Tampereen ammattikorkeakoulu

FortiGate palomuurit ja niiden hyödyntäminen ICT Elmon toimistoverkossa

Anni Lehtomäki

OPINNÄYTETYÖ
Toukokuu 2020

Tietojenkäsittely
Tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely
Tietoverkot

LEHTOMÄKI, ANNI:
FortiGate palomuurit ja niiden hyödyntäminen ICT Elmon toimistoverkossa

Opinnäytetyö 31 sivua
Toukokuu 2020

Opinnäytetyön tavoitteena oli uudistaa ICT Elmon jo vanhentunut toimistoverkon palomuuriratkaisu hyödyntäen Fortinetin FortiGate-palomuureja. Uudistuksessa haluttiin käyttää FortiGate palomuureja, jotta niiden kanssa toimiminen sekä laitteiden ympäristöt tulevat tutuiksi, ja valmistajan palomuureja olisi entistä helpompi hyödyntää tulevissa asiakasprojekteissa.

Tarkoituksena oli saada toimintaan uusi toimistoverkkoympäristö uusilla palomuureilla, joiden ansiosta sisäverkon valvonta ja ylläpito helpottuvat, kun kaikki verkon aktiivilaitteet vaihtuvat yhden valmistajan ja näin ollen yhden hallinnan alle.

Opinnäytetyössä tarkastellaan kuinka Fortinetin FortiGate-palomuureja voidaan konfiguroida, miten palomuuriympäristöstä saadaan vikasietoinen ja mitä ongelmia kyseisten laitteiden kanssa on esiintynyt. Opinnäytetyössä kuvataan toimistoverkon koko uudistusprosessi laitteiden saapumisesta uuden verkon yliheittoon asti. Projektin aikaiset ongelmat ja niiden ratkaisut dokumentoitiin myös työhön.

Asiasanat: palomuuri, lähiverkko, konfigurointi

ABSTRACT

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

LEHTOMÄKI, ANNI:
FortiGate Firewalls and Their Usage in ICT Elmo’s Office Network.

Bachelor's thesis 31 pages
May 2020

The goal of this thesis was to implement a refurbishment of ICT Elmo’s office network using Fortinet’s FortiGate firewalls. FortiGate firewalls were chosen for this project to learn more about the firewalls themselves and for their usage in future customer environments.

The purpose was to get a working firewall environment in ICT Elmo’s office network using the new firewalls. Maintaining the network after the implementation would get easier due to the used devices being only from one vendor and so having only one dedicated place to maintain them all.

The thesis explains how FortiGate firewalls can be configured, how to establish a high availability environment and problems with said firewalls. The journey from devices’ arrival to the implementation is explained in this thesis along with any problems arisen during the firewall project.

Key words: firewall, LAN, configuration

SISÄLLYS

1 JOHDANTO 6
2 PROJEKTIN ESITTELY 7
3 PALOMUURIEN KONFIGUROIMINEN 8
3.1 Aloitus 9
3.2 HA eli High Availability 11
3.3 Interfacet ja niiden konfiguroiminen 16
3.4 Tunnelointi 19
3.5 Palomuurisäännöt 22
4 TOIMISTOVERKON UUDISTAMINEN 25
4.1 Lähtötiedot 25
4.2 Laitteet 25
4.3 Konfiguroiminen 25
4.4 Yliheitto ja testaus 27
5 ONGELMAT PROJEKTISSA 28
6 POHDINTA 30
LÄHTEET 32

ERITYISSANASTO

VLAN	Virtual Local Area Network, virtuaalinen lähiverkko
VPN	Virtual Private Network, virtuaalinen erillisverkko
BGP	Border Gateway Protocol, reititysprotokolla
HA	High Availability, järjestelmän korkea saatavuus
DHCP	Dynamic Host Configuration Protocol, käytetään mm. IP-osoitteiden jaossa.
IP-osoite	Neliosainen numerosarja, jonka avulla laitteet juttelevat toisilleen.
Backup	Varmuuskopio tai varmuuskopiointi
Host Name	Laitenimi
Konfigurointi	Laitteen asetusten määritys
Interface	Fyysinen tai virtuaalinen liitäntä laitteessa
Uplink	Portti, josta laite on yhdistynyt verkkoon
Portti	Fyysinen liitäntä laitteessa

1 JOHDANTO

Opinnäytetyössä käsitellään Fortinetin FortiGate palomuurin peruskonfigurointia ja ICT Elmon toimistoverkon uudistusprojektia, joka toteutettiin kokonaisuudessaan FortiGate palomuureilla. Projektissa poistettiin kokonaan vanhan toimistoverkon laitteet, jotta tilalle saatiin vaihdettua täysin uusia, ja myös asiakastuotannossa käytettäviä palomuureja ja verkkolaitteita. Toimistoverkko haluttiin uudistaa, koska vanha verkko alkoi olla jo iäkäs ja sen toiminta ei ollut enää yhtä tehokasta, lisäksi haluttiin lisää kokemusta FortiGate laitteista, joka hyödyttää myös tulevaisuuden asiakasprojekteja.

Opinnäytetyön tavoitteena on saada ICT Elmon vanha toimistoverkko palomuurin osalta tuotua hallitusti alas ja nostaa uusi palomuuritoteutus palvelemaan paremmin toimiston uusiutuneita tarpeita. Tavoitteena on tehdä uusi palomuuriratkaisu toimimaan ICT Elmon toimistoverkkoon. Projektissa vanha verkko tullaan uusimaan uusilla laitteilla ja parantamaan verkon tietoturvaa sekä toiminnallisuutta. Opinnäytetyössä käydään läpi palomuuriprojektin eri vaiheet, laitteiden saapumisesta valmiiden laitteiden yliheittoon sekä testaukseen. Opinnäytetyössä selostetaan tarkemmin, miten FortiGaten palomuureja konfiguroidaan hieman eri tavalla kuin useimpia muita markkinoilla olevia, sekä samalla tutustutaan Fortinetin FortiGate palomuurin toimintaan sen graafisen käyttöliittymän kautta.

Opinnäytetyön tarkoituksena on antaa ICT Elmolle hyvä ja toiminnallinen verkonuudistus yhdessä ICT Elmon työntekijöiden kanssa. Tarkoituksena on tarkastella projektin tuloksia, tutkia FortiGaten konfiguroimista, kartoittaa mahdollisia ongelmakohtia ja kehittää osaamista tuleviin FortiGate projekteihin.

Opinnäytetyö tulee hyödyttämään ICT Elmoa, sillä siinä rakennetaan täysin uusi toimistoverkko yritykselle. Projektin myötä toimistoverkkoa saa paremmin valvotuksi eikä sisäverkko tule enää pätkimään uusien laitteiden myötä. Projektissa on vaihdettava vanhan palomuurilaitteen tilalle täysin uudet palomuurit, jotka tulevat toimimaan palomuuriparina ylläpitäen toimiston verkkoyhteyden, vaikka toiseen laitteeseen tulisikin ongelmia.

2 PROJEKTIN ESITTELY

ICT Elmon toimistoverkon uudistuksessa uudistetaan kaikki sisäverkon verkkolaitteet. Ennen verkosta löytyi monen eri valmistajan tuotteita esimerkiksi palomuurina toimi Ciscon valmistama laite, kytkiminä toimivat Extremen laitteet ja langattoman verkon tukiasemina Ruckus. Nykyään sisäverkossa käytössä on vain yhden valmistajan, Fortinetin, tuotteita. Palomuurit ovat toteutettu FortiGate palomuureilla, kytkimet FortiSwitch:llä ja langattoman verkon tukiasemat FortiAP:llä.

Laitteiden vaihto monelta eri valmistajalta vain yhdelle tuo helppoutta verkon pystyttämiseen sekä ylläpitämiseen. Fortinet on suunnitellut laitteensa niin, että kaikkia wlan-peilejä sekä kytkimiä pystytään hallitsemaan ja muokkaamaan suoraan palomuurin kautta, ja näin ollen eri hallintaportaaleista toiseen hyppiminen vähentyy.

Ennen varsinaisen projektin aloitusta sain käyttöön samanmerkkisen, joskin pienemmän FortiGate palomuurin, johon pääsin tutustumaan ennen varsinaisten laitteiden saapumista Suomeen. Tämän avulla FortiGaten käyttöliittymä tuli jokseenkin tutuksi, sillä vaikka projektissa käytettävät palomuurit olivat eri mallia, oli käyttöliittymä kaikissa samanlainen.

Opinnäytetyössä on käytetty kuvia ja vertauksia ICT Elmon palomuurinprojektiin. Tietoturvasyistä kuvista ja tekstistä on jätetty suorat viittaukset verkkoon tekemättä sekä kuvista on sensuroitu arkaluontoisia asioita kuten IP- ja VLAN tietoja.

3 PALOMUURIEN KONFIGUROIMINEN

Palomuuria tarvitaan ylläpitämään tietoturvallista verkkoa. Sen tehtävänä on sallia haluttua liikennettä, mutta estää kaikki muu liikenne. Palomuuri tunnistaa halutun liikenteen sille määriteltyjen sääntöjen mukaan ja sallii silloin vain sääntöjen mukaisen liikenteen palomuurin läpi (Forcepoint, What is a Firewall? n.d.). Palomuurin ja sen sääntöjen ansiosta verkkoon kohdistuvaa haittaliikennettä pystytään estämään ennen kuin se päätyy itse sisäverkkoon. Palomuuri helpottaa myös eri sisäverkkojen hallintaa palomuurisäännöillä ja VLAN:eilla sekä mahdollistaa VPN-yhteydenoton haluttuihin sisäverkkoihin. Palomuurien verkkoja pystyy yhdistämään muihin verkkoihin niin sanotun VPN-tunnelin avulla, tällöin kaksi tai useampi erillinen verkko eri laitteissa muuttuu yhdeksi verkoksi. Vaikka VPN-yhteyksiä ja -tunneleita, IP-osoitepohjaisia sääntölistoja ja VLANeja pystytään rakentamaan myös esimerkiksi reitittimien päälle, tarvitaan palomuuria tunnistamaan tilanteita, jossa halutaankin määrittää liikennettä protokollien, eikä IP-osoitteiden mukaan. Palomuurin avulla voidaan eri osoitteille määritellä protokolla perusteiset oikeudet samaan verkkoon, jollekin osoitteelle on voitu sallia vain HTTPS-liikenne, kun taas toinen osoite voi ottaa yhteyttä vain SSH-liikenteen kautta (Agrawal n.d.).

