Haaga-Helia
ammattikorkeakoulu Oy

Suunnitelma yrityksen tietoverkon segmentointiin

Valtteri Aalto

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2019

Haaga-Helia ammattikorkeakoulu Oy

Tiivistelmä

24.5.2019

Tekijä(t)
Valtteri Aalto

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Raportin/Opinnäytetyön nimi
Suunnitelma yrityksen tietoverkon segmentointiin

Sivu- ja liitesivumäärä
32

Opinnäytetyön tarkoituksena oli perehtyä yrityksen tietoverkon segmentointiin ja kuinka sillä voidaan parantaa tietoverkon tietoturvaa. Kyseessä on toiminnallinen opinnäytetyö ja opinnäytetyön tavoitteena oli tuottaa suunnitelma yrityksen tietoverkon segmentointiin ja kuvata sen toteutus. Suunnitelman toimeksiantaja oli kuvitteellinen ohjelmistoalan yritys. Opinnäytetyön tekeminen alkoi maaliskuussa 2019 ja se valmistui toukokuussa 2019.

Opinnäytetyön aiheen valintaan vaikutti myös se, että opinnäytetyön tekijän työpaikalla oli meneillään tietoverkon segmentointiprojekti, jossa hän oli päävastuullinen.

Tietoperustassa käsitellään tietoliikenteen yleistä teoriaa, tietoverkkoarkkitehtuureja, tietoverkon segmentointia, mikrosegmentointia, tarvittavat laitteet tietoverkon segmentointia varten ja tietoverkon segmentoinnilla saavutettavat tietoturvahyödyt.

Työn tuloksena syntyi suunnitelma kohdeyrityksen tietoverkon segmentointiin ja kuvaus sen toteutuksesta. Tietoverkon segmentointi toteutettiin suunnitelman mukaisesti, käyttäen VLAN segmentointia, ja yrityksen sisäverkkoon luotiin 13 uutta aliverkkoa ja virtuaalilähiverkkoa.

Johtopäätöksenä todettiin, että tietoverkon segmentointi on erittäin tärkeä osa tietoverkon tietoturvaa ja sen laiminlyöminen on tullut kalliiksi tietomurtojen kohteeksi joutuneille yrityksille, jotka ovat joutuneet maksamaan jopa satoja miljoonia vahingonkorvauksina.

Asiasanat
tietoverkon segmentointi, tietoliikenne, tietoturva

Sisällys

1 Johdanto

Mitä on tietoverkon segmentoiminen? Tietoverkon segmentoinnilla tarkoitetaan tietoverkon jakamista pienempiin osiin, eli segmentteihin. Tietoverkon segmentoinnilla pyritään parantamaan tietoverkon tietoturvaa ja suorituskykyä. Tietoverkon segmentoinnin voi toteuttaa muutamalla eri tavalla, tässä työssä keskitytään perinteiseen VLAN-segmentointiin.

Viime vuosina paljastuneissa laajoissa tietomurroissa yksi yhdistävä tekijä on ollut se, että tietomurron kohteeksi joutuneiden yritysten sisäverkko on monesti ollut puutteellisesti segmentoitu. Tästä johtuen hyökkääjät ovat päässeet liikkumaan verkossa vapaasti, varastamaan dataa ja saastuttamaan laitteita.

Hyvä esimerkki on 2013 yhdysvaltalaiseen Target-tavarataloon kohdistunut hyökkäys. Hyökkääjät pääsivät käsiksi Targetin asiakastietokantaan ja maksukorttitietoihin ja saivat haltuunsa 60 miljoonan asiakkaan yhteystiedot ja 41 miljoonan asiakkaan maksukorttitiedot, mukaan lukien luottokorttien CVC-koodit. Tutkimuksissa todettiin, että Targetin verkko oli huonosti segmentoitu ja asiakas- ja maksukorttidataa ei oltu eristetty muusta verkosta PCI-DSS standardin suositusten mukaisesti. Mikäli Targetin verkko olisi ollut asianmukaisesti segmentoitu ja asiakas- ja maksukorttidata olisi eristetty muusta verkosta, hyökkääjät eivät parhaimmassa tapauksessa olisi saaneet saaliikseen lainkaan asiakas- tai maksukorttidataa.

Tietoverkon segmentointi on yrityksen tietoverkon tietoturvan kulmakivi, joka pitää olla huolellisesti tehty. Kun tietoverkko on perusteellisesti segmentoitu, tietoverkon tietoturvaa voidaan lähteä rakentamaan pidemmälle muilla keinoilla, kuten palomuurien avulla.

Tämän opinnäytetyön tarkoitus on perehtyä tietoverkon segmentointiin, käsitellä hieman yleistä tietoliikenteen teoriaa, tietoverkkoarkkitehtuureja, tarkastella tietoverkon segmentoinnilla saavutettavia tietoturvahyötyjä ja luoda suunnitelma yrityksen tietoverkon segmentointia varten, sekä kuvata suunnitelman toteutus.

Päätin tehdä opinnäytetyöni yrityksen tietoverkon segmentoinnista koska aihe on mielenkiintoinen ja ajankohtainen minun työpaikallani.

Opinnäytetyön tutkimuskysymykset ovat:

- Miksi verkon segmentointi kannattaa tehdä?
- Miten verkon segmentointi voidaan toteuttaa?
- Mitä tietoturvahyötyjä voidaan saavuttaa verkon segmentoinnilla?

Opinnäytetyön tuotoksena syntyy suunnitelma yrityksen tietoverkon segmentoimista varten ja sen toteutuksen kuvaus.

2 Keskeiset käsitteet

VLAN

Virtual Local Area Network, virtuaalilähiverkko. Virtuaalilähiverkot mahdollistavat fyysisen lähiverkon jakamisen loogisiin broadcast domaineihin.

LAN

Local Area Network, lähiverkko. Lähiverkko on rajatulla alueella toimiva tietoliikenneverkko, joka muodostuu tietokoneista ja muista verkkolaitteista.

Broadcast domain

Broadcast domainilla tarkoitetaan laitteiden joukkoa, jotka kuuluvat samaan verkkosegmenttiin ja voivat siten tavoittaa toisensa broadcast liikenteellä.

Broadcast

Yleislähetys, joka lähetetään kaikille broadcast domainin jäsenille.

Verkkosegmentti

Verkkosegmentti on tietoverkon osa.

OSI-viitemalli

Open Systems Interconnection Reference Model on viitemalli, jolla kuvataan tiedonsiirtoprotokollat seitsemässä eri kerroksessa.

Data Link Layer (Layer 2)

OSI-mallin 2. kerros, Data Link Layer, eli siirtoyhteyskerros. Siirtoyhteyskerroksen tehtävä on siirtää dataa laitteiden välillä lähiverkossa MAC-osoitteiden perusteella.

Network Layer (Layer 3)

OSI-mallin 3. kerros, Network Layer, eli verkkokerros. Verkkokerros mahdollistaa mm. pakettien reitittämisen eri verkoissa olevien laitteiden välillä.

Application Layer (Layer 7)

OSI-mallin 7. kerros, Application Layer, eli sovelluskerros. Sovelluskerros on OSI-mallin ylin kerros, ja se toimii rajapintana käyttäjien ja tietoverkkoa hyödyntävien sovellusten välillä, mahdollistaen käyttäjien ja sovellusten välisen kommunikoinnin.

Internet protocol suite (TCP/IP)

Internet protocol suite, jota kutsutaan myös TCP/IP:ksi sen vuoksi, että TCP ja IP-protokollat ovat sen keskeisimmät protokollat, on konseptimalli ja joukko kommunikointiprotokollia, jota käytetään Internetissä ja muissa tietoverkoissa. TCP/IP mahdollistaa tiedonsiirron ja kuvaa, miten data tulisi muuntaa pakettimuotoon, osoitteistaa, lähettää, reitittää ja vastaanottaa.

IP-protokolla

Internet Protocol on TCP/IP mallin keskeisin kommunikointiprotokolla. IP-protokollan tehtävä on välittää IP-paketteja IP-verkossa laitteiden välillä IP-pakettien otsikkotiedoista löytyvien IP-osoitteiden perusteella. IP-protokollasta on kaksi versiota, IPv4 ja IPv6.

IP-osoite

Internet Protocol-osoite on jokaisen IP-verkossa olevan laitteen uniikki osoite, jonka avulla laitteet pystyvät tavoittamaan toisensa verkkokerros-tasolla. IPv4-osoitteet ovat 32-bittisiä ja IPv6-osoitteet ovat 128-bittisiä.

Flat network tietoverkkoarkkitehtuuri

Flat network tietoverkkoarkkitehtuurissa tietoverkkoa ei ole segmentoitu, ja kaikki laitteet ovat samassa broadcast domainissa.

MAC-osoite

Media Access Control-osoite on osoite, jonka avulla laitteet voivat tavoittaa toisensa siirtoyhteyskerros-tasolla. Jokainen MAC-osoite on uniikki ja se on kovakoodattu laitteen verkkosovittimeen.

Aliverkko

IP-verkon osaa kutsutaan aliverkoksi.

Yksityisverkko

Tietoverkko, joka käyttää yksityiseen käyttöön tarkoitettua IP-osoiteavaruutta, jota ei reititetä Internetissä. IANA (Internet Assigned Numbers Authority) on varannut tietyt IP-osoiteavaruudet ainoastaan yksityisverkkojen käyttöön.

ARP

Address Resolution Protocol. ARP on prokolla, jonka avulla Ethernet-verkoissa selvitetään IPv4-osoitetta vastaava MAC-osoite.

Access Layer

Hierarkisen tietoverkkoarkkitehtuurin liityntäkerros, jonka avulla laitteet voidaan yhdistää lähiverkkoon.

Distribution Layer

Hierarkisen tietoverkkoarkkitehtuurin jakelukerros, jossa mm. reititetään liityntäkerroksesta vastaanotetut paketit.

Core Layer

Hierarkisen tietoverkkoarkkitehtuurin runkokerros, jossa aggregoidaan jakelukerroksen laitteilta vastaanotettu data.

ACL

Access-control list, eli pääsynhallintalista. Pääsynhallintalistoilla voidaan filtteröidä verkkoliikennettä IP-osoitteiden ja protokollaporttien perusteella.

Palomuurisääntö

Palomuurisääntöjen avulla palomuurilla voidaan filtteröidä verkkoliikennettä IP-osoite-, protokollaportti- ja applikaatiotasolla. Palomuurisääntöihin on myös mahdollista konfiguroida tietoturvaskannauksia, kuten Antivirus, IPS, Application control jne.

Palomuuri

Palomuuri on järjestelmä, joka monitoroi sisään- ja ulospäin menevää verkkoliikennettä ja suodattaa paketteja palomuurisäännöstön perusteella. Palomuuri voi olla ohjelmisto- tai laitteistopohjainen.

Seuraavan sukupolven palomuuri (Next-generation Firewall, NGFW)

Nykyaikainen, monipuolisilla tietoturvaominaisuuksilla varustettu tilallinen palomuuri.

