SAVONIA

OPINNÄYTETYÖ - AMMATTIKORKEAKOULUTUTKINTO
TEKNIIKAN JA LIIKENTEEN ALA

YRITYKSEN SISÄVERKON LAITTEIDEN UUDISTAMINEN

TEKIJÄ/T: Janne Halonen

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Tutkinto-ohjelma Tietotekniikan tutkinto-ohjelma	
Työn tekijä(t) Janne Halonen	
Työn nimi Yrityksen sisäverkon laitteiden uudistaminen	
Päiväys 26.9.2021	Sivumäärä/Liitteet 20
Toimeksiantaja/Yhteistyökumppani(t) ITC-Solution Group Oy	

Tiivistelmä

Opinnäytetyöni oli projektityö, jossa toteutettiin uusi sisäverkko ITC-Solution Group Oy:lle. Työ toteutettiin Fortinetin laiteratkaisuilla. Yritys halusi yhtenäistää ja modernisoida laitekantaansa ja tarjota jatkossa asiakkailleen pääasiassa Fortinetin verkkoratkaisuja. Myös yrityksen tietoturvaa pyrittiin parantamaan modernimmilla ratkaisuilla. Työtä tullaan käyttämään tarjottavien verkkoratkaisujen esittelyssä asiakkaille.

Työssä uusittiin Kuopion toimitiloihin palomuuri, yksi kytkin sekä kaksi langatonta tukiasemaa. Iisalmen ja Viitasaaren toimipisteille uusittiin palomuurit. Lisäksi yrityksen VPN-yhteydet suunniteltiin ja toteutettiin uudelleen.

Työn tuloksena yritys sai toimivat ja tietoturvalliset laiteratkaisut. Työn avulla asiakkaille voidaan helpommin esitellä ja tarjota verkkoratkaisuja, jotka on toteutettu kokonaan Fortinetin tuotteilla. Jatkokehityksenä palomuurilaitteet voitaisiin kahdentaa, jotta yhteydet olisivat entistä vakaammat.

Avainsanat
Palomuurit, kytkimet, tukiasemat ja VPN

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport	
Degree Programme Degree Programme in Information Technology	
Author(s) Janne Halonen	
Title of Thesis Renewal of Internal Network Equipment	
Date 26.9.2021	Pages/Appendices 20
Client Organisation /Partners ITC-Solution Group Oy	

Abstract

My thesis was carried out in a project commissioned by ITC-Solution Group Oy. The goal of the thesis was to replace the company's internal network equipment with modern solutions made by Fortinet. The company wanted to unify and renew their old network devices. The goal was also to get to know Fortinet's devices better so they can be offered for the company's customers.

In the project the firewall, one switch and two wireless access points were renewed at the company's premises in Kuopio. At Iisalmi and Viitasaari premises the firewalls were replaced. The company's remote connections were redesigned and implanted to the firewalls.

As a result, the company has now working and secure network equipment solutions. The result of this thesis will be used to introduce the company's customers to Fortinet devices and offer these devices as a network solution. This project could be continued by duplicating all the firewall devices to minimize downtime.

Keywords
Firewalls, switches, access points and VPN

ESIPUHE

Tahdon kiittää ITC-Solution Group Oy:tä opinnäytetyön aiheesta sekä avustta sen toteutuksessa. ITC-Solution Groupilta tahdon antaa erityiskiitokset Petri Hyväriselle työssä tukemisesta sekä opinnäytetyön aiheen tarjoamisesta. Kiitokset myös Savonian opettajalle Veijo Pitkäselle oppitunneista, jotka saivat kiinnostuksen heräämään verkkolaitteisiin.

Kuopiossa 26.9.2021
Janne Halonen

SISÄLTÖ

KUVALUETTELO

LYHENTEET JA MÄÄRITELMÄT

Palomuuri	Verkkolaite, jonka tarkoitus on estää pääsy verkosta toiseen
Kytkin	Verkkolaite, joka yhdistää pakettikytkentäisen verkon osia
Tukiasema	Verkkolaite, joka yhdistää langattomat verkkolaitteet kiinteään verkkoon
VPN	Virtual Private Network, muodostaa näennäisen suojatun lähiverkon laitteiden välille julkisen verkon yli
IPsec	Internet Protocol Security, joukko prokollia, jotka määrittävät verkkoliikenteen salauksen laitteiden välillä
SSL	Secure Sockets Layer, liikenteen salauksessa käytetty protokolla
PoE	Power over Ethernet, virransyöttö verkkojohtoa pitkin
Firmware	Laitteen perustoiminnoista huolehtiva ohjelma
LDAP	Lightweight Directory Access Protocol, avoimen lähdekoodin protokolla tunnistautumista varten
LAN	Local Area Network, Lähiverkko
VLAN	Virtual Local Area Network, Virtuaalinen lähiverkko
WAN	Wide Area Network, laajoja maantieteellisia alueita peittävä verkko
OSI	Open Systems Interconnection, seitsenkerroksinen malli tiedonsiirtoprotokollista
DHCP	Dynamic Host Configuration Protocol, protokolla, jonka tarkoituksena on jakaa IP-osoitteita tietoverkon laitteille
Domain	Verkkotunnus. Kirjaimista koostuva nimi, joka yhdistetään IP-osoitteeseen
DNS	Domain Name System, järjestelmä, joka muuntaa verkkotunnukset IP-osoitteiksi
Powershell	Microsoftin kehitämä Windowsin ohjelma käyttöjärjestelmän konfigurointiin ja hallintaan skripteillä
ACME	Automated Certificate Management Enviroment, sertifikaatian automaattiseen luontiin käytettävä protokolla

1 JOHDANTO

Opinnäytetyö käsittelee Fortinetin Fortigate, Fortiswitch ja FortiAP laitteiden konfigurointia. Työssä käsitellään myös etäyhteyksien konfigurointia Fortigate-palomuuriin ja etäyhteyksien merkitystä yritykselle. Tässä dokumentissa kuvataan työn vaiheita sekä syitä valittujen tekniikoiden käyttämiseen sekä esitellään ITC-Solution Group Oy:lla käytössä olevia Fortinetin laitteita. Työ toteutettiin projektityönä yhdessä yrityksen kanssa.