Palomuurien konfiguroiminen, eli niille asetusten määrittäminen, on pakollinen toimenpide, joka pitää tehdä ennen kuin laitteen voi ottaa käyttöön. Ilman oikeanlaista konfiguraatiota palomuuri ei voi toimia. Palomuurille on ainakin asetettava IP-osoite, joko kiinteänä osoitteena tai DHCP:ltä saatavana, reitti sisäverkon liikenteelle ulkoverkkoon sekä liikenteen ulkoverkkoon salliva sääntö. Palomuurin valmistajasta riippuen osa näistä on voinut olla valmiiksi konfiguroituna.

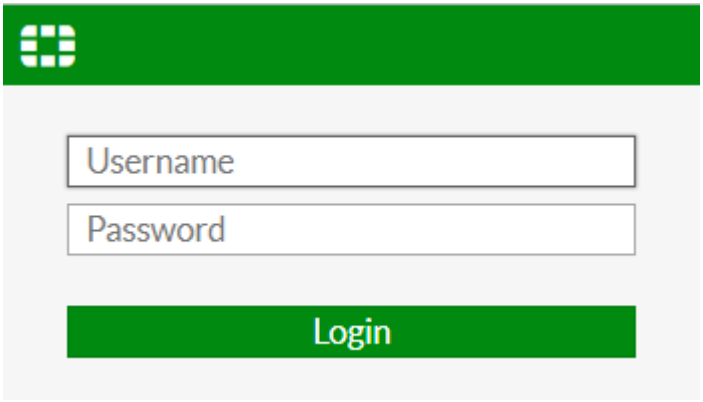
FortiGate on painottunut käyttämään graafista käyttöliittymää. Palomuurin asetukset konfiguroidaan pääsääntöisesti graafisen käyttöliittymän kautta. Valikot ovat selkeitä luettavia ja käyttäjä pääsee myös helposti katsomaan tarkempia tietoja jo valmiiksi konfiguroiduista asetuksista joko valitsemalla edit tai view haluamansa asetuksen kohdalta. Tämän jälkeen sivulle aukeaa tiedot kyseisestä valinnasta. Tässä pitää kuitenkin muistaa se, että tiedot eivät välttämättä ole samalla lailla ilmaistuja kuin asetusta konfiguroidessa, ja osaa asetuksista ei välttä-

mättä pääse enää muokkaamaan jälkikäteen. Esimerkiksi portin VLAN id:tä, virtual LAN eli virtuaalinen lähiverkko, ei pääse muokkaamaan enää jälkikäteen edes komentokehotteen kautta. Vaihtoehdot tällaisessa tilanteessa on poistaa vanha liitäntä ja tehdä uusi tilalle oikeilla asetuksilla, tai ottaa laitteesta backup, editoida tekstieditorilla konfiguraatiosta VLAN id oikeaksi ja tämän jälkeen palauttaa palomuurin konfiguraatiot hyväksikäyttäen tätä uutta muokattua backup tiedostoa. Tästä tietysti aiheutuu se ongelma, että palomuurin on käynnistettävä itsensä uudelleen, jolloin kaikki liikenne lakkaa palomuurin takana oleville käyttäjille sekä palveluille.

Vaikkakin FortiGate on selkeästi painottunut graafiseen näkymään, ei tämä tarkoita sitä, etteikö palomuureista puuttuisi komentokehote kokonaan. Osa komennoista on nopeampi ajaa laitteeseen komentokehotteen kautta kuin yksitellen kliksutella graafiselta puolelta. Käyttäjä pääsee siirtymään komentokehotteeseen graafiselta puolelta koska tahansa nappia painamalla, jolloin sivulle ilmestyy musta tekstilaatikko. Komentoja, jotka olivat helpompi laittaa laitteeseen komentoliittymän kautta, oli muun muassa BGP-konfiguraatiot sekä joissain tapauksissa uuden staattisen reitin luominen. Palomuuriprojektin aikaisessa ohjelmistoversiossa oli mukana bugi, mikä satunnaisesti esti uuden staattisen reitin luomisen kertoen, että kyseinen gateway, eli oletusyhdyskäytävä, on jo käytössä. Tämän bugin pystyin kiertämään lisäämällä reitin komentokehotteen kautta.

3.1 Aloitus

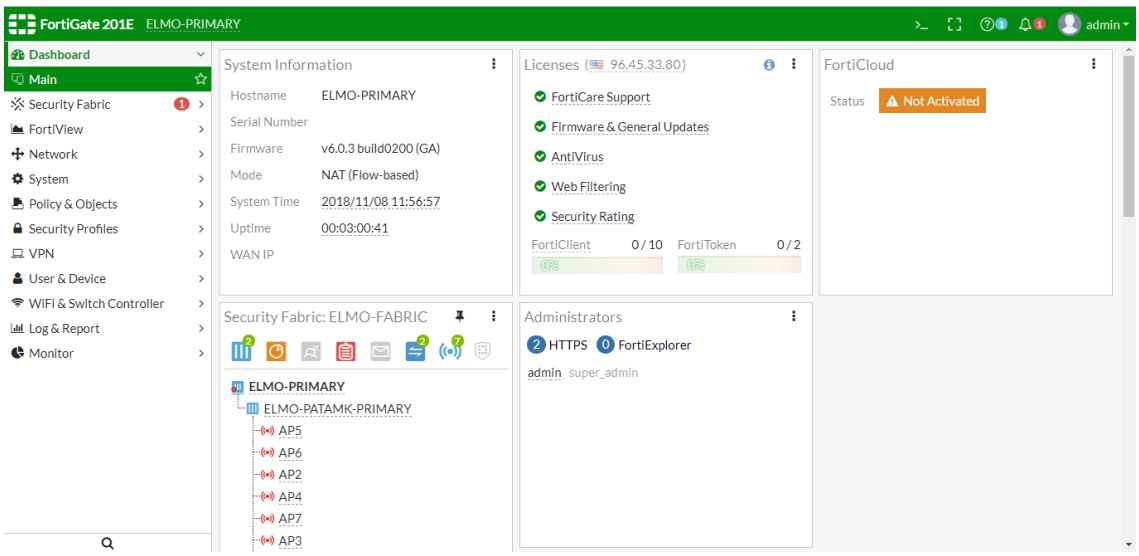
Ennen kuin varsinaisen konfiguroimisen pääsee aloittamaan, on päästävä laitteeseen itsessään sisälle. Laitteen hallintaan pääsee helpoiten laittamalla oman tietokoneensa kiinni johonkin sisäverkolle tarkoitetuista porteista, näiden porttien määrä riippuu FortiGaten mallista. Kun tietokone on kiinni FortiGatessa ja FortiGate on päällä, pääsee tietokoneen selaimella osoitteessa https://192.168.1.99 palomuurin hallintaan. Fortinet on auttanut käyttöönotossa ja jokaisen uuden FortiGate laitteen päältä löytyy kuvallinen ohje, kuinka käyttäjä pääsee laitteeseen käsiksi.



KUVIO 1. FortiGate login ruutu

Ennen kuitenkin varsinaisen hallintasivun aukeamista kysyy palomuuri käyttäjältään salasanaa. Mikäli tämä on ensimmäinen kerta, kun palomuuriin ollaan menossa, on oletuskäyttäjä *admin* ja oletussalasanaa ei ole, vaan kenttä jätetään tyhjäksi. Laitteen kirjautumisasetukset kannattaa käydä vaihtamassa ensitöikseen laiteen nimen ohella. Admin käyttäjän salasanan pääsee muokkaamaan valikosta System -> Administrator ja sieltä valitsemalla admin-käyttäjän. Jos palomuuriin halutaan lisäturvaa sallimaan vain admin kirjautumiset tietyistä osoitteista, löytyy saman valinnan alta trusted host kohta, johon voidaan määritellä mistä on sallittua päästä kirjautumissivustolle. Trusted host osoitteita määritellessä tulee olla tarkkana oikeinkirjoituksen kanssa, sillä jos vahingossa palomuurille näppäillään väärä IP-osoite, ei siihen pääse enää kirjautumaan sisälle ja virhe on käytävä korjaamassa konsoliyhteyden kautta.

Kirjautuessa sisään FortiGate ohjaa käyttäjän aina palomuurin etusivulle. Ruudun yläoikealta löytyy yleiset ilmoitukset ja huomautukset sekä käyttäjäasetukset, kuten käyttäjän uloskirjautuminen. Tärkein painike kuitenkin tästä palkista on ensimmäinen vasemmalta katsottuna, ”>_” näköinen valinta, jonka takaa saa auki komentokehotteen. Komentokehotteen voi joko avata puoliksi peittämään FortiGaten käyttöliittymä tai sen voi avata halutessaan toiseen ikkunaan, jolloin palomuuria on helpompi selailla.