3 Tietoperusta

3.1 Broadcast domain

Broadcast domainilla tarkoitetaan laitteiden joukkoa, jotka ovat samassa verkkosegmentissä ja sitä kautta voivat tavoittaa toisensa broadcast liikenteen avulla. Broadcast liikenne lähetetään aina kaikille broadcast domainin jäsenille, jonka takia se kuormittaa verkkoa huomattavasti. (René Molenaar 2019.)

ARP-kyselyt ovat hyvä esimerkki broadcast liikenteestä. ARP-kysely tehdään, kun Ethernet-kehystä lähettävä laite ei tiedä kohdelaitteen MAC-osoitetta. Lähettävä laite lähettää ARP-kyselyn, jossa on kohdelaitteen IP-osoite broadcastina kaikille broadcast domainin jäsenille. Laitteet vertaavat IP-osoitetta omaansa ja IP-osoitteen omaava laite lähettää vastauksen ARP-kyselyyn, jossa se kertoo oman MAC-osoitteensa. (study-ccna.com 2019a.)

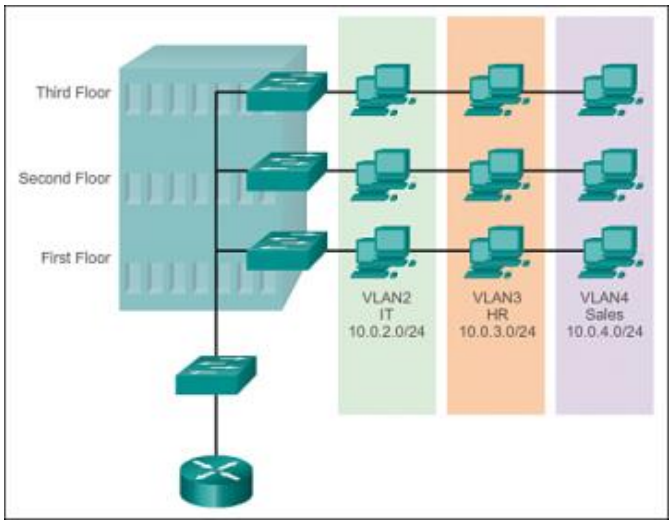
Broadcast domain voidaan jakaa useampaan loogiseen siirtoyhteyskerros-segmenttiin virtuaalilähiverkkojen avulla, jolloin jokainen virtuaalilähiverkko muodostaa oman loogisen broadcast domainin. Kun verkko jaetaan useampaan eri virtuaalilähiverkkoon, broadcast liikenne vähenee, jolloin verkon suorituskyky paranee. (Cisco Press 2014b.)

3.2 Virtuaalilähiverkko

Virtuaalilähiverkko on looginen broadcast domain, ja sen vuoksi virtuaalilähiverkko voidaan ulottaa useamman fyysisen verkkosegmentin läpi. (Cisco Press 2014b.)

Virtuaalilähiverkkojen avulla tietoverkkoa voidaan segmentoida siten, ettei laitteen fyysisellä sijainnilla ole merkitystä, koska virtuaalilähiverkot perustuvat loogisiin yhteyksiin. Kuvassa 1 on kuvattu rakennus, jossa on kolme eri kerrosta. Joka kerroksessa on oma kytkin ja kytkimille on konfiguroitu kolme eri virtuaalilähiverkkoa, VLAN2, VLAN3 ja VLAN4. (Cisco Press 2014b.)

Jokaisessa kerroksessa on myös kolme tietokonetta, joista jokainen kuuluu eri virtuaalilähiverkkoon. Kytkimellä liikenne välitetään oikeaan virtuaalilähiverkkoon virtuaalilähiverkon tunnuksen perusteella. Virtuaalilähiverkon kannalta sillä ei ole merkitystä ovatko virtuaalilähiverkkoon kuuluvat laitteet kiinni samassa kytkimessä, kunhan kytkimeen on konfiguroitu kyseinen virtuaalilähiverkko. (Cisco Press 2014b.)



Kuva 1. Virtuaalilähiverkot (Cisco Press 2014b)

3.3 IP-osoitteet ja aliverkot

Jokaisella tietoverkossa olevalla laitteella ja sijainnilla pitää olla osoite, jolla sen voi tavoittaa. Tietoverkkojen tapauksessa se osoite on IP-osoite. Laitteet kommunikoivat keskenään IP-verkossa IP-osoitteiden avulla. Jokaisen IP-osoitteen pitää olla uniikki omassa verkossaan. (Justin Ellingwood 2014.)

IP-protokollasta on olemassa kaksi versiota, IPv4 ja IPv6. IPv4 on tällä hetkellä käytetympi, mutta IPv6:n käyttö yleistyy jatkuvasti johtuen sen sisältämistä parannuksista ja sen takia, ettei IPv4-osoitteiden määrä tule riittämään kaikille tulevaisuudessa Internetiin kytkettäville laitteille. (Justin Ellingwood 2014.)

IP-osoitteet jaetaan kahteen osaan, laite- ja verkko-osaan. IP-laiteosoitteen avulla voidaan tunnistaa laite, jonne voidaan lähettää IP-paketteja. IP-verkko-osoitteen avulla voidaan taas tunnistaa spesifi verkkosegmentti, johon voi kuulua useampi laite. (Cisco Systems 2018b.)

IPv4-osoitteet koostuvat 32-bitistä, jotka jaetaan neljään 8-bitin osaan, eli oktettiin. Oktetit erotetaan toisistaan pisteillä, ja ne ilmaistaan numeroina. Oktetin arvo voi olla pienimmillään 0 ja suurimmillaan 255. IPv4-osoite esitetään tässä muodossa: 192.168.0.5. Sama IP-osoite binäärimuodossa: 11000000 10101000 00000000 00000101 (Justin Ellingwood 2014.)

IPv6-osoitteet ovat 128-bittisiä, ja ne koostuvat kahdeksasta 16-bittisestä heksadesimaaliarvosta, jotka erotetaan toisistaan kaksoispisteillä. Esimerkki IPv6-osoitteesta: 4FDE:0000:0000:0002:0022:F376:FF3B:AB3F. IPv6-osoitteen ensimmäiset 64-bittiä ilmaisevat verkko-osan, ja loput ilmaisevat laiteosan. (Juniper Networks 2019.)

IP-osoitteita on rajallinen määrä, ja niiden lukumäärä määräytyy IP-osoitteen bittien perusteella. IP-osoitteiden IPv4-osoitteet ovat 32-bittisiä(2^{32}), joten IPv4-osoitteita on yhteensä 4 294 967 296. IPv6-osoitteet ovat taas 128-bittisiä(2^{128}), joten niitä on yhteensä huikeat 340 282 366 920 938 463 463 374 607 431 768 211 456, eli noin 340 undekiljoonaa IP-osoitetta. (RIPE NCC 2014.)

Luokallinen IP-osoitteistus

Alun perin IP-osoitteet jaettiin viiteen eri luokkaan, A, B, C, D ja E. Luokat määritellään IP-osoitteen neljällä ensimmäisellä bitillä, joiden avulla voidaan tunnistaa mihin luokkaan IP-osoite kuuluu. A-luokassa IP-osoitteen ensimmäinen bitti on 0 ja se tarkoittaa sitä, että kaikki IP-osoitteet 0.0.0.0-127.255.255.255 välillä kuuluvat A-luokkaan. B-luokan IP-osoitteissa ensimmäinen bitti on 1, ja toinen bitti on 0. B-luokan IP-osoitteita ovat 128.0.0.0-191.255.255.255 välillä olevat IP-osoitteet. (Justin Ellingwood 2014.)

C-luokan IP-osoitteissa kahden ensimmäisen bitin arvo on 1, ja kolmannen bitin arvo on 0. C-luokan IP-osoitteita ovat 192.0.0.0-223.255.255.255 välillä olevat IP-osoitteet. D-luokan IP-osoitteissa ensimmäisten kolmen bitin arvo on 1, ja neljännen bitin arvo on 0. D-luokan IP-osoitteita ovat 224.0.0.0-239.255.255.255 välille osuvat IP-osoitteet. (Justin Ellingwood 2014.)

E-luokassa neljän ensimmäisen bitin arvo on 1, E-luokan IP-osoitteita ovat 240.0.0.0-255.255.255.255 välille osuvat IP-osoitteet. D-luokan IP-osoitteet ovat varattu multicasting protokollille, jotka mahdollistavat IP-paketin lähettämisen usealle eri laitteelle samanaikaisesti. E-luokan IP-osoitteet ovat varattu kokeilulliseen käyttöön, eikä niitä käytetä juurikaan. (Justin Ellingwood 2014.)

Internet protokolla varaa 255.0.0.0-255.255.255.255 välillä olevat IP-osoitteet broadcast liikennettä varten, eikä kyseisiä IP-osoitteita tulisi laskea tavallisiksi E-luokan osoitteiksi. (Bradley Mitchell 2018.)

A-C luokat jakoivat verkko- ja laiteosat eri lailla mahdollistaakseen eri kokoiset verkot. A-luokan osoitteissa ensimmäisen oktetin jäljellä olevat bitit määrittivät verkko-osoitteen ja loput oktetit määrittivät laiteosoitteet. (Justin Ellingwood 2014.)

B-luokan osoitteissa ensimmäisen oktetin jäljellä olevat bitit ja toinen oktetti määrittivät verkko-osoitteen ja loput oktetit määrittivät laiteosoitteet. (Justin Ellingwood 2014.)

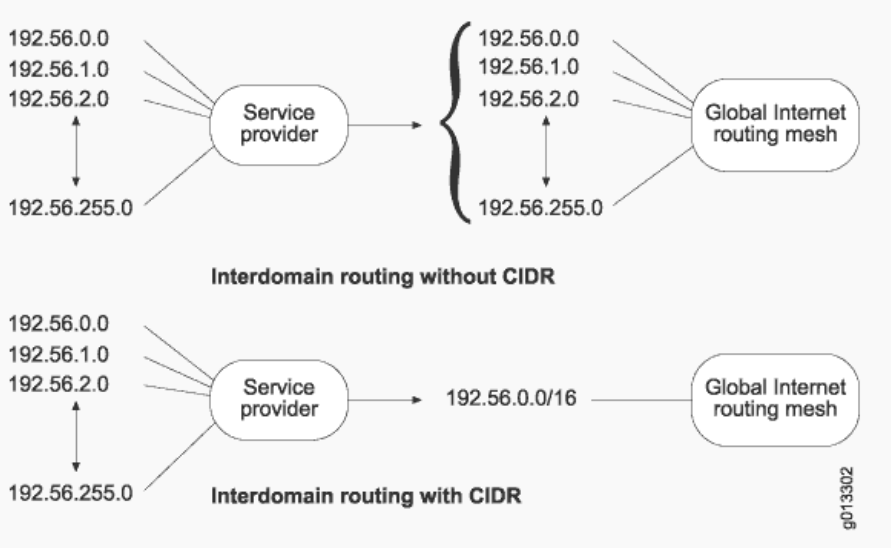
C-luokan osoitteissa kolme ensimmäistä oktettia olivat varattu verkko-osoitteelle ja jäljellä oleva neljäs oktetti määritti laiteosoitteet. (Justin Ellingwood 2014.)

