia oli noin 75 000. [1, s. 66–68, 2.]

Vastaavan kaltaisesti levinneitä haittaohjelmia nähtiin vielä useampi Slammerin jälkeisenä aikana. Yksi syy näiden haittaohjelmien tehokkaaseen leviämisen oli huono tietoturvan taso sen aikaisissa

tietokoneissa. Vuonna 2003 Windows-tietokoneiden mukana ei edes tullut vakiona minkäänlaista palomuuria. Näin ollen melkein mihin tahansa Windows-tietokoneeseen pystyi ottamaan internetistä yhteyden mihin tahansa avoinna olevaan porttiin. Nopeasti levinneiden haittaohjelmien jälkeen laitevalmistajat alkoivat panostamaan laitteiden tietoturvaan. Etenkin huonosta tietoturvasta arvosteltu Microsoft käänsi suuntansa ja muuttui lopulta mallikuvaksi muille. Palomuurit ja muut suojausjärjestelmät kehittyivät ja yleistyivät, jolloin pahimmat verkkomatoepidemiat alkoivat häviämään ja lähes katosivat. Viimeinen suuri verkkomato oli vuonna 2008 löydetty Conficker, joka saastutti yli 10 miljoonaa tietokonetta. [1, s. 69.]

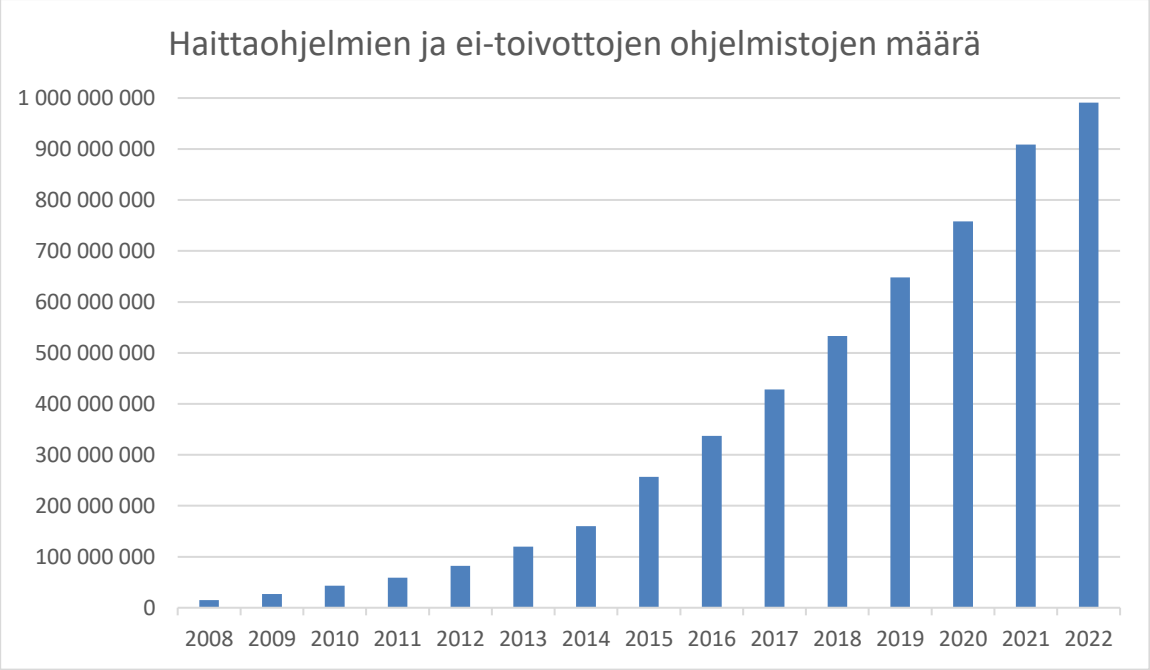
Palomuurien ja verkkolaitteiden kehittyessä itsestään leviävät haittaohjelmat ovat käytännössä hävinneet pois. Nykyiset haittaohjelmat tarvitsevat leviämiseen käyttäjiltä jotain aktiivista toimintaa, kuten saastuneen ohjelman suorittamista tietokoneella. [1.]

Myös haittaohjelmien luonne on muuttunut viimeisten 40 vuoden aikana paljon. Haittaohjelmat olivat 1980- ja 90-luvuilla usein melko harmittomia siinä mielessä, että ne eivät aiheuttaneet käyttäjille suurta vahinkoa. Haittaohjelman tarkoitus saattoi olla vain nähdä se, kuinka tehokkaasti se leviäisi tai osoittaa jonkin tietyn palvelun haavoittuvuus. Nykypäivän haittaohjelmat ovat useimmiten tehty hyötymistarkoituksessa. Niiden kehittäjät pyrkivät hyötymään uhreiksi joutuneiden kustannuksella. Haittaohjelmat voivat muun muassa lukita käyttäjän koneen ja vaatia lunnasrahoja tai valjastaa käyttäjän tietokoneen osaksi laajempaa bottiverkkoa. Nykyisiä haittaohjelmia levitetään useimmiten erilaisten huijausten avulla, joilla lopulta käyttäjä saadaan suorittamaan tietokoneellaan haitallinen ohjelma. Nykyisten haittaohjelmien tyypillisin leviämiskeino on sähköpostin kautta lähetyt kalasteluviestit. Usein niissä lähettäjä esittäytyy jonain legitiiminä tahona ja viestin tavoitteena on saada huijattua käyttäjä joko avaamaan linkki tai lataamaan koneelleen haittaohjelman toimintaa edesauttava tiedosto. [1, 3.]

2.2 Haittaohjelmien ja verkkoliikenteen määrä

AV-TEST on saksalainen riippumaton tutkimuslaitos, joka on 15 vuoden ajan perehtynyt tietojärjestelmien turvallisuuteen. Heidän tutkimusosastollansa on koottuna yksi maailman suurimmista haittaohjelmien kokoelmista. Tällä hetkellä AV-TEST-tutkimuslaitoksen arvion mukaan maailmassa olisi kaikkiaan noin 1,4 miljardia erilaista haittaohjelmaa tai ei-toivottua ohjelmistoa (kuva 1). Ei-toivottu ohjelmisto (PUA) tarkoittaa sellaista ohjelmistoa, jolla on ominaisuuksia ja kykyjä käyttäytyä siten, että ne voivat saattaa käyttäjän laitteen vaaraan tai tuhlata laitteen ja käyttäjän

resursseja. Niitä ei vielä lasketa haittaohjelmistoiksi, mutta nykyiset palomuurit pyrkivät estämään niiden käytön (14). AV-TEST havaitsee yli 450 000 uutta haittaohjelmaa tai ei-toivottua ohjelmistoa päivittäin. Vuonna 2021 he havaitsivat kaikkiaan noin 150 miljoonaa uutta haittaohjelmaa ja 9 miljoonaa ei-toivottua ohjelmaa. Tämä tarkoittaa sitä, että joka sekunti havaitaan vähintään 3 uutta haittaohjelmaa tai ei-toivottua ohjelmaa. [4.]



Kuva 1. Haittaohjelmien ja ei-toivottujen ohjelmiston määrä vuodesta 2008 eteenpäin. Vuoden 2022 lukuun on laskettu tammi-syyskuun luvut [4].

Myös verkkoliikenteen määrä verkossa on kasvanut viime vuosina voimakkaasti. Ciscon vuonna 2018 tekemän arvion mukaan vuonna 2022 internetissä liikkuisi globaalisti noin 150 000 gigabittiä dataa joka sekunti (kuva 2).

Year	Global internet traffic
1992	100 GB per day
1997	100 GB per hour
2002	100 GB per second
2007	2,000 GB per second
2017	46,600 GB per second
2022	150,700 GB per second

Kuva 2. Verkkoliikenteen määrä internetissä maailmanlaajuistesti eri vuosina [5].

Verkkoliikenteen ja haittaohjelmien määrän kasvu osoittaa, että verkkoympäristöt ja -laitteet täytyy suojata myös jatkossa mahdollisimman hyvin.

2.3 Palomuurien tarve

Tietotekniikan termi ”palomuuri” on syntynyt verrannollisesti suoraan käytännön palomuurista, jonka tehtävä on fyysisesti estää tulen leviäminen ja joka konkreettisesti voi tarkoittaa esimerkiksi tulenkestävien rakennusmateriaalien käyttöä. Tietotekniikassa palomuurin tehtävä on estää ei-toivottu liikenne eri verkkojen välillä. Tyypillisin paikka palomuurille on yksityisen ja ulkoisen verkon välillä. [6, s. 54.]

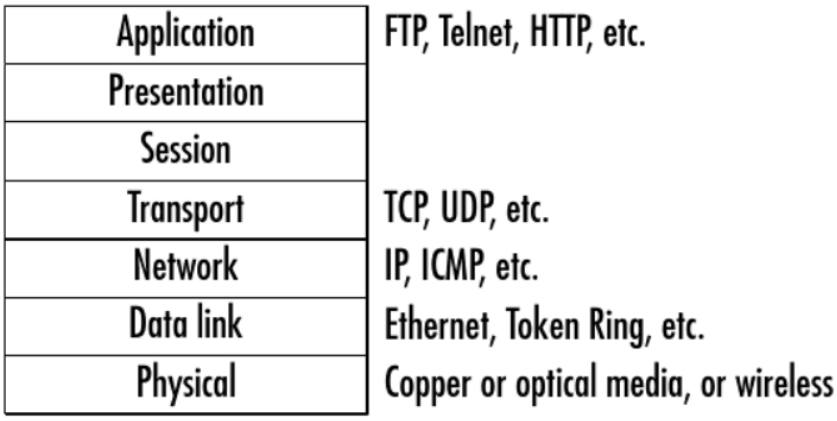
Ensimmäiset palomuurin kaltaiset laitteet kehitettiin 1980-luvun lopussa [7]. Siihen asti uskottiin pitkälti laitteiden kykyyn suojata itse itsensä verkon haitallisilta hyökkäyksiltä. Verkon laajentuessa ja uhkien kasvaessa tällainen suojaustyyli kuitenkin osoittautui hankalaksi ja riskialttiiksi, jolloin alettiin kehitellä parempia keinoja suojata verkon laitteita. [6, s. 54.]

Yksinkertaisimmillaan palomuuri toimii siten, että palomuuriin tehdään haluttu konfiguraatio, joka sallii halutut paketit palomuurin läpi ja estää muut paketit. Palomuuri tarkastelee sen läpi liikkuvien pakettien osioita, kuten lähettäjän IP-osoite, vastaanottajan IP-osoite, lähettäjän portin numero, vastaanottajan portin numero sekä protokolan tyyppi, ja päästää paketit läpi, jos osiot vastaavat sallittujen arvojen listalla olevia arvoja. [8, s. 1.]

Palomuurit ovat nykyään välttämättömiä osia verkon suojaamisessa ja niitä on otettu laajasti käyttöön useimmissa yrityksissä ja instituutioissa suojaamaan yksityistä verkkoa. Tyypillisesti palomuuri asennetaan sisä- ja ulkoverkon, yleensä internetin, välille, jolloin kaikki paketit näiden verkkojen välillä kulkevat palomuurin kautta. [6, s. 54.]

2.4 Erilaiset palomuurit

Ensimmäiset palomuurit toimivat OSI-mallin kuljetus- tai verkkotasolla (kuva 3). Ne määrittelivät paketteja yksinkertaisten tietojen, kuten vastaanottajan ja lähettäjän IP-osoitteiden mukaan. Tällaisista palomuureista on olemassa sekä tilattomia että tilallisia versioita. 1990-luvun alussa kehitettiin myös OSI-mallin ylimmällä, eli sovellustasolla, toimivia palomuureja, jotka pystyivät suorittamaan tarkempaa pakettien tarkastelua (kuva 3). 2000-luvun alussa suurin osa palomuureista oli näiden edellä mainittujen yhdistelmiä, jotka hyödynsivät kaikkia eri palomuurien hyviä puolia. [9.]



Kuva 3. OSI-mallin eri tasot sekä esimerkkejä niiden käyttämistä protokollista [6, s. 56].

2.4.1 Tilaton palomuuri

Tilaton palomuuri toimii tutkimalla jokaisen yksittäisen paketin lähettäjän ja vastaanottajan IP-osoitteita sekä portin numeroa, jotka sijaitsevat OSI-mallin kuljetus- ja verkkotasoilla. Tällaista pakettia kutsutaan TCP/IP-paketiksi. TCP/IP-paketin portin numero määräytyy sen mukaan, mihin palveluun se haluaa paketin lähettää. Esimerkiksi HTTP-protokola käyttää porttia 80, joten kaikki

HTTP-palvelimelle tulevat paketit määrittävät määränpääportiksi portin 80. Useimmiten kohdeportti on määritelty IP-osoitteen perään. Esimerkkinä 192.168.10.133:80, jossa 192.168.10.133 toimii palvelimen IP-osoitteena ja :80 määrittää kohdeportiksi portin 80. [10, s. 193.]

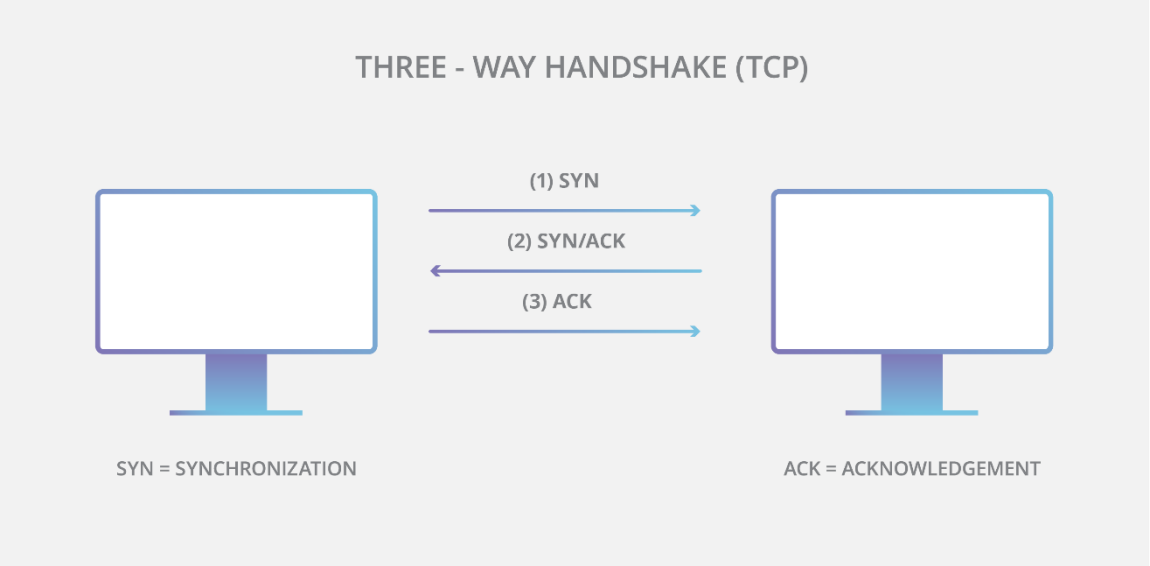
Tilattomaan palomuuriin täytyy tehdä säännöstö, johon se vertaa sen läpi pyrkiviä paketteja. Säännöstöön voidaan kieltää tai sallia eri IP-osoitteita ja määritellä niille kielletyt ja sallitut portit. Esimerkkinä sähköpostipalvelimeen voidaan sallia liikenne SMTP-porttiin 25 ja kieltää liikenne muihin portteihin. [10, s. 194.]