KUVIO 2. FortiGate etusivu

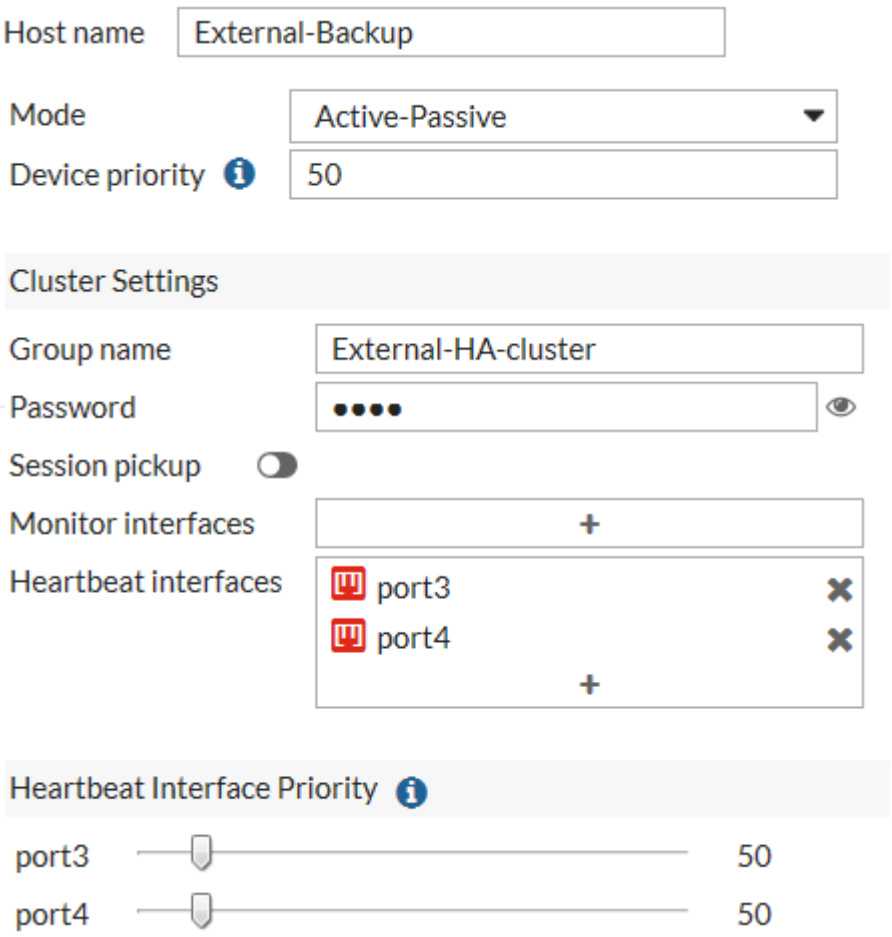
Etusivulta pääsee nopeasti vilkaisemaan palomuurin tiedot sekä tilanteen. Palomuurin nimi näkyy sekä ”System Information” kentässä että yläpalkissa, jossa se seuraa jokaiseen valikkoon mukana. Muita tärkeitä ovat Firmware sekä laitteen muisti ja prosessoritiedot. FortiGate seuraa koko ajan laitteen prosessorin ja muistin tehoja, sekä ilmoittaa mikäli laitteella on jotakin epätavallista käynnissä, esimerkiksi korkeasta muistinkäytöstä ilmestyy myös varoituspalkki hallintasivun yläreunaan. Firmware kohtaan ilmestyy myös pieni merkki, mikäli laitteeseen on saatavilla uudempi päivitys. Etusivu on lähinnä tarkoitettu nopeaksi katselmukseksi palomuurin tilaan, josta näkee nopeasti laitteen yleiset tiedot ja tilan sekä huomautukset jos jotain uutta on tarjolla, itse konfiguroimisessa ei etusivua juurikaan tarvita. Käyttäjä pystyy kustomoimaan etusivun juuri itselleen sopivaksi, tietolaatikoita pystyy raahaamaan pitkin etusivua ja niitä on myös mahdollista lisäillä ja poistaa.

3.2 HA eli High Availability

HA, High Availability eli tässä tapauksessa palomuurien kahdennus, varmistaa toimistoverkon yhteyksien toiminnan. Toimistolla lähes kaikkeen toimintaan tarvitaan yhteyksiä internettiin ja jos yhteys syystä tai toisesta katkeaisi, seisoisivat työt sen aikaa tekemättöminä. Siksipä toimistoverkossa on käytössä palomuurien kahdennus. HA on tärkeä osa ympäristöä, jolla halutaan olevan korkea vikasietoisuus. ICT Elmon tapauksessa toimistoverkko kestää jopa kahden palomuurin ha-

joamisen, ennekuin yhteys olisi kokonaan alhaalla. Oikein konfiguroitu HA pelastaa lähes aina verkon kaatumisen laiterikolta tai mahdolliselta internet-yhteyden katkeamiselta, mikäli molemmat laitteet ovat kytketty eri internet-yhteyden taakse.

Palomuurien kahdennus, eli HA, on helppo pystyttää toimimaan kahden eri FortiGate palomuurin välille. FortiGaten palomuurissa on erikseen HA-valikko, jonka takaa konfiguroidaan laitteiden välinen kahdennus. ICT Elmonkin toimistoverkossa jokaista palomuuria on kaksi, kaksi muuria toimistolla ja kaksi muuria itse laitetilassa. Nämä kaksi toimivat melkein kuin yhtenäisenä laitteena, mutta kuitenkin vain niin, että liikenne liikkuu ainoastaan toisen muurin lävitse. Jos päämuuri vikaantuisi, huomaisi toissijainen muuri tämän ja automaattisesti vaihtaisi liikenteen kulkemaan itsensä kautta.



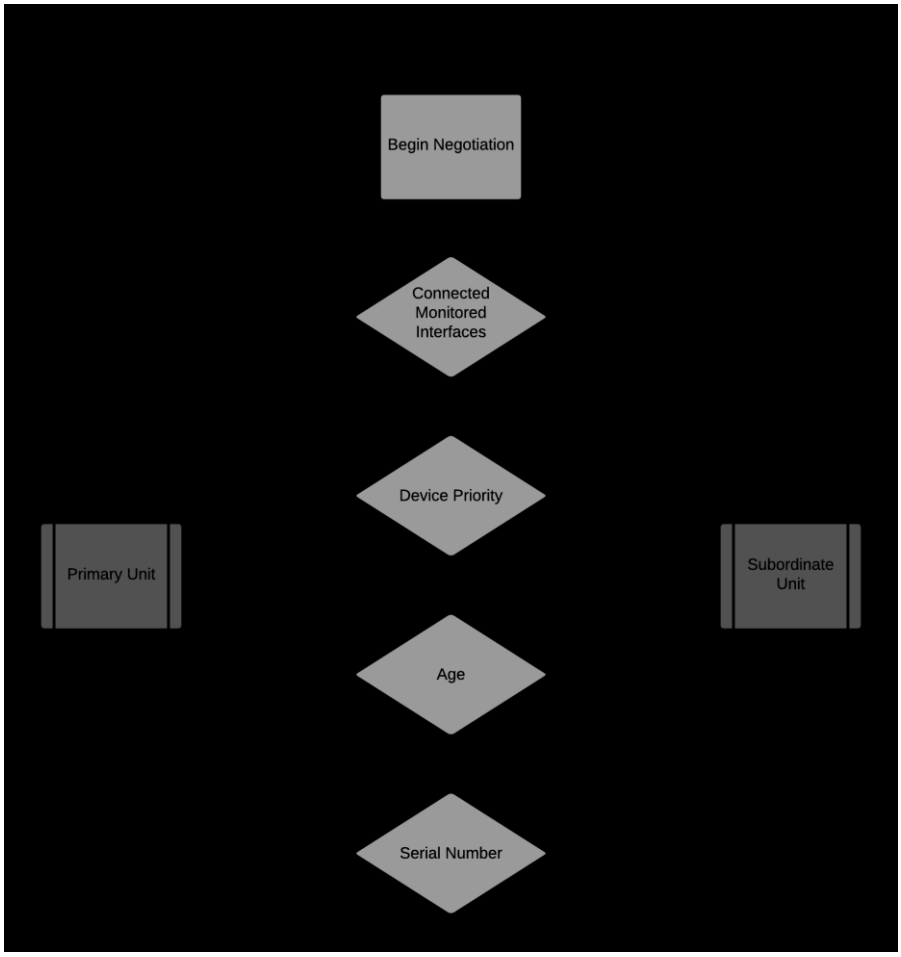
KUVIO 3. HA asetusten valikko (Dickie 2018)

Ennen konfiguroinnin aloittamista tulee varmistaa, että HA-pariin kuuluvat palomuurit ovat samalla päivitystasolla ja hearbeat-liitännät eivät jaa DHCP-osoitteita eivätkä sähköä (Fortinet_h, High availability with two FortiGates. n.d.).

Kun High Availabilityä lähdetään konfiguroimaan aukeaa Ha valikosta ylläolevan näköistä valikkoa. Valikossa asetetaan laitteelle haluttu HA host name, tämän ei tarvitse olla sama kuin laitteen host name, jokin kuvaava nimi on kuitenkin hyvä, sillä laitteen HA host name tulee näkyviin HA-sivulle sen jälkeen, kun HA-konfigurointi on valmis.

Mode on laitteiden väliset asetukset, tässä on kaksi vaihtoehtoa. Mode voi olla Active-Active, jolloin muurit tekevät samalla myös kuormanjakoa, tällöin yksi muuri omaksuu primaariroolin ja jakaa liikennettä eteenpäin muille muureille itsensä mukana lukien. Active-Active on edellä mainitusta syystä raskaampi laitteelle kuin Active-Passive mode ja kuormittaa palomuurin muistia sekä prosessoria (Fortinet_f Active-passive and active-active. n.d.). Active-Passivea käytettiin ICT Elmon toimistoverkossa. Kyseisessä Active-Passive valinnassa määritellään konfiguroinnin yhteydessä, kumpi laitteista on primaari- ja kumpi toissijainen laite. Active-Passive parissa vain aktiivinen laite hoitaa palomuurin tehtäviä. Laiteparin IP-osoite ja MAC-osoite on aina primäärilaitteen hallussa. Mikäli parissa vaihtuu primäärilaite, siirtyy myös IP ja MAC-osoite uudelle laitteelle (Fortinet_b, About active-passive failover. n.d.). Laite, jonka Device Priority on korkeampi, valitaan ensimmäiseksi primaari palomuuriksi. Tämä ei kuitenkaan tarkoita sitä, että aina kun laitteet aloittavat neuvottelut uudesta primaarilaitteesta, laite jolla on suurempi Device Priority, tulisi automaattisesti primaariksi.

FortiGatet valitsevat seuraavan primaarilaitteen kuvion 4 ketjun mukaisesti. Jos monitoroituja portteja ei ole, FortiGatet valitsevat laitteen sen iän perusteella, vanhimmasta palomuurista tulee uusi primaarilaite. Ikä nollaantuu, kun laite sammutetaan, mutta myös silloin kun laitteen monitoroidun portin yhteys katkeaa tai kun se on irrotettu. Tämä voi aiheuttaa ongelmia silloin kun varamuuriksi haluttu palomuuri ottaakin itselleen primaarilaitteen tittelin esimerkiksi silloin, kun päämuuri on jouduttu käynnistämään uudelleen. Tilanteen voi korjata komennolla *diagnose sys ha reset-uptime*, komento resetoi laitteen iän, jolloin kyseisestä laitteesta pitäisi muuttua uusi primaari.



KUVIO 4. Uuden primaarilaitteen valintapolku (Fortinet_c, HA override n.d.).