Opinnäytetyön tarkoituksena on uudistaa ITC-Solution Group Oy:lle heidän tietoverkkolaitteensa Fortinet-valmistajan laitteilla. Jokaisen toimipisteen palomuurit alkoivat olla vanhoja ja jokaisella toimipisteellä oli erilaiset laitteet. Yrityksen jokaiselle toimipisteelle uusittiin palomuurit uusiin Fortigate 40F-palomuureihin. Lisäksi Kuopion toimipisteelle vaihdettiin uudet Wi-Fi 6-tekniikkaa tukevat FortiAP 231F-tukiasemat vanhojen Ubiquity-tukiasemien tilalle ja lisättiin yksi uusi Fortiswitch-kytkin olemassa olevien kytkinten rinnalle. Vanhat palomuurit Iisalmessa ja Kuopiossa ovat olleet Sonicwall-valmistajan ja Viitasaarella Ubiquityn.

Opinnäytetyö toteutettiin ITC-Solution Group Oy:n tarpeesta. Palomuurien vaihdolla pyritään yhtenäistämään yrityksen laitekantaa toimipisteiden välillä ja parantamaan etäyhteyksiä ja langatonta verkkoa. Aiemmin jokaisella toimipisteellä on ollut erilaiset laitteet. Tukiasemien vaihdolla pyritään parantamaan langattomia yhteyksiä Kuopion toimitiloissa. Aiemmilla laitteilla langattomat yhteydet ovat olleet heikot eivätkä yhteydet aina ole toimineet ollenkaan.

Asiakkailleen yritys tarjoaa myös jatkossa ainoastaan Fortinetin verkkolaitteita ja yritys haluaakin myös omien laitteidensa olevan samoja kuin asiakkaille tarjottavat laitteet. Työtä tullaan käyttämään apuna Fortinetin verkkolaiteratkaisujen esittelyssä ja tarjoamisessa asiakkaille. ITC-Solution Group Oy näki työn tarpeellisena myös oppimisen kannalta sillä entuudestaan Fortinetin tuotteista ei yrityksellä ollut juurikaan kokemusta.

2 VERKKOLAITTEET

2.1 Fortinet valmistajana

Fortinet on yhdysvaltalainen verkkolaitteiden ja kyberturvallisuustuotteiden valmistaja. Fortinet valmistaa sekä fyysisiä että virtuaalisia palomuureja. Yritys aloittikin toimintansa valmistamalla pääosin fyysisiä palomuureja. Palomuureihin on saatavilla VPN-yhteyksiä varten Forticlient VPN-ohjelmisto, jonka avulla etäkäyttäjät voivat käyttää sisäverkon resursseja etänä. Nykyisin tuotteisiin kuuluu lisäksi kytkimiä, langattomia tukiasemia sekä erinäisiä pilvipalveluita omien laitteidensa hallintaan. Kyberturvallisuuteen liittyviä tuotteita palomuurien lisäksi ovat DDoS-hyökkäysten estoon liittyvät palvelut, sähköpostin suojaukseen liittyvät palvelut sekä identiteetin ja pääsynhallintaan liittyvät ratkaisut. Yritys päätyi valitsemaan Fortinetin laitteet, koska Fortinet tarjoaa laitteleen hyvän tuen Yritys päätyi valitsemaan Fortinetin laitteet, koska Fortinet tarjoaa monipuolisia helposti hallittavia kokonaisuuksia. Lisäksi Fortinetin laitteiden ominaisuudet koettiin sopiviksi yrityksen sekä asiakkaiden ympäristöihin.

2.2 Fortigate

Fortigate on Fortinetin pääasiallinen tuote. ITC-Solution Group valitsi palomuurikseen Fortigate 40F-palomuurin. Uusi palomuuri korvasi vanhan Soniwall TZ200-palomuurin. 40F-palomuurissa on oletuksena yksi WAN-portti, yksi portti Fortiswitch-kytkintä varten, sekä kolme normaalia LAN-porttia. Portteja kuitenkin voi muuttaa tarpeen tullen erilaisiksi. Lisäksi laitteessa on console-portti hallintaa varten.

Fortigate-palomuureja on mahdollisuus hallita sekä graafisen käyttöliittymän että komentokehotteen kautta. Työssä jouduttiin käyttämään molempia tekniikoita laitteen hallintaan. Lisäksi palomuurin hallintaan voidaan käyttää Forticloud-pilvipalvelua, jolla palomuuria pääsee hallitsemaan myös etänä. Forticloud tulee rekisteröidä laitteeseen erikseen, jonka jälkeen laitteeseen voi ottaa etäyhteyden Forticloudista. Sekä pilvestä että paikallisesti palomuuriin voi syöttää myös graafisen käyttöliittymän kautta komentokehotteen komentoja. Pelkkää komentokehotetta pystytään käyttämään laitteessa olevan console-portin kautta ottamalla yhteys esimerkiksi Teraterm-ohjelmalla. Lisäksi komentokehotetta voidaan käyttää ottamalla palomuuriin SSH-yhteys, joka sisäverkon puolelta on oletuksena päällä.