Tilattoman palomuurin suurin heikkous on se, että se luottaa sen läpikulkevien pakettien antamiin tietoihin ja toimii niiden mukaan. Järjestelmään tunkeutuja voi käyttää eri tekniikoita, joilla hän pystyy muuttamaan lähtevien pakettien IP-osoitteita. Tilaton palomuuri ei pysty tunnistamaan tällaista muuteltua pakettia aidosta. [10, s. 194.]

Toinen tilattoman palomuurin heikkous on se, että se tarkastelee jokaista sen läpi kulkevaa pakettia yksittäisenä pakettina, eikä ota sen tarkastelussa huomioon aiemmin tai myöhemmin läpikulkevia paketteja. Tilattoman palomuurin suurimpia etuja taas on sen nopeus, helppokäyttöisyys ja edullisuus. Se suodattaa paketit nopeasti, eikä sen käyttöönotto vaadi suurta konfiguroimista. [10, s. 194–195.]

2.4.2 Tilallinen palomuuri

Tilallinen palomuuri eroaa tilattomasta siinä, että se pitää kirjaa verkkoistunnoista ja tunnistaa saman istunnon paketit yhdeksi kokonaisuudeksi. Kun palvelin muodostaa yhteyden toiseen palvelimeen, se lähettää ensin SYN-paketin, johon kohde palvelin vastaa SYN/ACK-paketilla, johon lähettäjä vielä vastaa ACK-paketilla (kuva 4). [11.] Kun palomuuri saa SYN-paketin käsiteltäväksi, se tunnistaa uuden yhteyden ja merkkaa sen ylös yhteystaulukkoon. Kun palomuuri saa käsiteltäväkseen muita paketteja, se vertaa niiden tietoja yhteystaulukon tietoihin. Jos yhteystaulukosta löytyy täsmäävä yhteys, palomuuri päästää paketit läpi. [6, s. 56.]



Kuva 4. Kahden palvelimen välinen kolmivaiheinen TCP-kättely [11].

Tilallisen palomuurin heikkous on se, että yhteyksiä tarkistaessaan se joutuu käyttämään tietokoneen resursseja. Tällöin siihen voidaan kohdistaa DDoS-hyökkäyksiä, joissa palvelimelle lähetetään suuria määriä paketteja, eikä sillä riitä resurssit käsittelemään paketteja tarpeeksi nopeasti. [12.]

2.4.3 Sovelluspalomuuri

Sovelluspalomuuri tarkastaa jokaisen yksittäisen paketin kuljetus- ja verkkotason lisäksi myös sovellustasolla, joka on ISO-mallin kaikista korkein taso (kuva 3). Sovelluspalomuuri tietää, miten erilaiset sovellukset toimivat ja millaisia paketteja niiden pitäisi lähettää sekä vastaanottaa. Näin ollen se pystyy tarkemmin analysoimaan paketteja ja estämään niiden eteenpäin ohjaamisen, jos ne eivät vastaa sovelluksen käyttämiä paketteja. [10, s. 195.]

Sovelluspalomuuri toimii myös välityspalvelimena ulkoisen ja sisäisen palvelimen välillä. Ulkoiselle palomuurille ei siis anneta sisäisen palvelimen osoitetta, vaan palomuurin osoite. Tällöin liikenne kulkee ensin vain palomuurille, joka analysoi paketit ja joko lähettää tai estää pakettien kulkeutumisen sisäiselle palvelimelle. Sovelluspalomuuri voi myös tallentaa sisäisten palvelimien paketteja omaan muistiin, jolloin se pystyy vastaamaan ulkoisille palvelimille suoraan. [10, s. 196.]

Sovelluspalomuurin huono puoli on se, että se vaatii enemmän resursseja pakettien analysointiin, mikä hidastaa verkon nopeutta. Lisäksi se vaatii tilalliseen ja tilattomaan palomuuriin verrattuna

enemmän konfigurointia ja ylläpitoa, mikä vie resursseja. Lisäksi palomuuri ei pysty tunnistamaan uusia protokollia ja sovelluksia, jos niitä ei erikseen konfiguroida. [10, s. 196.] [11, s. 57.]

2.5 Palomuurin merkitys nykyisessä verkkoympäristössä

Palomuurien pääasiallinen tehtävä on pysynyt niiden syntyhetkestä nykypäivään samana; se estää epätoivotun liikenteen verkon eri laitteiden välillä. Tällä tavalla voidaan estää erilaisten haittaohjelmien pääsy suojattavan verkon laitteille. Nykyiset palomuurit osaavat erottaa huomattavasti tarkemmin epätoivotun liikenteen toivotun liikenteen seasta ja näin toimimaan tehokkaammin.

Haittaohjelmien estämisen lisäksi palomuurit suojaavat verkon yksityisyyttä. Verkon laitteet voivat sisältää arkaluontoista tietoja, johon pääsy halutaan sallia vain tietyille tahoille. Palomuureilla voidaan hallita pääsyä verkon eri osiin ja näin varmistaa esimerkiksi tietosuojan toteutuminen. [13.]

Nykyisillä palomuureilla voidaan myös monitoroida verkon käyttöä tehokkaasti. Palomuurien kautta kulkevaa liikennettä voidaan tarkastella ja verkon ylläpitäjät voivat tehdä monitoroinnin perusteella kehittää verkkoa tehokkaammaksi tai paremmin suojatuksi. [13.]

3 Projektin esittely

Kajaanin ammattikorkeakoulun tietojärjestelmälaboratorio on koulun muusta verkosta erillään oleva verkkokokonaisuus, joka sisältää muun muassa oman fyysisen konesalin. Laboratorio on opettajien ja työntekijöiden lisäksi käytössä myös laajasti opiskelijoiden erilaiseen käyttöön. Tietojärjestelmälaboratorio antaa opiskelijoille laajan verkkoympäristön käyttöön, mikä edesauttaa oppimisessa ja taitojen kehittämisessä.

Yksi oleellisimpia asioita tietojärjestelmälaboratorion verkkoympäristössä on sen palomuuri. Palomuurin kautta kulkee verkkoympäristön eri verkkojen liikenne. Samalla palomuurissa määritellään, millainen liikenne sallitaan ja mikä estetään kulkemasta palomuurin läpi.

Tietojärjestelmälaboratoriossa on ollut käytössä Paloalton palomuuri. Projektin päätavoite on saada vaihdettua Paloalton palomuuri uuteen Fortigaten palomuuriin siten, että verkkoympäristön nykyinen toiminnallisuus säilyy tai muuttuu paremmaksi sekä suorittaa palomuurin vaihtaminen niin, että siitä ei aiheudu ongelmia tietojärjestelmälaboratorion päivittäiselle toiminnalle. Projekti suoritettaan yhteistyössä opiskelijoiden ja tietojärjestelmälaboratorion ylläpitäjien kesken.

Palomuuri pitää vaihtaa kahdesta pääsyystä: Paloalton palomuurin lisenssit ovat vanhentumassa ja nykyinen palomuuri sisältää vain 1Gbps nopeutta tukevia portteja. Paloalton lisenssien vanhentuessa palomuurista poistuu toimintoja ja oleellisimpana puutteena palomuuri ei enää päivitä uusimpia haittaohjelmien signeerauksia (14). Uusi Fortigaten palomuuri sisältää myös 10Gbps nopeutta tukevia portteja, jolloin tietojärjestelmälaboratorio voisi hyödyntää kaiken mahdollisen Funetin tarjoaman kapasiteetin ulkoverkkoon liikennöidessä.

4 Projektin lähtötilanne

Projektin alkaessa tietojärjestelmälaboratorion konesaliin oli jo valmiiksi asennettu fyysisesti kaksi kappaletta Fortinetin valmistamia Fortigate 600E -palomuuria (kuva 5). Niille oli rakennettu hallintayhteys palomuurin management-portin kautta. Näin palomuuria pystyi konfiguroimaan suoraan tietojärjestelmälaboratorion työasemilta. Lisäksi niille oli konfiguroitu toimintakuntoon valmiiksi High Availibity, eli kahdennus. Kahdennuksen ansioista palomuureille tehtävät määritykset voitiin tehdä vain yhdelle palomuurille, josta ne siirtyivät automaattisesti toiselle palomuurille.

Kuva 5. Fortigate 600E -palomuuri. [15]

5 Palomuurin määritykset

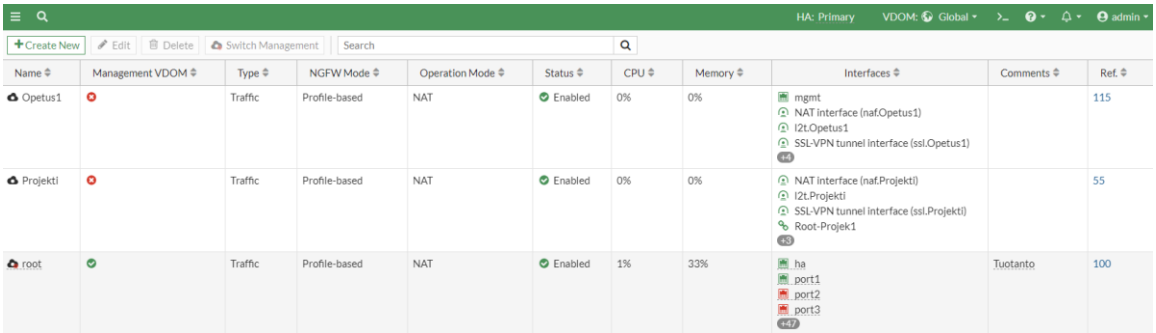
Valtaosa vaadittavasta konfiguroinnista tehtiin suoraan itse palomuuriin sen oman graafisen hallintaympäristön kautta. Vaadittavaa tietoa ja ohjeistusta konfigurointiin haettiin suoraan valmistajan omasta dokumentaatiosta heidän nettisivuiltaan, josta löytyy hyvin kattavasti tietoa eri laitteiden konfiguroinnista ja ominaisuuksien toiminnasta.

5.1 VDOM

Fortigate-palomuuri voidaan jakaa useampaan virtuaaliseen domainiin (VDOM), mikä mahdollistaa usean eri verkkoympäristön toimimisen toisistaan erillään samalla palomuurilla. Vakiona suurin osa Fortigate-palomuureista tukee kymmenen eri VDOMin käyttöä. Jokaiselle eri VDOMille pitää määrittää erikseen erilaiset määritykset, kuten esimerkiksi palomuurisäännöt ja reitit ykset.

Jotta useita VDOM:ja saadaan käyttöön, pitää ensin kytkeä sen asetus päälle ”System -> Settings” -sivulta. Sivulta löytyy ”System Operation Settings” -kohdan asetuksia ”Enable Virtual Domain”, joka pitää aktivoida. Tämän jälkeen palomuurin graafiseen hallintanäkymään tulee oikealle ylös näkyviin VDOM-valikko, josta voidaan valita se VDOM, jota halutaan käsitellä. Palomuuri luo automaattisesti root-VDOMin, jonne siirtyy kaikki sen hetkiset määritykset. Valikosta löytyy root-VDOMin lisäksi myös Global-VDOM, jonka kautta määritetyt asetukset koskevat kaikkia palomuurille määritettyjä VDOMeja.

VDOMien asetuksia voidaan tarkastaa ja muuttaa ”System -> VDOM” -sivulta (kuva 6). Lisäksi sieltä voidaan luoda uusia VDOM:ja ”Create New” -napin takaa.



Kuva 6. VDOMien hallintasivun näkymä.

Tietojärjestelmälaboratorion ympäristössä VDOM-ominaisuus on hyödyllinen, koska sillä saadaan rajattua ympäristöjä erilleen toisistaan ja rajattua pääsyä palomuuriin tiettyihin alueisiin eri henkilöille. Laboratorion verkko jaettiin kolmeen eri VDOMiin: Opetus, projekti ja root. Opetus-VDOM kattaa opiskelijoiden käytössä olevan verkot. Projekti-VDOM sisältää verkot sellaisille projekteille, jotka halutaan pitää erillään vapaammista opiskelijaverkoista. Root-VDOM sisältää tuotantoverkot ja toimii myös palomuurin hallinta-VDOMina. Rajaamalla opiskelijoiden käytössä olevat verkot opiskelija-VDOMiin opiskelijoille pystyttiin mahdollistamaan pääsy palomuuriin ja antamaan heille oikeus tehdä tarvittavia muutoksia, kuten palomuurisääntöjä, itsenäisesti opiskelijaverkkoihin siten, että he eivät pääse muutamaan tai näkemään tuotantopuolen määrityksiä.

5.2 Interfacet / verkkojen määritys

Fyysiset ja virtuaaliset interfacet, eli portit ja liitännät, mahdollistavat verkkoliikenteen kulkemisen eri sisä- ja ulkoverkkojen välillä. Interfaceja voidaan tarkastaa ja muokata ”Network -> Interfaces” -sivulta. Palomuuriin on valmiiksi tehty fyysiset interfacet, jotka kuvaavat palomuurin fyysisiä portteja. Uusi interface luodaan ”Create New -> Interface” -painikkeen takaa.