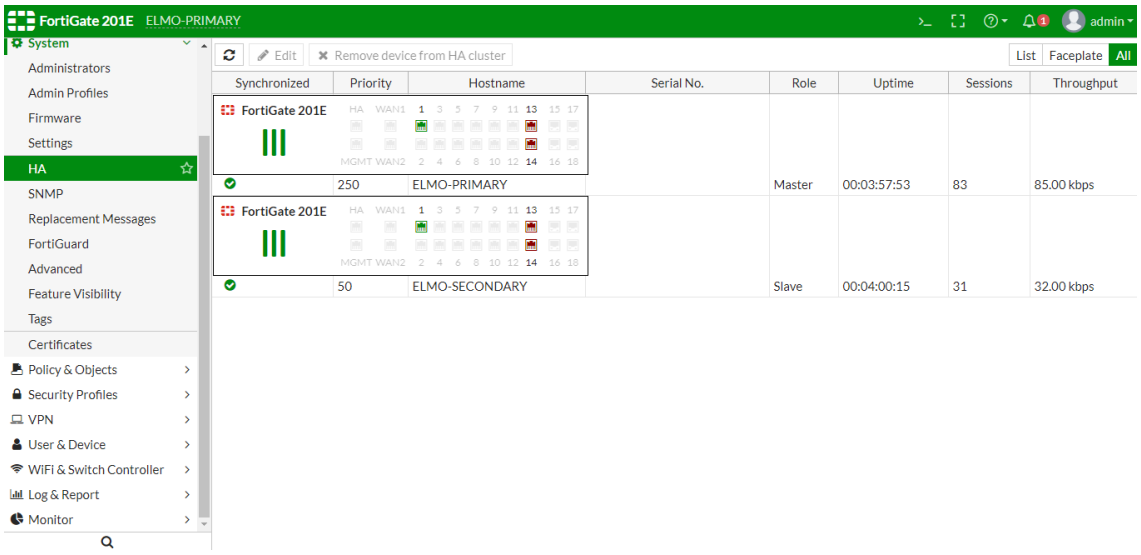
Diagnose sys ha reset-uptime komennolla päästään myös testaamaan ja tarkistamaan toista muuria. Kun muurien välinen HA on määritetty, pääsee käyttäjä katsomaan vain ja ainoastaan nykyistä primaarilaitetta. Tiedot kyllä tallentuvat molemmille laitteille ja laitteet synkronoivat toistensa kanssa tietyn väliajoin, mutta jos jotain asetuksia halutaan laittaa vain toiselle muurille, esimerkiksi uniikit nimet, täytyy konfiguroijan ottaa joko suoraan johdolla yhteys toissijaiseen muuriin tai käyttää yllämainittua komentoa, jolloin toissijainen palomuuri ylennetään primaarilaitteeksi.

Cluster Settings osiosta määritellään HA-ryhmälle nimi sekä salasana, näiden täytyy täsmätä vastapuolella olevan muurin asetusten kanssa. Monitor interfaces kohtaan voi valita listasta portin, jota laite kuuntelee siltä varalta, että tästä portista yhteys katkeaa. Jos palomuureja käytetään myös kahden eri yhteyden varmistuksessa niin, että molempiin muureihin tulee oma erillinen yhteys internettiin,

on monitored interface kohtaan laitettava laitteen internet-yhteyden portti. Muuten laite ei tiedä internetyhteyden katkenneen ja jatkaa toimintaansa päämuurina.

Heartbeat portit vahtivat HA-parin toimintaa ja pitävät laitteet synkronoituna, eli ne jakavat samat asetukset toisilleen mitkä ovat määritelty sen hetken primaarilaitteessa. ICT Elmon tilanteessa on käytetty Fortinetin suosittelemaa kahta porttia seuraamaan laitteiden HA-tilannetta. Yhtä porttia käyttäessä olisi vaara, että heartbeat portti ei toimisi oikein ja aiheuttaisi molempien laitteiden siirtymisen primaarilaitteeksi ja näin ollen hajottaisi lähiverkkoympäristön. (Fortinet_a, HA heartbeat and communication between cluster units, n.d.)

Kun HA on konfiguroitu toimivaksi, pitäisi HA-valikosta avautua näkymä missä molemmat laitteet sekä niiden tiedot näkyvät. Kuviossa 5 on esimerkki Elmon toimistoverkon HA-näkymästä. Kuviossa ollaan kiinni laitteessa ELMO-PRIMARY, joka on myös HA:ssa Master, eli primaarilaite. Tiedoissa näkyy myös molemmille laitteille määritelty Priority, niiden rooli eli onko laite primaari vai ei sekä Uptime ja muita monitorointitietoja. Laitteiden kuvista näkee myös sen, että Heartbeat portit ovat 13 sekä 14, ja että portissa yksi on kiinni jotain. Näihin laitteisiin ei ole vielä määritelty monitoroituja uplink-portteja. Uplink-porttina puhutaan yleensä portista, joka on yhteydessä suurempaan verkkoon, tässä tapauksessa internettiin. (Naidu, 8.10.2011.)



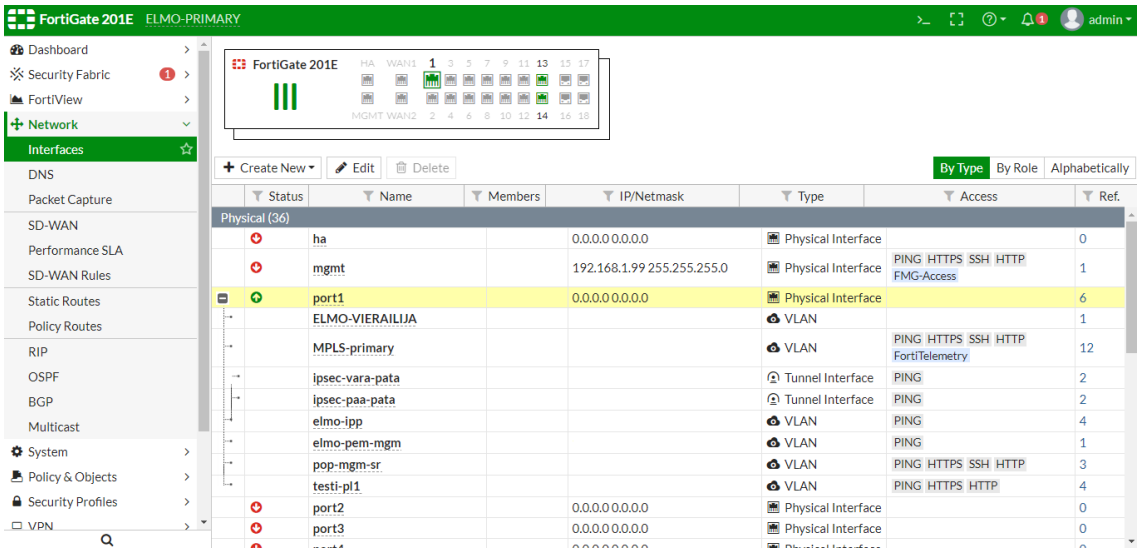
KUVIO 5. HA-valikko konfiguroinnin jälkeen

3.3 Interfacet ja niiden konfiguroiminen

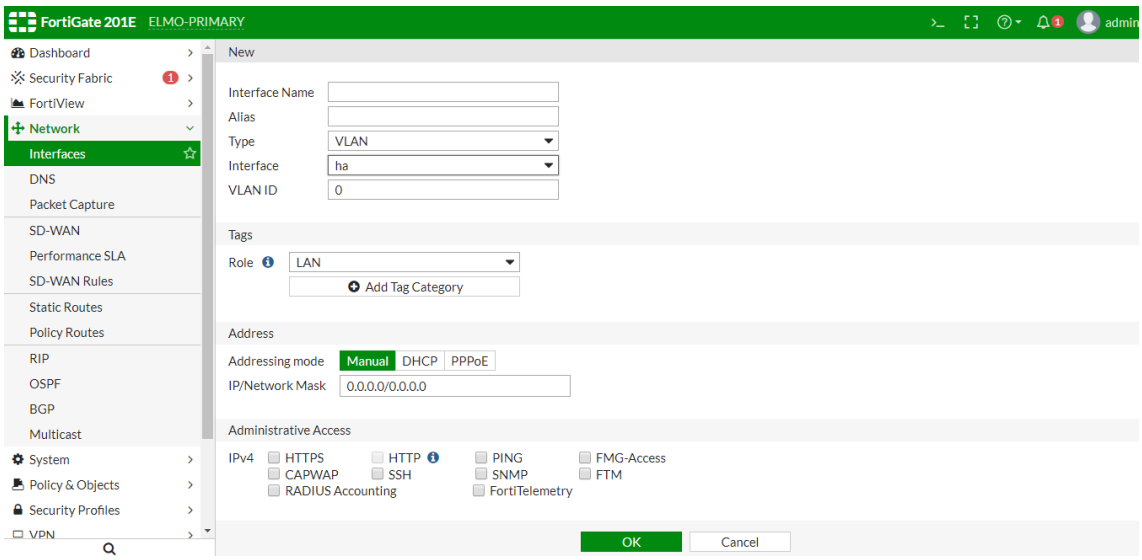
Interfacet, eli laitteen portit ja liitännät, määrittä minkä kautta yhteys kulkee palomuurilta eteenpäin. Interface etusivulta näkee nopeasti mitkä portit ovat käytössä FortiGaten profiilikuvasta sekä luettelosta, jossa on listattu niin fyysiset kuin virtuaaliset liitännät. Fyysisten porttien virtuaaliliitännät saa auki painamalla plussaa kyseisen portin vieressä. Porttien Type kohdassa näkyy, minkälaisesta portista on kyse, fyysiset portit ovat Physical Interface, VLAN tarkoittaa virtuaalista LAN-verkkoa ja tunneliyhteys on eri toimipisteiden välisten FortiGatejen välinen yhteys, tai vastaavasti jonkun toisen tunnelointiin kykeneväisen laitteen välinen yhteys, missä laitteet juttelevat toiselleen.

Liitännästä saa lisätietoja, kun hiiren vie haluamansa liitännän päälle ja odottaa hetkisen, paremmin tiedot saa kuitenkin, kun aktivoi haluamansa liitännän niin että sen tausta muuttuu keltaiseksi ja painamalla edit yläpalkista. Tämän jälkeen pääsee käyttäjä muokkaamaan haluamaansa kohtaa.

Kuten kuviosta 6 näkyy, joskus pelkät fyysiset portit eivät riitä, vaan portin alle on luotava virtuaalinen liitäntä. Virtuaalinen liitäntä toimii kuten fyysinen, mutta jakaa paikkansa muiden virtuaalisten liitäntöjen kanssa fyysisen portin alla. Tämä ei kuitenkaan tarkoita sitä, että kaikki liikenne joka fyysiseen porttiin tulee, menisi automaattisesti kaikkiin sen alla oleviin virtuaalisiin portteihin. Liikenteen näiden liitäntöjen välillä määrää VLAN.