CIDR

Vuonna 1993 kehitetty CIDR (Classless Interdomain Routing) korvasi luokallisen IP-osoitteistuksen. (Cisco Systems 2004.)

CIDR kehitettiin parantamaan Internetin reitityksen skaalautuvuutta. CIDR:in avulla voidaan pienentää globaalin Internet-reitityksen reititystaulujen kokoa, kuten voidaan havaita kuvasta 2. CIDR:ssä IP-verkko esitetään prefiksin avulla, joka on IP-osoite, jossa esitetään myös verkko-osan bittien lukumäärä, esimerkiksi 192.56.0.0/16. Esimerkkiosoitteessa /16 tarkoittaa verkko-osan bittien lukumäärää, joka voidaan ilmaista myös 255.255.0.0 verkkomaskilla. (Juniper Networks 2014.)

Kuva 2. CIDR (Juniper Networks 2014)



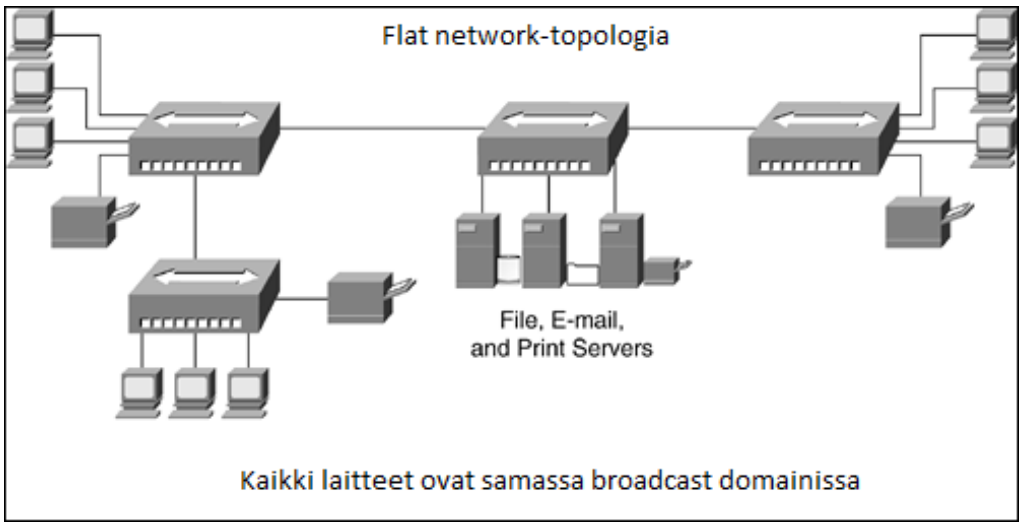
3.4 Tietoverkkoarkkitehtuurit

Flat network tietoverkkoarkkitehtuuri

Flat network tietoverkkoarkkitehtuurissa verkkoa ei ole segmentoitu ja kaikki laitteet ovat samassa broadcast domainissa. (etutorials 2019.)

Lähiverkot olivat 1990-luvun alkupuolella yleensä toteutettu flat network-tietoverkkoarkkitehtuurin mukaisesti. Lähiverkko tyypillisesti koostui yhdestä tai useammasta hubista, johon oli kytketty kaikki työasemat ja palvelimet. (Edrawsoft 2019.)

Hubit operoivat OSI-mallin Layer 1-tasolla. Hubit toimivat siten, että kun joku hubin porteista vastaanottaa sähköisen signaalin, hubi lähettää saman signaalin jokaiseen porttiin vastaanottavaa porttia lukuun ottamatta. Tämän takia kaikki hubissa kiinni olevat laitteet vastaanottavat saman datan, vaikka se koskisi vain yhtä laitetta, joka aiheuttaa turhaa verkkoliikennettä. Hubin portit toimivat half-duplexina, joka tarkoittaa sitä, että vain yksi laite voi kommunikoida verkossa kerrallaan. (Geek University 2019a.)



Kuva 3. Lähiverkon flat network verkkotopologia (mukaillen etutorials.org 2019)

Flat network tietoverkkoarkkitehtuuri on tietoturvariski. Tämä johtuu siitä, että kaikki laitteet ovat samassa lähiverkossa ja liikennettä laitteiden välillä ei ole rajoitettu millään tavalla. Tämä mahdollistaa sen, että haittaohjelmat voivat saastuttaa laitteita vapaasti lähiverkon sisällä. (Sage Data Security 2019.)

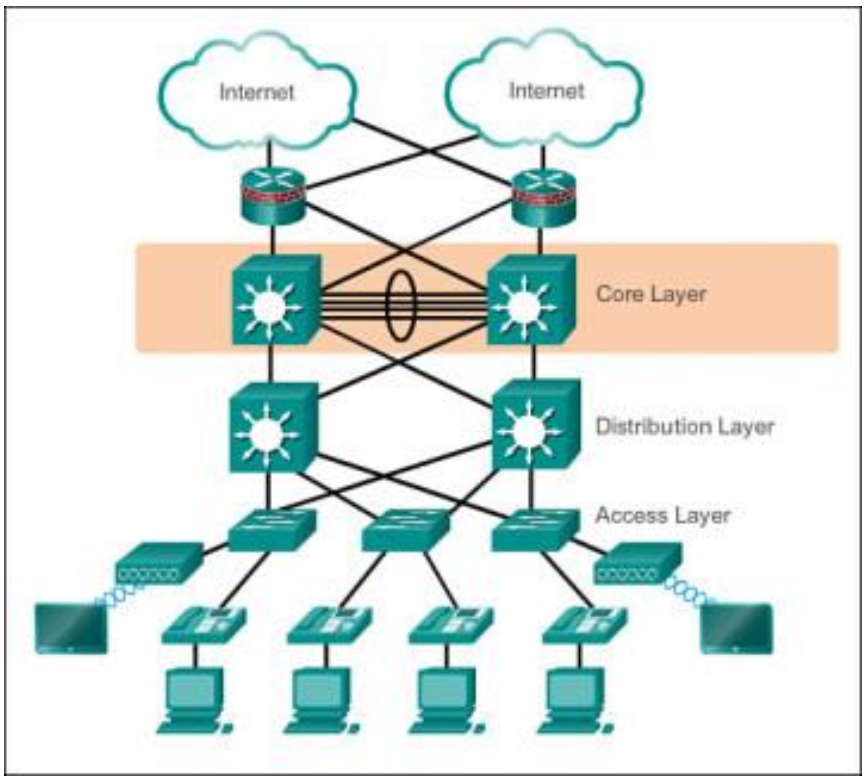
Toinen huomattava ongelma flat network tietoverkkoarkkitehtuurin verkossa on suorituskyky. Kaikki laitteet ovat samassa broadcast domainissa, jonka vuoksi verkossa

liikkuu paljon turhaa broadcast liikennettä. Kun verkko jaetaan useampaan loogiseen broadcast domainiin virtuaalilähiverkkojen avulla, broadcast liikenne vähentyy huomattavasti ja se välitetään vain kyseisen virtuaalilähiverkon jäsenille. (Cisco Press 2014b.)

Puutteistaan huolimatta, flat network tietoverkkoarkkitehtuuri voi olla riittävä pienissä lähiverkoissa, joissa on vähän laitteita, jolloin broadcast liikenteen määrä on vähäinen. (Edrawsoft 2019.)

Hierarkkinen tietoverkkoarkkitehtuuri

Flat network-tietoverkkoarkkitehtuurin tilalle tarvittiin parempi tapa tietoverkkojen suunnitteluun. Cisco Systems kehitti hierarkkisen tietoverkkoarkkitehtuurin vastaamaan tähän tarpeeseen. Hierarkkisessa tietoverkkoarkkitehtuurissa tietoverkko segmentoidaan virtuaalilähiverkoilla, jotta päästään eroon flat network tietoverkkoarkkitehtuurin rajoitteista. Hierarkkinen tietoverkkoarkkitehtuuri koostuu kolmesta eri kerroksesta: liityntä, jakelu- ja runkokerros. Jokaisella kerroksella on oma roolinsa, ne koostuvat erilaisista laitteista ja ne sisältävät eri toiminnallisuuksia. Joissain verkoissa jakelu- ja runkokerroksen toiminnallisuudet ovat sulautettu samaan laitteeseen, tälläistä tietoverkkoarkkitehtuuria kutsutaan two-tier collapsed coreksi. (Cisco Press 2014a.)



Kuva 4. Kolmikerroksinen hierarkkinen tietoverkkoarkkitehtuuri (Cisco Press 2014a)

Liityntäkerros (Access layer)

Liityntäkerroksen tarkoitus on tarjota laitteille pääsy verkkoon ja se toteutetaan yleensä siirtoyhteyskerroksessa toimivilla kytkimillä ja langattomilla tukiasemilla. (Cisco Press 2014a.)

Liityntäkerros tarjoaa mm. seuraavat palvelut:

- Pakettikytkentä siirtoyhteyskerroksessa
- Porttikohtaisia turvaominaisuuksia
- Spanning tree-protokolla silmukoiden estoa varten
- Power-over-Ethernet toiminnallisuus virransyöttöön, jolla voidaan antaa virtaa esim. WLAN tukiasemille.

(Cisco Press 2014a.)

Jakelukerros (Distribution layer)

Jakelukerroksen tehtävä on aggregoida liityntäkerroskytkimiltä saatu data ja sen jälkeen siirtää se runkokerrokseen. (Cisco Press 2014a.)

Jakelukerros tarjoaa mm. seuraavat palvelut:

- Lähiverkkolinkkien aggregointi
- Pääsynhallintalistat ja pakettien filtteröinti
- Lähiverkkojen ja virtuaalilähiverkkojen välinen reititys.
- Broadcast domainien hallinta.

(Cisco Press 2014a.)

Runkokerros (Core layer)

Runkokerroksen tehtävä on aggregoida kaikki jakelukerroksen kytkimiltä tuleva data, jonka vuoksi runkokerroksen kytkimet ovat yleensä todella suorituskykyisiä. (Cisco Press 2014a.)

Runkokerroksessa huomioitavia asioita:

- Runkokerroksella tulisi olla korkea saatavuus

- Runkokerroksen pitää olla vikasietoinen
- Skaalautuvuus tulisi hoitaa suorituskykyisemmällä laitteella, eikä laitteiden lisäämisellä
- Laskentatehoa vaativien toimenpiteiden, kuten tietoturvaominaisuuksien tai Quality of servicen käyttöä tulisi välttää runkokerroksessa

(Cisco Press 2014a.)

