TAMPEREEN
AMMATTIKORKEAKOULU

YRITYKSEN TIETOVERKON RAKENTAMINEN

Jyri Loukola

Opinnäytetyö
Toukokuu 2018
Insinööri (AMK)
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Insinööri (AMK)
Tietoliikennetekniikka ja tietoverkot

Jyri Loukola:
Yrityksen tietoverkon rakentaminen

Opinnäytetyö 22 sivua
Toukokuu 2018

Opinnäytetyö käsittelee yrityksen verkon rakennetta ja teoreettisia osia mitä tarvitsee ottaa huomioon sitä rakennettaessa. Verkkosuunnitteluun käytettiin enemmän aikaa ja vaivaa kuin itse verkon rakentamiseen.

Työssä käydään läpi perusasioita kuituliitännöistä, ethernet liitännöistä, perusreitityksestä, OSPF pohjaisesta automaattisesta reitityksestä ja IPsec salatuista virtuaaliverkoista. Kuituliitännöissä käydään liittimet millä kytketään verkon aktiivilaitteisiin ja erilaiset kuidut joita käytettiin työssä. Reitityksestä käydään läpi säännöt minkä mukaan reititetään paketteja verkoista toiseen. OSPF käytössä esitellään miten OSPF-palvelu löytää toisensa.

Seuraavaksi esitellään vanhan verkon heikkoudet ja syyt miksi muutos tehdään. Käydään läpi uuden laitteiston rakenne ja perus asiat jokaisesta laitteesta. Lopuksi esitellään lisäpalveluita, mitkä on rakennettu verkkoa varten. Nämä palveluiden tarkoitus on siirtää vanhoja laitteita uuteen verkkoon.

Pohdinnassa esitellään mikä muuttaa verkkoa tulevaisuudessa. Myös kerrotaan ongelmista ja hidasteista mitä tuli verkkoa rakentaessa.

Asiasanat: reititys, salaus, verkko

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Bachelor of Engineering

Jyri Loukola:
Building company's network

Bachelor's thesis 22 pages
May 2018

This thesis covers building companys network and theoretic parts that needs to be considered in building. More time and effort was used on network planning, than on building the network.

Thesis goes through basics of fiber connection in network, normal ethernet cabling, basic routing, automatic routing with OSPF and secure channels with IPsec. What kind of connections are used when connecting to networks active components, and differfent kind of fibers that are mentioned in this thesis, are reviewed in fiber cabling section. Routing goes through very basic rules of routing and how they are build on byte level. OSPF explaines how different OSPF finds each other and how they calculate routes.

The next section introduces problems in old network and reasons to change them. The new network and basic roles of routers are discussed next. In the end under discussion are extra services, that are build for network and for network devices like printers. Reason for these services is to ease the migration and help old devices.

The discussion section takes look at the future and how it may change network. It also discloses what were problems when building the network.

Key words: routing, encryption, network

SISÄLLYS

LYHENTEET JA TERMIT

OSPF	Open Shortest Path First
ip	Internet Protocol
SFP	Small form-factor pluggable transceiver
ethernet	Paketti pohjainen lähiverkko

1 JOHDANTO

Nykypäivänä teollisuusyrityksellä on useasti tarpeena tietoverkko, jota pystytään hallitsemaan. IOT (Internet Of Things) on luonut suuren paineen hallittavalle verkolle. Tietoverkon tarkoituksena on joustaa ja muuttua uusien laitteiden myötä. Se on työkalu laitteille, jotka tuottavat rahaa. Nykyään on myös siirrytty laitteissa pilvimalliin, joka vaatii suuren määrän kaistaa avoimeen internettiin. Useasti verkko on ensimmäinen asia, joka tarvitsee muutosta, kun esitellään uusia tuotantolaitteita, jotta pystytään eristämään eri valmistajien laitteet toisistaan.

Lopputulokseen, joka pystyy kasvamaan yrityksen mukana, tarvitaan suunnitelmallisuutta verkon puolesta. Suunnitelmallinen verkko sisältää valmiit ohjaukset IP-alueiden käyttöä varten. Tässä dokumentissa esitellään pienehkön verkon modernisointi ja siihen tarvittavat tekniikat.

2 VERKON TEORIA

2.1 Kuitu

Yleisimmät valokuituliitynnät vaativat laitteisiin asennettavat muuntimet, jotka muuttavat sähköisen signaalin optiseksi signaaliksi ja optisen signaalin sähköiseksi signaaliksi.

Datan siirrossa valokuitua käytetään siirtämään dataa pitkiä matkoja, siirrettäessä dataa paikoissa, joissa on suuria määriä sähkömagneettista häiriötä, ja kun tarvitaan suuria määriä kaistaa. Nykyaikaisessa verkkosuunnittelussa se on heikentänyt Ethernetin asemaa kytkimien välisessä tiedonsiirrossa.

SFP (Small form-factor pluggable transceiver) on fyysinen liitäntä tämänlaisille muuntimille. Ne voidaan irrottaa laitteesta ilman, että laitetta sammutetaan. SFP sisältää yhden lähettävän ja yhden vastaanottavat kanavan. Kumpikin kanava sisältää normaalin lähetyksen ja loogisesti invertoidun pinnin. Eli lähetys sisältää kaksi pinniä. Toinen jännitteellisesti vastakohta toisesta. Tällöin voidaan poistaa ulkopuolisia jännite muutoksia. Maksimivirrankulutus kanavaa kohden on 300mA, eli se sisältää kaksi 3.3V virtalähdettä itse moduulia varten. Moduulin lähetykselle ja vastaanotolle annetaan maksimitehoksi 1W (INF-8074i Rev 1.0.)

Kuvassa 1 on esimerkki single mode SFP:stä. Single mode tarkoittaa kaapelia, joka on tarkoitettu yhdelle aallonpituudelle. Single mode on tarkoitettu pidemmän kantaman lähetykseen, ja se on yleisesti käytetty Internet-palveluntarjoajan verkoissa.

Kuva 1. SFP-moduuli.

Single mode tukee pitempiä yhteyksiä isommalla nopeudella, mutta se on hinnaltaan suurempi. Multi mode kuitu on halvempi lähettimien ja itse kuitujen osalta.