Interfaceille on useita eri tyyppivaihtoehtoja. Eri tyypeillä on oma tarkoituksensa ja niille on myös ovat asetuksena, jotka tulevat näkyviin, kun haluttu tyyppi valitaan Type-kenttään. Tietojärjestelmälaboratorion ympäristössä tarvittiin seuraavia interfaceja:

- VLAN, virtual local area network, joka mahdollistaa laboratorion LAN-verkon jakamisen pienempiin verkkoihin virtuaalisesti,
- Redundant Interface, joka mahdollistaa usean fyysisen interfacen yhdistämisen samaan tehtävään, joka käytännössä kahdentaa liikennöinnin fyysiset reitit,
- Tunnel Interface, joka toimii IPSec-tunneleiden liikenteen liikennöintiin,
- VDOM Link, jonka avulla voidaan mahdollistaa liikennöinti eri VDOMien välillä.

Käytännössä tehtiin tarvittavat VLAN:it samalla tavalla, kuin ne olivat olleet entisessä palomuurissa. Valittiin interfacen tyypiksi VLAN ja määritettiin sen nimi, VLAN ID sekä verkko samalla tavalla, kuin kyseinen VLAN oli määritetty aikaisemmassa palomuurissa. Nämä VLAN:it pidettiin toistaiseksi disabled-tilassa, jolloin ne eivät olleet vielä käytössä. VLAN:it otettaisiin käyttöön sitten, kun verkkoliikenne muutettaisiin kulkemaan vanhalta palomuurilta uudelle.

Poikkeus VLANien määrityksissä tuli opetusverkkoihin. Tähän asti opiskelijaverkot oli jaoteltu vuosikurssin mukaan, jolloin jokaiselle ryhmälle oli olemassa omat sandbox- ja DMZ-verkot. Nyt haluttiin yksinkertaistaa ja helpottaa opetusta ja projektityöskentelyä yhdistämällä eri ryhmien verkot keskenään. Näin uudelle palomuurille tehtiin vain yksi sandbox- ja yksi DMZ-verkko opiskelijoiden käyttöön. Samalla jäljelle jääneiden verkkojen koko kasvatettiin 16-maskin verkoiksi, jolloin niissä oli kaikkiaan 65 534 vapaata osoitetta.

VDOM-linkit tehtiin seuraavaksi. Linkkejä piti tehdä kaksi kappaletta: toinen ”root-opetus” -vdomien välille ja toinen ”root-projekti” -vdomien välille. Uudet linkit tehdään Global-VDOMin alla ”Network → Interfaces → Create New → VDOM Link” -sivulta. IP-osoitteiksi määritimme vapaasta osoiteavaruudesta omat verkot linkkien käyttöön.

Tunnel Interfacet palomuuri loi automaattisesti, kun tunnelit luotiin myöhemmin. Palomuuri käyttää tunnel interfaceja eri tunneleiden liikenteen ohjaamiseen.

5.3 Palomuurisääntöjen luonti

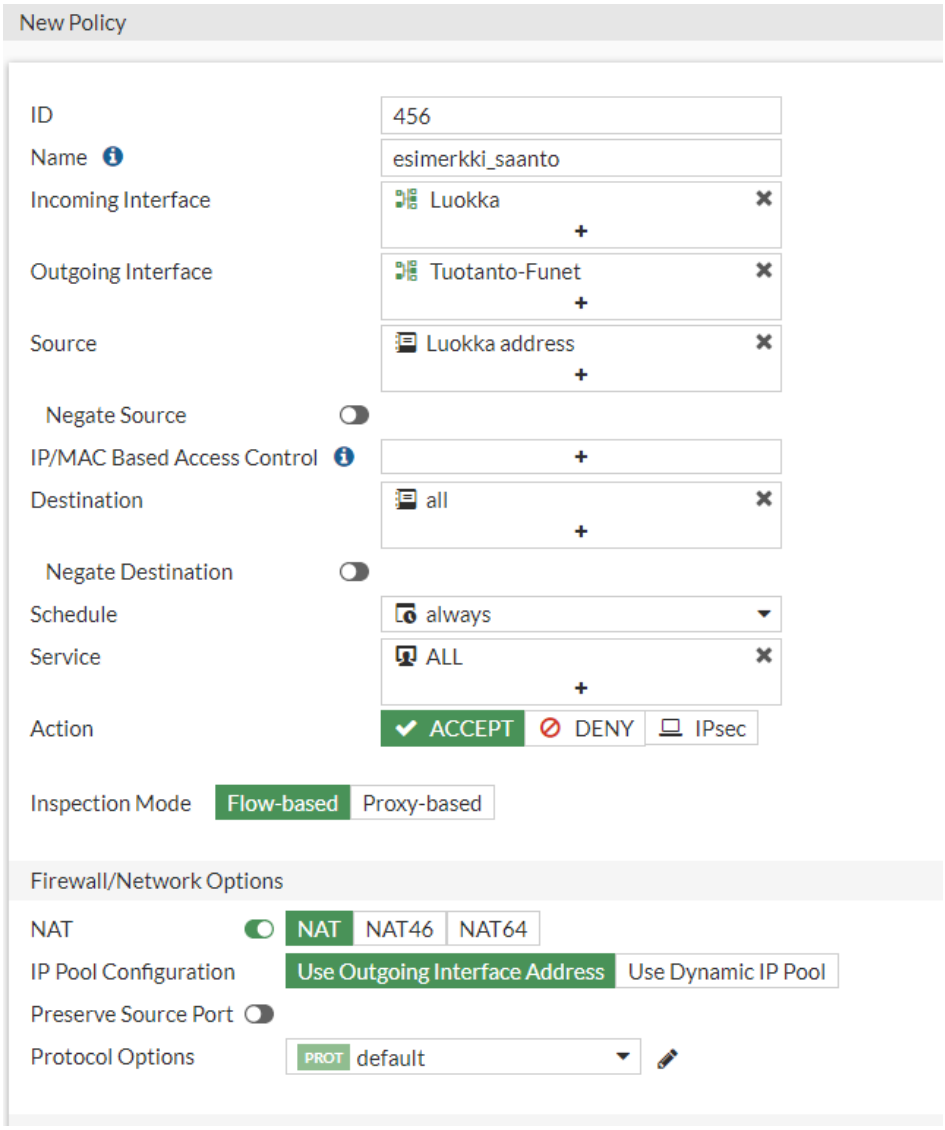
Palomuurisäännöt ovat hyvin keskeinen osa palomuurin toimintaa ja useat muut palomuurin ominaisuudet vaativat määrityksiä myös palomuurisääntöihin. Kaikki palomuurin läpimenevä liikenne pitää kulkea jonkin säännön kautta. Säännöt määrittävät ja kontrolloivat sitä, mitä liikennettä menee, minne liikenne menee ja miten liikenne prosessoidaan.

Palomuurisääntöjä voi tarkastaa ja tehdä ”Policy & Objects -> Firewall Policy” -sivulla. Palomuuri käy sivun säännöt läpi ylhäältä alaspäin ja käyttää liikenteelle sitä sääntöä, joka ensimmäisenä vastaa kyseistä liikennettä. Oikealta yläreunasta voidaan valita ”Interface Pair View”, joka näyttää palomuurisäännöt ryhmitettyinä lähde- ja kohdeinterfaceihin, tai ”By Sequence”, joka näyttää säännöt yhtenä listana ilman ryhmittelyä. Poikkeuksen näihin tekee sellainen tilanne, jossa säännöissä on käytetty useampaa lähde- tai kohde-interfacea. Silloin pelkästään ”By Sequence” -vaihtoehto on käytettävissä.

Uusi sääntö tehdään sivun ”Create New” -painikkeen kautta. Sääntö voidaan myös luoda tiettyyn kohtaan napsauttamalla hiiren kakkospainiketta jonkin säännön kohdalla ja valitsemalla ”Insert Empty Policy -> Above/Below”. Olemassa oleva sääntö voidaan kopioida klikkaamalla säännöstä hiiren kakkospainikkeella ja valitsemalla ”Copy” ja sitten ”Paste -> Above/Below”. Sääntöön täytyy määritellä seuraavat asiat (kuva 7):

- ID, joka on yksilöllinen jokaiselle säännölle (palomuuri antaa automaattisesti seuraavan vapaan ID-numeron, jos sitä ei käsin määritetä),
- Lähde- ja kohde-interface
- Lähde- ja kohdeosoitteet
- Protokollat, jotka määrittävät, mitkä portit koskevat sääntöä.

Lisäksi säännölle voidaan määritellä muun muassa myös nimi, turvaprofiilit (security profiles), NAT- ja lokimääritykset sekä kommentti. Sääntöön voidaan myös määrittää, onko sääntö käytössä vai ei.



Kuva 7. Esimerkkisääntö, joka sallii liikenteen Luokka-verkosta ulkoverkkoon (Funet) kaikilla mahdollisilla porteilla käyttäen liikenteelle lähdeosoitteena Tuotanto-Funet -interfacen osoitetta.

5.4 Turvaprofiilit (Security Profiles)

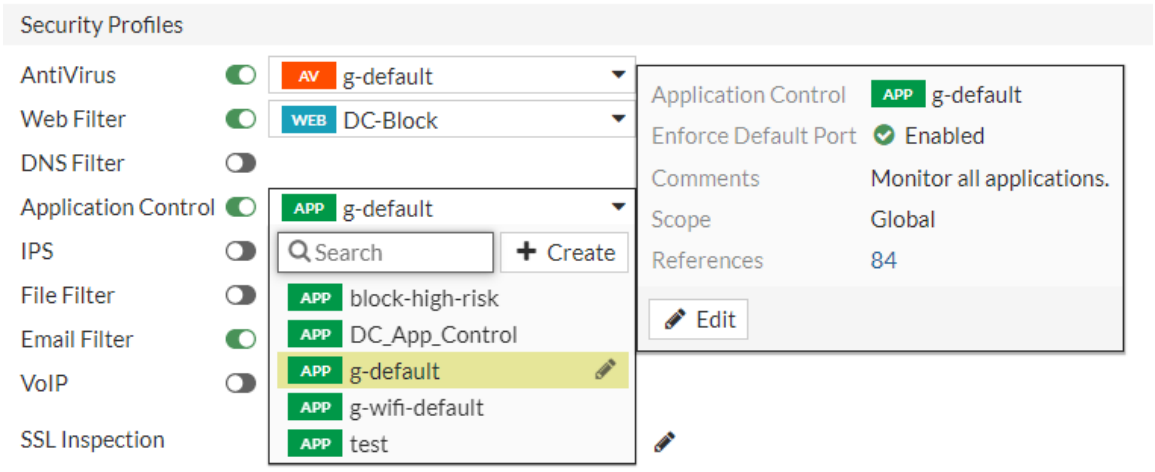
Palomuurisääntöihin voidaan määrittää erilaisia turvaprofiileja, joiden avulla liikennettä pystytään monitoroimaan ja rajaamaan tarkemmin kuin vain porttitasolla. Turvaprofiilien avulla voidaan hyödyntää palomuurin sovellustason ominaisuuksia. Palomuurissa on jokaiselle profiilityypille olemassa oma vakioprofiili. Profiileja voi myös tehdä itse, jolloin ne voidaan määrittää toimimaan halutulla tavalla. Saatavilla olevat turvaprofiilit riippuvat siitä, onko palomuurisääntöön valittu ”Inspection Mode = Flow-based” vai ”Inspection Mode = Proxy-based”. Flow-based-tila priorisoi liikenteen nopeutta ja sujuvuutta, kun taas Proxy-based-tila priorisoi liikenteen perusteellisuutta. Flow-based-tilassa turvaprofiilityyppejä on seuraavanlaisia:

- Antivirus, joka tarkkailee, sisältääkö liikenne haittaohjelmia.
- Web filter, joka monitori ja estää käyttäjiä pääsemästä tietyille nettisivuille.
- DNS Filter, joka monitoroi ja suodattaa DNS-kyselyjä perustuen niiden domain-arvioon.
- Application Control, joka monitoroi ja suodattaa applikaatioita kaikissa porteissa.
- IPS (Intrusion Prevention System), joka estää yhteydet botnet-verkkoihin.
- File Filter, joka estää tiedostojen lataamisen perustuen niiden tyyppiin ja protokolaan.
- Email Filter, joka estää sähköpostien lähettämisen ja vastaanottamisen tietyistä IP-osoitteista tai verkoista.
- VoIP, joka turvaa SIP- ja SCCP-yhteydet estämällä niitä pitkin tehtävät hyökkäykset.
- SSL Inspection, joka pystyy tutkimaan salatun liikenteen purkamalla salauksen ja salaamalla sen uudestaan tarkistuksen jälkeen.

Proxy-based-tilassa edellisten turvaprofiilityyppien lisäksi tarjolla on myös:

- Video-filter, joka monitoroi ja rajoittaa YouTube-videoiden katsomista perustuen niiden kategoriaan ja kanaviin.
- ICAP, joka pystyy siirtämään palomuurin tehtäviä erillisille palvelimille.
- Web Application Firewall, joka tunnistaa ja estää tunnettuja verkkosovellushyökkäyksiä.

Näitä turvaprofiileja pyrittiin käyttämään luoduissa palomuurisäännöissä. Turvaprofiileja voidaan ottaa säännössä käyttöön asettamalla ”Security Profiles”-kohdan alla haluttu turvaprofiilityyppi aktiiviseksi ja esiin tulleesta valikosta valitsemalla haluttu turvaprofiili (kuva 8).



Kuva 8. Turvaprofiilien käyttöönotto näkymä palomuurisäännön asetuksissa.

Kaikki säännöt tehtiin flow-based-tilassa, koska liikenteen tehokkuus oli ympäristölle tärkeintä. Turvaprofiileina käytettiin palomuurin omia vakioprofiileja, lukuun ottamatta web-filter-profiilia. Palomuuriin tehtiin itse toinen web-filter-profiili, joka rajoitti enemmän liikennettä eri nettisivuille, kuin palomuurin oma vakioprofiili. Tämä itse tehty profiili sitten liitettiin sääntöön, jota pitkin tietojärjestelmälaboratorion tietokoneiden liikenne kulki julkiverkkoon. Näin laboratorion tietokoneilla ei enää päässyt niin vapaasti surffaamaan eri nettisivuilla.