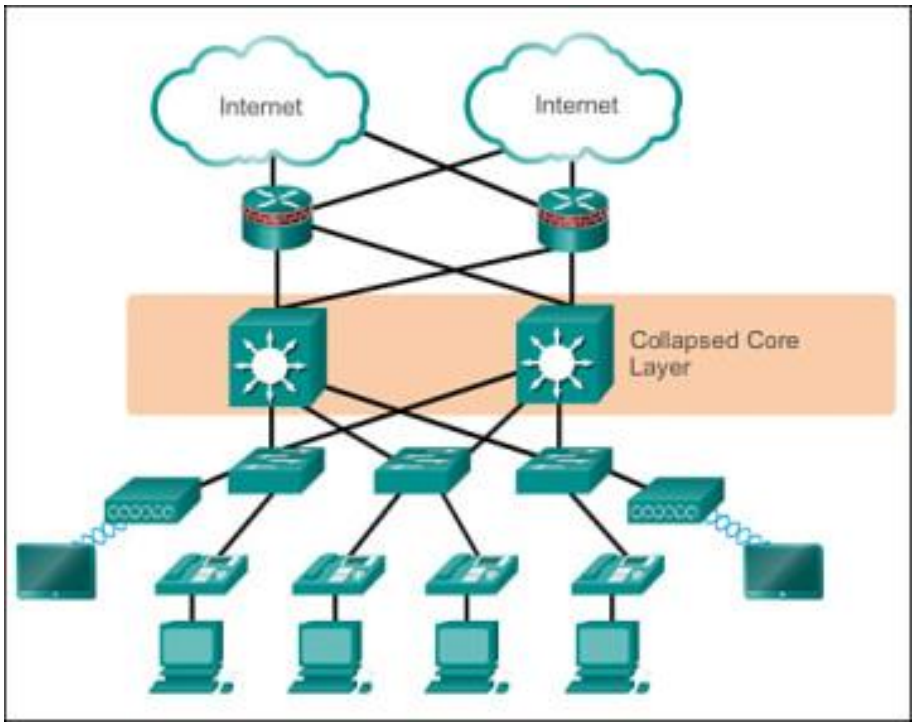
Hierarkkisen tietoverkkoarkkitehtuurin hyödyt

- Suorituskyky: Hierarkkisen tietoverkkoarkkitehtuurin avulla voidaan rakentaa erittäin suorituskykyisiä verkkoja.
- Parempi hallittavuus ja vianselvityksen helpottuminen: Kun verkko koostuu eri kerroksista, se on helpompi hallita ja vianselvitys helpottuu, kun vika voidaan eristää tiettyyn kerrokseen.
- Skaalautuvuus: Arkkitehtuuri skaalautuu hyvin ja mahdollistaa verkon kasvun.
- Vikasietoisuus: Liityntä-, jakelu- ja runkokerrosten välillä on useampi linkki ja laitteet ovat kahdennettu.

(Cisco Press 2014a.)

Two-Tier Collapsed core tietoverkkoarkkitehtuuri

Two-Tier Collapsed coressa jakelu- ja runkokerroksen toiminnallisuudet ovat sulautettu samaan laitteeseen. Kerrosten yhdistämisellä haetaan kustannussäästöjä, sillä pienemmässä verkossa erillistä runkokerrosta ei välttämättä tarvita, ja kaksikerroksisella mallilla saavutetaan useimmat kolmikerroksisen mallin hyödyt. (Cisco Press 2014a.)



Kuva 5. Two-Tier Collapsed core tietoverkkoarkkitehtuuri. (Cisco Press 2014a)

3.5 Tietoverkon segmentointi

Tietoverkon segmentoinnilla tarkoitetaan tietoverkon jakamista pienempiin tietoverkkosegmentteihin. Tietoverkkoa voidaan segmentoida OSI-mallin siirtoyhteyskerros-tasolla virtuaalilähiverkkojen avulla ja verkkokerros-tasolla aliverkotuksen avulla. Siirtoyhteyskerros-tason verkkosegmenttiä kutsutaan broadcast domainiksi ja IP-verkkoon kuuluvaa verkkokerros-tason segmenttiä kutsutaan aliverkoksi. (Test King 2019. Explain Network Segmentation and Basic Traffic Management Concepts)

Tietoverkon segmentoinnilla yleensä tavoitellaan parempaa verkon suorituskykyä ja tietoturvaa. Kun tietoverkko jaetaan useampaan loogiseen broadcast domainiin, saadaan vähennettyä verkon broadcast liikennettä, joka parantaa verkon suorituskykyä. Lisäksi verkon tietoturva paranee, kun eri palvelut ovat omissa verkoissaan. (Cisco Press 2014b.)

3.6 Mikrosegmentointi

Mikrosegmentointi on verkon virtualisointiin perustuva tekniikka, jolla voidaan jakaa verkko omiin segmentteihin ja turvallisuusvyöhykkeisiin virtuaalikone-tasolla ja määritellä tietoturvasäännöstö jokaiselle virtuaalikoneelle. (VMware 2019.)

Mikrosegmentointi on vaihtoehto perinteiselle VLAN-segmentoinnille. Virtuaalilähiverkko-segmentoinnissa on rajoitteena virtuaalilähiverkkojen määrä, maksimissaan 4096, kun taas mikrosegmentoinnissa käytettäviä VXLAN:eja voi olla jopa 16 miljoonaa. (Trevor Pott 2017.)

Yksi mikrosegmentoinnin hyöty virtuaalilähiverkko-segmentointiin verrattuna ovat parempi tietoturva, kun liikennettä voidaan rajoittaa virtuaalikone-tasolla perinteisen aliverkko-tason sijaan. (Trevor Pott 2017.)

3.7 Tietoverkon segmentointia varten tarvittavat verkkolaitteet

Tietoverkon segmentoimista varten OSI-mallin siirtoyhteyskerros- ja verkkokerros-tasoilla tarvitaan kytkin, jotta voidaan kytkeä laitteita lähiverkkoon ja määritellä tarvittavat virtuaalilähiverkot, sekä joko reititin tai palomuuri aliverkottamiseen ja reitittämään liikennettä aliverkkojen välillä. Tietoturvan kannalta palomuuri on parempi ratkaisu, koska reitittimen tietoturvaominaisuudet rajoittuvat lähinnä pääsylistoihin, kun taas palomuurille voidaan määritellä erilaisia palomuurisääntöjä ja tietoturvaominaisuuksia.

Kytkin

Kytkin on siirtoyhteyskerroksessa toimiva verkkolaite, joka prosessoi ja välittää Ethernet-kehyksiä lähiverkoissa MAC-osoitteiden perusteella. Kytkimen avulla laitteet voidaan kytkeä lähiverkkoon, jossa laitteet voivat kommunikoida MAC-osoitteiden avulla. Kytkimen porttien toiminta poikkeaa hubista, siten, että ne toimivat Full-Duplex-moodissa, jolloin laite voi lähettää ja vastaanottaa dataa samanaikaisesti. (Geek University 2019b.)

Kytkimille voidaan määritellä virtuaalilähiverkkoja, joiden avulla voidaan yhdistää yhden tai useamman fyysisen lähiverkon laitteet samaan loogiseen broadcast domainiin. (Cisco Systems 2018c.)

Ethernet-kehyksien sisälle on useimmiten enkapsuloitu IP-paketteja, jotka ovat verkkokerros-tason datayksiköitä. IP-pakettien reitittämiseen toisiin aliverkkoihin tarvitaan reititin. (Marcin Bialy 2018.)

Reititin

Reititin on verkkokerroksessa toimiva verkkolaite, joka reitittää datapaketteja eri tietoverkkojen välillä IP-osoitteiden perusteella. Reitittimen avulla eri aliverkoissa olevat laitteet voivat kommunikoida keskenään. (study-ccna.com 2019b.)

Reitittimet reitittävät paketteja reititystaulun reittitietojen perusteella. Reititystauluun voidaan lisätä reittitietoja manuaalisesti staattisilla reiteillä, jonka lisäksi voidaan käyttää dynaamisten reititysalgoritmien laskemia reittitietoja. (Cisco Systems 2019d.)

Palomuuri

Palomuuri on järjestelmä, joka monitoroi sisään- ja ulospäin menevää verkkoliikennettä ja suodattaa paketteja palomuurisäännöstön perusteella. Palomuuri voi olla ohjelmisto- tai laitteistopohjainen. (Forcepoint 2019.)

Palomuureja on eri tyyppisiä, ensimmäiset palomuurit olivat niin kutsuttuja tilattomia palomuureja. Tilaton palomuuri tekee staattista pakettisuodatusta ennalta määritetyn palomuurisäännöstön perusteella. Tilaton palomuuri suodattaa paketteja vertaamalla IP-paketin otsikkotietoja, kuten pakettien lähde- ja kohde IP-osoitteita, protokollaa ja lähde- ja kohdeportteja palomuurisääntöihin. Palomuurisääntöjen perusteella palomuuri joko hyväksyy paketin tai hylkää paketin. (tutorialspoint 2019.)

Tilattomien palomuurien lisäksi on olemassa myös tilallisia palomuureja. Tilallinen palomuuri eroaa tilattomasta palomuurista siten, että se pitää kirjaa palomuurin sessioiden tilatiedoista. Palomuuri ylläpitää tilataulua, josta palomuuri voi tarkistaa kuuluuko paketti olemassa olevaan sessioon, vai onko kyseessä uusi sessio. Jos paketti kuuluu olemassa olevaan sessioon, paketti sallitaan eikä sitä prosessoida enempää. Tilallinen palomuuri käyttää tilattoman palomuurin tapaan palomuurisääntöjä päätöksen tekoon pakettien käsittelyssä, mutta tilattomaan palomuurin verrattuna, tilallinen palomuuri voi käyttää myös session tilatietoa apuna, kun se prosessoi paketteja palomuurisäännöstön mukaisesti. (Fortinet, Inc. 2018f.)

Palomuurisäännöt käsitellään palomuurisääntöjen järjestyksen mukaan ylhäältä alaspäin, joten palomuurisääntöjen järjestyksellä on suuri merkitys. Palomuuri vertaa seuraavia paketin tietoja palomuurisäännöstöön: mistä verkkoliitännästä paketti tuli palomuurille, paketin lähdeosoite, kohdeosoite, mihin verkkoliitäntään paketti tulisi reitittää reititystaulun perusteella, mihin kohdeporttiin paketti on lähetetty ja paketin aikaleimaa. Jos palomuurisäännöstöstä löytyy sääntö, joka vastaa paketin tietoja, palomuuri käsittelee paketin palomuurisäännön mukaisesti, eikä seuraavia palomuurisääntöjä käsitellä. (Fortinet, Inc. 2018d.)

Palomuuri suorittaa vain yhden palomuurisäännön per paketti, paketti ei voi osua kahteen palomuurisääntöön. Yleensä palomuurisäännöstön pohjalle on määritelty niin sanottu implisiittinen kieltosääntö, jonka tarkoituksena on hylätä kaikki liikenne, joka ei osu sitä ylempänä oleviin sääntöihin. Tämän vuoksi palomuurisääntöjen järjestykseen tulee kiinnittää erityistä huomiota. Jos esimerkiksi kaiken liikenteen kieltävä palomuurisääntö on vahingossa laitettu säännöstön kärkeen, palomuurisääntöjen käsittely loppuu siihen, koska kaikki liikenne osuu siihen sääntöön. (Fortinet, Inc. 2018d.)