SFP sisältää sarjamuotoisen väylän, jonka tarkoituksena on esitellä laitteelle pieni määrä vain luku-muodossa olevaa dataa. Sen koko on 256 bittiä SFP MSA mukaan, ja se sisältää lähettimen ominaisuudet, valmistajan, fyysisen muodon, muuntimen valmistajan sekä muuta tietoa. Monet valmistajat ovat kasvattaneet tätä muistiavaruutta ja lisänneet erilaisia kopion suojauksia.

2.2 Ethernet

Ethernet koostuu kahdesta tai useammasta parista parikaapelia. Maksimissa tukee 4 parillista RJ45-liitintä. RJ45-liitin kuuluu RJ-perheeseen (Registered Jack). Muita perheeseen kuuluvia on esimerkiksi RJ11, jota käytetään vanhakantaisten puhelinten kanssa. RJ11 on ainoastaan pienempi liitin ja on sen takia fyysisesti RJ45-liittimen kanssa. Kuvassa 2 näkee fyysisen eron.

Kuva 2. RJ11- ja RJ45-liitinten erot

Tällöin talo voidaan johdottaa Ethernetia varten, mutta käyttää vielä puhelinverkkoa. Tällainen yhteensopivuus eteen- ja taaksepäin tekee verkon rakentamisesta modulaarista. Tällöin pystytään käyttämään uudempia tekniikoita vanhojen tekniikoiden rinnalla.

Nykyaikainen Ethernet-kaapeli käyttää CAT 6A luokan kaapelia ja 8P8C (8 points 8 contacts). 8P8C liitin tarkoittaa liitintä, jossa on paikka 8 pinnille ja niistä on käytössä 8 pinniä. Tällainen kaapeli on suojattu sisäiseltä sekä muista lähteistä aiheutuvalta ylikuulumiselta. Kaapeli pystyy jopa 10 Gbps nopeuteen koko 100 metrin matkalta. 100 metriä on maksimi pituus CAT5-,CAT5E-, CAT6- ja CAT6A-kaapeleille. Pidemmillä matkoilla signaalin laatu kärsii liikaa. Maatason vaihtelut pitkissä vedoissa aiheuttavat pätkimistä ja nopeuden tippumista. Myös isot sähkömoottorit aiheuttavat sähkömagneettista häiriötä kaapeleihin. Siksi talosta taloon linjoissa ja suuri häiriöisissä tiloissa käytetään kuitua.

2.3 Reititys

IP-pohjaisissa verkoissa tarvitaan reititystä. Reitityksellä tarkoitetaan IP-verkkojen välillä tapahtuvasta siirrosta. Eli paketit siirtyvät verkosta toiseen. IP-verkko on joko fyysisesti tai loogisesti rajoitettu alue. Fyysisesti eriytetty alue tarkoittaa laitteistoa, joka ei rajoita OSI-mallin tasolla 2. Tällöin laitteet ovat yleensä tyhmiä kytkimiä tai yksinkertaisia toistimia eli hubeja.

Loogisesti rajoitetussa verkossa laitteet on rajoitettu toisistaan OSI-mallin tasolla 2. Fyysinen linkki voi olla, mutta loogista ei. Tämä on lähellä GRE-tunnelointia mutta OSI-mallin 2 tasolla. Eli pakettiin lisätään uusi tietue, jota kytkimet käyttävät rajoitukseen. Tätä kutsutaan VLAN-tietueeksi (IEEE-SA Standards Board.).

Reitittäminen tapahtuu peitteen mukaan. Peite määrittää kuuluuko IP-osoitteesta tuleva paketti omaan fyysiseen verkkoon vai ulkoiseen verkkoon. Kuvassa 3 on esimerkki normaalista kotiverkosta. Tarkistaessa, kuuluuko nimenomainen paketti verkkoon vai kuuluuko se ulkopuoliseen verkkoon, laite lukee oikealta vasemmalle maskia. Maski kertoo, mitkä bitit ovat tärkeitä reititykselle. 255.255.255.0-maskilla olevat verkot ohittavat viimeisen oktetin ja vertailevat vain kolmea ensimmäistä oktettia (rfc791).

Verkon nimi	Verkon laitteet
11000000.10101000.00000000.00000000	192.168.0.0/24
11111111.11111111.11111111.00000000	255.255.255.0

Kuva 3. Normaali koti-IP-verkko. (rfc791)

Jos paketti ei kuulu lähiverkon osoitteisiin, se siirtyy reititystauluun. Eri valmistajat esittävät reititystaulun hieman eri tavoin. Kuvassa 4 on esimerkki Linux-pohjaisesta reititystaulusta. Kuvassa ensimmäisenä näkyvä default via 10.8.3.74 tarkoittaa osoitetta, jonka kautta lähetetään paketit, joille ei löydy kohdetta muualta taulusta.

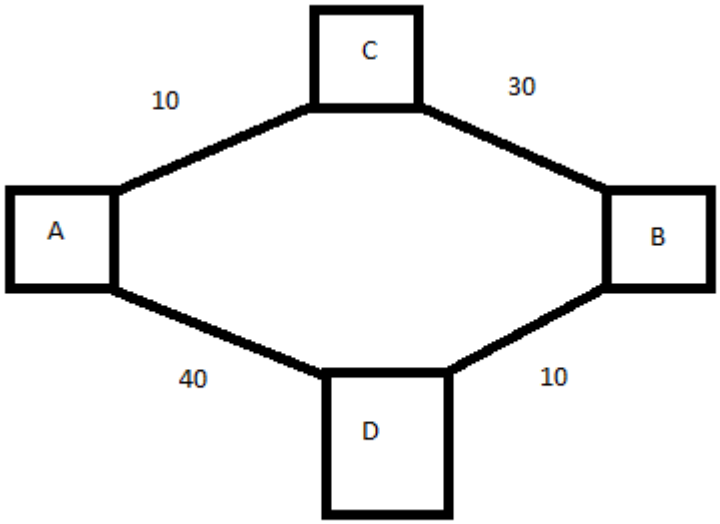
```
default via 10.8.3.74 dev eth0
10.8.0.2 dev tun4  proto kernel  scope link  src 10.8.0.1
10.8.0.4 dev tun5  proto kernel  scope link  src 10.8.0.3
10.8.0.6 dev tun1  proto kernel  scope link  src 10.8.0.5
10.8.0.8 dev tun0  proto kernel  scope link  src 10.8.0.7
10.8.0.10 dev tun2  proto kernel  scope link  src 10.8.0.9
10.8.0.101 dev tun3  proto kernel  scope link  src 10.8.0.100
10.8.0.201 dev tun6  proto kernel  scope link  src 10.8.0.200
10.8.3.74/31 dev eth0  proto kernel  scope link  src 10.8.3.75
10.144.0.0/16 dev zt1  proto kernel  scope link  src 10.144.148.219
172.22.0.0/16 dev zt0  proto kernel  scope link  src 172.22.148.219
```