2.2.1 Palomuurin määritykset

Ennen työn aloitusta tutkittiin yrityksen dokumentointia vanhasta palomuurista. Vanhasta palomuurista selvitettiin tarvittavat tiedot IPsec VPN-yhteyksien muodostamista varten Iisalmeen ja Viitasaarelle, sisä- ja ulkoverkon IP-osoitteet, tiedot LDAP-tunnistautumista varten sekä palomuurin säännöt. Myös palomuurin firmware päivitettiin uusimpaan versioon ennen asetusten muutoksia. Työn kirjoitushetkellä uusin firmwaren versio on FortiOS 7.0.1.

Palomuuriin määritettiin sisäverkon ja ulkoverkon osoitteet sekä staattinen reititys ulkoverkkoon. Staattinen reitti määritettiin verkkoon 0.0.0.0/0.Täten liikennöinti kaikkiin osoitteisiin joita ei löydy palomuurin reititystaulukosta ohjataan ulos portista WAN1. Sisäverkkoon määritettiin kuuluviksi palomuurin portit 1–3. Palomuurin määritettiin myös tietyt osoitealueet joista palomuurin hallintaan

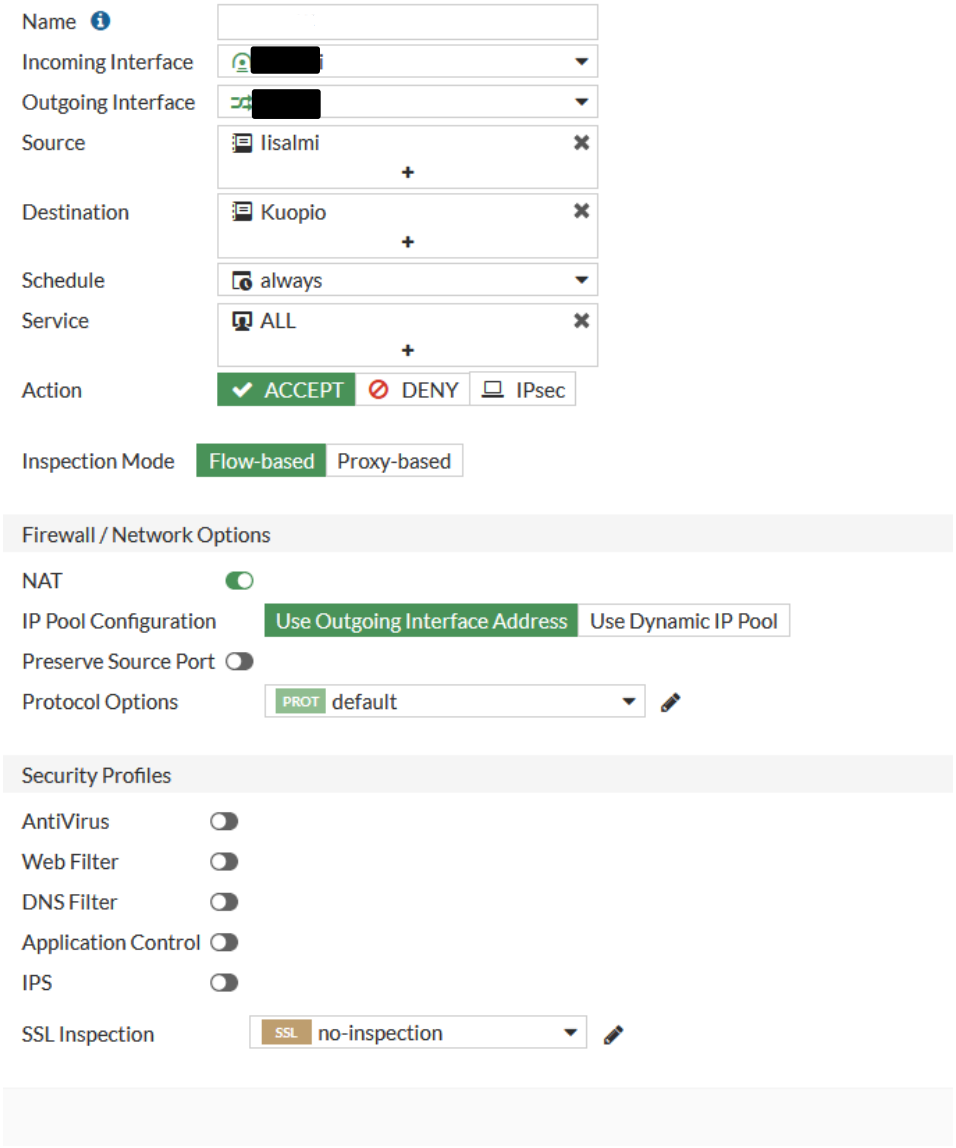
pääsee. Palomuuriin sallittiin pääsy sisäverkon osoitteista sekä toimiston langattomasta verkosta. Muista osoitteista saapuvat yhteydet on estetty. DNS-palvelimiksi määritettiin sisäverkossa toimivat palvelimet.

2.2.2 Palomuurin säännöt

Palomuurin sääntöjen selkeyttämistä varten palomuuriin luotiin osoitealueille nimet. Osoitealueet nimettiin toimipisteiden mukaan: Kuopio, Iisalmi ja Viitasaari. Liikennöinti sallittiin Iisalmesta ja Viitasaarelta VPN-tunnelin kautta sekä Kuopiosta takaisin Iisalmeen ja Viitasaarelle. Toimiston langattomasta verkosta sallittiin yhteydet sisäverkkoon ja ulkoverkkoon. Langattomista verkoista Vieras ja shop pääsy sallittiin vain ulkoverkkoon. Sisäverkon osoitteista pääsy ulkoverkon kaikkiin osoitteisiin on oletuksena sallittu eikä tätä asetusta nähty tarpeelliseksi muuttaa. Kaikki muu liikenne, jota ei ole erikseen sallittu on oletuksena palomuurissa estetty.