FortiGate palomuurien tietoturvaominaisuudet

FortiGate palomuureille voidaan määrittää tietoturvaprofiileja, joiden perusteella palomuurisäännössä määritellylle verkkoliikenteelle tehdään profiilissa valitut tietoturvaskannaukset. Palomuurin keskeisimmät tietoturvaominaisuudet ovat Antivirus, Application control, Intrusion Prevention System, SSH/SSL Inspection, Web filtering ja Data Leak Prevention. (Fortinet, Inc. 2018e.)

Application control tunnistaa mitä applikaatioita yrityksen verkossa käytetään ja sen avulla voi filtteröidä applikaatioliikennettä. Jos yritys on linjannut, että tiettyjä applikaatioita ei saa käyttää, niiden käyttö voidaan estää application controllilla. (Fortinet, Inc. 2018e.)

Antivirusskanneri tutkii verkkoliikenteen sisältöä, ja pyrkii havaitsemaan virukset, tietokonemadot, troijalaiset ja muut haittaohjelmat. Antivirusskanneri käyttää virustunnistetietokantaa saastuneiden tiedostojen tunnistamiseen. Mikäli se havaitsee tunnisteen tiedoston sisällä, se toteaa tiedoston saastuneeksi ja suorittaa antivirusprofiilissa määritetyt toimenpiteet. (Fortinet, Inc. 2018b.)

Antivirusprofiilissa voidaan konfiguroida virussuojaus päälle HTTP, FTP, IMAP, POP3, SMTP, ja NNTP liikenteelle. Mikäli palomuurilla on SSL/SSH sisällön skannaus ja tarkistus päällä, antivirussuojaus voidaan konfiguroida myös HTTPS, IMAPS, POP3S, SMTPS, ja FTPS liikenteelle. (Fortinet, Inc. 2018a.)

Intrusion Prevention System havaitsee IPS tunnisteiden avulla, jos hyökkääjä yrittää hyväksikäyttää käyttöjärjestelmien ja applikaatioiden tunnettuja tietoturvahaavoittuvuuksia ja estää haitallisen liikenteen. IPS tunnistaa myös, jos saastunut kone yrittää kommunikoida ulospäin. Kuten esimerkiksi tunnetun command-and-control haittaohjelman tapauksessa, missä saastunut kone yrittää hakea C&C palvelimelta toimintaohjeita. (Fortinet, Inc. 2018e.)

SSH/SSL Inspection toiminnallisuutta käytetään salatun liikenteen purkuun, koska ilman sitä palomuuri ei pysty skannaamaan salattua liikennettä. SSL/TLS inspection toimii siten, että palomuuri vastaanottaa päätelaitteelle tarkoitetun salatun liikenteen päätelaitteen puolesta, purkaa salauksen ja skannaa liikenteen kuten tavallisen salaamattoman liikenteen, jonka jälkeen palomuuri salaa liikenteen ja lähettää sen päätelaitteelle. Ennen kuin SSL/SSH inspection keksittiin, selainliikenteen skannaamisen pystyi ohittamaan käyttämällä salattua HTTPS-protokollaa salaamattoman HTTP:n sijaan. (Fortinet, Inc. 2018e.)

Palomuurin Web filtering toiminnallisuus koostuu kolmesta komponentista, FortiGuard Web filteröinti palvelu, URL filteröinti, web sisällön filteröinti. FortiGuard Web filtering palvelun avulla voidaan rajoittaa käyttäjien pääsyä verkkosivustoille. Palvelun avulla on kategorisoitu 60 miljoonaa verkkosivustoa ja 2 miljardia verkkosivua 77:ään eri kategoriaan. URL filteröinnin avulla voit estää tai sallia pääsyn haluttuun URL-osoitteeseen. Web sisällön filteröinnin avulla voit estää pääsyn sivustolle siellä esiintyvien sanojen tai lauseiden perusteella. (Fortinet, Inc. 2018e.)

Data Leak Prevention etsii verkkoliikenteestä tiettyjä datamalleja, ja sillä voidaan estää ennaltamääritetyn datamallin mukaisen tiedon lähettäminen. Datamalliin voidaan määrittää esimerkiksi luottokorttinumeroiden tai henkilötunnusten formaatti. Mikäli verkkoliikenteestä löytyy datamallin mukaista dataa, liikenne estetään, sallitaan tai lokitetaan palomuurisäännön mukaisesti. (Fortinet, Inc. 2018c.)

4 Tietoverkon segmentoinnilla saavutettavat tietoturvahyödyt

Perinteiset tietoverkot ovat suunniteltu estämään lähinnä ulkoisia uhkia ja tietoturvaominaisuudet ovat suunnattu tarkistamaan lähinnä ulkoverkosta sisään tulevaa liikennettä, jonka vuoksi sisäverkon sisällä liikkuvaan liikenteeseen ei välttämättä kiinnitetä juurikaan huomiota. (Sage Data Security 2019.)

Olen tehnyt töitä tietoliikenteen- ja tietoturvan parissa reilut viisi vuotta, ja työni kautta myös tietoverkkojen segmentointi on tullut tutuksi. Kokemukseni mukaan tietoverkon segmentointi on yrityksen tietoverkon tietoturvan kannalta yksi oleellisimmista asioista, ja tietoverkon ensimmäinen puolustuslinja. Palomuuri on tietoturvan kannalta paras tapa toteuttaa tietoverkon segmentointi, jotta segmentoinnista saadaan irti maksimaalinen hyöty. Ilman palomuuria verkkoliikenteen tietoturvaskannaukset ei onnistu, ja pääsynhallinnan toteuttaminen on hankalaa.

Korkean tietoturvan saavuttamiseksi huolellisesti segmentoidun tietoverkon lisäksi tarvitaan myös mahdollisimman tarkasti määritellyt palomuurisäännöt. Palomuurisäännöissä tulisi sallia vain pakolliset yhteydet ja muu verkkoliikenne tulisi estää. Lisäksi palomuurin tulisi tehdä verkkoliikenteelle tietoturvaskannauksia, kuten Antivirus, IPS, Application control yms. Jos hyökkääjä pääsee murtautumaan yrityksen verkkoon, ja yrityksen verkko on segmentoitu ja palomuurin takana, hyökkääjän liikkuminen verkossa hankaloituu huomattavasti.

Segmentoimattomassa verkossa hyökkääjän saastuttama laite pääsee saastuttamaan kaikki verkon koneet vapaasti ilman, että palomuuri pystyy puuttumaan verkkoliikenteeseen. Tämä johtuu siitä, että segmentoimattomassa verkossa kaikki laitteet ovat samassa aliverkossa, jolloin laitteet voivat tavoittaa toisensa suoraan, eikä verkkoliikennettä reititetä palomuurilla, jonka vuoksi palomuuri ei näe verkkoliikennettä eikä siten voi suodattaa sitä. Jos verkko on segmentoitu, ja laitteet ovat eri aliverkoissa, palomuuri reitittää verkkoliikenteen aliverkkojen välillä ja se voi suodattaa liikennettä ja tehdä tietoturvaskannauksia verkkoliikenteelle, jonka avulla haittaliikenne voidaan estää.

Pääsynhallinnan toteuttaminen on helpompaa, kun arkaluontoinen data ja käyttäjät ovat eri verkkosegmenteissä. Käyttäjien pääsyoikeudet dataan voidaan rajata siten, että heillä on pääsy vain heidän tarvitsemaan dataan. (Eric Dosal 2018.)

5 Tietoverkon segmentoinnin suunnittelu ja toteutus

5.1 Kohdeyritys

Tietoverkon segmentoinnin suunnitelman toimeksiantaja o kuvitteellinen suomalainen ohjelmistoalan yritys. Lähtötilanteessa yrityksessä työskenteli 350 henkilöä ja yrityksellä oli yksi toimipiste. Tietoverkon segmentoinnin tavoitteena oli parantaa yrityksen sisäverkon tietoturvaa ja suorituskykyä.

5.2 Lähtötilanteen kartoitus

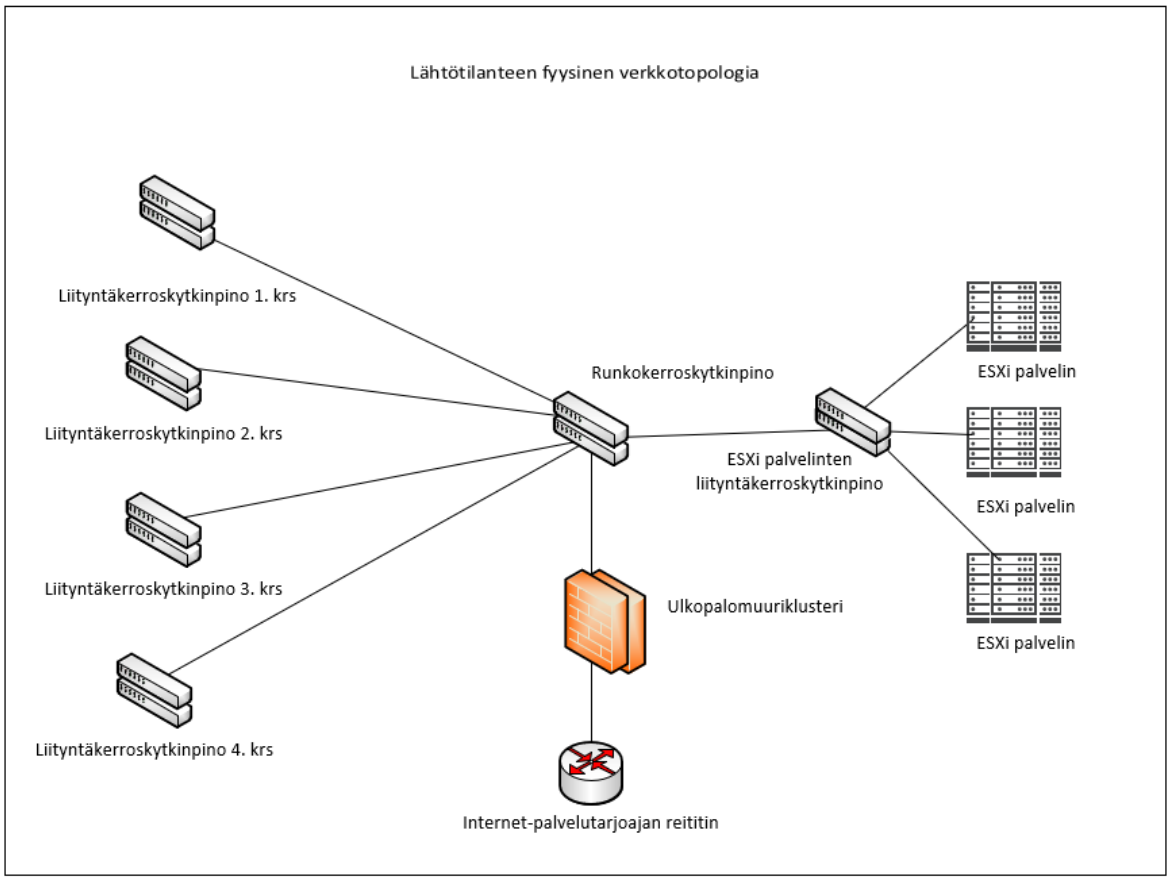
Lähtötilanteen kartoituksen tarkoituksena oli kartoittaa yrityksen sisäverkon nykytila ja arkkitehtuuri. Lähtötilanteessa yrityksen sisäverkko koostui 172.16.0.0/21 yksityisverkosta, joka oli jaettu kolmeen aliverkkoon. Yrityksen sisäverkon arkkitehtuuri oli lähimpänä two-tier collapsed corea, jossa runkokerroskytkin hoitaa myös kolmikerroksisessa mallissa jakelukerroksen laitteelle kuuluvat tehtävät.