KUVIO 6. Interface etusivu



KUVIO 7. Uuden liitännän luominen

Mikäli halutaan luoda uusi virtuaalinen liitäntä tulee painaa Create New ja käyttäjä pääsee valikkoon, jossa määritellään liitännän ominaisuudet. Valinnoista ensimmäisiä ovat Interface name, jossa määritellään uudelle liitännälle nimi, ja Type, jossa valitaan minkälainen liitäntä on kyseessä. Interface kohta on tärkeä saada oikein VLAN ID kanssa. Interface laatikossa valitaan minkä fyysisen portin alle uusi liitäntä luodaan. VLAN ID kertoo mitä VLAN:ia kyseinen liitäntä kuuntelee. Uusi liitäntä, jossa fyysinen portti tai VLAN ID ei täsmää, ei koskaan saa oikeita tietoja ja näin ollen ei toimi tai ei ole ollenkaan kytkettynä, mikäli esimerkiksi portti 1 on kytketty mutta uusi liitäntä olikin konfiguroitu portti 2 alle. Uutta liitäntää luodessa on hyvä muistaa, että luomisen jälkeen VLAN ID:tä ei pysty enää muokkaamaan, vaan koko portti on luotava uudelleen tavalla tai toisella. Ainoa järkevä ratkaisu tuotantoympäristössä on ottaa laitteesta backup konfiguraatio, käydä muuttamassa tekstieditorissa vanha VLAN uudeksi ja ajamalla tämä uusi konfiguraatio takaisin laitteeseen, joka taas käynnistää itsensä uudella konfiguraatiolla. Tästä aiheutuu se, että tuotannossa oleva laite käy alhaalla ja aiheuttaa näin katkon yhteyteen.

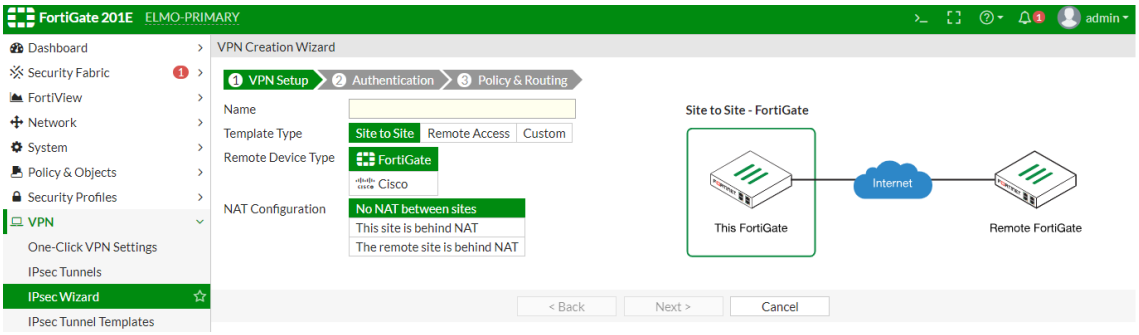
Tag kohta ei ole liitännän toiminnan kannalta tärkeä kohta, mutta jos käyttäjä haluaa erikseen merkata minkä tyyppinen liitäntä on kyseessä voi hän sen tähän valita. Tässä kohtaa ei saa siis mitään pilalle, vaikka kirjoittaisi jotain aivan muuta kuin mitä liitäntä oikeasti on.

Address osiossa määritellään liitännälle IP-osoite. Jos tästä liitännästä on haluttu tehdä esimerkiksi sisäverkkoon vierailijaverkkoa, tulee tähän silloin sisäverkon osoite, esimerkiksi 192.168.1.1 ja haluttu maski minkä kokoista verkkoa ollaan tekemässä. Kahta samaa osoitetta ei voi kuitenkaan olla liitännöillä ja se on otettava huomioon, mikäli halutaan tehdä monta eri sisäverkon liitäntää. Kuviosta 7 ei näy, mutta samaisessa valikossa pystytään helposti asettamaan DHCP-pooli kyseisen liitännän käyttöön. Fortigate on tässä suhteessa helppokäyttöinen, ettei käyttäjän tarvitse alkaa itse rakentamaan DHCP:tä toimintaan ja varaamaan sille osoiteavaruuksia. Valikossa on nappi, jota painamalla saa käyttöönsä suoraan DHCP:n kyseisen liitännän alle. Fortigate automaattisesti asettaa DHCP-poolin sen mukaan minkä IP-osoitteen on antanut kyseiselle liitännälle, tässä poolissa käytössä ovat kaikki seuraavat osoitteet mitkä maskin puolesta ovat saatavilla. Näitä osoiteavaruuksia voi käyttäjä halutessaan jälkikäteen vaihdella, jos verkko sitä vaatii. Toinen vaihtoehto on erillinen DHCP-palvelin, jonne liitännän käyttäjät pitää ohjata. DHCP-asetusten advanced kohdasta löytyy vaihtoehto relay, joka toimii samalla tapaa kuin Ciscon ip-helpper, eli tähän kohtaan laitetaan DHCP-palvelimen IP-osoite, joka jakaa käyttäjille IP-osoitteet. Kun ulkopuolinen DHCP-palvelin on käytössä, ei tarvitse konfiguroida erikseen palomuurille DHCP-avaruutta.

Administrative Access tarkoittaa sitä mitkä protokollat sallitaan verkosta palomuurilaitteelle. Jos tähän sallitaan https, pääsee kyseisen verkon käyttäjät nettiselaimellaan kiinni palomuuriin sen liitännän oletusyhdyskäytävän osoitteella. Tämä kohta ei siis mitenkään toimi palomuurisääntönä, eikä säätele minkälaista liikennettä sallitaan ulos tai sisään tästä liitännästä. Liikenne ulos tästä verkosta sallitaan myöhemmin palomuurisäännöillä. Sisäverkon osoitteisiin olisi hyvä jättää ainakin PING päälle ongelmanratkaisua varten. Myös erilaiset palvelut sisäverkossa saattavat vaatia eri oikeuksia, esimerkiksi Fortinetin FortiAP tukiasemat vaativat, että portissa on sallittuna CAPWAP. Jos FortiGatea halutaan hallita keskitetysti FortiManagerin kautta, on silloin uplink-porttiin sallittava FMG-access, joka tarkoittaa FortiManagerin ja FortiGaten välistä liikennettä. Huomioitavaa protokollien valinnoissa on se, että käyttäjä voi vahingossa kieltää oman pääsynsä laitteen graafiseen hallintaan, jos hän ottaa https/http valinnan pois portista, johon on kytkeytyneenä. Kun hallinta graafiselle puolelle katkeaa, voidaan konsoliyhteydellä konfiguroida takaisin sallitut protokollat.

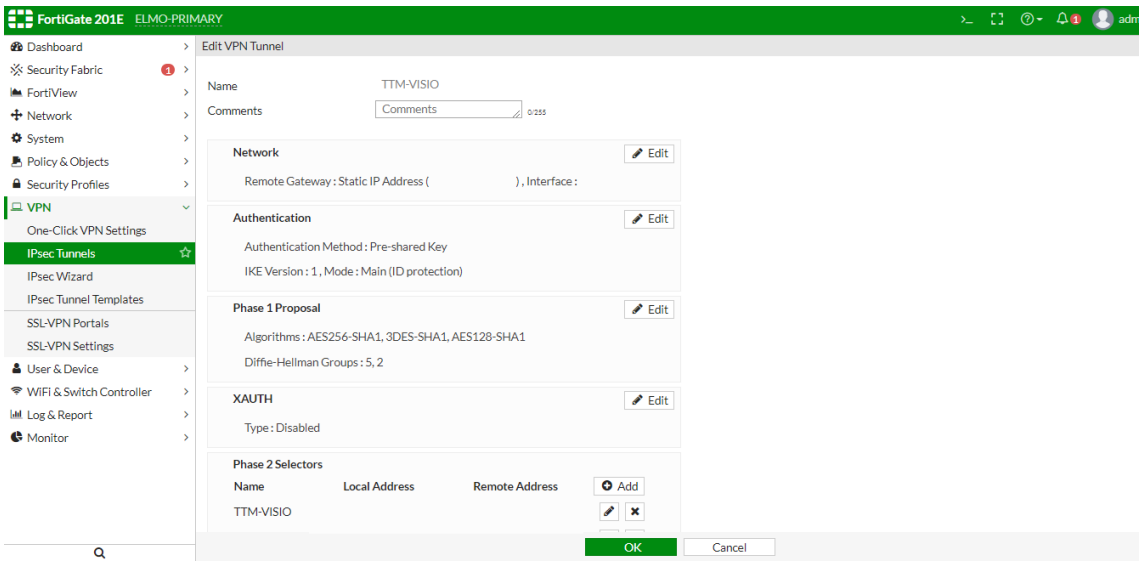
3.4 Tunnelointi

VPN tunnel eli Virtual Private Network tunneli voidaan tehdä kahden eri toimipisteen välille. Tämän ollessa konfiguroitu pystyvät eri verkot keskustelemaan keskenään, vaikka toimipisteiden välillä liikenne kulkisikin internetin kautta eikä laitteita ole kytketty toisiinsa fyysisesti. Kaksi erillistä toimipistettä toimivat siis virtuaalisesti yhtenä verkkona. Verkkojen ollessa näin konfiguroituna, pääsee toisesta verkosta toiseen verkkoon, vaikka katsomaan verkkolevyjä ilman, että toisen toimipisteen työntekijän pitäisi ottaa itse VPN-yhteys siihen verkkoon, jonne verkkolevy on konfiguroitu.



KUVIO 8. Tunneli wizard

Uuden VPN-tunnelin pystyy rakentamaan joko suoraan IPsec Wizardin kautta tai valitsemalla create new IPsec Tunnel välilehdeltä, molemmat avaavat kuitenkin samanlaisen VPN Creation Wizardin. Valintoja tässä on kaksi tavalliselle site-to-site tunnelille, voit antaa FortiGaten huolehtia tunnelin luomisesta tai voit tehdä sen kokonaan itse. Suosittelen käyttämään Custom toimintoa, muuten FortiGate luo kourallisen sääntöjä ja objekteja tunnelia varten, joita ei oikeastaan edes tarvitse, eikä custom tunneli ole liian vaikea toteuttaa.