TAULUKKO 1. Palomuurin säännöt

Säännön nimi	Lähde	Kohde	Toiminto
VLAN1toWAN	VLAN1	WAN	Sallittu
IisalmitoKuopio	Iisalmi	Kuopio	Sallittu
vierastoWAN	ITC Vieras WLAN	WAN	Sallittu
ITCWLANtoWAN	ITC WLAN	WAN	Sallittu
KuopiotoIisalmi	Kuopio	Iisalmi	Sallittu
KuopiotoViitasaari	Kuopio	Viitasaari	Sallittu
shoptoWAN	Shop WLAN	WAN	Sallittu
VPN	SSLVPN	Kuopio	Sallittu
ViitasaaritoKuopio	Viitasaari	Kuopio	Sallittu



Kuva 1. Esimerkki palomuurin säännön luomisesta

Palomuurin säännön määrityksissä määritetään portti, johon liikenne saapuu sekä portti, josta liikenne poistuu. Tämän lisäksi määritetään IP-osoite tai aliverkko, josta liikenne saapuu sekä IP-osoite tai aliverkko, johon liikenteen on määrä kulkea. Säännöille voidaan lisäksi määrittää aikataulu. Sääntöjen määrityksiin voidaan myös lisätä mitkä palvelut saavat säännön läpi kulkea tai mitkä estetään. Sääntöihin myös määritetään käyttävätkö nämä NAT:ia vai eivät.

2.2.3 Palomuurin vaihto

Palomuurin vaihtoa varten sovittiin yrityksen sisäisesti 15 minuutin käyttökatko. Vaihdon yhteydessä vanha palomuuri purettiin kytkentäkaapista. Uuteen palomuurin kytkennät tehtiin vastaaviin portteihin kuin vanhassa laitteessa. Palomuurin vaihdon jälkeen yhteydet toimipisteiden välillä testattiin ja viat yhteyksissä korjattiin. Vaihdon yhteydessä ilmenneitä vikoja oli palomuurin liian tiukoissa säännöissä, sekä Iisalmen suuntaan olevassa VPN-tunnelissa.

2.3 Fortiswitch

Fortiswitch on Fortinetin kytkinratkaisu. Kytkimiä on tarjolla OSI Layer 2 tai Layer 3 tasoisina. Myös PoE-virransyötöllisiä kytkimiä on tarjolla. Kytkimeksi verkonpäivitykseen valittiin Fortiswitch 108E-POE. Kytkimen tarkoituksena on syöttää virtaa langattomille tukiasemille. Kytkimessä on kahdeksan PoE-virransyötöllistä porttia ja lisäksi kaksi SFP-porttia. 8-porttinen kytkin riittää nykyisellään ja myös tulevaisuudessa yrityksen tukiasemille hyvin, joten isomman kytkimen hankintaa ei nähty tarpeelliseksi.

Fortiswitch 108E:n kytkentäkapasiteetti on 20 Gbps ja paketteja kytkin pystyy käsittelemään 30 miljoonaa sekunnissa. Verkkoviiveeksi luvataan 4 mikrosekuntia. Laite on varustettu 256 megatavun DRAM-muistilla ja 32 megatavun FLASH-levyllä.

Laitetta voidaan hallita joko itsenäisesti tai se voidaan liittää Fortigate-palomuuriin, jolloin hallinta tapahtuu palomuurin kautta pilvipalvelusta tai paikallisesti kirjautumalla. Jos laitetta käytetään itsenäisesti, voi sen hallintaan käyttää laitteen console-porttia tai hallita laitetta Forticloudin kautta. Palomuurin kautta hallittavaa laitetta hallitaan samoilla tavoilla kuin palomuuria voi hallita.

2.3.1 Kytkimen yhdistäminen palomuuriin

Kytkintä päätettiin hallita palomuurin kautta, jotta yhden laitteen kautta päästään hallitsemaan koko yrityksen verkkoa. Fortigate tunnistaa automaattisesti kytketyn Fortiswitch-kytkimen. Kytkimen yhdistäminen palomuuriin sallitaan Fortigaten käyttöliittymän kautta. Tämän yhdistämisen voi myös automatisoida palomuurista, jolloin palomuuri automaattisesti sallii kytkinten yhdistämisen palomuuriin. Fortigate 40F-palomuurissa oletuksena johto kytketään palomuurin porttiin A. Fortiswitch 108E:ssä johto kytketään mihin tahansa porteista 7-10. Molemmissa laitteissa portit voi myös määrittää käsin haluamikseen, jos näitä portteja ei ole mahdollista käyttää.

Ennen kytkimen yhdistämistä palomuuriin tulee palomuurin portti A konfiguroida käyttämään laitteen sisäistä aikaa, jolloin kytkin saa itselleen saman ajan ja aikavyöhykkeen. Jos aikatieto kytkimen ja palomuurilla ei ole sama, ei kytkin onnistu yhdistymään palomuurin kanssa. Tällöin kytkin toimii, mutta laitetta ei voida juurikaan hallita.

Kytkimen yhdistäminen tapahtuu Fortigaten graafisesta käyttöliittymästä kohdasta WiFI & Switch Controller. Kun kytkin on yhdistetty voi kytkimen portteja ja virtuaalisia lähiverkkoja (VLAN) hallita palomuurin käyttöliittymän kautta.