Yrityksen sisäverkkoon oli konfiguroitu kolme virtuaalilähiverkkoa, VLAN 10 työasemille, sekä VLAN 20 ja VLAN 21 palvelimille. Virtuaalilähiverkkojen aliverkot on kuvattu taulukossa 1. Yrityksen omassa VMware ESXi-virtualisointiympäristössä oli lähtötilanteessa 500 virtuaalipalvelinta. Palvelin- ja työasemaverkko olivat liian suuria ja niiden sisällä kulki todella paljon broadcast liikennettä, jonka vuoksi verkot tuli jakaa useampaan eri virtuaalilähiverkkoon ja aliverkkoon.

Lähtötilanteen virtuaalilähiverkot ja aliverkot

Taulukko 1. Lähtötilanteen virtuaalilähiverkot ja aliverkot

Virtuaalilähiverkko	**Nimi**	**Aliverkko**	**Käytettävissä olevien IP-osoitteidenmäärä**
VLAN 10	Työasemat	172.16.0.0/23	510
VLAN 20	Palvelimet 1	172.16.4.0/23	510
VLAN 21	Palvelimet 2	172.16.6.0/23	510



Kuva 6. Lähtötilanteen fyysinen verkkotopologia.

Lähtötilanteen fyysiseen topologia koostui Internet-palveluntarjoajan reitittimestä, ulkopalomuuriklusterista, verkkokerroksessa toimivasta runkokerroskytkinpinosta, joka reitittää sisäverkkojen liikenteen, toimipisteen neljästä liityntäkerroskytkinpinosta ja ESXi-palvelinten liityntäkerroskytkinpinosta.

5.3 Yrityksen tarpeiden selvitys

Yrityksen sisäverkko ei lähtötilanteessa täyttänyt yrityksen uudessa tietoturvapolitiikassa määriteltyjä tietoturvavaatimuksia. Tietoturvapolitiikassa määriteltiin, että tietoverkon tulisi olla segmentoitu siten, että tuotanto-, projekti- ja kehitysdata sijaitsevat eri tietoverkoissa. Lisäksi siinä määriteltiin, että sisäverkkojen verkkoliikenteeseen pitää olla näkyvyys ja verkkoliikenteelle pitää tehdä tietoturvaskannauksia, jotta voidaan varmistua siltä, ettei tietoverkkojen välillä kulje haittaliikennettä.

Lähtötilanteessa verkkoliikenteeseen ei ollut näkyvyyttä, koska sisäverkkojen liikenne reititettiin runkokerroskytkimellä, eikä kytkimeltä saatu liikennelokia ulos mielekkäässä muodossa.

Liikennettä ei myöskään rajoitettu sisäverkossa, koska runkokerroskytkimelle ei oltu määritelty pääsylistoja. Tietoturvaskannauksia ei myöskään pystytty toteuttamaan, koska sisäverkkojen liikenne reititettiin runkokerroskytkimellä, ja kytkimet eivät kykene tekemään tietoturvaskannauksia toisin kuin palomuurit.

Tämän vuoksi asiakas määritteli, että sisäverkko tulee segmentoida tarkemmin ja sisäverkon tietoturvaa on parannettava palomuurin avulla. Lisäksi asiakas määritteli, että verkkoliikennettä tulisi voida suodattaa IP-osoitteiden ja protokollaporttien lisäksi myös paketin sisällä olevan sovellusdatan perusteella.

5.4 Tietoverkon segmentoinnissa huomioitavat asiat

Ennen kuin verkkoa lähdettiin segmentoimaan, oli tärkeää kartoittaa mahdollisimman tarkasti, millaisia laitteita verkossa on, mitkä ovat laitteiden käyttötarkoitukset ja kuinka monta laitetta verkkoon tullaan kytkemään. Kun nämä tiedot oli selvitetty, voitiin lähtemään hahmottelemaan kuinka moneen virtuaalilähiverkkoon verkko tulisi jakaa ja minkä kokoisia aliverkkoja tarvitaan. Lisäksi piti päättää millä teknologialla tietoverkon segmentointi toteutetaan ja mitä laitteita tarvitaan.

5.5 Toteutustavan valinta

Tietoverkon segmentoinnin toteutus mikrosegmentoinnilla tulisi kalliiksi, sillä sitä varten jouduttaisiin ostamaan kalliit lisenssit verkkoinfrastruktuurin virtualisoinnin mahdollistavaan teknologiaan kuten esim. VMware NSX, joten päädyttiin VLAN-segmentointiin. Sisäverkon segmentointia varten asennetaan uusi sisäpalomuuriklusteri, joka kytketään runkokerroskytkimiin. Sisäverkon virtuaalilähiverkot määritellään uudelleen ja yrityksen käytössä olevasta 172.16.0.0/21 privaattiverkosta allokoidaan omat aliverkot jokaiselle virtuaalilähiverkolle. Sisäpalomuureille luodaan palomuurisäännöstö, jossa sallitaan vain tarvittavat yhteydet ja muu liikenne estetään.

5.6 Laitteet

Runkokerroskytkimet

Runkokerroskytkinpino koostuu kahdesta Cisco Nexus C36180YC-R kytkimestä. Taulukossa 2 on tietoja kytkimen suoritustehosta ja ominaisuuksista.

Taulukko 2. Cisco Nexus C36180YC-R kytkimen tekniset tiedot (Cisco Systems 2018a)

Kytkinportit	48x 1/10/25G Gigabit Ethernet SFP/SFP+/SFP28, 6x 100 Gigabit Ethernet QSFP28 uplinks
Pakettikytkentäkapasiteetti	3,6 Tbps
Paketin välitysnopeus	1 670 000 000 pakettia sekunnissa
MAC-osoitteiden maksimimäärä	750 000
IPv4 reittien maksimimäärä	256 000
Virtuaalilähiverkkojen maksimimäärä	4096
Muisti	32 Gigatavua
Tallennustila	128 Gigatavua

Tbps = Terabittiä sekunnissa

Palomuurit

Sisä- ja ulkopalomuuriklusterit koostuvat kummatkin kahdesta Fortinet FortiGate 600E palomuurista. Palomuurit ovat seuraavan sukupolven palomuureja, joissa on kattavat UTM (Unified Threat Management) ominaisuudet, kuten Intrusion Protection System(IPS), Antivirus, Application control, Data leak prevention, Web filtering ja SSL/SSH inspection. Taulukossa 3 on tietoja palomuurin suoritustehosta ja ominaisuuksista.

Taulukko 3. Fortinet FortiGate 600E palomuurin tekniset tiedot (Fortinet, Inc. 2019, 5)

Palomuurin IPv4 suoritusteho 1518 / 512 / 64 bitin kokoisilla UDP paketeilla	36 / 36 / 27 Gbps
IPSec VPN suoritusteho 512 bitin paketeilla	20 Gbps
IPS suoritusteho [2]	10 Gbps
NGFW suoritusteho [4]	9,5 Gbps
Threat Protection suoritusteho [5]	7 Gbps
Application Control suoritusteho	15 Gbps
Samanaikaisten TCP sessioiden maksimimäärä	8 000 000
Uusien TCP sessioiden määrä sekunnissa	450 000
Palomuurisääntöjen maksimimäärä	10 000
IPSec VPN tunnelien maksimimäärä	2000
SSL VPN suoritusteho	7 Gbps
SSL VPN samanaikaisten käyttäjien maksimimäärä	10 000
SSL liikenteen purkamisen suoritusteho	8 Gbps
Samanaikaisten sessioiden maksimimäärä missä puretaan SSL liikennettä	800 000
Kytkinportit	2x Gigabit Ethernet RJ45 MGMT/HA, 8x Gigabit Ethernet RJ45, 8x Gigabit Ethernet SFP, 2x 10 Gigabit Ethernet SFP+

Gbps = Gigabittiä sekunnissa

[2] IPS suoritusteho mitataan lokitus päällä.

[4] NGFW suoritusteho mitataan palomuuri, IPS ja Application Control päällä lokituksen kanssa.

[5] Threat Protection suoritusteho mitataan palomuuri, IPS, Application Control ja Malware Protection päällä lokituksen kanssa.

Liityntäkerroskytkimet

Liityntäkerroskytkinpinot koostuvat kolmesta Cisco Catalyst C9200L-48P-4X kytkimestä. Kytkimessä on Power over Ethernet toiminnallisuus, eli se pystyy antamaan virran suoraan kytkinportista langattomille tukiasemille. Tämä helpottaa langattomien tukiasemien käyttöönottoa. Taulukossa 4 on tietoja kytkimen suoritustehosta.

Taulukko 4. Cisco Catalyst C9200L-48P-4X kytkimen tekniset tiedot (Cisco Systems 2019a)

Kytkinportit	48x 10/100/1000 Ethernet RJ45 PoE+, 4x 10 Gigabit Ethernet SFP+ uplinks
Pakettikytkentäkapasiteetti	176 Gbps
Pakettikytkentäkapasiteetti pinottuna	256 Gbps
Paketin välitysnopeus	130 950 000 pakettia sekunnissa
MAC-osoitteiden maksimimäärä	16 000
IPv4 reittien maksimimäärä	11 000
Virtuaalilähiverkkojen maksimimäärä	1024
Muisti	2 Gigatavua
Tallennustila	4 Gigatavua

ESXi-palvelinten liityntäkerroskytkimet

ESXi-palvelinten liityntäkerroskytkinpino koostuu kahdesta Cisco Catalyst C9500-48Y4C kytkimestä. Taulukossa 5 on tietoja kytkimen suoritustehosta ja ominaisuuksista.