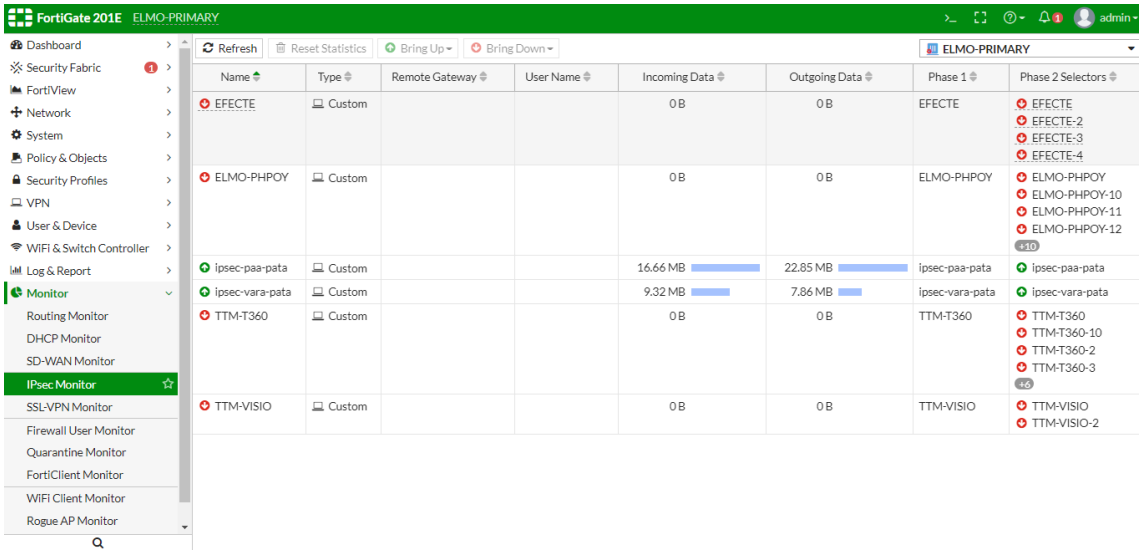


KUVIO 9. Valmiin tunnelin tarkastelu

Jotta tunneli pystytään luomaan kahden pisteen välille, tarvitsee molempien puolien olla samanlaiset. Tämä tarkoittaa siis sitä, että pre-shared key, tunnelin päiden osoitteet, suojaus ja jaetut verkot täsmäävät toisessa päässä vastinkappaleeseen. Kun tunnelia lähdetään luomaan, ensimmäisenä pitää määrittää kehenkä ollaan yhteydessä, eli kohtaan Remote Gateway tulee vastapään laitteelle konfiguroitu IP-osoite, sekä määritetään minkä liitännän takaa tämä löytyy. Malliesimerkkikuvista on tietoturvasyistä poistettu kaikki IP-osoitteet näkyvistä. Authenticationissa olevan pre-shared key täytyy olla sama kuin vastapäässä sekä IKE versio, joita on valittavana version 1 sekä version 2. Phase 1 kohdassa valitaan haluttu salaus, palomuuri tarjoaa tähän valmiiksi monta erilaista vaihtoehtoa, joita voi muokata tai halutessaan tehdä kokonaan uuden. Salauksen on täsmättävä toisen pään laitteen salauksiin. Phase 2 määritellään mainostetut verkot, local address, eli paikallinen osoite, on kyseiseltä palomuurilta toiselle laitteelle mainostettavat verkot ja Remote Address, eli vastapään osoitteet, ovat toiselta laitteelta mainostettavia verkkoja, näiden verkkojen pitää täsmätä molemmissa päissä tai tunneli ei toimi. Phase 2 kohtassa tulee myös määrittää salaus kyseiselle vaiheelle, tämä onnistuu samalla lailla kuin Phase 1 eli käyttäjä voi itse valita valmiista tai muokata haluamansa salauksen (Fortinet_e, Configuring IPsec VPN on HQ. n.d.).

Kun tunneli on luotu, tulee se näkyviin monitorointisivulle IPsec Monitor välilehden alle. Kuviosta 10 nähdään että tunnelit ipsec-vara-pata ja ipsec-paa-pata

ovat ylhäällä ja niissä on myös tulevaa sekä lähtevää liikennettä, kaikki muut tunnelit ovat alhaalla eikä niissä ole liikennettä.



KUVIO 10. VPN-tunnelien valvonta

Koska graafiselta puolelta ei saa selvää miksi tunnelit eivät ole ylhäällä, on vianselvitys tehtävä komentokehotteen kautta debug-komennoilla. Itse olen törmännyt enimmäkseen ongelmiin, joissa tunnelien päiden asetukset eivät kohtaa ja tämän takia tunnelit eivät nouse ylös. Fortinet on julkaissut omilla sivuillaan vianselvitykseen käytettäviä komentoja, joilla tunnelien yhdenvertaisuutta voidaan tarkastella (Fortinet_d, Troubleshooting IPsec VPNs, n.d.).

#diagnose vpn ike log-filter dst-addr4 xxx.xxx.xxxx.xxxx <- tunnelin kohde
#diagnose debug application ike -1
#diagnose debug enable

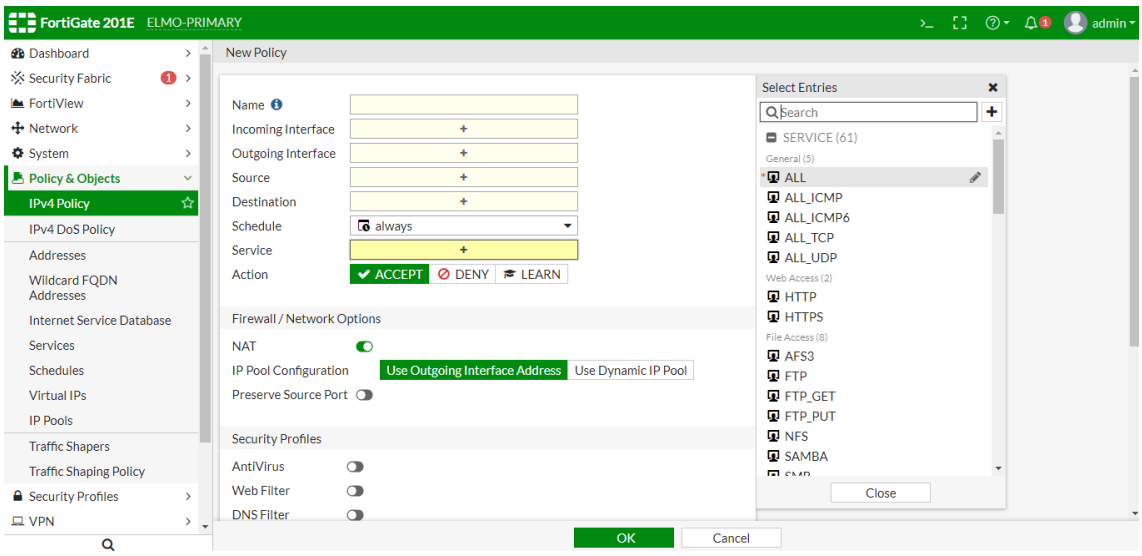
Kun komento laitetaan päälle, alkaa palomuuri tuottamaan tekstiä tunnelin kättelyn eri vaiheista. Jos tänne ei ilmesty minkäänlaista tekstiä, on jokin tunnelissa todella vialla. Debug antaa suuntaa mistäpäin ongelmaa voisi lähteä ratkaisemaan, jos Phase 1 pystytään kättelemään, on vika silloin Phase 2:ssa. Jos teksti ilmoittaa, että tunnelin jaettu avain ei ole yhteensopiva, on silloin jommankumman laitteen tunnelin salasana kirjoitettu väärin. Fortinet mainitseekin yleisimmäksi syylliseksi tunnelin toimimattomuuteen väärin konfiguroidut tunnelien päät, joiden asetukset eivät täsmää toisiinsa (Fortinet_g, IPsec VPN troubleshooting, n.d.).

3.5 Palomuurisäännöt

Palomuurisäännöt ovat ohjeita palomuurille kuinka sen pitää reagoida liikenteeseen. Aina kun palomuuri kohtaa liikennettä se vertaa sitä sen sääntölistaan. Jos palomuuri löytää liikenteelle vastaavan säännön, laite toimii sen mukaan. Sääntöjä palomuurille voi olla liikenteen kieltäminen, salliminen, tietyn toiminnon tekeminen, jos liikenne osuu sääntöön, tai vaikkapa liikenteen tarkastelu. Ilman palomuurisääntöjä, palomuurista ei olisi juurikaan hyötyä.
Jotta käyttäjät pääsisivät ulos palomuurin sisäverkosta, tulee liikenne sallia erillisillä palomuurisäännöillä. Oletuksena kaikki liikenne on kiellettyä, joten sisäverkolle on tehtävä ensin sääntö, että siitä pääsee ulos. Kaikki mikä ei ole erikseen sallittua muurilta on automaattisesti kielletty. Tämä siis tarkoittaa sitä, että jos muurilta haluaa verkkoon enemmän kuin yksi sisäverkko, on jokainen näistä käytävä erikseen siellä sallimassa, vaikka yhteydet tulisivat saman fyysisen portin kautta.

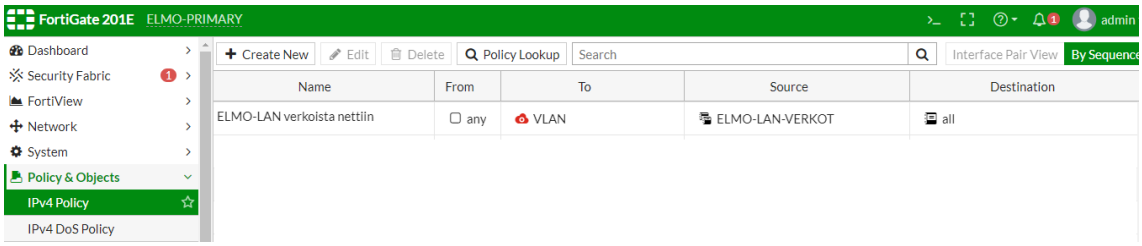
Kun uutta palomuurisääntö aletaan luomaan, tulee käyttäjän navigoida itsensä ensin Policy & Objects alta löytyvään IPv4 Policy välilehden alle. Kyseiseltä välilehdeltä löytyy heti yksi sääntö, joka estää kaiken liikenteen kaikkialle ja kaiken aikaa. Se on viimeinen palomuurisääntö, Policy 0 Implicit Deny, eli jos mihinkään aikaisempaan sääntöön ei ole osunut liikennettä tulee tämä voimaan ja estää liikenteen. Tähän ei tarvitse käyttäjän koskea. Käyttäjän on luotava uusia sääntöjä 0 Policyn rinnalle, että liikenne toimii.