2.3.2 Kytkimen määritykset

Ennen määrityksiä kytkin päivitettiin uusimpaan firmwareen. Työn tekohetkellä uusin firmware oli FortiSwitchOS 7.0.1 Kytkimeen määritettiin manuaalisesti yksi VLAN. Muut VLAN:t ovat laitteen automaattisesti luomia. VLAN:lle määritettiin oma aliverkkonsa ja tämä VLAN toimii myös DHCP-palvelimena tukiasemille. Tukiasemat yhdistettiin tähän VLAN:iin. Tukiasemat saavat IP-osoitteensa DHCP:llä, jotta ne pääsevät liikennöimään yrityksen verkossa. Jos tukiasemia olisi useampia, olisi niille hyvä määrittää kiinteä IP-osoite selkeyden vuoksi. Pienemmässä ympäristössä Fortinet suosittelee DHCP:n käyttämistä.

quarantine.fortilink (quarantine)	4093
voice.fortilink (voice)	4091
video.fortilink (video)	4090
rspan.fortilink (rspan)	4092
onboarding.fortilink (onboarding)	4089
nac_segment.fortilink (nac_segment)	4088
_default.fortilink (_default)	1

KUVA 2. Kytkimen virtuaaliset lähiverkot

2.4 FortiAP

FortiAP on Fortinetin ratkaisu langattomia tukiasemia varten. Tukiasemat saavat tarvitsemansa virran joko PoE:lla tai verkkovirrasta 12V:n muuntajan kautta. Saatavilla on sekä ulko- että sisätukiasemia. Kuten Fortiswitch-kytkimiä, myös tukiasemia voidaan hallita itsenäisesti tai palomuurin kautta. Myös tukiasemien hallinta päätettiin toteuttaa palomuurin kautta.

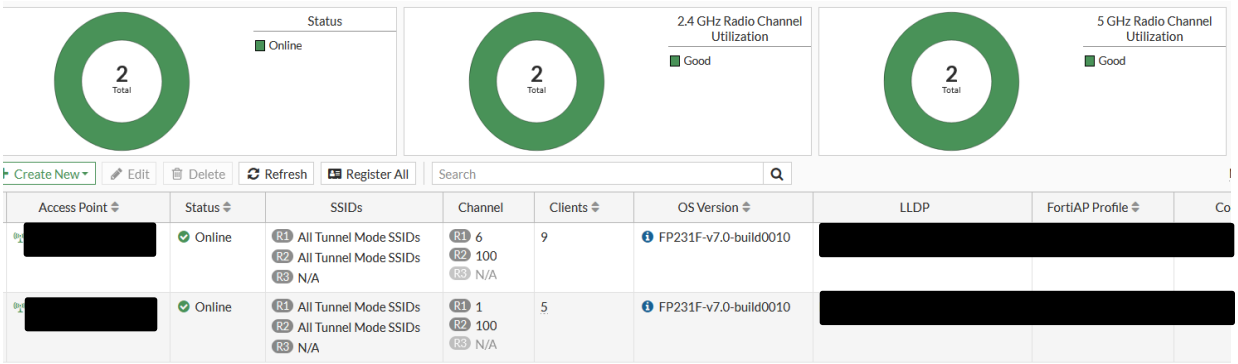
Tukiasemiksi valikoitui FortiAP 231F. Vanhat tukiasemat olivat malliltaan Ubiquity Unify UAP-AC-PRO. Vanhat tukiasemat oli yrityksessä todettu epävakaiksi ja epävarmoiksi toiminnaltaan. Esimerkiksi kaikki tietokoneet eivät aina saaneet IP-osoitetta ollenkaan tukiasemien kautta. Tukiasemia asennettiin tiloihin kaksi, toinen yrityksen toimistotiloihin ja toinen myymälään. Aiemmin tukiasemia oli kolme. Myymälän ja toimistotilojen lisäksi varastossa oli yksi tukiasema, mutta uudella ratkaisulla kaksi tukiasemaa riitti kattamaan koko yrityksen toimitilat.

FortiAP 231F on sisäkäyttöön tarkoitettu tukiasema, joka tukee myös Wi-Fi 6:sta. Wi-Fi 6 on uusin Wi-Fi sukupolvi ja tarjoaa edeltäjäänsä verrattuna suuremmat datanopeudet, sekä paremman taajuusalueen. Lisäksi Wi-Fi 6 tarjoaa suuremman kantaman ja paremmat suorituskyvyn useammalle laitteelle. FortiAP 231F tukiasemat tukevat jopa 16 samanaikaista SSID:tä.

2.4.1 Tukiasemien yhdistäminen palomuuriin

Tukiasemat yhdistetään palomuuriin Fortigaten graafisesta käyttöliittymästä kohdasta WiFI & Switch Controller. Tukiasemat voivat olla liitettynä mihin tahansa kytkimeen, kunhan tämä kytkin pääsee liikennöimään palomuurille. Kun palomuuri on tunnistanut uuden tukiaseman, tulee tämän kytkeminen palomuurin hallittavaksi hyväksyä palomuurin hallinnasta.

Tukiasemien yhdistämistä varten VLAN1 määritettiin jakamaan palomuurin aikaa. Jos aikatieto ei täsmää palomuurin ja tukiasemien välillä, ei yhdistäminen onnistu. Jos yhdistäminen palomuuriin ei onnistu, eivät tukiasemat jaa määritettyjä verkkoja eikä yhdistäminen langattomaan verkkoon esimerkiksi tietokoneella onnistu ollenkaan.



KUVA 3. Tukiasemien hallinnan päänäkymä

2.4.2 Langattomat verkot

Palomuurissa määritettiin verkot toimiston ja myymälän käytettäväksi, sekä yrityksen vieraille. Vain toimiston langattomasta verkosta on pääsy sisäverkon resursseihin, muille verkoille pääsy on sallittu ainoastaan julkiverkkoon.

Langattomat verkot luotiin samalla SSID:llä ja salasanalla kuin vanhoissa laiteissa. Täten langattomien verkkojen käyttäjien ei tarvinnut uudistuksen myötä tehdä muutoksia laitteisiinsa, jos vanhaan langattomaan verkkoon oli jo entuudestaan yhdistetty.