Kuva 4. Linux-reititystaulu

Esimerkiksi alimmainen rivi kertoo, miten pääsee 172.22.0.0/16-verkkoon. Tähän verkkoon pääsee lähettämällä paketin 172.22.148.219-liittymästä. Näitä pystytään yhdistelemään. Esimerkiksi, kun tiedetään, että 192.168.3.0/24-verkkoon päästään 172.22.145.210-osoitteen kautta, lisätään uusi reitti. Default-reitti yleensä vie yleiseen internettiin, mutta sen ei ole pakko. Se on vain 0.0.0.0-maskilla oleva reitti, eli ei tarkisteta mitään aluetta. Jos verkossa on monia eri reittejä samaan verkkoon, ne järjestetään tärkeysjärjestykseen metric-määrityksen mukaan. Jokaisella reitillä on metric, joka määrää sen tärkeyden. Jos kahdella reitillä on sama metric, tapahtuu yhteentörmäyksiä. Linux ja Windows lähettävät käyttäen satunnaisesti kumpaakin, ja tällöin vastaus TCP-pakettiin voi lähteä eri tietä kuin TCP-paketti tuli. Tämä aiheuttaa pakettikatoa ja virheitä. Siksi käsintehdyt reititystaulut ovat yksinkertaisia, eikä niitä muuteta. Yrityksen sisäisen verkon reittien automaattiseen jakoon ja tasaamiseen on kehitelty erilaisia protokollia. Esimerkiksi OSPF- ja RIP-protokollat.

2.4 OSPF-protokolla

OSPF (open shortest path first) on automaattinen reititysprotokolla. Yksinkertaisimmillaan se kerää suoraan kiinni olevat reitittimet ja jakaa niihin oman reititystaulunsa. Näitä lähimmäisiä kutsutaan neighbour-reitittimiksi. Kun jokainen neighbour-reititin tekee saman, jokainen reititin tietää reitit jokaiseen verkkoon. Tämän jälkeen OSPF summaa reitillä olevat metric-arvot saaden yhden metric-arvon tietylle verkolle. Tästä on yksinkertainen esimerkki kuvassa 5. Kun OSPF valitsee reittiä A–B, se summaa A–C–B-reitin sekö A–D–B-reitin, ja valitsee pienemmän. Vertailuna RIP-protokolla ei tee metric-arvojen laskemista, vaan käsittelee näitä kahta reittiä samanarvoisina.



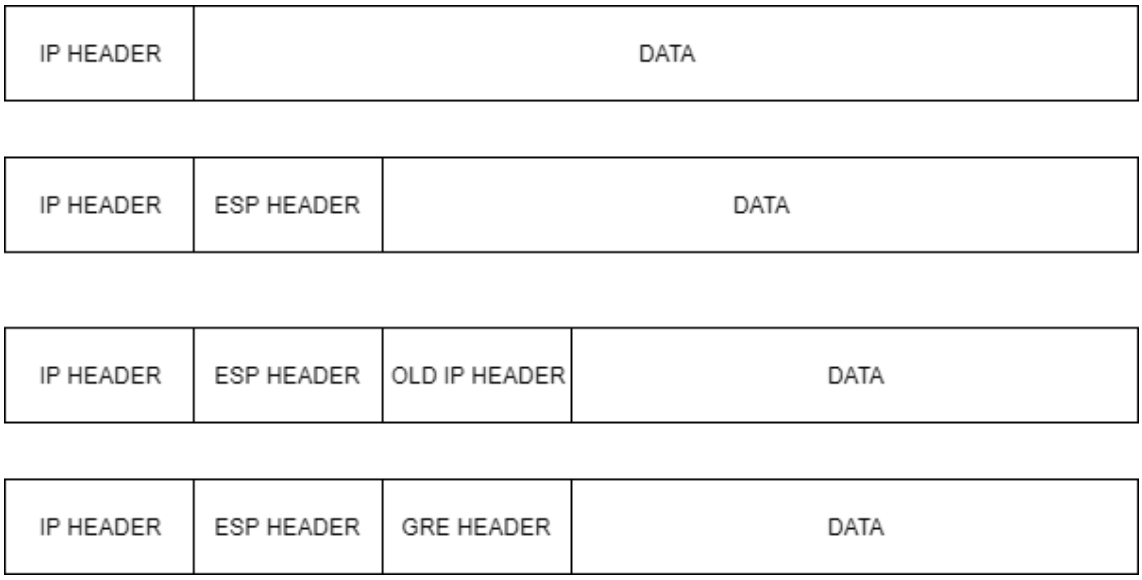
Kuva 5. Kaksi reittiä OSPF-verkossa.

OSPF syö itsessään osan linkkibudjetista, eli käyttää jokaista verkkolinkkiä etsiessään ja tarkistellessaan neighbour-laitteita.

2.5 IPsec-protokolla

IPsec (IP Security Architecture) on salausprotokolla, joka toimii osi-mallin kerroksella 3. Tällöin se pystyy kuljettamaan kerroksen 4 paketteja. Eli se pystyy salaamaan UDP- ja TCP-paketteja. Ipsec:ä käytetään joko varmistamaan paketin sisältö ja koskemattomuus eli AH tai salaamaan paketti. Salattu muoto on yleisempi näistä kahdesta. Salattua muotoa on myös kahta erilaista. Toinen lisää pakettiin uuden IP-tunnisteen ja ESP-tunnisteen.