5.5 Liikenteen reititys

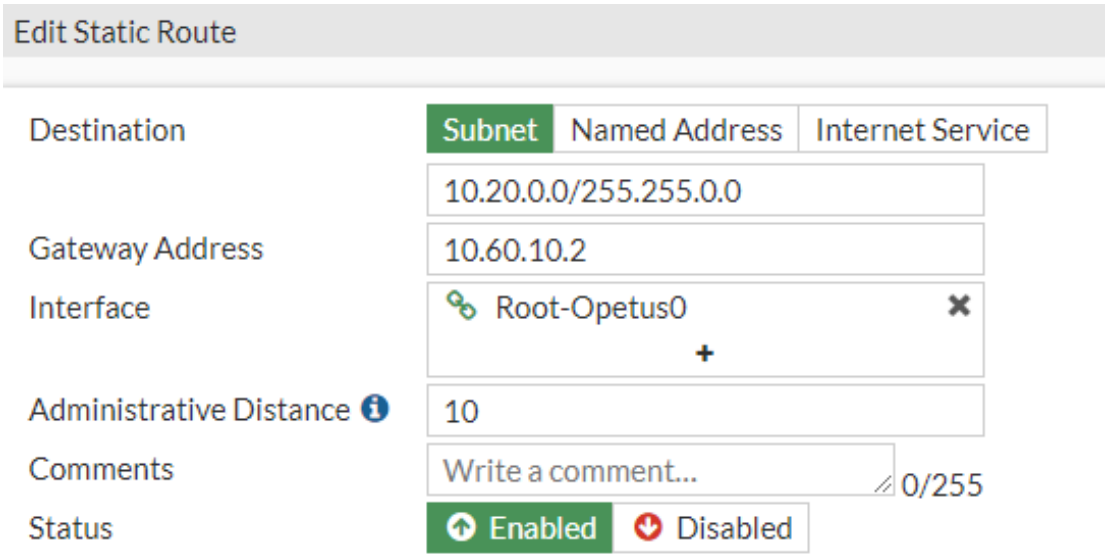
Olennainen osa palomuurin toimintaa on reitittää palomuurille saapunut liikenne oikein. Palomuuri osaa automaattisesti reitittää liikenteen kohdeosoitteen mukaan oikeaan interfaceen, jos interfacelle määritetty verkko sisältää kohdeosoitteen. Esimerkiksi jos VLAN-interfacelle nimeltä ”toimisto” on määritetty verkko 10.20.30.0/24, niin palomuuri ohjaa automaattisesti 10.20.30.50 osoitteeseen tulevan liikenteen ”toimisto”-VLANiin.

Usein kuitenkin tulee vastaan tilanteita, että tietyt verkot sijaitsevat jonkin interfacen takana, mutta verkkoja ei ole määritetty suoraan interfaceen. Yleisin tällainen tilanne muodostuu julkiverkkoon suuntautuvan liikenteen kanssa. Silloin palomuurille voidaan tehdä staattinen reitti,

joka ohjaa kaikki sellaiset yhteydet, joille se ei löydä muuta kohdetta, siihen interfaceen, jonka takana on julkiverkon yhteys. Toinen tällainen tilanne tulee vastaan myös esimerkiksi silloin, kun halutaan liikennöidä sellaisiin verkkoihin, jotka sijaitsevat eri VDOMien takana. Palomuurille täytyy tehdä staattinen reitti, joka ohjaa eri VDOMien takana sijaitsevien verkkojen liikenteen kyseisen ”VDOM Link” -interfaceen, jolloin liikenne ohjautuu oikein toiseen VDOMiin (kuva 9).

Staattisia reittejä tarkastellaan ja tehdään Fortigate-palomuurissa sivulta ”Network -> Static Routes”. Uusi reitti tehdään Create New -painikkeen takaa. Reittiin pitää määrittää seuraavat asiat:

- Destination, eli liikenteen lopullinen kohdeverkko, -osoite tai -palvelu,
- Gateway Address, eli osoite, johon liikenne ohjataan,
- Interface, johon liikenne ohjataan,
- Administrative Distance, joka määrittää reitin arvojärjestyksen, jos samaan lopulliseen kohdeosoitteeseen on määritetty useampi reitti,
- Enable / Disable, eli määrittää, onko reitti aktiivinen vai ei.



Kuva 9. Staattinen reitti, joka ohjaa 10.20.0.0/16-verkkoon liikennöivät yhteydet Root-Opetus0 ”VDOM-link” -interfaceen osoitteeseen 10.60.10.2. Tämä mahdollistaa root-VDOMissa sijaitsevien verkkojen liikennöinnin Opetus-VDOMiin verkkoon 10.20.0.0/16.

5.6 IPsec-tunnelit

IPsec-tunnelit mahdollistavat virtuaalisen erillisverkon luomisen eri laitteiden välille. Tätä hyödyntämällä voidaan luoda julkiverkon yli turvallisia ja salattuja yhteyksiä. Tunnelin kautta kulkeva liikenne salataan kokonaan, jolloin edes lähettäjän ja vastaanottajan IP-osoitteet eivät voi paljastua ulkopuolisille. [16.]

Fortigate-palomuurissa IPsec-tunnelit määritetään ”VPN -> IPSec Tunnels” -sivulta. Kun painetaan sivun yläreunassa olevaa ”Create New” -painiketta, niin palomuuri ohjaa käyttäjän ”VPN Creation Wizard” -sivulle, jonka kautta tunnelin voi määrittää ohjatusti. Täältä käyttäjä voi valita ensin mallityypin riippuen siitä, että millainen tunneli on tarkoitus tehdä. Tunnelin tyypiksi voidaan valita myös ”Custom”, jolloin käyttäjän pitää määrittää itse kaikki asetukset, kuten verkot, autentikointi ja salaus.

Tietojärjestelmälaboratoriosta oli olemassa ennestään kaksi IPsec-tunnelia. Yksi koulun supertietokone Bullille ja toinen koulun tietohallinnon (KamIT) palomuurille. Tunnelit aiottiin pystyttää uudelle palomuurille samoilla asetuksilla kuin entinen, jolloin tunnelit voitaisiin muodosta jo olemassa olevista dokumentaatioista kopioiden. Ainoastaan tunnelien salausavaimet vaihdettaisiin uusiin. Bullin tunneli määritettiin kuntoon ennen laboratorion liikenteen yliheittoa uudelle palomuurille ja KamIT:n tunneli määritettäisiin yliheiton jälkeen. Tämä tehtiin näin sen takia, koska laboratorion ylläpitäjät hallinoivat myös Bullin omaa palomuuria, mikä taas mahdollisti meidän kontrolloida tunnelin molempia päitä ja näin perehtyä sekä ymmärtää tunnelin muodostaminen Fortigate-palomuurissa.

Bullin tunneli muodostettiin samoilla määrityksillä kuin entinen sekä Fortigate-palomuuriin että Bullin omaan palomuuriin, mutta tunneli ei noussut aktiiviseksi ja alkanut välittämään liikennettä. Tunnelin määritykset poistettiin ja ne tehtiin uudestaan edellistä kertaa tarkemmin, mutta edelleenkään tunneli ei noussut aktiiviseksi. Tässä vaiheessa ongelmaksi epäiltiin laboratorion kytkinverkon määrityksiä. Eri kytkimien välisiä yhteyksiä testattiin ja todettiin, että Fortigate-palomuurin ja siinä kiinni olevan konesalin kytkimen välinen liikenne ei jostain syystä kulkenut. Fortigate-palomuurin hallintayhteyteen olimme käyttäneet palomuurin management-porttia, jolle oli kytkimellä määritetty oma portti ja verkko. Bullin tunnelin liikenne oli määritetty kulkemaan palomuurin muita fyysisiä portteja pitkin ja niille oli kytkimelle määritetty omat porttinsa, jotka oli yhdistetty kytkimessä port channel -toiminolla toimimaan samoina portteina. Port channel -porttiin kuuluvat portit oli konfiguroitu erikseen siten, että tarvittavien VLAN:ien liikenne sallittiin,

mutta samat konfiguroinnit puuttuivat itse port channel -toiminnon konfiguroinneista. Kun lisäsimme puuttuvat VLAN-konfiguroinnit port channel -toiminnon konfigurointiin, niin yhteys Fortigate-palomuurin ja Bullin palomuurin välillä alkoi toimimaan ja tunneli nousi aktiiviseksi ja alkoi toimimaan oikein.

5.7 Etäyhteys

Tietojärjestelmälaboratorion verkkoon haluttiin mahdollistaa pääsy laboratorion käyttäjille myös laboratorion ulkopuolelta. Tällainen yhteys voidaan Fortigate-palomuuriin toteuttaa joko IPSec VPN -tunnelilla tai sitten SSL VPN -yhteydellä. Päädyimme määrittämään SSL-VPN -tunnelin, koska se tarjosi enemmän ominaisuuksia. SSL VPN mahdollistaa turvallisen tavan olla yhteydessä laboratorion verkkoon. Se käyttää liikennöintiin HTTPS-protokolaa ja mahdollistaa etäyhteyden käyttämisen tunneli- tai web-muodossa.

SSL VPN määritetään ”VPN → SSL-VPN Settings” -sivulla. Sivulta voidaan määrittää erilaisia asetuksia SSL VPN -liikenteelle. Laboratorion ympäristössä määritettiin seuraavat yhteysasetukset:

- Enable SSL-VPN, eli aktivoitiin SSL VPN käyttöön,
- Listen on Interface(s), eli määritettiin ne interfacet, joista sallittaan SSL VPN -yhteydet,
- Listen on Port, eli määritettiin se portti, josta vastaanotetaan SSL-VPN yhteyksiä,
- Server Certificate, eli määritetiin mitä sertifikaattia SSL VPN -yhteys käyttää,
- Restrict Access = Allow access from any host, eli sallittiin SSL VPN -yhteydet mistä tahansa osoitteesta,
- Idle logout, eli määritettiin missä ajassa SSL VPN -yhteys katkeaa automaattisesi, jos liikennettä ei kulje yhteyden läpi.

Tunnelimuodon asetuksiin määritettiin ”Address Range” -kohtaan spesifi verkkoavaruus, josta SSL-VPN -yhteydellä yhdistävät osapuolet saisivat oman IP-osoitteen. ”DNS Server” -kohtaan asetimme yhteyden käyttämään samoja DNS-palvelimia, kuin palomuuri käyttää omiin palveluihinsa. ”Authentication/Portal Mapping” -kohdassa voidaan määritellä, millainen portaali kullekin käyttäjällä näkyy heidän avatessaan SSL VPN -yhteyden web-muodossa. Valitaan ”Create New”, jonka jälkeen määritetään käyttäjä tai käyttäjäryhmä, sekä joko full-, tunnel- tai web-access -portaali.

SSL-VPN -portaaleja voidaan tarkastella ja määrittää ”VPN → SSL-VPN Portals” -sivulta. Palomuurissa on vakiona määritelty jo full-, tunnel- ja web-access -portaalit.

5.8 Lokitiedot

Palomuuri kerää erilaisia lokitietoja, joista voidaan tarkastella muun muassa palomuurille tulevaa liikennettä tai ylläpitäjän tekemiä muutoksia. Erilaiset lokitiedot tallentuvat eri lokitiedostoihin. Lokitiedot löytyvät ”Log & Report” -sivun alta. Lokien tallentamiseen liittyviä määrityksiä voi tarkastaa tai muokata ”Log & Report -> Log settings” -sivulta.

Oletuksena palomuuri tallentaa lokeja sisäiselle levylle ja säilyttää niitä viikon, jonka jälkeen ne poistuvat automaattisesti. Tätä määritystä voidaan muuttaa myös CLI:n kautta komennoilla

- ”config log disk setting”
- ”set maxium-log-age x”, jossa x tarkoittaa lokien säilytysaikaa päivissä.

On myös suotavaa, että lokitiedostot tallennetaan säännöllisesti jollekin ulkoiselle palvelimelle. Tällä varmistetaan se, että esimerkiksi laiterikon sattuessa lokitiedot eivät häviä. Lisäksi tallentamalla lokit, niitä voidaan säilyttää pitempään ja niitä voidaan tarkastella, jos sille tulee aihetta. Fortigate-palomuurissa lokitietojen muualle tallennus määritellään ”Log settings” -sivulta. Valmistajalla on olemassa oma lokitietojen tallennus- ja analysointityökalu nimeltään FortiAnalyzer. FortiAnalyzer tarvitsee oman lisenssin ja se täytyy myös erikseen konfiguroida jollekin palvelimelle. Lokitietojen tallennus FortiAnalyzeriin määritettään aktivoimalla ”Send logs to FortiAnalyzer” asetus ja määrittelemällä FortiAnalyzerin IP-osoite. Lokitiedot voidaan tallentaa myös johonkin täysin ulkopuoliseen lokienhallintapalvelimeen. Tämä onnistuu aktivoimalla asetus ”Send logs to syslog” ja määrittelemällä palvelimen IP-osoite.

Tietojärjestelmälaboratorion ympäristössä opiskelijat voivat harjoituksena pystyttää jonkin lokienhallintatyökalun. Tämän ansiosta meillä ei ollut tarvetta FortiAnalyzerille ja pystyimme tallentamaan lokit laboratoriossa sijaitsevalle toiselle palvelimelle. Projektin aikataulun takia ulkoisen lokienhallintatyökalun pystyttäminen toimintakuntoon jäi tekemättä ja se jätettiin harkitusti myöhemmäksi, koska oli kriittisempää saada määritettyä palomuurin muita toimintoja kuntoon.

5.9 NAT

NAT (Network Address Translation), eli osoitteenmuutos, on yksi tärkeimpiä verkkotekniikoista. Sen avulla pystytään mahdollistamaan useiden laitteiden verkkoliikennöinti yhdellä IP-osoitteella. NAT kehitettiin alun perin paikkaamaan IPv4-osoitteiden rajallista määrää. NAT-tekniikan avulla eri toimijat eivät tarvitse jokaiselle laitteelle uniikkia IP-osoitetta, vaan he pystyvät vain muutamalla uniikilla osoitteella mahdollistamaan lukuisille eri laitteille yhteyden julkiverkkoon. [17.]