KUVA 4. Yrityksen langattomat verkot

2.4.3 Tukiasemien vaihto

Tukiasemien vaihtoa varten sovittiin sisäisesti Kuopion toimipisteellä käyttökatko. Vanhat tukiasemat sekä niiden PoE-injektorit purettiin. Toimiston uusi tukiasema kiinnitettiin katossa kulkeviin rautoihin ja myymälän tukiasema kiinnitettiin seinään. Tukiasemien vaihtoja varten piti kytkentäkaappiin tehdä muutoksia. Vanhat kytkennät purettiin pois ja kytkettiin uudelleen kulkemaan Fortiswitch-kytkimen kautta.

3 ETÄYHTEYKSIEN MÄÄRITYS

VPN-yhteyden avulla käyttäjät voivat käyttää yrityksen sisäverkon resursseja mistä vain, kunhan käyttäjällä on toimiva verkkoyhteys. Lisäksi etäyhteyttä varten tarvitaan Forticlient VPN-ohjelmisto

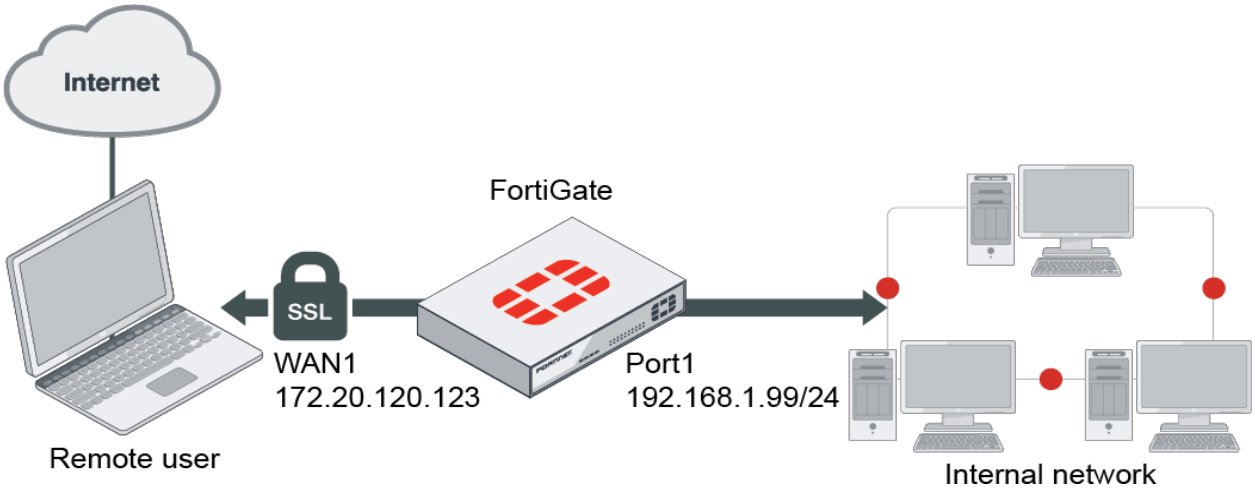
tai vaihtoehtoisesti voidaan käyttää web-sivulla toimivaa VPN-yhteyttä. VPN-yhteydet ovat yritykselle erittäin tärkeitä, sillä monesti esimerkiksi lähituessa toimivat henkilöt tarvitsevat noutaa asennuspaketteja yrityksen verkkolevyiltä. Yrityksellä on myös muutamia työntekijöitä, jotka tekevät töitä pääasiassa etänä.

3.1 SSLVPN

Etäkäyttäjien yhteydet toteutetaan Fortigatessa SSLVPN:llä kuten lähes kaikissa muissakin palomuureissa. Etäyhteyttä varten luotiin sertifikaatti Let's Encrypt -palvelulla. Sertifikaatin varmennusta varten luotiin itc.fi domainiin alidomain vpn.itc.fi joka osoittaa palomuurin WAN1-portin IP-osoitteeseen. Täten pystytään todentamaan, että etäyhteyttä otettaessa vastassa on juuri oikea laite.

Käyttäjätunnukset etäyhteyksiä varten tuotiin palomuuriin sisäverkossa sijaitsevalta Domain Controller palvelimelta LDAP-protokollalla. Käyttäjät voivat siis käyttää etäyhteyden muodostamiseen samaa tunnusta kuin tietokoneelle kirjautumiseen.

Itse SSLVPN-yhteys toteutettiin käyttämällä split tunnelingia. Tällöin vain yrityksen sisäverkkoon kohdistuva liikenne kulkee VPN:n kautta ja kaikki muu liikenne kulkee kuten ilman VPN:ää. Näin käyttäjän verkkoyhteyden nopeus säilyy lähes muuttumattomana. Ilman split tunnelingia kulkisi kaikki liikenne VPN-yhteyden ollessa päällä yrityksen toimitiloissa olevan palomuurin kautta ja käyttäjän yhteys saattaisi hidastua. Lisäksi VPN-yhteyteen määritettiin split DNS, jotta sisäverkkoon kulkevassa liikenteessä käytettäisiin sisäverkossa sijaitsevia DNS-palvelimia.



KUVA 5. Esimerkki topologia split tunnel VPN:stä

Jotta SSLVPN-yhteyttä voi käyttää tuli palomuuriin lisäksi luoda salliva sääntö näille yhteyksille. Säännössä sallitaan SSLVPN:n kautta liikennöinti yrityksen sisäverkkoon. Lisäksi sääntöön määritettiin käyttäjät, jotka yhteyttä voivat käyttää.