Tällöin purettaessa pakettia poistetaan nämä kaksi ja siirretään sisällä oleva paketti vastaanottajalle. Tämä on yleisempi sisäverkosta sisäverkkoon siirrettäessä yleisen verkon yli. Toinen muoto toimii pitämällä IP-tunnisteen ja lisäämällä sen perään ESP-tunnisteen. ESP-tunnisteen jälkeen loput paketista tulee salattuna. Kuvassa 6 on aluksi IP-paketti ilman minkäänlaista tunnelointia, toisena on IP-paketti käyttäen pelkkää salausta ja kolmantena on paketti, joka on tunnelimuodossa.



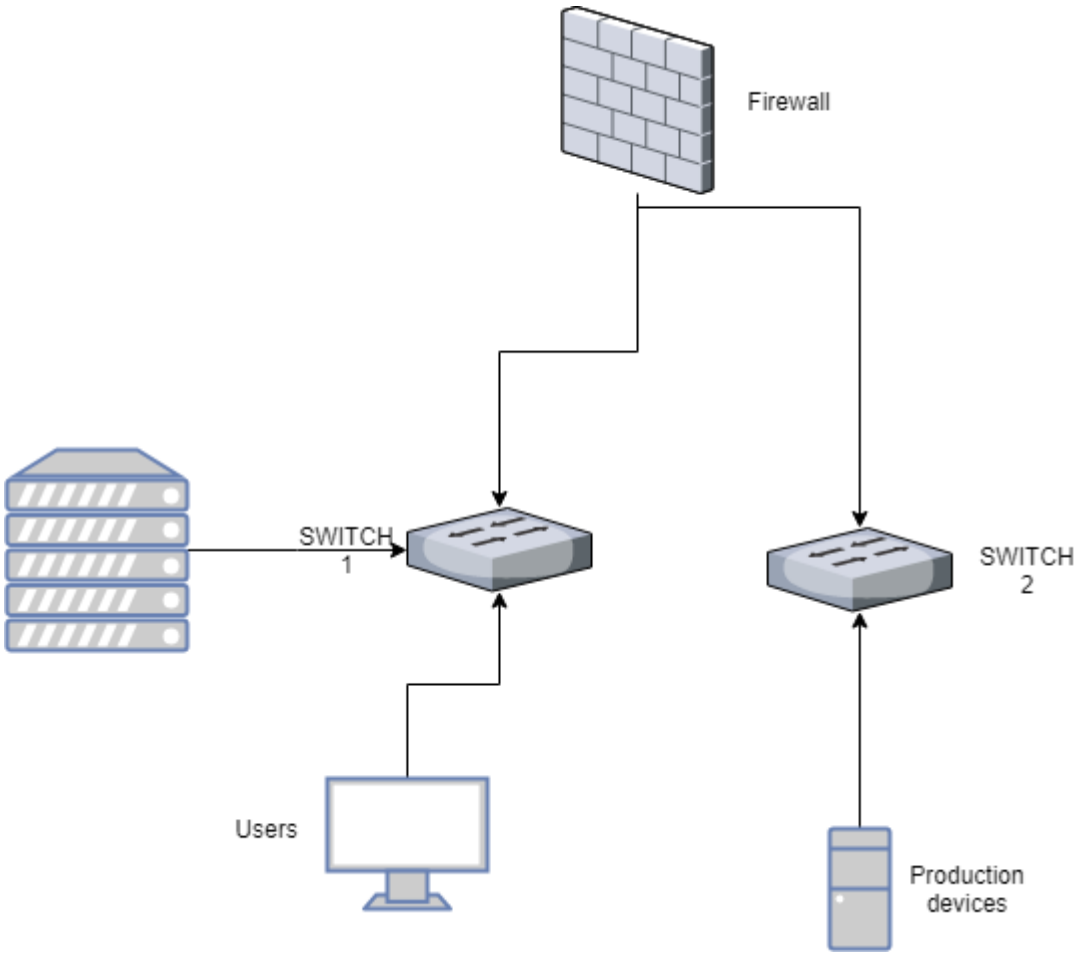
Kuva 6. Ipsec- ja GRE-tunnelit

GRE (https://tools.ietf.org/html/rfc2784) on yksinkertainen tunnelointi-protokolla. Se on täysin salaamaton ja lisää vaan uuden IP-tunnisteen pakettiin. Kuvassa 6 alimmaisena on GRE-tunneli, joka on salattuna IPsec. Tällöin se tiivistää paketin. GRE ei tue minkäänlaista salausta, ja se on tarkoitettu pelkkään tunnelointiin. GRE kuitenkin tukee verkkotasolla muita protokollia. Tärkein näistä on broadcast. OSPF käyttää broadcastia dynaamiseen naapurin etsintään.

3 KÄYTÄNTÖ

3.1 Vanha verkko

Vanha verkko koostui Internet-palveluntarjoajan tarjoamasta reitittimestä sekä parista jo vanhentuneesta kytkimestä. Palvelimet olivat paikallisia ja vanhoja. Niiden ongelmat alkoivat näkymään oikkuina. Haluttiin päästä pois yhden IP-alueen verkosta. Verkko ei pystynyt vastaamaan tasaisesti kasvavan yrityksen vaatimuksiin vaan oli hidasteena yrityksen halulle kasvaa. Haluttiin päästä eroon mahdollisimman monesta palvelimesta paikallisena. Sähköpostipalvelut haluttiin muuttaa pois yrityksen tiloista.



Kuva 7. Vanha verkko.

Vanha verkko oli yksinkertainen, mutta vaikeasti hallittava. Mitään ei voinut rajata omalle alueellensa ja esimerkiksi sulautetut laitteet tuotannosta pystyivät keskustelemaan käyttäjien laitteiden kanssa. Tuotannossa tarvittiin vielä erikseen Windows XP -käyttöjärjestelmällä olevia laitteita, joiden uusiminen olisi ollut hyvin kallista ja aikaa vievää. Nämä laitteet myös aiheuttivat tietoturvariskin: esimerkiksi käyttäjien uusiin koneisiin

iskevä virus pystyi hyökkäämään tuotannon koneiden kimppuun. Tuotannon koneet lopettavat toimintansa, jolloin tuotanto seisahtuu. Tuotannon laitteiden uusiminen kestää vuosia, ja on yleensä kallista. Muutenkin laitteisto tarvitsi modernisointia ja tulevaisuuteen katsomista.