Uusi sääntö luodaan samalta sivulta painamalla Create New, josta avautuu kuvion 11 näköinen valikko. Name, eli säännön nimi, on hyvä olla kuvaava, ettei jälkikäteen tarvitse metsästellä säännön tiedoista mikä sääntö on mahdollisesti kyseessä. Incoming ja outcoming interface kohtaan tulee kirjaimellisesti muurille liikenteen sisääntuleva ja ulostuleva liitäntä. Näihin valintoihin pystyy oletuksena laittamaan vain yhden portin, mutta asetuksen pystyy muuttamaan sallimaan useamman portin System valikon Feature Visibility välilehdestä.



KUVIO 11. Uuden palomuurisäännön luominen

Kuviossa 12 näkyy valmiiksi luotu palomuurisääntö, jossa määritellään ICT Elmon toimistoverkon pääsy internettiin. Säännössä näkyy, että liikenne kaikista liitännöistä on sallittu VLAN:iin, joka tässä yhteydessä kuvaa uplink-porttia, lähdeosoitteeksi on valittu vain toimistoverkon IP-osoitteet ja kohdeosoitteeksi kaikki muut osoitteet. Lähdeosoite voitaisiin jättää sallimaan kaikki osoitteet, mutta toteutuksessa on määritelty jokaiselle eri verkolle oma pääsy internettiin oman liitäntänsä kautta. Pienemmissä palomuuritoteutuksissa riittäisi, että liikenne sallittaisiin kaikista sisäverkon porteista ja osoitteista kaikkialle ulkoverkkoon.



KUVIO 12. Valmiit säännöt näkyvät IPv4 Policy välilehdellä

FortiGatessa kaikkia palomuurisääntöjä voi tarkastella välilehdeltä IPv4 Policy. Palomuuri lukee sääntöjä listasta ylhäältä alaspäin ja lopettaa sääntöjen lukemisen heti kun osuu ensimmäiseen sääntöön, joka koskee sen kohtaamaa liikennettä. Tästä voi ilmetä ongelmia, jos liikennettä sekä sallitaan ja kielletään samaan verkkoon, silloin konfiguroijan tulee löytää säännöille oikea paikka, jotta ne luetaan oikeassa järjestyksessä. Sääntöjen paikkaa voidaan vaihtaa listalla raa-

haamalla haluamansa sääntö oikealle paikalle, tai uutta sääntöä lisättäessä klikata oikealla hiirennäppäimellä haluttua paikkaa ja valitsemalla Insert Below tai Insert Above riippuen siitä halutaanko uusi sääntö klikatun säännön ala- vai yläpuolelle. Fortigate palomuuri tallentaa muutokset automaattisesti ja ottaa ne heti käyttöön, joten sääntöjen liikuttelussa tulee olla varovainen.

4 TOIMISTOVERKON UUDISTAMINEN

ICT Elmon toimistoverkko haluttiin uudistaa osaksi sen iän takia, mutta osaksi myös siksi että haluttiin tehdä ympäristö, joita myös myydään asiakkaille. Tämän takia laitteiksi toimistoverkkoon valikoitui Fortinetin tuotteet, FortiGate palomuurit, FortiSwitch kytkimet ja FortiAP langattoman verkon tukiasemat. Yhteydet toimistolle tulevat valokuidulla, joten palomuurien eteen asennettiin ZTE-kuitukytkimet, joista saatiin vedettyä Ethernet-kaapelilla yhteydet FortiGateihin.

4.1 Lähtötiedot

Vanha toimistoverkko toimi Ciscon palomuurin päällä, tämä tarkoitti myös sitä, että ennen uudistusta etätyöskentelijät ottivat yhteyden toimistoverkkoon Ciscon AnyConnect VPN kautta. Muutoksen myötä VPN-sovellus vaihtui Fortinetin omaan FortiClientiin. Toimistoverkon kytkimet olivat Extremen valmistamia, joita on edelleen toimistolla käytössä, tosin tällä kertaa toimistoverkon ulkopuolella. Langattomat tukiasemat olivat Ruckuksen valmistamia, mutta muuttuneiden työtilojen myötä ne eivät välttämättä olleet optimaalisesti sijoiteltu. Langaton yhteys myös pätki välillä eripuolilla toimistoa.

4.2 Laitteet

ICT Elmolle tilattiin vanhojen laitteiden tilalle 2 kappaletta FortiGate 81 ja 2 kappaletta FortiGate 200E. FortiGate 81 pari tuli käyttöön Patamäenkadun toimistotiloihin, eli näiden laitteiden läpi kulkee kaikki toimistolta lähtevä ja tuleva liikenne. Näistä suurimpien palomuurien, eli FortiGate 200E, läpi kulkee kaikki liikenne sisäverkosta internettiin. Muut sisäverkkoon tarvittavat tuotteet, eli FortiAP langattoman verkon tukiasemat ja FortiSwitch kytkimet tulivat kiinni toimistolla oleviin palomuureihin. Tukiasemia ja kytkimiä myös hallitaan palomuurien kautta.

4.3 Konfiguroiminen

Laitteiden konfiguroiminen tapahtui ICT Elmolla etukäteen sovittuina päivinä sovittujen henkilöiden kanssa. Konfigurointipäivät täytyi sovittaa kahden ICT Elmon

työntekijän aikataulujen kanssa sopiviksi, sillä he vastasivat projektin onnistumisesta.

Konfigurointipäivinä keskityttiin yleensä vain yhteen osa-alueeseen palomuurissa. Koska verkon piti olla suurimmalta osin täysin identtinen vanhan verkon kanssa, kuului konfiguroimiseen mukaan paljon vanhan verkon tutkiskelua ja siirtoa uusille laitteille. Koska FortiGaten ja Ciscon konfiguraatiot eivät mene yksi yhteen, joutui jokaisen asetuksen käymään asettamassa erikseen päälle ja antamassa sille oikeat parametrit. Konfiguroidessa laitteita ei harmillisesti pystynyt käyttämään suoraan hyväkseen valmiita konfiguraatioita mitä olisi saanut Ciscosta tulostettua, sillä vaikka molemmat ovat palomuureja ne toimivat eri käyttöjärjestelmän päällä. Fortinet on kehitellyt oman käyttöjärjestelmän FortiOS, jota heidän tuotteensa käyttävät ja jota Fortinet ahkerasti päivittää. Tämä eri käyttöjärjestelmästä johtuva pakollinen käsin tehtävä kopioiminen oli omalta osaltaan hieman puuduttavaa, varsinkin palomuurisääntöjen kanssa, joita laitteelta löytyi muutama. Hyvää kuitenkin oli se että, samalla tuli käytyä läpi kaikki vanhat palomuurisäännöt ja tarkistamaan onko jokin niistä mahdollisesti turha ja jota ei tarvitse tuoda enää uuteen toimistoverkkoon. Fortinet on myös kehitellyt FortiConverter ohjelman, jolla pystyisi kääntämään suosituimmista palomuurimalleista konfiguraatiot sopimaan Fortigatelle, mutta konfiguraatio ei aina mene aivan yksi yhteen ja tämän tarkistamiseen menee myös kauan aikaa.

Konfigurointi aloitettiin sillä, että jokaiseen muuriin ja kytkimeen mentiin asettamaan niille kuuluva Host Name, eli laitteen nimi, IP-osoitteet ja reitit. Tämän jälkeen jokainen langaton tukiasema käytettiin kiinni toimistolle tulevissa palomuureissa. Koska Fortinet on panostanut turvallisuuteen, ei yksikään tukiasema pääse nousemaan aktiiviseksi ennen kuin se käydään hyväksymässä palomuurilta. Managed FortiAPs välilehdelle ilmestyy uusi tunnistettu tukiasema omalla sarjanumerollaan, käyttäjän tulee hyväksyä uusi laite valitsemalla se aktiiviseksi listasta, painamalla Authorize sekä valita mitä asetuksia uusi tukiasema käyttää. Tämän jälkeen, vaikka laitteet kytketään johonkin muuhun porttiin kuin mistä ne hyväksyttiin, pitäisi tukiasemien nousta heti toimintaan eikä lisäkonfiguraatioita tarvita.

Eniten konfigurointia vaativat 200E palomuurit, jotka tulivat erilliseen laitetilaan. Nämä laitteet käsittelevät kaiken internet liikenteen, hallitsevat reitityksen ja VPN-yhteyksien luomisen sekä hoitavat palomuuriavaukset ulko- ja sisäverkkoon.

Hoidin laitteiden konfiguroinnin lähes yksin. Konfiguraatioista oli suurin osa jo valmiiksi suunniteltu ICT Elmon työntekijöiden puolesta tai valmiina esimerkkeinä vanhoissa Cisco ASA palomuureissa. Suurin osa omista projektin tehtävistäni olikin vanhan kopioimista uuteen, joskus pienillä muutoksilla. Itsenäistä työskentelyä ei projektin osalta ollut, sillä projektia pystyttiin edistämään vain toimistolla, ja vain projektiin kuuluvien työntekijöiden läsnä ollessa.

4.4 Yliheitto ja testaus

Yliheitto, eli toimistoverkon siirto uudelle yhteydelle, tehtiin toimiston työaikojen ulkopuolella, jotta se ei häiritsisi työskentelyä. Yliheitossa koko vanha toimistoverkko oli purettava, tämä tarkoitti myös kaikkien vanhojen johtojen poistoa, jotta uudet kytkimet saadaan vanhojen tilalle. Yliheitossa suurin osa ajasta meni fyysiseen työhön, ensin nyppiessä vanhat johdot pois ja uusien laitteiden myötä uusien johtojen laittamisissa oikeisiin portteihin. Vasta kun kaikki uudet laitteet ja johdot olivat paikoillaan pääsi ympäristöä testaamaan.

Testaus oli hyvin yksinkertainen, mikäli liikenne kulkee ulos, yhteys on kunnossa. Tätä testattiin toimistoverkossa olevien työasemien kautta sekä langattoman lähiverkon kautta. Täytyi myös varmistaa, että koneilla oli yhteys etäpalvelimeen ja että toimiston puhelinjärjestelmä toimi. Tätä testattiin avaamalla tiedostoja etäpalvelimelta sekä soittamalla puheluita ulos että sisäänpäin. Ainoastaan puhelinjärjestelmässä huomattiin vikaa.