IANA (Internet Assigned Numbers Authority) on globaali viranomainen, joka vastaa IP-osoitteiden jakamisesta eri toimijoille. Se on määrittänyt kolme eri verkkoa, jotka on varattu vain sisäiseen verkotukseen:

- 10.0.0.0–10.255.255.255
- 172.16.0.0–172.31.255.255
- 192.168.0.0–192.168.255.255

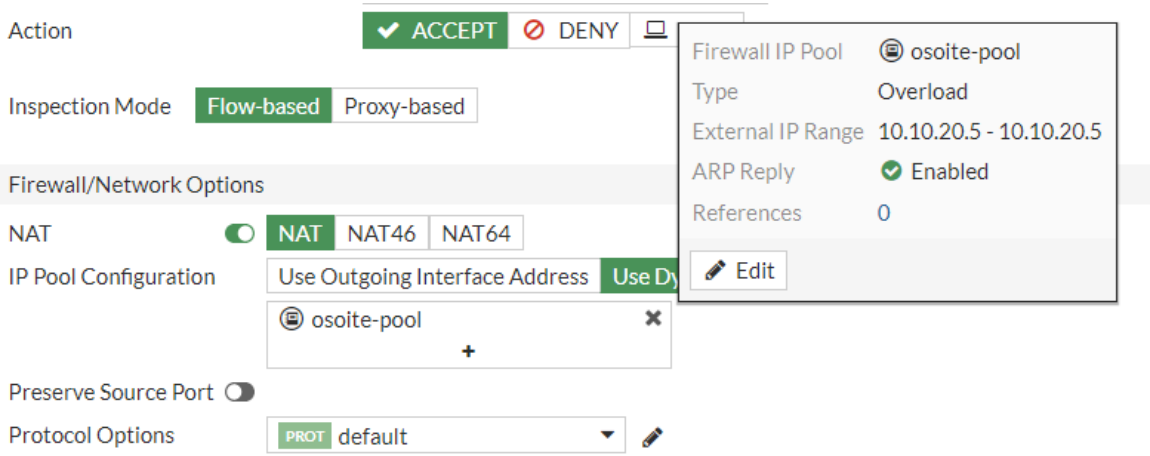
Näitä osoitteita eri toimijat voivat käyttää vapaasti omaan sisäiseen verkkoliikenteeseen. Käytännössä toimijat määrittävät näistä osoitteita erilaisia verkkoja tarpeen mukaan omien laitteiden välille ja sitten palomuurissa ulospäin liikennöidessä ne NAT-tekniikan avulla käyttäisivät julkiverkkoon kohdistuvaan liikenteeseen yhtä samaa IP-osoitetta. Tällöin julkiverkosta katsottuna yhden toimijan kaikki liikenne tulisi yhdestä samasta IP-osoitteesta. [17.]

Fortigate-palomuurissa voidaan NAT määrittää antamaan liikenteelle jokin lähdeosoite (SNAT) tai kohdeosoite (DNAT). Kun liikenteelle annetaan NAT-tekniikalla lähdeosoite, niin liikenteen vastapää näkee liikenteen tulevan palomuurille määritetystä osoitteesta, joka useimmiten on eri osoite, kuin mistä liikenne on alun perin lähtenyt. Kun liikenne saa NAT-tekniikalla jonkin palomuurille määritellyn kohdeosoitteen, niin liikenne ohjataan eri osoitteeseen, kuin minne alkuperäinen yhteys olisi tarkoittanut.

5.9.1 SNAT

Fortigate-palomuurissa SNAT määritellään palomuurisäännössä. Palomuurisääntö voidaan tehdä ”Policy & Objects -> Firewall Policy” -sivulta. Säännön määrityksistä löytyy ”Firewall / Network Options” -kohdasta NAT-asetus, joka pitää aktivoida. Sen jälkeen voidaan määrittää, käytetäänkö

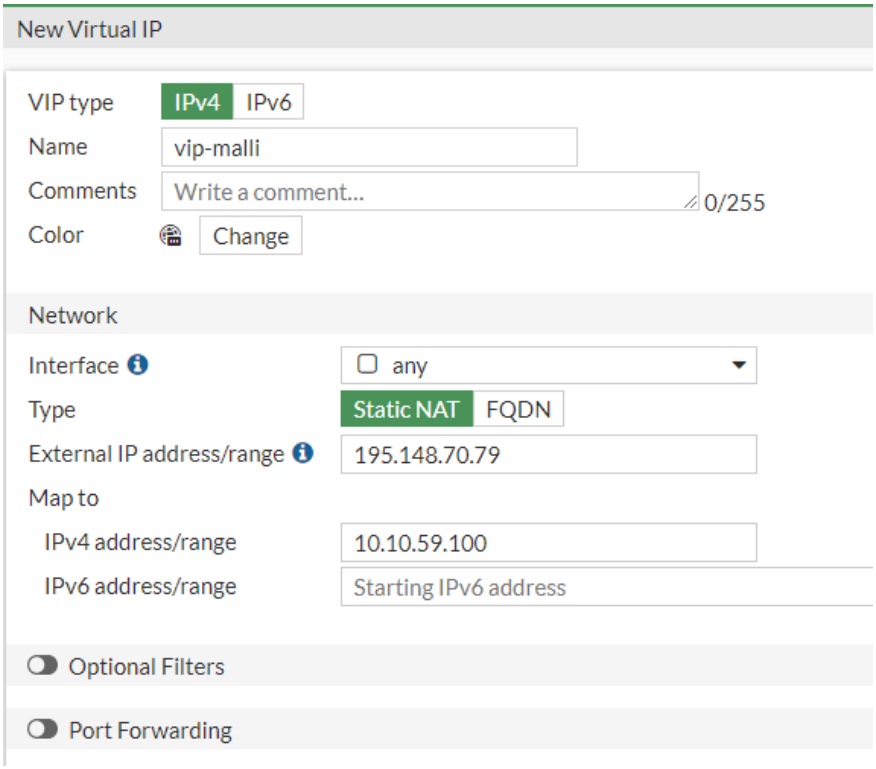
lähdeosoitteena lähdeverkon IP-osoitetta vai jotain käsin määritettyä osoitetta tai osoiteavaruutta (kuva 10). Lisäksi voidaan määrittää liikenteelle myös tietty lähdeportti, mutta on huomioitava, että yhdestä lähdeportista voi olla vain yksi yhteys aktiivisena kerrallaan.



Kuva 10. SNAT-asetus palomuurisäännössä. Kuvassa käytetään dynaamista osoiteavaruutta, joka määrittää liikenteen saamat lähdeosoitteet. Tässä tapauksessa käytössä on ”osoite-pool” -niminen osoiteavaruus, joka sisältää vain yhden IP-osoitteen 10.10.20.5.

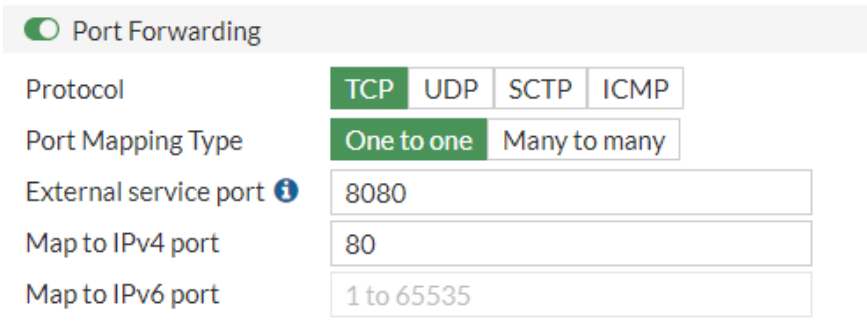
5.9.2 DNAT / VIP

Fortigate-palomuurissa DNAT tehdään määrittämällä ensin VIP-objekti (Virtual IP) ja sitten liittämällä se palomuurisääntöön. VIP-objekti luodaan ”Policy & Objects -> Virtual IPs” -sivulta ”Create New -> Virtual IP” -painikkeen alta. Ensin valitaan, määritetäänkö VIP IPv4- vai IPv6-osoitteiden liikennettä varten. Seuraavaksi pitää määrittää lähdeosoite tai osoiteavaruus kohtaan ”External IP Address/Range” ja kohdeosoite kohtaan ”Mapped IP Address/Range” (kuva 11). Käytännössä siis lähdeosoitteeksi määritetään sellainen osoite, johon kohdistuu verkkoliikennettä muualta ja kohdeosoitteeksi määritetään sellainen osoite, johon tuo lähdeosoitteesta tuleva liikenne ohjataan.



Kuva 11. VIP-objekti, joka ohjaa julkiseen IP-osoitteeseen 195.148.70.79 tulevan liikenteen sisäverkon osoitteeseen 10.10.59.100.

VIP-objekti voidaan myös määrittää toimimaan porttitasolla. Tämä mahdollistaa esimerkiksi sen, että samaan lähdeosoitteeseen tulevaa liikennettä voidaan ohjata useisiin eri kohdeosoitteisiin, kun vain lähdeliikenteeseen määritellään määritysten mukainen oikea portti. Tähän vaadittavat määritykset aukeavat tehtäviksi, kun aktivoidaan ”Port Forwarding” -asetus. Ensin valitaan käytettävä protokolla ja sitten lähdeosoitteen portti kohtaan ”Extrenal Service Port” ja kohdeosoitteen portti kohtaan ”Map to Port” (kuva 12).



Kuva 12. VIP-objektin porttitason määritykset, jossa julkiverkon osoitteen porttiin 8080 tuleva liikenne ohjataan sisäverkon osoitteen porttiin 80.

Jotta VIP-objekti määrityksineen alkaa toimimaan, pitää se vielä määrittää johonkin palomuurisääntöön ”Destination”-kenttään. Luodut VIP-objektit voidaan valita osoiteluettelosta suoraan.

5.10 Käyttäjät

Fortigate-palomuurissa verkon käyttöä voidaan rajata käyttäjäkohtaisesti erilaisilla määrityksillä. Palomuurille voidaan määrittää sekä paikallisia että ulkoisia käyttäjiä. Paikalliset käyttäjät määritetään suoraan palomuuriin. Ulkoiset käyttäjät ovat esimerkiksi erillisellä AD-palvelimella sijaitsevia käyttäjiä, joiden tiedot palomuuria voi hakea tarvittaessa. Tietojärjestelmälaboratorion verkkoympäristössä on käytössä yksi erillinen kahdennettu AD-palvelin, jolle on määritetty kaikki verkon käyttäjien tarvitsemat tunnukset. Palomuuriin ei siis määritetty omia tunnuksia eri käyttäjille, vaan haluttiin käyttää AD-palvelimella olevia tunnuksia LDAP-yhteydellä.

AD-palvelin saadaan määritettyä palomuuriin ”User & Authentication → LDAP Servers” -sivulta. ”Create New” -napin takaa päästään määrittämään tarvittavat AD-palvelimen määritykset, kuten nimi, IP-osoite, käytettävä portti ja AD-palvelimen käyttäjätunnukset. Koska AD-palvelin on kahdennettu, niin palomuuriin määritettiin erikseen molempien AD-palvelimen tiedot, jolloin se pystyy hakemaan tiedot kummalta vain.

AD-palvelimella käyttäjät on jaoteltu erilaisiin ryhmiin, joille on sitten sallittu oikeuksia eri paikkoihin. Myös palomuuriin haluttiin samalainen toimintatapa, jolloin avauksia/pääsyjä ei sallita yksittäisille käyttäjille, vaan kokonaisille käyttäjäryhmille. Tässä tilanteessa palomuuriin kannattaa määrittää erilaisia käyttäjäryhmiä, joita sitten voidaan linkittää esimerkiksi palomuurisääntöihin. Käyttäjäryhmiä voidaan luoda ”User & Authentication → User Group → Create New” -sivulta. Täällä voidaan luoda palomuuriin sekä paikallisia että ulkoisia käyttäjäryhmiä. Koska halusimme käyttäjäryhmät ulkoiselta AD-palvelimelta, niin valitsemme ryhmän tyypiksi ”Firewall” ja sitten määritämme ”Remote Groups” -kohtaan halutun ulkoisen käyttäjäryhmän. Palomuuri näyttää kaikki määritetyn AD-palvelimen käyttäjäryhmät, joita voidaan valita tarvittaessa useampi.

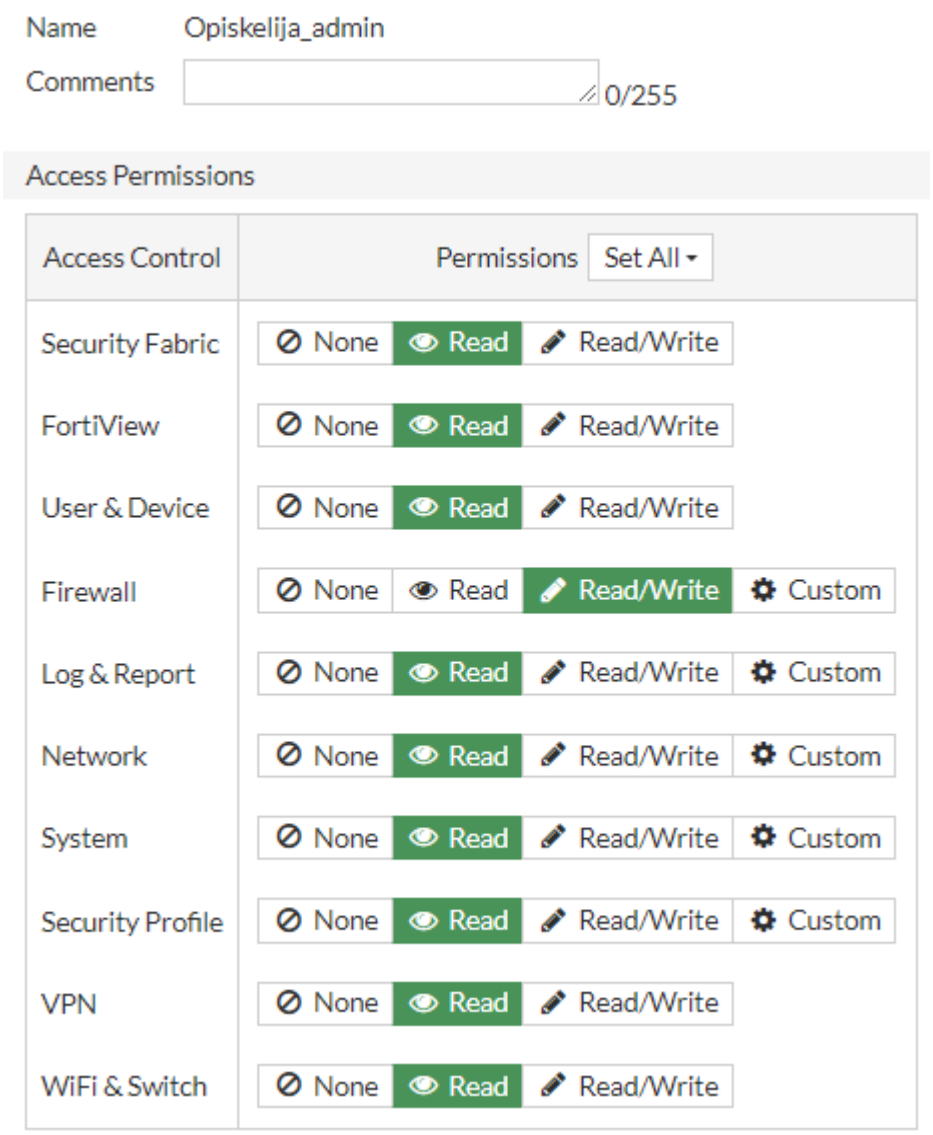
5.11 Admin-oikeudet

Palomuuriin haluttiin määrittää eri käyttäjäryhmille erilaisia admin-oikeuksia. Tietojärjestelmälaboratorion ylläpitäjille haluttiin sallia täydet oikeudet palomuurin konfigurointiin, kun taas opiskelijoille haluttiin sallia vain tarvittavat oikeudet palomuurisääntöjen tekemiseen Opetus-VDOMiin. Käyttäjätunnukset pitää hakea tietojärjestelmälaboration AD-palvelimelta.