3.2 Uusi verkko

Työssä tarkoituksena on määritellä ja suunnitella henkilömäärältään pienen yrityksen verkko ja siihen kuuluvat laitteet. Yrityksellä on suuri määrä tuotannon laitteita, jotka tarvitsevat suojatun verkon itselleen. Suurin osa palvelimista on ulkoistettu ja siirretty palveluntarjoajien konesaleihin. Tämä monimutkaistaa verkkoratkaisua ja pakottaa käyttämään laitteistoa, joka pystyy kättelemään eri valmistajien kanssa. Lisäksi jokainen palveluntarjoaja haluaa käyttää vähän erilaista tekniikkaa. Yhteistyö eri konesalien välillä ilman, että data kulkee paikallisen verkon kautta pitää olla mahdollista. Näiden takia tarvitaan suunnitelma siitä, miten pilkotaan yksityiset osoitteet.

Internet-palveluntarjoaja tarjoaa kuituliittymän, joka sisältää kahdeksan ulkoista staattista IP:tä. Kuituliittymä päätyy palveluntarjoajan omaan kytkimeen. Ethernet yhdistetään verkon reunakytkimeen, josta pääasialliseen reitittimeen. Tämän reitittimen pääasiallisena tarkoituksena on toimia muuntimena ulkoisten ja sisäisten osoitteiden välillä. Tämä toimii samalla sisäisille reiteille yhdyskäytävänä. NAT-kerros ajetaan tässä laitteessa.

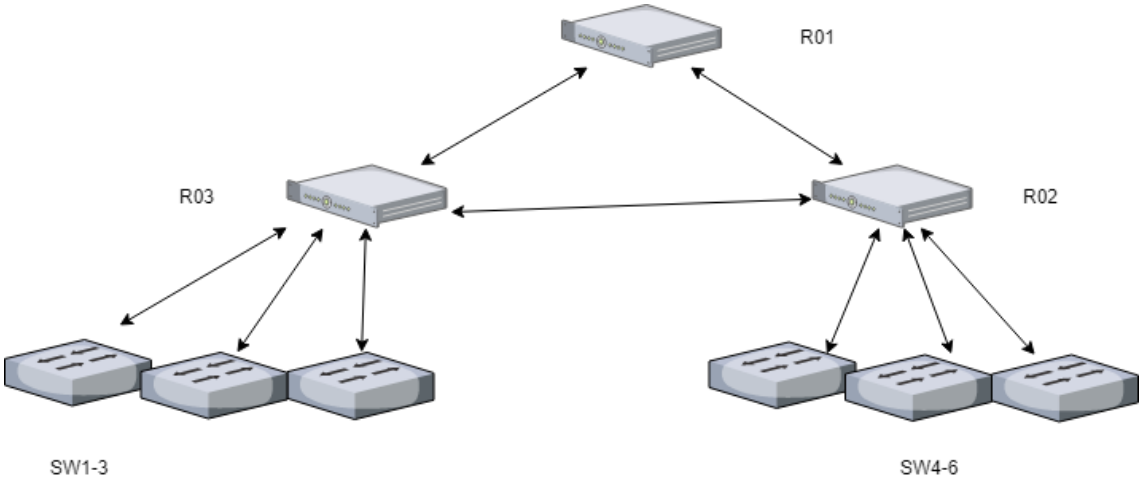
Tarkoituksena ei ole palvella mitään muuta ulkoista osapuolta kuin salattuja kanavia paikallisella laitteistolla. Sähköposti hoidetaan ulkoistettuna palveluna ja yhdistettynä omiin hakemistopalveluihin. Hakemistopalvelut toimivat ulkoisessa palvelinsalissa. Microsoftin hakemistopalveluita varten on paikallisena pelkästään yksi palvelin, joka toimii samalla DNS- ja DHCP-palvelimina.

Migraatioalueeksi valittiin192.168.0.0/16. Kyseiselle alueelle ei määritetä uusia osoitteita. Tämä sen takia, että vanha verkko oli määritetty tälle alueelle. Tarkoituksena on siirtää tuotannon laitteet ilman katkosta tuotannossa uuteen verkkoon.

Paikallisille palvelimille on jaettuna omat verkko-osoitealueet. Nämä on jaettu tarkoituksen perusteella. Toimisto- ja käyttäjäpalveluita tarjoavat ovat omalla alueellaan. Tulostimille on jaettuna omat verkot.

3.3 Looginen rakenne

Looginen rakenne koostuu kahdesta osasta, jotka keskustelevat toisten kanssa. Alueet ovat sisäverkko, joka näkyy kuvassa 8, ja ulkoverkko, joka näkyy kuvassa 9. Lähiverkossa R01 toimii porttina eri osien välillä. Sen pääasiallinen toimi on reitittää ulkoverkon palveluiden, kuten Internetin, ja sisäverkon asiakkaiden välillä. Palvelimet yhdistyvät myös R01.