Testauksessa piti olla myös mukana uusi VPN-yhteys, sillä seuraavana päivänä kun toimisto olisi auki tarvitsisi etätyöntekijät yhteyden toimistolle. VPN testauksessa ei tullut uusia ongelmia. VPN on toiminut muutamaa poikkeustilannetta lukuun ottamatta hyvin toimistolla.

5 ONGELMAT PROJEKTISSA

Vaikka projekti oli laaja ja jokseenkin monimutkainen, suuremmilta ongelmilta vältyttiin. Koska uusi toimistoverkko rakennettiin aluksi rinnakkain vanhan toimistoverkon kanssa, ei virheet konfiguraatiossa aiheuttanut katkoja yhteydessä. Tämä oli tietysti hyvä päätös, sillä toimistoverkkoa rakennettiin arkipäivisin työajan puitteissa ja ainoastaan yliheitot vanhasta verkosta uuteen verkkoon tehtiin toimistoajan ulkopuolella illalla tai viikonloppuna.

Ainoat varsinaiset ongelmat tulivat BGP-reitityksen reittivalinnan kanssa. Toimistoverkon palomuurien sekä laitetilassa olevien palomuurien välissä oleva yhteys oli kahdennettu kahdella eri kuitureitillä, joista toista priorisoitiin liikenteessä. Yliheitossa testasimme, kuinka verkkoliikenne kääntyy toiselle reitille, kun pääyhteys on poikki. Liikenne vaihtui, kuten pitikin, varayhteydelle pääyhteyden mentyä poikki, mutta kun pääyhteys oli avattu uudestaan ei verkkoliikenne suostunut palaamaan pääreitille, vaan liikenne jatkui varayhteyden kautta.

BGP-ongelma tuli vastaan ensimmäisessä yliheitossa, joka järjestettiin illalla. Vaikka palomuurien välisen BPG- reitityksen konfiguraatioihin tehtiin muutoksia ja testauksia tämän illan, ei sitä saatu toimimaan toivotulla tavalla, vaan reitti pysyi aina varayhteyden päällä. Ongelmaan ratkaisu löydettiin muokkaamalla reitityksen arvoja. Molemmissa yhteyksissä, niin vara- kuin pääyhteydessä, oli sama Local Preference arvo, jolloin reitti ei osannut valita parempaa reittiä, sillä molemmat reitit olivat samanarvoisia. Ongelman korjaamiseksi pääyhteyden Local Preference arvoa nostettiin ja varayhteyttä mainostettiin pidemmällä AS Path:lla päämuurille, jonka jälkeen yhteys kääntyi halutusti takaisin pääyhteydelle.

Ongelmaa tuotti myös puheluiden toimiminen. Toimistolla on osalla käytössä puhelinohjelmisto, jolla onnistuu niin sisäiset puhelut kuin ulkoiset puhelut. Yliheiton jälkeen toimistoverkkoon pystyi kyllä soittamaan ja vastaanottaja kuuli ulkoisesta puhelusta kaiken, mutta itse soittaja ei kuullut toimistolla olevasta yhtään mitään. Ongelmaan oli onneksi nopea korjaus, yhden palomuurisäännön poistaminen, jonka jälkeen puhelun molemmat osapuolet kuulivat toisensa. Nämä olivat kuitenkin tärkeitä testata ennakkoon toimistoajan ulkopuolella, sillä muuten esimerkiksi asiakaspalvelussa olisi voinut olla aamulla ongelmia, jos asiakkaat eivät olisi kuulleet asiakaspalvelijasta mitään.

Kun koko toimistoverkko oli saatu valmiiksi ja testaukset tehtyä, tuli yhtenä aamuna täysin odottamaton ongelma. Koko toimistoverkko ja kaikki muut laitteet, jotka olivat kytketty ATK-sähköverkkoon, menivät päälle ja pois useita kertoja peräkkäin. Tämä koski myös palomuureja, kytkimiä ja wlan -tukiasemia toimistolla. Koska satuin olemaan juuri oikealla paikalla oikeaan aikaan, huomasin vian aiheuttaja pian. Aamulla siivooja oli imuroimassa asiakaspalvelun tiloja ja ihmetteli, miksi imuri menee pois päältä vähän väliä. Mainitsi että kyllä aina ennen on pystynyt tilat imuroimaan mutta nyt tapahtuu jotain mitä ei ennen ole tapahtunut. Tämän jälkeen siivooja vaihtoi imurin toiseen pistorasiaan ja laitteiden sammuminen loppui. Siivooja oli siis vahingossa kytkenyt oman imurinsa ATK-pistokkeeseen, joka on tarkoitettu vain ATK-laitteille. Ilmeisesti imuri kuormitti sähköverkkoa juuri sen verran, että se alkoi pätkimään. Onneksi kuitenkaan mitään vauriota ei sisäverkon laitteille tullut nopeasta uudelleen käynnistymisestä ja sammumisesta huolimatta. Tämä ongelma siirrettiin eteenpäin korjattavaksi muille henkilöille.

Projektin päättymisen jälkeen on esiintynyt kaksi ongelma, jossa ensimmäisessä alakerrassa sijaitsevassa toimistotilassa ei toiminut langaton verkko. Yhteys pätki ja saattoi katketa kokonaan hetkeksi. Mitään erikoista ei kuitenkaan yhteydessä huomattu koneilta eikä langattoman verkon kanssa ollut mitään ongelmaa muualla toimistossa, ainoastaan alakerran tietty tila koki pätkimisongelmia. Huomattiin että kyseisen tilan wlan-tukiasema sammui itsestään ilman mitään komentoa. Kyseisen ongelman aiheutti siis rikkinäinen laite, eikä virheet konfiguroinnissa.
Toisessa ongelmassa liikenne ei vaihtunutkaan oikealle palomuurille HA:n kanssa, tämä johtui kuitenkin vain väärin konfiguroiduista monitored HA porteista, jotka eivät osanneet haistella oikeita portteja poikkeustilanteen varalta.

6 POHDINTA

Palomuurinprojektiin osallistuminen oli mielenkiintoinen tehtävä. Projektissa tutustuttiin uudenlaiseen palomuuriympäristöön ja sen toimintaan, sekä samalla saatiin tärkeää tietoa kuinka vastaavanlaisen toteutuksen pystyisi tekemään myös asiakasympäristössä, joka oli yksi haluttu piirre koko projektissa.

Projektissa onnistuttiin hyvin, sillä kaikki konfiguroinnit saatiin tehtyä ajallaan ja ripeään tahtiin, ainoastaan laitteiden hidas toimitus hidasti merkittävästi projektin valmistumista. Projektille oli varattu viikossa ainakin yksi kokonainen työpäivä, jonka aikana oli tarkoitus edistää muuria niin paljon kuin päivän osa-alueelta ehdittiin. Välillä tosin ICT Elmon työntekijöiden muut työt saattoivat keskeyttää projektia, ja projektia oli pakko jatkaa vasta seuraavalla kerralla, tällaisia kertoja oli projektissa muutama. Projektin jälkeen ei tullut mittavia ongelmia, jotka olisivat vaatineet paljon vianselvitys, palomuurilaitteiden vaihtoa tai pahimmassa tapauksessa paluuta vanhoihin laitteisiin. Kaikki ongelmat projektin jälkeen olivat fyysisiin laitteisiin liittyviä tai helposti korjattavia konfigurointivirheitä, jotka olivat vain unohtuneet määritellä uutta palomuuriympäristöä pystyttäessä.

Välistä projekti eteni omaan makuuni hieman liian vauhdilla, välillä ei ollut aikaa paneutua miksi näin tehdään, kun se oli jo tehty kopioimalla vanhasta laitteesta asetuksia uuteen. Vaikka hoidinkin lähes kaiken palomuurin konfiguroimisen, siitä suurin osa oli ennalta määriteltyä tai minulle kerrottiin mitä pitää painaa ja milloin, mikä tietysti vähensi omatoimista oppimista. En silti sanoisi, ettenkö olisi oppinut palomuuria käsitellessä yhtään mitään.

Projektista on ollut minulle hyötyä työelämässä. Nykyään toimin päivittäin FortiGate palomuurien parissa, ja toimistoverkkoprojekti toi minulle hurjan etumatkan osaamiseen. Osaan navigoida valikoita ja tiedän mitä tehdään minkäkin välilehden alla, osaan myös soveltaa oppimaani uusiin palomuuritoteutuksiin.

Kehittämistä projektissa olisi ollut se, että minulle olisi annettu paremmin aikaa uuden oppimiselle sekä itse oivaltamiselle, näille ei projektin tiukan aikataulun vuoksi jäänyt aikaa konfigurointipäivinä. Jos jälkikäteen olisi halunnut kerrata

mitä päivällä tuli tehtyä, olisi se pitänyt tehdä lähes ulkomuistista, sillä laitteisiin pääsi käsiksi vain toimistolla.

LÄHTEET

Agrawal Abhishek. n.d. Introduction of Firewall in Computer Network. Luettu 25.5.2020. https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/

Forcepoint. What is a Firewall? Luettu 25.5.2020. https://www.forcepoint.com/cyber-edu/firewall

Fortinet_a. n.d. HA heartbeat and communication between cluster units. Luettu 16.4.2019. https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverHeartbeat.htm

Fortinet_b. n.d. About active-passive failover. Luettu 16.4.2019. https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverAP.htm

Fortinet_c. n.d. HA override. Luettu 18.5.2020. https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_FGCP_override.htm

Fortinet_d. n.d. Technical Tip: Troubleshooting IPsec VPNs. Luettu 18.5.2020. https://kb.fortinet.com/kb/documentLink.do?externalID=FD46611

Fortinet_e. n.d. Configuring IPsec VPN on HQ. Luettu 9.5.2019. https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/783623/configuring-ipsec-vpn-on-hq

Fortinet_f. n.d. Active-passive and active-active HA Luettu 23.3.2020. https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_FGCP_ap_aa.htm

Fortinet_g. n.d. IPsec VPN troubleshooting. Luettu 19.5.2020. https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/168495

Fortinet_h. n.d. High availability with two FortiGates. Luettu 8.11.2018. Linkki päivitetty 1.6.2020 https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/661074/high-availability-with-two-fortigates

Naidu Latchum. 8.10.2011. Uplink Ports vs Normal Ports. Luettu 18.5.2020. https://community.cisco.com/t5/switching/uplink-ports-vs-normal-ports/td-p/1781011