Admin-oikeuksia jaotellessa pitää ensin luoda admin-profiilit, joissa määritetään mitä oikeuksia kyseisellä profiililla on. Admin-profiilit luodaan ja tarkastellaan Global-VDOMissa ”System → Admin Profiles” -sivulta. Uusi profiili luodaan ”Create New” -painikkeen takaa ja ”Access Permissions” -kohdassa määritellään profiiliin luku- ja kirjoitusoikeudet palomuurin eri ominaisuuksiin. Seuraavaksi tehdään admin-tunnus ”System → Administrators” -sivulta ”Create New” -painikkeesta. Määritykset tehtiin seuraavasti:

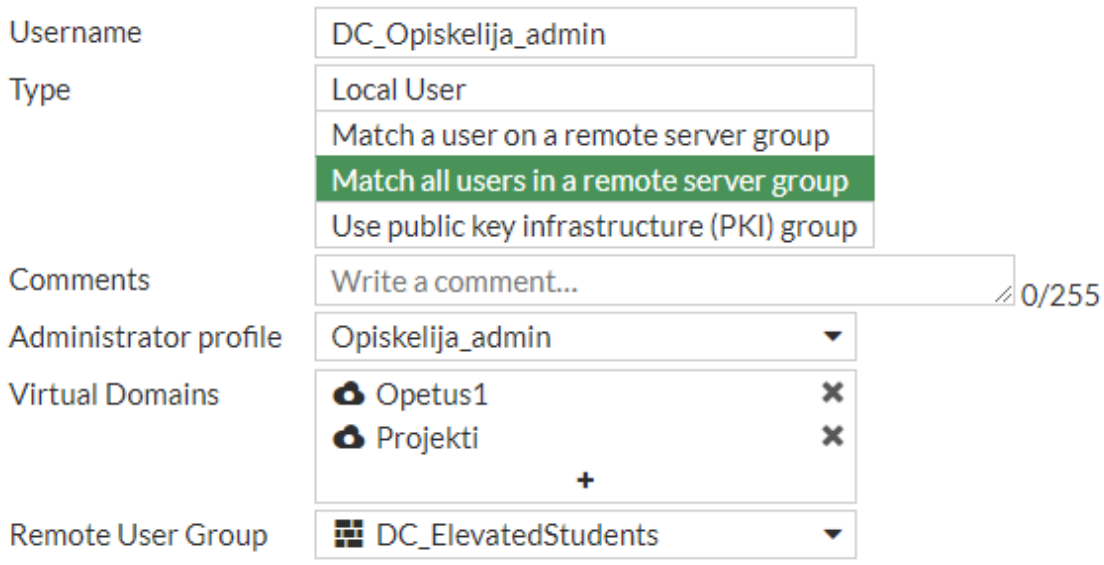
- Type = Match all users in a remote server group, jolloin palomuuri hakee käyttäjäprofiilit ulkoiselta palvelimelta,
- Administator profile = edellisessä kohdassa luotu admin-profiili, joka määrittää sallittavat oikeudet,
- Virtual Domains = valitaan ne VDOMit, joihin halutaan kyseisen admin-tunnuksen vaikuttavan,
- Remote User Group = valitaan jokin luotu käyttäjäryhmä, jonka käyttäjätunnuksille halutaan määrittää luotava admin-tunnus.

Fortigate-palomuurissa on olemassa valmiiksi ”super_admin” -admin-profiili, jolla on kaikki mahdolliset oikeudet palomuuriin. Tietojärjestelmälaboratorion ylläpitäjille luotiin oma admin-tunnus, jolle määritettiin tämä ”super_admin” -admin-profiili. Opiskelijoita varten luotiin ”Opiskelija_admin” admin-profiili, jolle sallittiin lukuoikeudet kaikkiin ominaisuuksiin, mutta kirjoitusoikeudet ainoastaan palomuurisääntöjen tekemiseen vaadittaviin oikeuksiin (kuva 13).



Kuva 13. Opiskelija-admin -admin-profiili, jossa määritelty kirjoitusoikeudet vain Firewall-ominaisuuksiin.

Lisäksi luotin uusi admin-tunnus nimeltä ”DC_Opiskelija_admin”, johon linkitettiin luotu ”Opiskelija_admin” -admin-profiili. Tämä admin-tunnus määritettiin toimimaan vain Opetus- ja Projekti-VDOMissa, joten opiskelijat eivät pääse käsiksi root-VDOMin määrityksiin (kuva 14).



Kuva 14. DC_Opiskelija_admin -admin-tunnuksen määritykset.

5.12 Päivitykset

Päivitykset eivät palomuurin käyttöönottovaiheessa ole kriittisin asia, mutta tulevaisuutta varten selvitettiin, kuinka palomuuri saa hankittua sekä käyttöjärjestelmä- että tietokantapäivityksensä.

Yksittäisen Fortigate-palomuurin käyttöjärjestelmäpäivitys onnistuu ”System -> Firmware” -sivulta. Käyttäjä voi valita palomuurin ehdottaman käyttöjärjestelmäversion ”All Upgrades” -kohdan alta tai sitten voidaan käsin siirtää palomuurille haluttu versio. Eri käyttöjärjestelmäversiot voidaan ladata laitevalmistajan FortiCloud-sivuilta, jonne kirjaudutaan luoduilla tunnuksilla. Aina ennen päivittämistä kannattaa varmistaa valmistajan omasta päivitystyökalusta, voiko nykyisestä versiosta siirtyä suoraan päivitettävään versioon vai pitääkö välissä päivittää johonkin toiseen versioon. Kyseinen työkalu löytyy valmistajan omista julkisista dokumentaatioista nimellä ”Upgrade Path Tool Table”.

Uusimmissa käyttöjärjestelmissä useamman palomuurin, jotka ovat HA-tilassa, päivitys onnistuu ”System -> Fabric Management” -sivulla. Kyseiseltä sivulta voidaan tarkistaa nykyisen käyttöjärjestelmän versio sekä tarkastaa olisiko uusia päivityksiä saatavilla. Jos halutaan päivittää vain yksi palomuuri, niin valitaan listasta oikea palomuuri ja painetaan Upgrade-nappia. Jos halutaan päivittää kaikki HA-klusteriin kuuluvat laitteet, niin silloin edetään ”Fabric Upgrade” -napista. Näiden

nappien takaa palomuuri tarjoaa suoraan valittavissa olevat käyttöjärjestelmäversiot. Valitaan haluttu versio ja ajankohta päivitykselle. Palomuuri hoitaa itse päivityksen loppuun.

Fortigate-palomuurit päivittävät haittaohjelmatietokantaansa valmistajan oman FortiGuard-palvelun kautta. FortiGuard päivittää jatkuvasti tietokantaansa uusien haittaohjelmien ja haavoittuvuuksien osalta. Palomuuri hakee verkon kautta päivityksiä tietokantaan automaattisesti. FortiGuardin asetuksia pystyy muuttamaan ”System -> FortiGuard” -sivulta. Lisäksi sieltä voi tarkastaa muun muassa, että milloin viimeisimmät päivitykset tietokantoihin on haettu.

6 Palomuurin käyttöönotto tuotantoympäristöön

Kun palomuurille oli määritetty kaikki tarvittava, niin seuraavana vuorossa oli itse verkkoliikenteen yliheitto entiseltä palomuurilta uudelle. Yliheitto piti suorittaa siten, että siitä syntyisi mahdollisimman vähän haittaa tietojärjestelmälaboratorion normaalille toiminnalle. Lisäksi oli tärkeää selvittää yliheiton jälkeen mahdollisesti syntyvät ongelmat ja ratkaista ne.

6.1 Liikenteen yliheitto

Kun kaikki määritykset oli tehty valmiiksi uuteen palomuuriin, niin seuraavaksi piti ohjata liikenne kulkemaan entisen palomuurin sijasta uudelle palomuurille. Tietojärjestelmälaboratorion muu verkotus oli asennettu kuntoon siten, että liikenne pystyi kulkemaan uudelle palomuurille samalla tavalla kuin entiselle. Uudella palomuurilla interfacet oli asetettu disabled-tilaan, jolloin se ei kuitenkaan vastaanottanut liikennettä.

Yliheitto suoritettiin ottamalla vanhasta palomuurista verkkojohdot irti ja ajamalla uuden palomuurin interfacet aktiiviseksi muurin hallinnasta. Tällöin oli myös mahdollista kääntää liikenne kulkemaan takaisin vanhaa palomuuria pitkin helposti tekemällä edellä mainitut asiat päinvastoin. Tämän jälkeen laboratorion liikenne alkoi kulkemaan uuden palomuurin kautta. Laboratorion verkkoliikenne katkesi noin kahdeksi minuutiksi. Katkos ei itsessään aiheuttanut ongelmia, koska laboratorion verkkoympäristö ei sisällä sellaisia laitteita tai järjestelmiä, jotka vaatisivat katkeamatonta yhteyttä.

6.2 Syntyneet ongelmat

Yliheiton jälkeen aloimme tarkistamaan, että kaikki laboratorion järjestelmät toimisivat edelleen oikein. Lisäksi odotettiin yhteydenottoja laboratorion käyttäjiltä, kuten opettajilta ja opiskelijoilta, jos he huomaisivat, että jokin heidän järjestelmänsä ei toimi oikein. Näitä ongelmia sitten selvitettiin ja ratkaistiin sitä mukaa, mitä niitä ilmeni.

Kaikkiaan ongelmia ilmeni vähemmän, kuin mihin olimme valmistautuneet. Rikki menneet yksittäiset palvelut ratkesivat uusilla ja paremmilla palomuurisäännöillä. Näppäilyvirheitä IP-osoitteiden osalta ilmeni ainoastaan yhdessä VIP-objektissa, jossa sisä- ja ulkoverkon osoitteet oli määritetty toistensa paikalle.

6.2.1 Tiedostojärjestelmän valvontamonitori

Heti yliheiton jälkeen huomasimme, että laboratorion konesalin tiedostojärjestelmä Cephin valvontamonitori ei enää toiminut. Valvontajärjestelmä ei saanut haettua tiedostojärjestelmän dataa, jolloin monitorin taulut olivat tyhjiä. Tarkistimme vielä kaikki järjestelmään liittyvät palvelimet ja ne toimivat edelleen oikein.

Ongelmaksi osoittautui lopulta se, että valvontamonitorin liikenne jäi palomuuriin kiinni puutteellisen palomuurisäännön takia. Olimme tehneet palomuuriin sellaiset säännöt, että sisäverkon osoitteista pääsi palvelimien sisäverkon osoitteisiin ja julkiverkosta pääsi palvelimen julkisiin osoitteisiin. Nyt kuitenkin sisäverkosta pyrittiin saamaan yhteys palvelimen julkiverkon osoitteeseen. Kun teimme entisen lisäksi uuden säännön, jossa liikenne sallittiin sisäverkosta palvelimen julkiveron osoitteeseen, niin liikenne alkoi toimimaan ja valvontamonitori alkoi näyttää taas dataa oikein.

Tällainen tilanne syntyi siksi, koska emme osanneet ottaa huomioon entisen ja nykyisen palomuurin eroavaisuuksia liikenteen uudelleenohjauksessa (NAT). Paloalton palomuuri suoritti uudelleenohjauksen riippumatta palomuurisäännöistä. Tämä tarkoittaa sitä, että kun Paloalton palomuuriin oli tehty NAT-sääntö, joka ohjasi jonkin ulkoverkon osoitteeseen tulevan liikenteen sisäverkon osoitteeseen, niin palomuuri ohjaisi aina kyseisen säännön julkiverkon osoitteeseen tulevan liikenteen sisäverkon osoitteeseen. Fortigate-palomuuri toimi eri tavalla kuin Paloalto-palomuuri. Fortigate-palomuureissa tällainen NAT-sääntö tehdään palomuurisääntöön lisättävällä VIP-objektilla. Liikenteen uudelleen ohjaus toimii vain, jos VIP-objekti on lisätty johonkin palomuurisääntöön.

Kun teimme yllä olevat johtopäätökset liikenteen uudelleenohjauksesta, niin huomasimme myös muita järjestelmiä ja palveluita, jotka eivät tulisi toimimaan halutulla tavalla, vaikka niistä ei vielä suoraan meille ilmoitusta tullut. Lisäsimme tarvittavia sääntöjä palomuurille, jotta sisäverkosta voidaan liikennöidä palvelimien julkisiin osoitteisiin.

6.2.2 Liikenne Bull-supertietokoneelle ei toiminut

Kajaanin ammattikorkeakoululla on käytettävissä myös supertietokone nimeltään Bull. Tietojärjestelmälaboratorion ja Bullin väillä pitää kulkea salattuja yhteyksiä, jotka olimme toteuttaneet IPSec-tunnelilla. Jostain syystä kyseinen liikenne ei kuitenkaan toiminut.