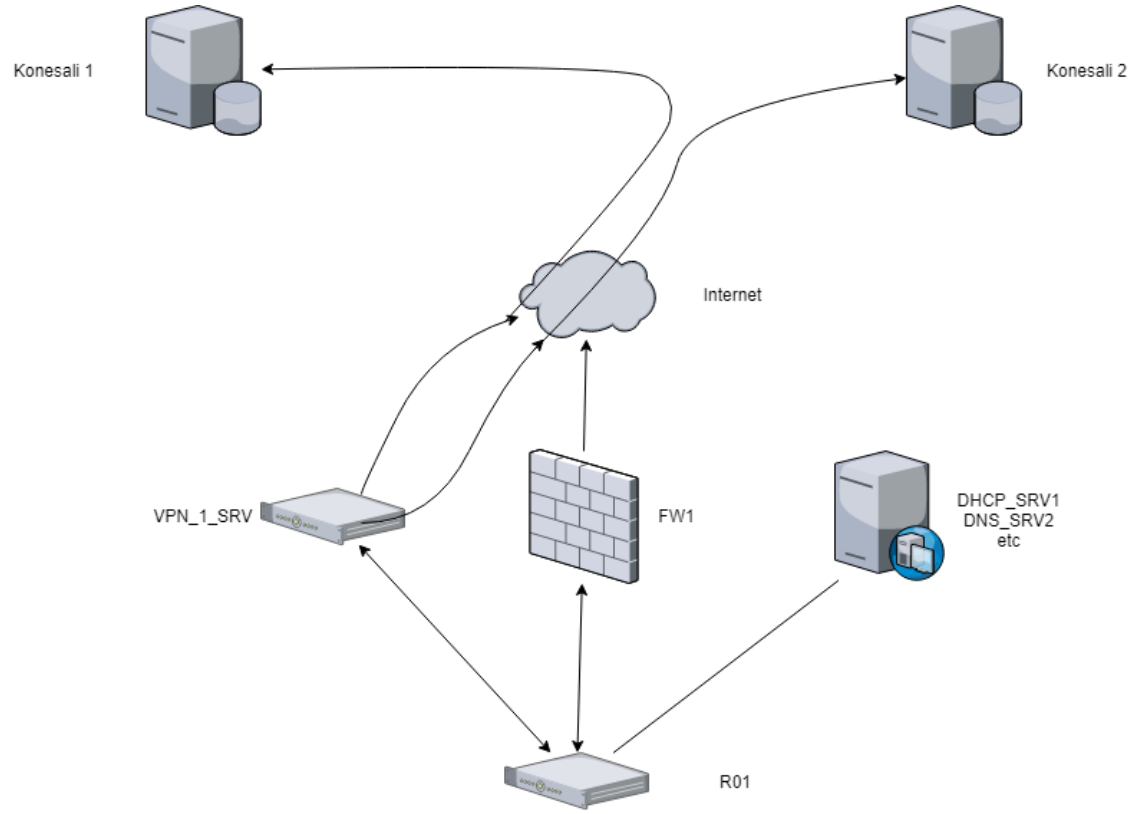


Kuva 8. Lähiverkko.

Ulkoverkon palveluiden puolella on palomuuri, jonka kautta suodatetaan vapaaseen Internettiin menevä liikenne. R01 kokoaa reitit ja verkot, jotka on tarkoitettu ulkoverkkoon, ja siirtää ne palomuurille. Palomuuri tekee näille osoitteenmuutoksen ja siirtää ne ulkoverkkoon. VPN_1_SRV toimii IPsec-protokollaanhyväksikäyttäen tienä eri konesaleihin. Se sisältää OSPF-palvelun, jonka tarkoituksena on automaattisesti siirtää reitit, jotka se oppii konesaleilta R01:n käyttöön. Jos halutaan varayhteys konesaleihin, VPN_1_SRV kahdentaa ja asentaa käyttämään 4G/LTE-varayhteyttä. Tällöin käytössä on konesaleihin kaksi erilaista reittiä. Pääsääntöisesti käytetään kuituyhteyttä, mutta kuituyhteyden ollessa pois käytöstä käytetään varayhteyttä.

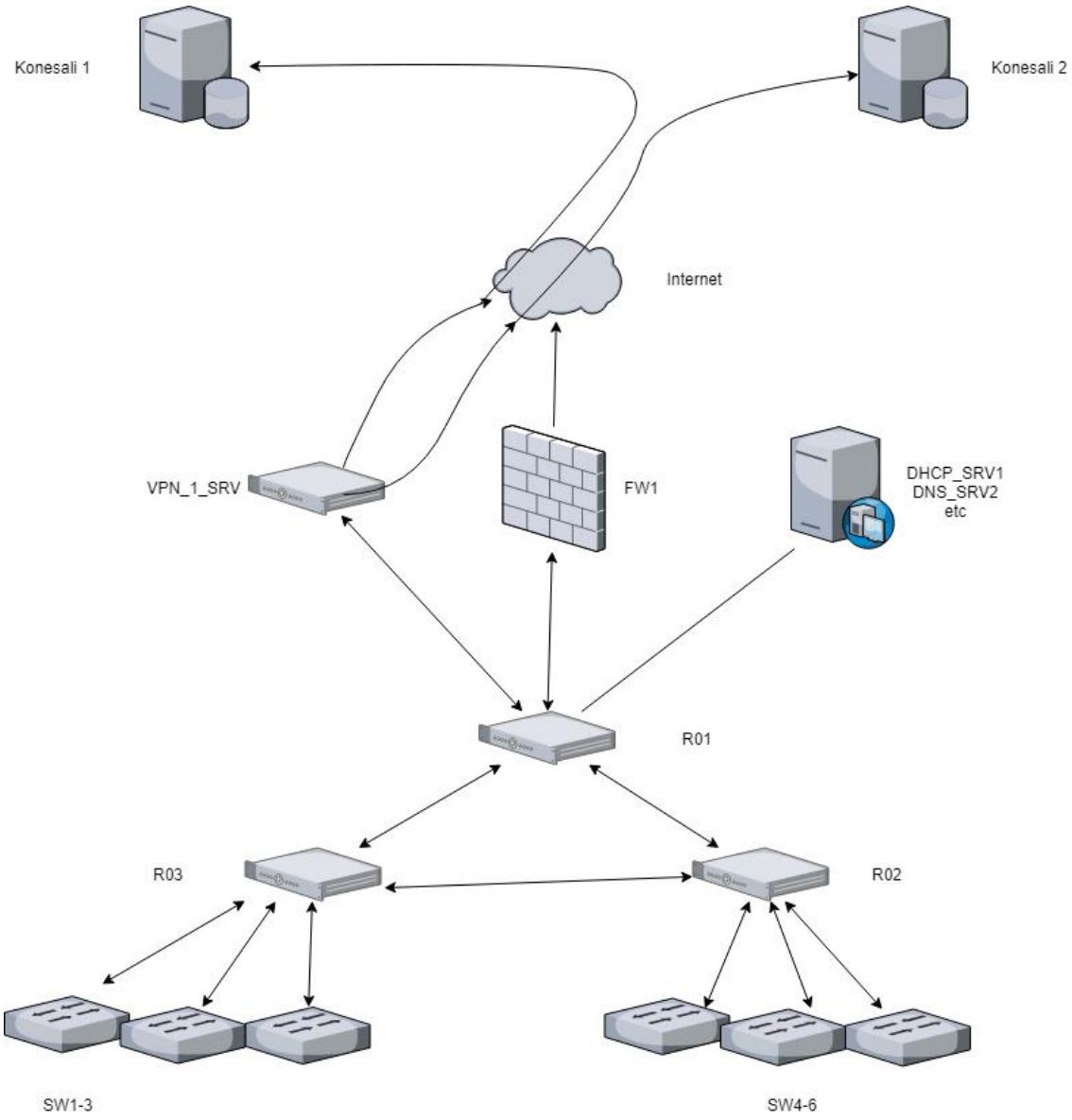
FW1 esittelee default gateway -reitin verkkoon. Tällöin R02 ja R03 osaavat reitittää pakettinsa FW1. Jos tarvitaan varayhteys, esitellään FW1 rinnalle FW2, joka yhdistetään esim. 4G-reitittimen kautta. Kun FW2:lle annetaan alempi metric-arvo, sitä käytetään