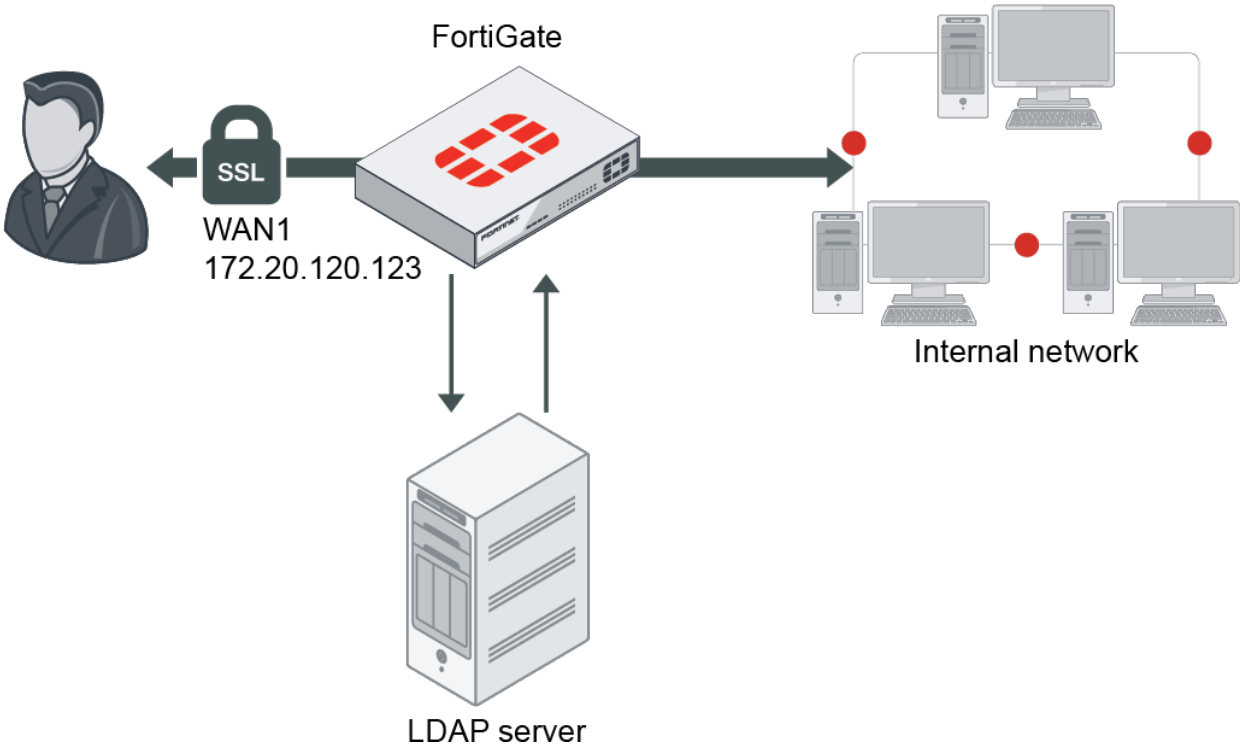
3.1.1 LDAP

LDAP-protokollalla voidaan hakea käyttäjien tunnistetiedot Windows-palvelimella sijaitsevasta Active Directorysta. Palomuuriin määritettiin palvelin, josta tiedot haettiin sekä tarvittavat parametrit. Parametreissä määritettiin OU sekä paikallinen domain, josta käyttäjien tiedot haetaan. Näillä tiedoilla

palomuuri pääsee LDAP:lla hakemaan palvelimelta käyttäjänimet ja salasanat palomuuriin. Käyttäjänimi haetaan Active Directorysta käyttäjän alta attribuutista sAMAccountname. Tämän lisäksi määritetään palvelimen portti, jota tiedonhaluun käytetään.

Ennen tietojen hakua tulee kuitenkin Active Directoryyn määrittää käyttäjä, joka saa hakea LDAP:lla tiedot. Tämän käyttäjän tiedot määritetään palomuuriin LDAP asetusten alle. Tällä käyttäjällä LDAP todentaa itsensä palvelimelle käyttäjätietojen hakua varten.

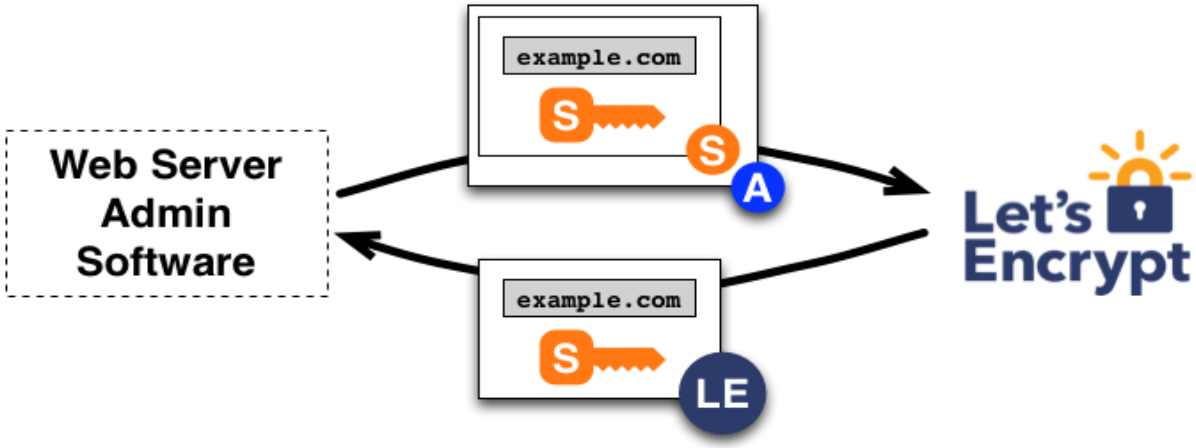
Kun käyttäjät on tuotu palomuuriin, voidaan palomuurin VPN-asetuksista määrittää nämä käyttäjät sallituiksi ottamaan VPN-yhteyksiä. Tarvittaessa myös paikallisia käyttäjiä voidaan luoda.