Ongelmaksi osoittautui jälleen väärin määritetyt palomuurisäännöt. IPSec-tunnelin vaatimat säännöt oli kopioitu entisestä palomuurista, mutta huomasimme, että Paloalto-palomuuri toimi tässäkin asiassa eri tavalla kuin Fortigate-palomuuri. Olimme tehneet palomuurisäännön siten, että tunnelin päätä edustaneeksi interfaceksi oli laitettu se VLAN, jonka alle tunneli oli määritetty. Liikenne ei kuitenkaan toiminut näin. Sääntöön piti muuttaa interfaceksi itse tunnelin oma interface. Tämän muutoksen jälkeen liikenne toimi taas oikein.

6.2.3 Opetusverkkojen muuttuneet osoitteet

Suurimpaan osaan opetusverkkojen laitteiseen oli IP-asetukset määritetty käsin, jolloin tietojärjestelmälaboratorion käyttäjät pystyivät hallinnoimaan laitteitaan, palvelimiaan ja omia IP-osoitteitaan paremmin. Uudella palomuurilla nämä entiset opetusverkot oli nyt yhdistetty kahdeksi isommaksi verkoksi, jolloin laitteille ja palvelimille määritetyt IP-asetukset olivatkin nyt väärin konfiguroitu. Näiden laitteiden käyttäjät joutuivat varaamaan uudesta isommasta IP-osoiteavaruudesta itselleen uudet IP-osoitteet ja päivittämään hallinnoimiensa laitteiden ja palvelimien IP-asetukset oikeiksi. Käytännössä käyttäjien piti käydä vaihtamassa IP-asetuksiin mahdollinen uusi IP-osoite, aliverkkopeite ja yhdyskäytävä.

Tämä muutos ei ollut vahinko, vaan tietoinen päätös, joka kuitenkin edellytti laboratorion käyttäjiltä muutoksia heidän hallinnoimiinsa laitteisiin ja palvelimiin, mikäli he halusivat niiden pystyvän jatkossa liikennöimään laboratorion verkossa.

7 IPv6-osoitteiden käyttöönotto

Kun palomuuri oli onnistuneesti saatu vaihdettua ja tietojärjestelmälaboratorion verkkoliikenne toimi halutusti, niin tietojärjestelmälaboratorion ylläpitäjät halusivat, että myös IPv6-osoitteiden toimintaa pitäisi tutkia juuri palomuurin määritysten kannalta. Entisellä palomuurilla oli jo IPv6-osoitteen toiminnassa, mutta palomuurin vaihdettua niiden toiminta lakkasi toimimasta puutteellisten määritysten vuoksi. IPv6-osoitteilla tapahtuva liikennöinti ei ollut kriittistä laboratorion toiminnalle, joten siihen ei käytetty resursseja kuin vasta palomuurin vaihtamisen jälkeen.

Tavoitteena oli mahdollistaa laboratorion tietokoneiden ja palvelimien liikenne myös IPv6-osoitteilla nykyisten IPv4-osoitteiden rinnalla. Tämä tultaisiin todentamaan pystyttämällä laboratorion verkkoon sellainen palvelin, joka toimisi vain IPv6-osoitteilla sekä johon voisi yhdistää laboratorion tietokoneilta ja julkiverkosta.

Liikenteen testaamiseen käytettiin Opetus-DMZ, Opetus-Sandbox ja Luokka-verkoissa sijaitsevia palvelimia. Lisäksi Opetus-DMZ verkon palvelimelle haluttiin päästä kiinni myös julkiverkosta.

7.1 Lähtötilanne

Tietojärjestelmälaboratorion verkkoympäristöön oli jo aikaisemmin varattu omat IPv6-osoitteet. Osoiteavaruudet oli myös määritetty valmiiksi laboratorion eri verkoille. Eli tehtäväksi jäi siis valmiiden osoitteiden määrittäminen oikein palomuurille.

Jos Fortigate-palomuurissa halutaan käyttää IPv6-osoitteita, niin niiden käyttö pitää ensin mahdollistaa ”System > Feature Visibilty” -sivulta. ”Core Features” -toimintojen alta löytyy ”IPv6”-ominaisuus, joka pitää ottaa käyttöön. Tämä lisää muun muassa interface-asetuksiin ja sääntömäärityksiin myös IPv6-osoitteille kohdat IPv4-osoitteiden rinnalle. Tämä ominaisuus oli jo aikaisemmassa vaiheessa otettu käyttöön tulevaisuutta varten.

7.2 Palvelimien asennus ja määritykset

IPv6-osoitteilla liikennöintiin testaamiseen käytettiin HTTP-palvelinta, joka sijaitsi Opetus-DMZ verkossa. Palvelin pystytettiin verkkoon käyttämällä laboratorion virtualisointialustaa. Palvelimen

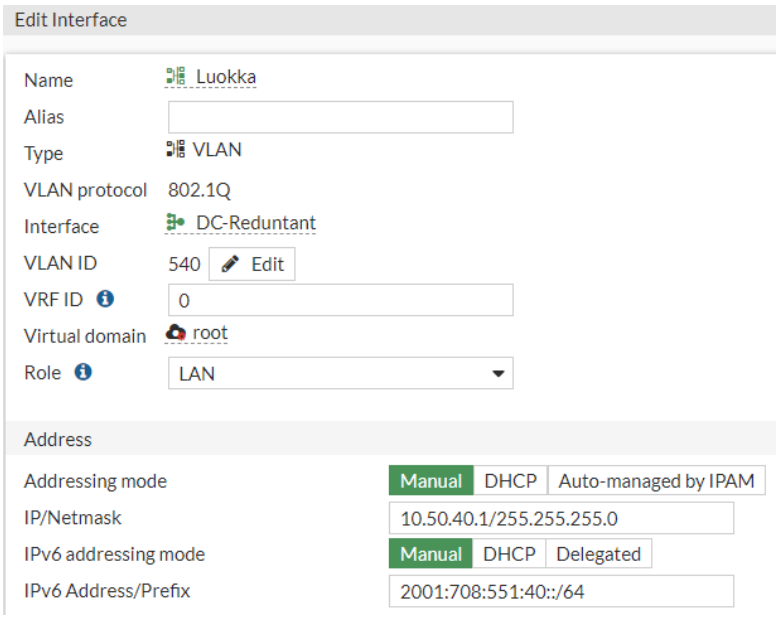
käyttöjärjestelmänä toimi Ubuntu Server 20.04 ja siihen asennettiin Apache HTTP-palvelin, koska ne olivat ennestään tuttuja ja helppoja käyttää. Apache määritettiin toimimaan sekä IPv4- että IPv6-osoitteilla.

Lisäksi toinen palvelin pystytettiin Opetus-Sandbox-verkkoon. Tämä palvelin toimisi puhtaasti testikoneena, jolla on tarkoitus testata yhteyttä Opetus-DMZ- ja Opetus-Sandbox-verkkojen välillä.

7.3 IPv6-osoitteiden määritys verkolle

IPv6-osoitteiden määrittäminen verkolle tapahtuu lähes samalla tavalla kuin IPv4-osoitteilla. Määritys tapahtuu verkon asetuksissa, jotka saadaan auki ”Network -> Interfaces” -sivulta. Verkon asetuksissa määritetään haluttu IPv6-osoite ja prefix kohtaan ”IPv6 Address/Prefix”. Tässä tapauksessa verkot määritettiin niin, että verkolle:

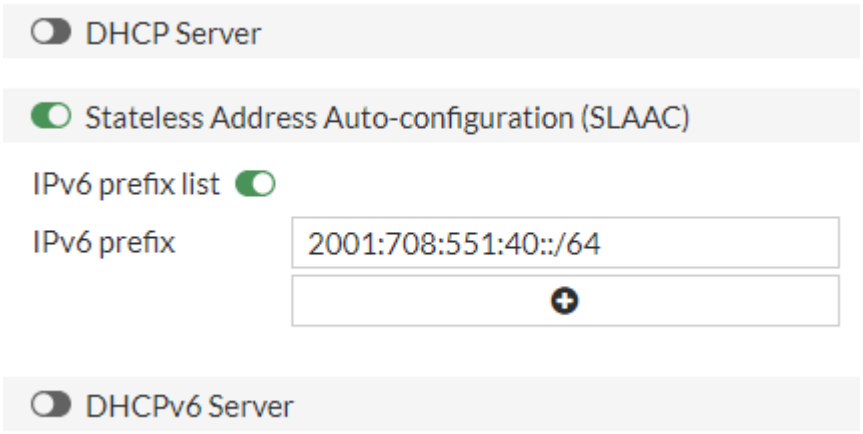
- ”Opetus-DMZ” tuli verkko 2001:708:551:110::/64,
- ”Opetus-Sandbox” tuli verkko 2001:708:551:150::/64,
- ”Luokka ” tuli verkko 2001:708:551:40::/64 (kuva 13),
- ”Funet-Opetus” tuli verkko 2001:708:551:ffff::11/126.



Kuva 15. Luokka-verkolle on määritetty IPv4-verkko 10.50.40.1/24 ja IPv6-verkko 2001:708:551:40::/64.

Samalta sivulta voidaan myös määritellä verkolle SLAAC tai DHCPv6 päälle. SLAAC-termi muodostuu sanoista ”Stateless Address Autoconfiguration” ja käytännössä se jakaa automaattisesti verkon jokaiselle laitteelle uniikin IPv6-osoitteen. Se ei kuitenkaan pysty kertomaan laitteille DNS-palvelimen osoitetta. DHCPv6 pystyy osoitteiden jakamisen lisäksi myös kertomaan laitteille DNS-palvelimen sen mukaan, millä määrityksillä DHCPv6 on otettu käyttöön. [18.] [19.]

Tässä testivaiheessa järkevin ratkaisu oli käyttää IPv6-osoitteiden jakamiseen SLAAC:ia. DNS-määritykset tehtiin testipalvelimille käsin. Verkoille ”Opetus-Sandbox” ja ”Luokka” laitettiin SLAAC päälle, jolloin näiden verkkojen laitteet saavat automaattisesti oman IPv6-osoitteen (kuva 14). ”Opetus-DMZ” verkko haluttiin pitää staattisena. Se tarkoittaa sitä, että verkolle ei jaeta automaattisesti IP-osoitteita, vaan ne pitää aina määritellä verkon koneille käsin.



Kuva 16. Luokka-verkolle asetettu SLAAC, joka jakaa IPv6-osoitteita 2001:708:551:40::/64 -osoiteavaruudesta.

7.4 Liikenteen reititys ja salliminen

Fortigatessa IPv6-osoitteilla tapahtuva liikenne pitää erikseen sallia ja reitittää samalla tavalla, kuin IPv4-osoitteiden kanssa. Kun IPv6-toiminto otettiin ”Feature Visibility” -sivulta käyttöön, niin tarvittaviin paikkoihin on tullut IPv4-osoitteiden rinnalle myös mahdollisuus määrittää IPv6-osoitteiden liikenne.

Palomuurisäännöt tehdään sivulta ”Policy and object -> Firewall Policy”. Säännöt muodostetaan muuten samalla tavalla kuin IPv4-osoitteiden liikenteelle, mutta IPv4-osoitteiden sijasta käytetään IPv6-osoitteita niille tarkoitetuissa osoitekentissä. Testausta varten tehtiin kokonaan uudet

säännöt IPv6-osoitteilla tapahtuvaa liikennettä varten, vaikka ne olisi voitu myös lisätä olemassa oleviin avauksiin.

Myös reititys pitää muistaa määrittää uudelleen IPv6-osoitteden liikenteelle. Reitityksiä voidaan tehdä ja tarkastella ”Network -> Static Routes” -sivulta. IPv4- ja IPv6-osoitteille pitää olla erikseen omat reitit, eikä niitä voida yhdistää saman määrityksen alle niin kuin palomuurisäännöissä. Uudet reitit tehdään ”Create New → IPv6 Static Route” -painikkeen takaa, josta pääsee määrittämään tarvittavat määritykset. Tehtävät määritykset ovat samat kuin IPv4-osoitteilla, mutta pitää käyttää haluttuja IPv6-osoitteita.

7.5 Liikennöinti IPv6- ja IPv4-osoitteiden välillä

Fortigate-palomuuriin voidaan tehdä sellaiset määritykset, joiden avulla pystytään mahdollistamaan liikenne kahden eri palvelimen välillä, joista toinen käyttää liikennöintiin IPv4-osoitetta ja toinen IPv6-osoitetta. Käytännössä tämä onnistuu siten, että kohdepalvelimelle määritettään palomuuriin VIP, jonka avulla palomuuri mahdollistaa liikenteen kulkemisen IPv4- ja IPv6-osoitteiden välillä. Kohdepalvelimelle pitää siis palomuurilla määrittää sekä IPv4- ja IPv6-osoitteet, mutta itse palvelimilla niitä ei tarvitse määrittää. IPv4-osoitteesta liikennöinti IPv6-osoitteeseen vaatii NAT46-määritysten tekemisen. IPv6-osoitteesta liikennöinti IPv4-osoitteeseen vaatii NAT64-määrityksen.