vaihtoehtoisena reittinä ulkoverkkoon. Jos FW1 reitti ulkoverkkoon katkeaa, vaihdetaan käyttämään FW2. Tällainen vaihdos rikkoo IP-sessiot ja aiheuttaa käyttäjälle haittaa, mutta on automaattinen. Pieni häiriö verrattuna täyteen katkokseen on parempi. VPN-yhteydet eivät aiheuta tällaista häiriötä, ja liikehdintä konesaleihin tapahtuu katkeamatta.



Kuva 9. Ulkoverkko.

DNS- ja DHCP-palvelut ajetaan Windows-ympäristöstä. Näihin jätetään mahdollisuus klusterointiin. Palvelin tarjoilee R02 ja R03 DHCP-palvelun, jonka osoitteita ne jakavat DHCP-relay-protokollaa käyttäen. Tällöin hallinta pysyy yhdessä paikassa. DHCP-relay-palveluun annetaan sallituiksi osoitteiksi kaikkien reitittimien ja DHCP-palvelimet. DNS rakentuu Windows-pohjaisen DNS-palvelimen ympärille.



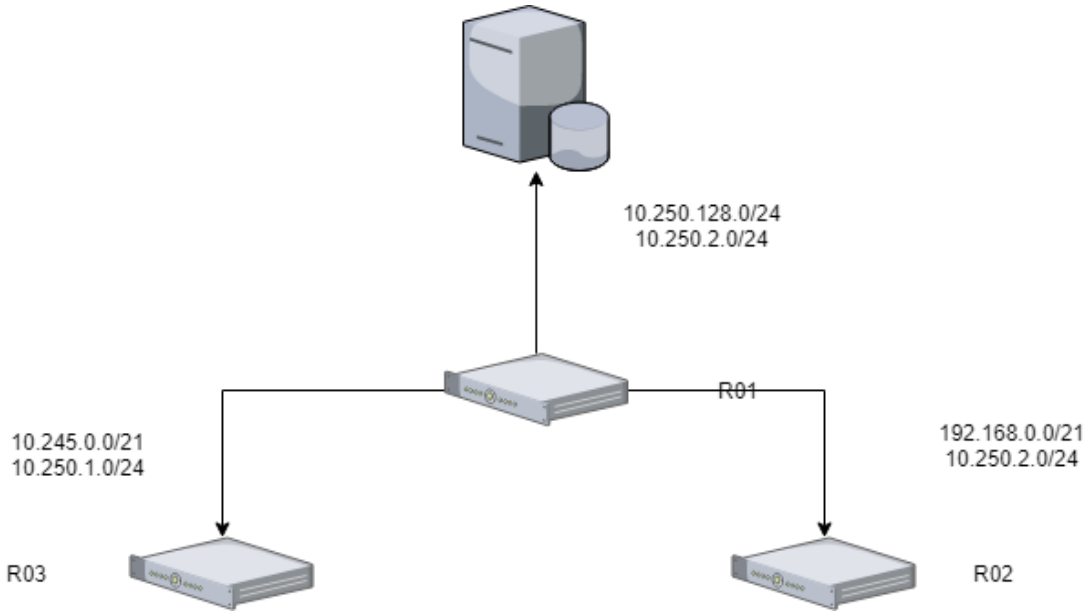
Kuva 10. Koko verkon kuvaus.

IP-alueet on jaettu valmiiksi suurempiin verkkoihin, joista osioidaan tarpeen mukaan osoitteita. Näin pystytään yhtenäistämään palomuurisääntöjä. Taulukossa 1 esitellään kaikki verkot, joita on jyvitetty. Kun ACL kirjoitetaan näiden verkkojen pohjalta, saadaan helposti laajennettava verkko. Uusiin laitteisiin määritetään kaikkiin sama pohja-ACL, jonka päälle lisätään tarkemmat säännöt.

Toimistoverkko	10.245.0.0/16
Hallintaverkko	10.250.0.0/17
Palvelinverkko	10.250.128.0/17
Tulostinverkko	10.251.0.0/18
Tuotantoverkko	192.168.0.0/16
Pisteestä pisteeseen osoitteet	10.23.0.0/23

Taulukko 1. IP-verkot.

R0- reitittimelle annetaan koko 10.245.0.0/21-verkko jaettavaksi. OSPF ei jaa suoraan tämän alle osuvia verkkoja, vaan jakaa yhtenä verkkona sen. Kuvassa 11 nähdään, miten verkot on jaettu eri reitittimille. Jokaisella on hallintaverkkoalue, josta jaetaan hallinta IP-laitteille. Tällaisia on esimerkiksi virtualisointialustojen hallintaliittymät.