Taulukko 5. Cisco Catalyst C9500-48Y4C kytkimen tekniset tiedot (Cisco Systems 2019b)

Kytkinportit	48x 1/10/25G Gigabit Ethernet SFP/SFP+/SFP28 + 4x 40/100G QSFP+/QSFP28 uplinks
Pakettikytkentäkapasiteetti	3,2 Tbps
Paketin välitysnopeus	1 000 000 000 pakettia sekunnissa
MAC-osoitteiden maksimimäärä	82 000
IPv4 reittien maksimimäärä	212 000
Virtuaalilähiverkkojen maksimimäärä	4094
Muisti	16 Gigatavua
Tallennustila	16 Gigatavua

Tbps = Terabittiä sekunnissa

Verkkolaitteiden suorituskyky

Verkkolaitteiden suorituskyky on todella hyvä ja se tulee riittämään vielä moneksi vuodeksi eteenpäin. Kytkinteknologia on ottanut suuria harppauksia viime vuosina ja sen vuoksi päästään todella suuriin pakettikytkentänopeuksiin. Palomuuriteknologia on myös kehittynyt huomattavasti viime vuosina, ja palomuuriklusterien suorituskyky on erittäin hyvä, vaikka käytössä olisi kaikki mahdolliset tietoturvaskannaukset.

5.7 Suunnitelma

Sisäverkon topologiaan lisätään sisäpalomuuriklusteri, sisäpalomuureille määritellään tarvittavat verkkoliitännät, virtuaalilähiverkot ja aliverkot suunnitelman mukaisesti. Samalla sisäverkkojen reititys siirtyy runkokerroskytkimeltä sisäpalomuureille. Yrityksen työasemaverkko jaetaan kahteen virtuaalilähiverkkoon, VLAN 10 ja VLAN 11, joille määritellään /24 prefiksin aliverkot, joissa niissä on 254 käytettävää IP-osoitetta. Kun työasemaverkko jaetaan kahteen erilliseen virtuaalilähiverkkoon, broadcast liikenne saadaan jaettua kahteen eri verkkoon ja verkon suorituskyky paranee.

Palvelinverkot ovat suuria, ja sen vuoksi niissä liikkuu paljon broadcast liikennettä, joten palvelinverkot pitää jakaa useampaan pienempään aliverkkoon. Lähtötilanteessa liikennettä ei rajoitettu mitenkään sisäverkkojen välillä, koska liikenne reititettiin runkokerroskytkimellä ja sinne ei oltu määritelty pääsynhallintalistoja. Mahdollisimman tarkan pääsynhallinnan saavuttamiseksi, ja jotta verkkojen broadcast liikenteen määrä saadaan järkevälle tasolle, palvelinverkot jaetaan 11:een eri virtuaalilähiverkkoon. VLAN 20 sisäisiä palveluja, kuten Active Directory, DNS yms. tuottaville palvelimille, VLAN 21 ja 22 tuotantopalvelimille, VLAN 23, 24, 25 ja 26 kehityspalvelimille, VLAN 27 ja 28 projektipalvelimille ja VLAN 29 ja 30 sisäisille kehityspalvelimille.

Uusien virtuaalilähiverkkojen aliverkot ovat kuvattu taulukossa 6. Ennen palomuurisääntöjen luomista selvitetään yrityksen IT-osaston kanssa mitä yhteyksiä pitää sallia eri järjestelmien välillä ja samalla päätetään mitä tietoturvaominaisuuksia sisäpalomuurilla otetaan käyttöön.

Uudet virtuaalilähiverkot ja aliverkot

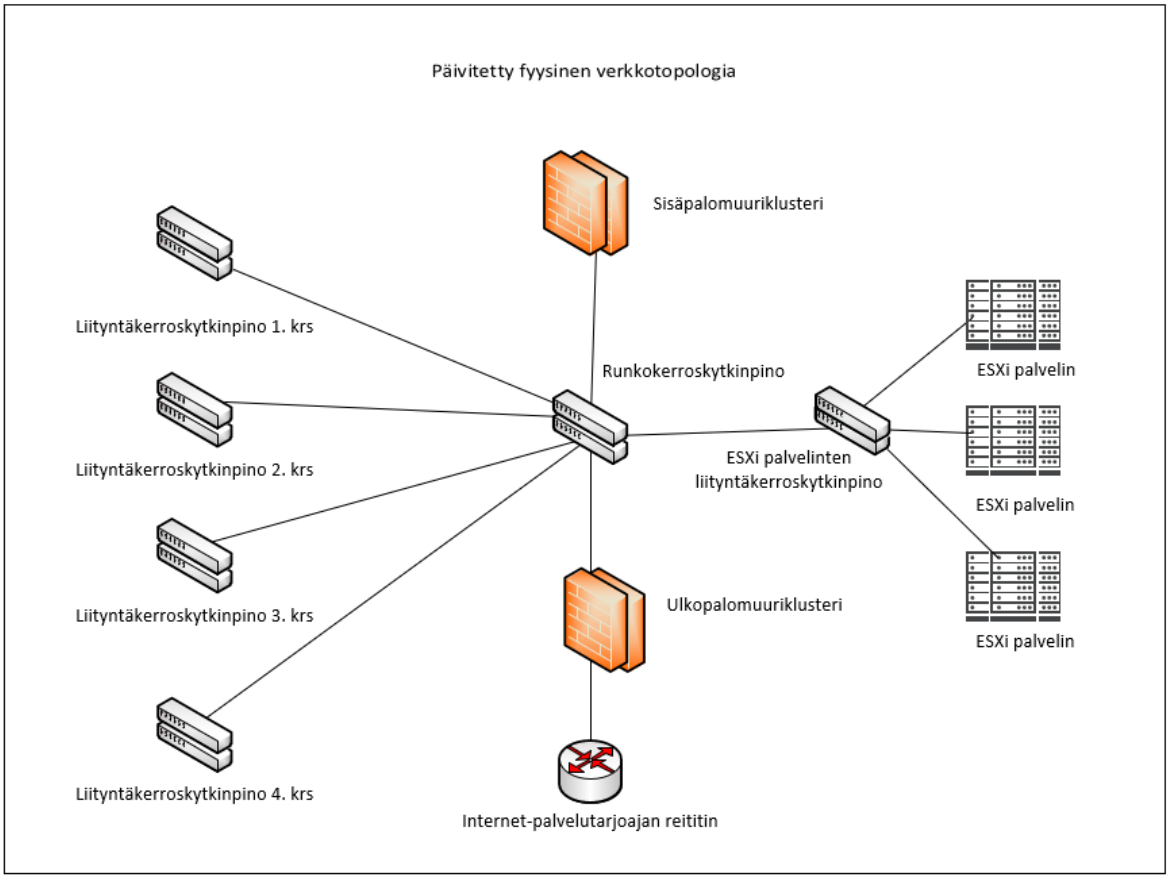
Taulukko 6. Uudet virtuaalilähiverkot ja aliverkot.

Virtuaalilähiverkko	Kuvaus	Aliverkko	Käytettävissä olevien IP-osoitteidenmäärä
VLAN 10	Työasemaverkko 1	172.16.0.0/24	254
VLAN 11	Työasemaverkko 2	172.16.1.0/24	254
VLAN 20	Sisäiset palvelut	172.16.2.0/27	30
VLAN 21	Tuotantopalvelimet 1	172.16.3.0/27	30
VLAN 22	Tuotantopalvelimet 2	172.16.3.32/27	30
VLAN 23	Kehityspalvelimet 1	172.16.4.0/26	62
VLAN 24	Kehityspalvelimet 2	172.16.4.64/27	30
VLAN 25	Kehityspalvelimet 3	172.16.4.96/27	30
VLAN 26	Kehityspalvelimet 4	172.16.4.128/27	30
VLAN 27	Projektipalvelimet 1	172.16.5.0/27	30
VLAN 28	Projektipalvelimet 2	172.16.5.64/27	30
VLAN 29	Sisäiset kehityspalvelimet 1	172.16.6.0/27	30
VLAN 30	Sisäiset kehityspalvelimet 2	172.16.6.64/27	30

5.8 Toteutus

Yrityksen sisäverkkoon asennetaan uusi sisäpalomuuriklusteri. Sisäpalomuureille konfiguroidaan uudet verkkoliitännät, sekä virtuaalilähiverkot ja aliverkot taulukon 6 mukaisesti. Uudet virtuaalilähiverkot konfiguroidaan myös runkokerroskytkimille, liityntäkerroskytkimille ja ESXi-palvelinten liityntäkerroskytkimille.

Sisäpalomuureille luodaan palomuurisäännöstö aiemmin tehdyn selvityksen perusteella, jossa kartoitettiin järjestelmien välille tarvittavat yhteydet. Palomuurisääntöihin konfiguroidaan aiemman selvityksen perusteella Intrusion Protection System, Antivirus, Application Control, Web Filtering ja SSL/SSH Inspection tietoturvaominaisuudet. Päivitetty fyysinen verkkotopologia löytyy kuvasta 7.



Kuva 7. Päivitetty fyysinen verkkotopologia

5.9 Tulokset

Suunnitelman toteutuksen myötä yrityksen sisäverkkoon konfiguroitiin 13 uutta aliverkkoa ja virtuaalilähiverkkoa. Työasemaverkko jaettiin kahteen uuteen virtuaalilähiverkkoon, VLAN 10, jonka aliverkko on 172.16.0.0/24 ja VLAN 11, jonka aliverkko on 172.16.1.0/24. Palvelinverkon kaksi alkuperäistä verkkoa poistettiin ja niiden tilalle luotiin 11 uutta aliverkkoa ja virtuaalilähiverkkoa käyttötarkoitusten perusteella. Sisäisille palveluille 1 aliverkko ja virtuaalilähiverkko, tuotantopalvelimille 2 aliverkkoa ja virtuaalilähiverkkoa, kehityspalvelimille 4 aliverkkoa ja virtuaalilähiverkkoa, projektipalvelimille 2 aliverkkoa ja virtuaalilähiverkkoa ja sisäisille tuotantopalvelimille 2 aliverkkoa ja virtuaalilähiverkkoa. Sisäverkon broadcast liikenne jakautuu nyt 13:n verkon kesken lähtötilanteen 3:n verkon sijaan, joka on huomattava parannus. Yrityksen sisäverkko vastaa nyt yrityksen uuden tietoturvapolitiikan vaatimuksia ja verkon tietoturva on moninkertaisesti parempi lähtötilanteeseen verrattuna. Segmentointiprojekti oli yrityksen johdon mielestä varsin onnistunut.

6 Yhteenveto

Verkon segmentoinnin suunnitelmaa tehdessäni lähestyin asiaa tietoturvanäkökulma edellä ja pyrin soveltamaan verkon segmentoinnin parhaita käytäntöjä. Pyrin luomaan kuvitteellisen yrityksen tietoverkon lähtötilanteen siten, että se on uskottava ja täysin mahdollinen tosielämässäkin. Tavoitteena oli luoda mahdollisimman tarkkaan segmentoitu sisäverkko, jotta segmentoinnista saadaan maksimaalinen hyöty irti ja, että aliverkkojen välistä liikennettä voidaan suodattaa palomuurilla mahdollisimman tarkasti.