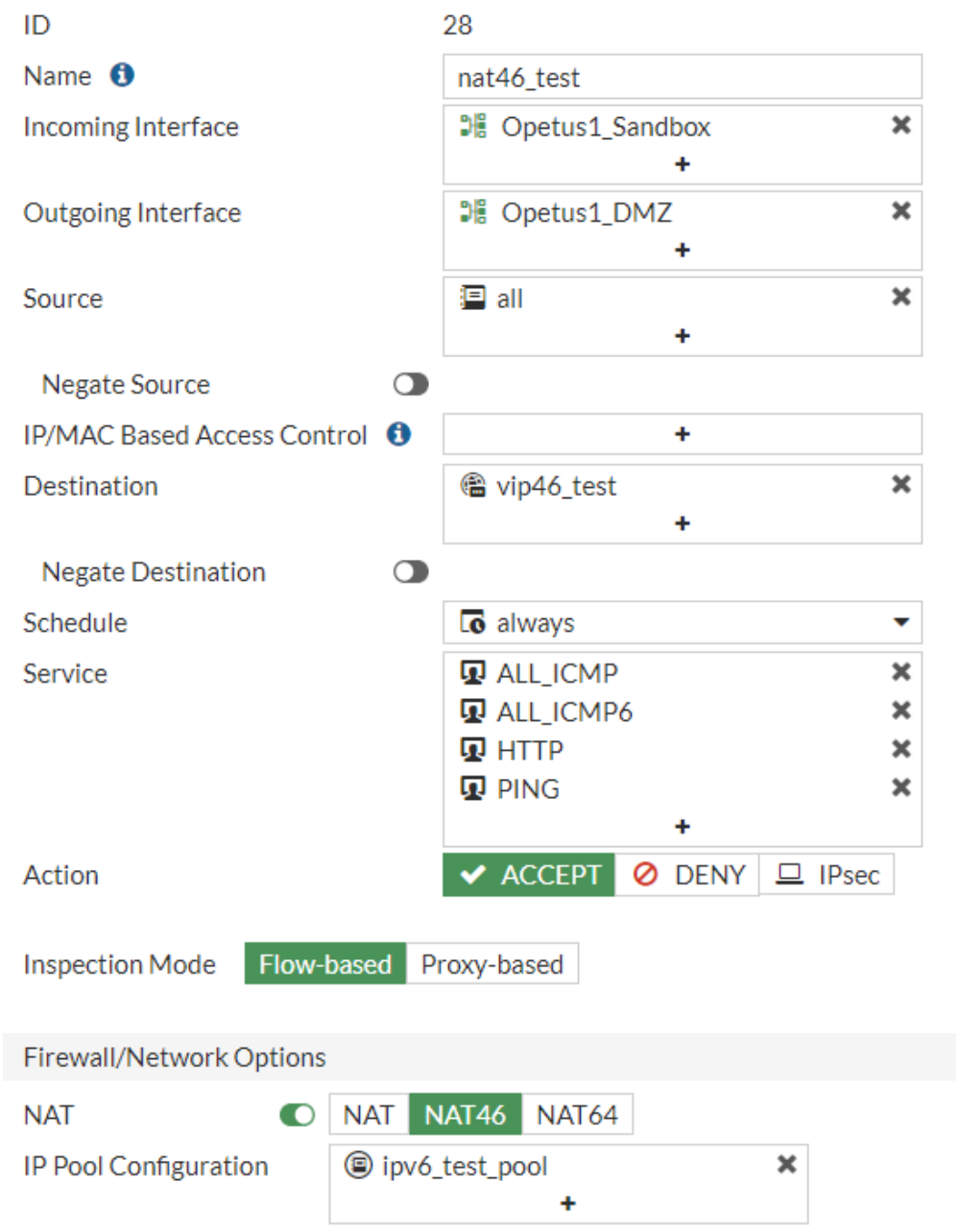
7.5.1 NAT46

Kun halutaan mahdollistaa IPv4-osoitteesta liikennöinti sellaiselle palvelimelle, jolla on vain IPv6-osoite, niin pitää tehdä tarvittavat NAT46-määritykset. Ensin täytyy tehdä uusi VIP ”Policy & Objects → Virtual IPs” -sivulta. VIP määritetään seuraavasti:

- VIP Type = IPv4,
- Type = Static NAT,
- External IP address/range = määritetään tähän jokin IPv4-osoite x, johon liikennöinnin aloittaja ottaa yhteyttä,

- Map to IPv6 address/range = kohdepalvelimen IPv6-osoite.

Tarvittaessa voidaan myös tehdä lisämäärityksiä, kuten portinohjaus, jos se on tarpeen. Tämän jälkeen luodaan uusi palomuurisääntö. Sääntö luodaan muuten normaalisti, mutta ”destination” -kenttään määritetään äsken luotu VIP. Lisäksi NAT kytketään päälle ja valitaan NAT-tyypiksi ”NAT46”. NATin IP-pooliksi määritetään sellainen IP-pool, joka sisältää IPv6-osoitteita. Nämä osoitteet näkyvät sitten liikenteen lähteenä kohdepalvelimella.



Kuva 17. Esimerkki palomuurisäännöstä, joka on tehty NAT46-määrityksillä.

Näiden määrityksien avulla palvelimelta, joka liikennöi IPv4-osoitteilla, voidaan ottaa yhteys IPv4-osoitteeseen x. Palomuuri ohjaa osoitteeseen x tulevan liikenteen kohdepalvelimelle IPv6-osoitteella ja käyttää liikenteen lähdeosoitteena NAT46 IP-pooliin määritettyjä osoitteita.

7.5.2 NAT64

NAT64 toimii lähes samalla periaatteella kuin NAT46, mutta siinä liikenteen lähteenä toimii IPv6-osoitetta liikennöintiin käyttävä palvelin, jonka tarvitsee muodostaa yhteys IPv4-osoitteen omaavaan kohdepalvelimeen. Ensin täytyy tehdä uusi VIP, joka määritetään seuraavasti:

- VIP type = IPv6,
- External IP address/range = määritetään jokin IPv6-osoite, johon lähdepalvelin muodostaa yhteyden
- Map to IPv4 address/range = Specify = kohdepalvelimen IPv4-osoite.

Tarvittaessa voidaan määrittää myös porttiohjaus tai VIP toimiaan vain tietyistä lähdeosoitteista. Sen jälkeen tehdään uusi palomuurisääntö, johon määritetään ”destination” -kentään juuri luotu VIP. Lisäksi NAT kytketään päälle ja NAT-tyypiksi valitaan NAT64. NATin IP-pooliksi määritetään sellainen pool, joka sisältää IPv4-osoitteita. Nämä osoitteet näkyvät kohdepalvelimella liikenteen lähdeosoitteina.

7.6 Lopputilanne

Kun tarvittavat IPv6-määritykset oli tehty, joihin kuului:

- IPv6-osoiteavaruuden ja SLAACin määrittäminen tarvittaviin interfaceihin,
- palomuurisääntöjen luonti
- staattisten reittien luonti

niin Opetus-Sandbox -verkosta pystyi liikennöimään Opetus-DMZ -verkossa sijaitsevaan testipalvelimeen sekä IPv4- että IPv6-osoitteilla. Lisäksi testipalvelimeen pystyi yhdistämään ulkoverkosta IPv6-osoiteella. Laboratorion työasemat saivat automaattisesti IPv4- ja IPv6-osoitteet ja ne pystyivät liikennöimään sisä- ja ulkoverkkoon käyttäen kumpaa osoitetta vaan.

8 Projektin onnistuminen

Projektin selkeä päätavoite oli saada uusi palomuuri käyttöön tietojärjestelmälaboratorion verkkoympäristöön määräaikaan mennessä. Käytännössä tämä tarkoitti sitä, että määräaikaan mennessä laboratorion verkkoliikenne toimisi uuden palomuurin kautta vähintään yhtä hyvin kuin ennen palomuurin vaihtamista. Lisäksi mahdollisuuksien mukaan hyödynnettäisiin uuden palomuurin ominaisuuksia, jotta laboratorion verkkoympäristöä voisi käyttää monipuolisemmin.

Projektin toinen tavoite oli selvittää IPv6-osoitteiden mahdolliset määritykset palomuurissa. Tämän kautta voitaisiin mahdollisesti alkaa taas hyödyntämään IPv6-osoitteita laboratorion verkkoympäristössä.

Projektin päätavoite täyttyi onnistuneesti. Palomuuri saatiin otettua käyttöön määräajassa ja kaikki tarvittavat ominaisuudet tietojärjestelmälaboratorion jokapäiväiseen toimintaan olivat käytettävissä. Entiseen palomuuriin verrattuna ominaisuuksia saatiin jopa lisättyä, esimerkiksi etäyhteyden muodostaminen tietolaboratorion verkkoon onnistui nyt myös verkkoselaimen kautta, eikä vaatinut erillistä ohjelmaa.

Myös IPv6-osoitteiden osalta tavoitteet saavutettiin. Tällä hetkellä tietojärjestelmälaboratorion työpisteiden tietokoneet saavat automaattisesti IPv4- ja IPv6-osoitteen ja ne pystyvät liikennöimään sisä- ja ulkoverkkoon molemmilla osoitteilla.

Suuria ongelmia ei palomuurin käyttöönotossa ilmennyt. Olimme varautuneet yliheitosta johtuviin ongelmiin ja ne saatiin selvitettyä nopeasti. Kaikkiaan käyttöönotto sujui hyvin. Tällä hetkellä uusi palomuuri on ollut käytössä yli vuoden ja konfiguraatiosta johtuvia ongelmia ei ole tullut vastaan. Muutama ongelmia on syntynyt, mutta ne ovat korjaantuneen palomuurin käyttöjärjestelmän päivityksellä. Muutoksia konfiguraatioon on tehty palomuurin käyttöönoton jälkeen, jotta palomuurin ominaisuuksia saadaan hyödynnettyä paremmin.

Aivan kaikkea haluttua ei saatu toimintaan. Suurimpana puutteena jäi tekemättä loppuun asti palomuurista erillinen lokienhallintapalvelin, jolle palomuurin lokit olisi tallennettu helposti katsottavaan muotoon. Saimme palomuurin lähettämään lokit erilliselle palvelimelle, mutta fiksua keinoa niiden hallinnointiin ja tutkimiseen ei saatu kasaan. Tämä johtui käytännössä vain ajanpuutteesta ja jätimme tämän osuuden harkitusti pois projektista.

Palautetta projektin onnistumisesta kysyttiin myös tietojärjestelmälaboratorion ylläpitäjältä Tuomo Huuskolta, jonka antoi projektista seuraavan palautteen:

> ”Projekti meni kokonaisuutena erittäin hyvin. Kaikki projektin tavoitteena olleet välttämättömät ominaisuudet saatiin testattua ja käyttöönotettua. Projektilla oli suhteellisen tiukka aikataulu, joka johtui aikaisempien palomuurien vanhentuvista lisensseistä ja muurien yhtäaikaista ylläpitoa haluttiin minimoida kustannussyistä. Tästä syystä myös iso osa palomuurin ominaisuuksista jäi vielä testaamatta, mutta näiden valinnaisten ominaisuuksien testaaminen ja käyttöönotto ei ollutkaan projektin päätavoite.
>
> Yhteistyö projektiin osallistuneiden kesken onnistui hyvin. Ylitsepääsemättömissä ongelmatilanteissa osattiin kysyä apua ja projektin eteneminen ei missään vaiheessa pysähtynyt, vaan eteni suunnitelmien mukaisessa tahdissa. Lisäksi projektin aikana opittuja asioita ja tutkittuja ominaisuuksia osattiin hyödyntää projektin käyttöönottovaihetta suunnitellessa, sekä käyttöönoton aikana. Vanhentuneita tai kömpelöitä toimintatapoja uskallettiin myös kyseenalaistaa ja useimmissa tapauksissa niitä korvaamaan löydettiin parempi käytäntö tai uusi palomuurin ominaisuus. Projektissa ei tullut vastaan suurempia epäonnistumisia ja suurin työ DC-labran ylläpitäjän näkökulmasta oli huolehtia, että projekti pysyi aikataulussaan, sekä varmistaa, että projektin jäsenet tutkivat palomuurin käyttöönottoon vaaditut ominaisuudet ennen muita ominaisuuksia.
>
> Palomuuri on toiminut käyttöönoton jälkeen hyvin. Muutamia pieniä ongelmia on tullut vastaan, mutta lähestulkoon kaikki niistä ongelmista on korjautunut päivittämällä palomuuria uudempaan versioon. Suurimmat muutokset, mitä palomuuriin on tehty käyttöönoton jälkeen, liittyy palomuurin fyysisiin portteihin, sekä siihen millaisessa käytössä ne ovat. Nämä muutokset tehtiin syystä, että palomuurissa on rajattu määrä 10Gbps-portteja ja ne haluttiin käyttää mahdollisimman tehokkaasti.
>
> Lopuksi haluan kiittää Onnia ja muita projektiin osallistuneita erinomaisesti tehdystä työstä. Ilman teitä tämä projekti olisi jäänyt aikataulustaan auttamattomasti jälkeen, sekä aiheuttanut huomattavan määrän ennenaikaisia harmaita hiuksia DC-labran ylläpidolle.”

Lähdeluettelo

1) Hyppönen Mikko. 2021. Internet

2) CyberHoot. 2020. SQL Slammer Virus. https://cyberhoot.com/cybrary/sql-slammer-virus/

3) Val Saengphaibul. 2022. A Brief History of The Evolution of Malware. https://www.fortinet.com/blog/threat-research/evolution-of-malware

4) AV-TEST. 2022. https://www.av-test.org/en/statistics/malware/

5) Cisco Visual Networking Index: Forecast and Trends, 2017–2022. 2018. https://cyrekdigital.com/uploads/content/files/white-paper-c11-741490.pdf

6) Amon, C. & Shimoski, R. J. 2003. The Best Damn Firewall Book Period.

7) Higgins, K. J. 2008. Who Invented the Firewall? https://www.darkreading.com/analytics/who-invented-the-firewall-

8) Liu, X. A. 2010. Firewall Design And Analysis.

9) Britannica. Firewall. https://www.britannica.com/technology/firewall

10) Wiley J. & Sons. 2008. Networking All-In-One Desk Reference for Dummies.

11) Cloudflare. What is an ACK flood DDoS attack? https://www.cloudflare.com/learning/ddos/what-is-an-ack-flood/

12) N-able. Stateful vs. Stateless Firewall Differences. https://www.n-able.com/blog/stateful-vs-stateless-firewall-differences

13) Firewall Benefits: The Importance of Firewall Security. https://www.fortinet.com/resources/cyberglossary/benefits-of-firewall

14) Paloalto Techdocs. What Happens When Licenses Expire? https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/subscriptions/what-happens-when-licenses-expire

15) Fortinet. Fortigate 600E Series. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf

16) Archon. What ISAn IPSec Tunnel? An Inside Look. https://www.archonsecure.com/blog/ipsec-tunnel-technology

17) Avi Networks. Network Address Translation. https://avinetworks.com/glossary/network-address-translation/

18) Network Academy. IPv6 Stateless Address Auto-configuration (SLAAC). https://www.networkacademy.io/ccna/ipv6/stateless-address-autoconfiguration-slaac

19) Fortinet Community. Technical Tip: How to setup the FortiGate to assign IPv6 addresses. https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-setup-the-FortiGate-to-assign-IPv6/ta-p/194156