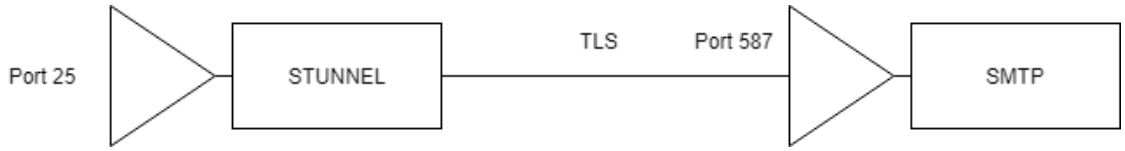


Kuva 11. Lähiverkon IP-alueet.

3.4 Verkon rakennetta tukevat palvelut

Palveluntarjoajan sähköpostipalvelimet eivät tue tällä hetkellä salaamatonta sähköpostia. Tämä on nykypäivänä hyvä asia, mutta vanhat laitteet ei tue tarpeeksi korkeaa salausta toimiakseen palvelun kanssa. Kyseistä ongelmaa varten perustetaan tunnelointipalvelu, joka salaa vanhojen laitteiden liikenteen ja lähettää pilveen. Stunnel on yksinkertainen

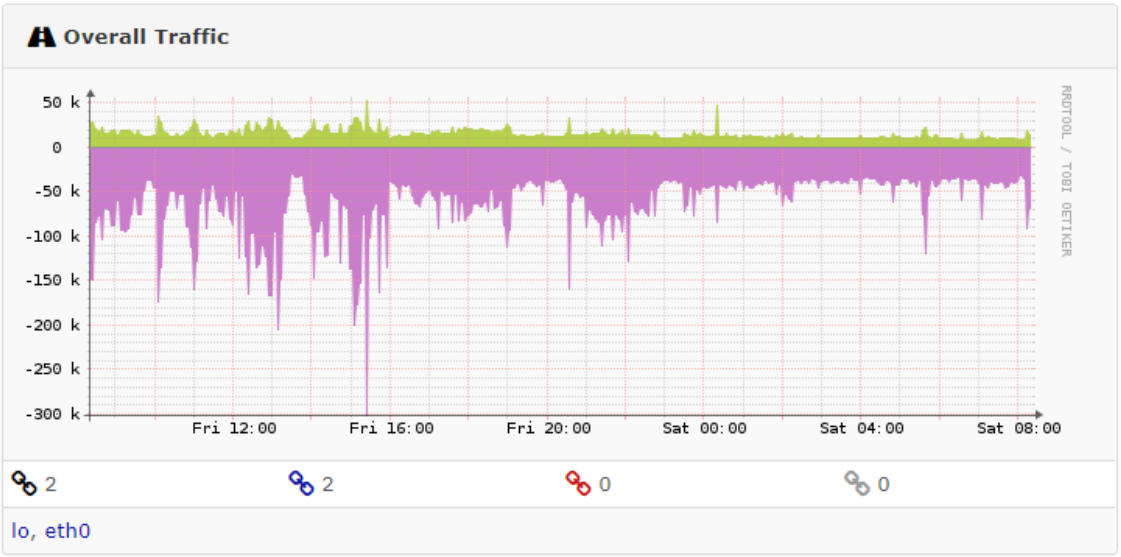
palvelu, joka tarjoaa tällaisen. Stunnel perustetaan mikropalveluksi konesali 2:een. Mikropalveluksi siksi, ettei se tarvitse lokaalia tallennustilaa. Pelkästään yksinkertaisen tiedoston, jonka mukaan se luo tunnelin.



Kuvat 12. Stunnel.

Stunnel kuuntelee kuvan 6 mukaan portissa 25. Se salaa liikenteen TLS-protokollan mukaan, ja lähettää liikenteen pilvipalveluun, joka purkaa salauksen ja siirtää SMTP-palvelulle. Tämän käyttö vähenee, kun tulostimia ja muita vanhoja laitteita vaihdetaan uusiin.

Verkon diagnostiikkaan ja palveluiden seurantaan käytetään librenms-pakettia. Tämän tarkoituksena on toimia syslog logi -palvelimena ja SNMP-viestien keskuksena. Tämä kerää ja järjestelee SNMP-viestit. Tärkeintä on kerätä viestit ajallisesti samassa järjestyksessä. Siksi ajallisesti, että voidaan logeista seurata mitä on oikeasti tapahtunut. Jos voidaan seurata paikallisesta tietokoneesta palvelimelle asti yhdestä paikasta, pystytään paikantamaan ongelmat suoraan. Kuvassa 13 on esimerkki yhden palvelimen liikenteestä. Siitä pystytään näkemään aktiiviset ajat ja kuinka paljon jää.



Kuva 13. Palvelimen liikenteen seuraaminen.

Hallintaverkon käyttäjien hallintaan käytetään erikseen luotavia tunnuksia, jotka eivät ole Windows domain-tunnuksia. Tunnukset on paikoitettu palomuurille, joka tarjoilee ulkoverkkoon Open VPN -tyyppisen VPN-liittymän. Tästä jaetaan VPN-sertifikaatit, joilla käyttäjät yhdistyvät.

4 POHDINTA

Työ tarkoituksena oli rakentaa pohja verkolle, jota on tulevaisuudessa helppo laajentaa. Itse projektin vastaanottajalle dokumentoitiin erikseen jokaisen laitteen asetukset tiedostoina.

Työn lopputulos miellytti asiakasta ja sitä on jo ehditty laajentaa käyttäjän halujen mukaan. Laitteisto on toiminut odotuksien mukaisesti ja tähän mennessä ei ole ongelmia syntynyt. Järjestelmän

Tulevaisuudessa järjestelmää laajentaessa voidaan käyttää määritettyjä alueita uusien verkkojen rakentamiseen. Esim. tulee uusi sivukonttori, joka tarvitsee verkkolaitteet ja palomuurit. IP-osoitteet lohkotaan valmiista paloista, luodaan virtuaalitunnelit servereitä varten ja tilataan laitteet.

LÄHTEET

IEEE-SA Standards Board. 1998. IEEE Std 802.1Q-1998. The Institute of Electrical and Electronics Engineers, Inc

SFP (Small Formfactor Pluggable) Transceiver. INF-8074i Rev 1.0 2000 s. 22. SFF Committee

Information Sciences Institute University of Southern California. 1981. rfc791 s. 20 https://tools.ietf.org/html/rfc791