Vaikka opinnäytetyöhöni ei kuulunut varsinaista laitteiden konfigurointia tai labraympäristön pystyttämistä, aihe ja verkkolaitteet, joilla verkon segmentointi toteutettiin, ovat minulle erittäin tuttuja työtehtävieni kautta. En koe, että labraympäristön pystyttämisestä tai laitteiden konfiguroinnista olisi ollut hyötyä, koska opinnäytetyö keskittyi verkon segmentoinnin suunnitelman luomiseen ja toteuttamiseen, eikä laitteiden käyttöönottoon tms.

Suunnitelman luominen ja toteuttaminen onnistui mielestäni kohtalaisen hyvin, ja yrityksen sisäverkko saatiin segmentoitua perusteellisesti. Sisäverkon aliverkkojen ja virtuaalilähiverkkojen määrä kasvoi 3:sta 13:een ja sen myötä sisäverkon broadcast liikenne saatiin jaettua uusien verkkojen kesken, joka on suuri parannus lähtötilanteeseen. Myös verkon tietoturvaan tuli huomattava parannus. Sisäverkkojen liikenne reititetään nyt sisäpalomuuriklusterilla, ja sen myötä verkkoliikenteeseen on täysi näkyvyys, sitä voidaan suodattaa tehokkaasti ja hyödyntää seuraavan sukupolven palomuurien tietoturvaominaisuuksia.

Yrityksen sisäverkon tietoturva parantui erittäin paljon ja nyt se täyttää yrityksen uuden tietoturvapolitiikan vaatimukset.

Johtopäätökset

Tietoverkkojen segmentointi on erittäin tärkeä osa tietoverkon tietoturvaa, ja sen merkitys korostuu nykypäivänä tietomurtojen yleistyessä. Segmentoimaton verkko on suuri tietoturvariski, ja otollinen ympäristö tietomurroille. Tietoverkon segmentoinnilla saadaan pienennettyä tietomurtojen vaikutusta merkittävästi ja parhaimmillaan, tarpeeksi tiukoilla palomuurisäännöillä, hienojakoisella segmentoinnilla ja tunnettujen tietoturvahaavoittuvuuksien paikkauksilla ne voidaan saada estettyä jopa kokonaan.

Tietoverkon segmentoinnin laiminlyönti on tullut kalliiksi tietomurtojen kohteeksi joutuneille yrityksille, jotka ovat joutuneet maksamaan jopa satoja miljoonia vahingonkorvauksina.

Mikäli verkkoa ei olla segmentoitu, käytettävissä olevat keinot tietoturvan koventamiseen vähenevät huomattavasti, sillä mm. palomuurit eivät pysty toimimaan tehokkaasti, jos verkkoa ei ole segmentoitu.

Yritysten tulisi siis ensin viedä läpi verkon segmentointiprojekti, jonka jälkeen voidaan alkaa rakentamaan tietoturvaa pidemmälle muilla keinoilla.

Kehittämisehdotukset

IP-osoitesuunnitelman luominen IPv6-osoitteille olisi luontainen jatkumo, koska IPv6:n käyttöönotto yleistyy jatkuvasti. Nyt kun virtuaalilähiverkot ovat jo tehty, uuden IP-osoitesuunnitelman tekeminen olisi helposti toteutettavissa.

Oppiminen ja ammatillinen kehitys

Opinnäytetyötä tehdessäni opin uusia asioita tietoverkon segmentoimisesta, sillä luin runsaasti lähdemateriaalia, jossa käsiteltiin tietoverkon segmentointia monipuolisesti. Opin uusia asioita aiheesta myös työni kautta sen takia, että työpaikallani on meneillään tietoverkon segmentointiprojekti, jossa minä olen päävastuullinen. Opinnäytetyön tekemisen kautta pystyin tarkastelemaan myös työpaikalla meneillään olevaa projektia eri näkökulmista ja peilaamaan sitä opinnäytetyössä tehtyyn segmentointisuunnitelmaan.

7 Lähteet

Bradley Mitchell 2018. IP: Classes, Broadcast, and Multicast. Luettavissa: https://www.lifewire.com/internet-protocol-tutorial-address-4057461. Luettu: 18.5.2019.

Cisco Systems 2004. CCNP 1: Advanced IP Addressing Management. Luettavissa: http://www.ciscopress.com/articles/article.asp?p=330807&seqNum=3. Luettu: 18.5.2019.

Cisco Systems 2019a. Cisco Catalyst 9200 Series Switches Data Sheet. Luettavissa: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html#FeaturesandBenefits. Luettu: 4.5.2019.

Cisco Systems 2019b. Cisco Catalyst 9500 Series Switches Data Sheet. Luettavissa: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/data_sheet-c78-738978.html. Luettu: 8.5.2019.

Cisco Press 2014a. Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design. Luettavissa: http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4. Luettu: 5.4.2019.

Cisco Press 2014b. Cisco Networking Academy's Introduction to VLANs. Luettavissa: http://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=4. Luettu: 1.3.2019.

Cisco Systems 2018a. Cisco Nexus C36180YC-R Switch Data Sheet. Luettavissa: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-3000-series-switches/datasheet-c78-739189.html. Luettu: 4.5.2019.

Cisco Systems 2018b. Configuring IPv4 Addresses. Luettavissa: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_ipv4/configuration/xe-3s/ipv4-xe-3s-book/configuring_ipv4_addresses.html. Luettu: 3.5.2019.

Cisco Systems 2019d. Configuring Static Routing. Luettavissa: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/unicast/503_u1_2/nexus3000_unicast_config_gd_503_u1_2/l3_route.html. Luettu: 23.4.2019.

Cisco Systems 2018c. Understanding and Configuring VLANs. Luettavissa: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html. Luettu: 2.5.2019.

Edrawsoft 2019. Hierarchical Network Design - Access Layer of the Hierarchical Network Design Model. Luettavissa: https://www.edrawsoft.com/Hierarchical-Network-Design.php. Luettu: 1.4.2019.

Eric Dosal 2018. 4 Security Benefits of Network Segmentation. Luettavissa: https://www.compuquip.com/blog/4-security-benefits-of-network-segmentation. Luettu: 24.4.2019.

etutorials 2019. Chapter 10. LAN Switched Network Design Flat Network Topology. Luettavissa: http://etutorials.org/Networking/Lan+switching+first-step/Chapter+10.+LAN+Switched+Network+Design/Flat+Network+Topology/ Luettu: 6.4.2019.

Forcepoint 2019. What is a Firewall? Firewalls Defined, Explained, and Explored. Luettavissa: https://www.forcepoint.com/cyber-edu/firewall. Luettu: 14.3.2019.

Fortinet, Inc. 2018a. AntiVirus. Luettavissa: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Antivirus/antivirus_chapter.htm. Luettu: 6.5.2019.

Fortinet, Inc. 2018b. Antivirus concepts. Luettavissa: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Antivirus/Antivirus%20concepts.htm. Luettu 21.5.2019.

Fortinet, Inc. 2018c. Data leak prevention concepts. Luettavissa: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/DLP/Data%20leak%20prevention%20concepts.htm. Luettu: 6.5.2019.

Fortinet, Inc. 2019. DATA SHEET FortiGate® 600E Series. Luettavissa: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf. Luettu: 6.5.2019.

Fortinet, Inc. 2018d. Policy order. Luettavissa: https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-firewall-52/Security%20Policies/Policy%20order.htm. Luettu: 17.5.2019.

Fortinet, Inc. 2018e. Security Profiles overview. Luettavissa: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Overview/overview_chapter.htm. Luettu: 12.5.2019.

Fortinet, Inc. 2018f. What is a Firewall? Luettavissa: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Concepts/What%20is%20a%20Firewall.htm. Luettu: 15.4.2019.

Gary Glover 2017. How Does Network Segmentation Affect PCI Scope? Luettavissa: https://www.securitymetrics.com/blog/how-does-network-segmentation-affect-pci-scope. Luettu: 29.4.2019.

Geek University 2019a. What is a network hub? Luettavissa: https://geek-university.com/ccna/what-is-a-network-hub/ Luettu: 1.3.2019.

Geek University 2019b. What is a network switch? Luettavissa: https://geek-university.com/ccna/what-is-a-network-switch/ Luettu: 13.3.2019.

Juniper Networks 2019. Understanding IPv6. Luettavissa: https://www.juniper.net/documentation/en_US/junos/topics/concept/ipv6-technology-overview.html. Luettu: 4.5.2019.

Juniper Networks 2014. IP Addressing Overview. Luettavissa: https://www.juniper.net/documentation/en_US/junose15.1/topics/concept/ip-addressing-overview.html. Luettu: 2.5.2019.

Justin Ellingwood 2014. Luettavissa: https://www.digitalocean.com/community/tutorials/understanding-ip-addresses-subnets-and-cidr-notation-for-networking. Luettu: 19.5.2019.

Kevin McCoy 2017. Target to pay $18.5M for 2013 data breach that affected 41 million consumers. Luettavissa: https://eu.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/ Luettu: 1.5.2019.

Marcin Bialy 2018. How does a switch work? Luettavissa: https://www.grandmetric.com/blog/2018/03/08/how-does-switch-work-2/ Luettu: 7.5.2019.

Omnisecu.com 2019. Cisco Three Layer / Three-tier Hierarchical Network Model. Luettavissa: http://www.omnisecu.com/cisco-certified-network-associate-ccna/three-tier-hierarchical-network-model.php. Luettu: 24.4.2019.

René Molenaar 2019. Luettavissa: https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/broadcast-domain. Luettu: 4.3.2019.

RIPE NCC 2014. Understanding IP Addressing and CIDR Charts. Luettavissa: https://www.ripe.net/about-us/press-centre/understanding-ip-addressing. Luettu: 20.5.2019.

Sage Data Security. The Security Benefits of Network Segmentation. Luettavissa: https://www.sagedatasecurity.com/blog/the-security-benefits-of-network-segmentation. Luettu: 6.4.2019.

study-ccna.com 2019a. ARP (Address Resolution Protocol) explained. Luettavissa: https://study-ccna.com/arp/ Luettu: 6.3.2019.

study-ccna.com 2019b. Network devices. Luettavissa: https://study-ccna.com/network-devices/ Luettu: 6.5.2019.

Test King 2019. Explain Network Segmentation and Basic Traffic Management Concepts Luettavissa: https://www.test-king.com/guide-explain-network-segmentation-and-basic-traffic-management-concepts.htm. Luettu: 3.4.2019.

Trevor Pott 2017. Microsegmentation Is the Future. Luettavissa: https://virtualizationreview.com/articles/2017/06/28/microsegmentation-is-the-future.aspx. Luettu: 5.4.2019.

Tutorialspoint 2019. Network Security – Firewalls. Luettavissa: https://www.tutorialspoint.com/network_security/network_security_firewalls.htm. Luettu: 23.4.2019.

VMware, Inc. 2019. Luettavissa: https://www.vmware.com/topics/glossary/content/micro-segmentation. Luettu: 1.4.2019.