KUVA 6. LDAP esimerkki topologia

3.1.2 Sertifikaatti

Sertifikaatti etäyhteyden todentamista varten luotiin palomuurin sisäänrakennetulla ACME-palvelulla. Sertifikaatin luonnissa syötetään sertifikaatin nimi, domain (vpn.itc.fi) ja sähköpostiosoite. Lisäksi määritetään aika, jonka jälkeen sertifikaatti uusitaan. Ajaksi määritettiin 60 päivää. Koska kyseessä oli ensimmäinen sertifikaatti joka laitteella luotiin, piti palomuuriin määrittää ACME-portti. Portin tulee olla ulkoverkkoon päin oleva portti eli tässä tapauksessa WAN1. Näin määritettynä sertifikaatti pystytään todentamaan automaattisesti ilmaisella Let's Encrypt -palvelulla. Sertifikaatti syötetään tämän jälkeen palomuurin SSLVPN-asetuksiin.



KUVA 7. Let's Encryptin toimintaperiaate

3.1.3 Etäyhteyden jakaminen Intunella

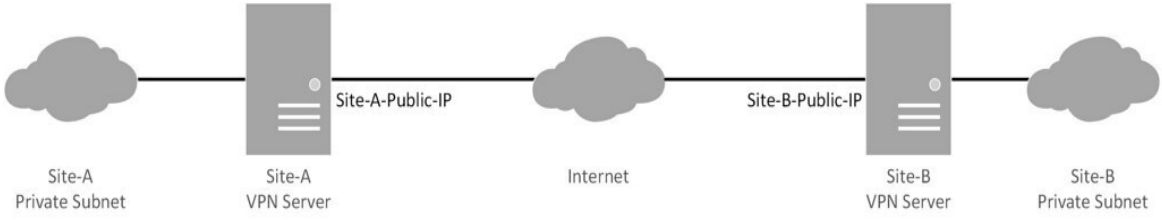
Etäyhteys jaettiin yrityksen tietokoneille Microsoft Endpoint Managerilla eli Intunella. Ensiksi Intunella jaettiin kaikille tietokoneille Forticlient VPN-ohjelmisto, jotta SSLVPN-yhteys voidaan määrittää Windowsin omaan VPN-ohjelmistoon. Ohjelmisto tuo Windowsin VPN:än tuen SSLVPN-yhteydelle. Windowsin VPN ei tue itsessään SSLVPN-yhteyksiä.

Asetukset Windowsin VPN:än määritettiin Powershell-skriptillä. Skripti tarkistaa alussa onko ITC Forti VPN niminen yhteys jo määritetty Windowsiin. Jos yhteys on jo määritetty, lopetetaan skriptin ajo. Jos yhteyttä ei ole määritetty, määrittää skripti tarvittavat asetukset SSLVPN-yhteyttä varten. Skriptin suoritus koneille määritettiin myös Intunella.

3.2 IPSEC VPN

VPN-yhteydet eri toimipisteiden välillä rakennettiin käyttäen IPsec VPN-tunnelia. Tunnelin avulla eri toimipisteet voidaan yhdistää näyttämään yhdeltä verkolta, vaikka liikenne välissä kulkeekin julkisen Internetin kautta. Näin Iisalmen ja Viitasaaren toimipisteiden työntekijät pääsevät käyttämään Kuopion palvelimilla olevia verkkojakoja ja intranetin palveluita.

Liikenne salataan ennen julkiverkkoon menoa, jotta se ei olisi kolmansien osapuolien luettavissa. VPN-tunnelin toisessa päässä oleva palomuuri purkaa salauksen, jotta tietoa pystytään taas lukemaan.



KUVA 8. Site-to-Site VPN

3.2.1 Iisalmi

Työn alkuvaiheessa Iisalmen toimipisteellä oli samanlainen Sonicwall TZ200 -palomuuri kuin Kuopiossakin. Vanha palomuuri jätettiin väliaikaisesti vielä käyttöön ja Kuopion uuteen palomuuriin määritettiin manuaalisesti IPsec VPN-tunneli Iisalmeen. Vanhasta Kuopion palomuurista otettiin asetuksista kuvat ja määritettiin uusi palomuuri samoilla asetuksilla.

Tunnelin muodostamista varten määritellään tunnelin toisen pään IP-osoite sekä paikallisen laitteen uloslähtevä portti sekä IP-osoite. Tunnelin yhteyden autentikointi tapahtuu esijaetulla avaimella. Tämä avain tulee olla sama yhteyden molemmissa päissä tai yhteys ei onnistu muodostumaan. Avaintenvaihtoon käytetään IKE-protokollaa. Näiden määritysten tulee olla identtiset Iisalmen palomuurissa, jotta VPN-tunneli voidaan muodostaa.

Tunnelin muodostuminen tapahtuu kahdessa eri vaiheessa. Ensimmäisessä vaiheessa määritellään salausalgoritmit sekä Diffie-Hellman -ryhmä. Näiden avulla julkiverkon yli kulkeva arkaluontoinen liikenne saadaan salattua eivätkä ulkopuoliset pääse salakuuntelemaan yrityksen liikennettä. Näiden määritysten tulee myös olla identtiset. Toisessa vaiheessa määritetään sisäverkon IP-osoitteet, joita tunnelin läpi kulkee sekä tunnelin toisen pään paikalliset sisäverkon IP-osoitteet. Nämä määritykset ovat tunnelin toisessa päässä päinvastaiset.

Myös Iisalmen palomuuri vaihdettiin Fortigate 40F-palomuuriksi. Palomuurin vaihdon yhteydessä myös VPN-tunneli toimipisteiden välillä luotiin uudelleen. Tunneli luotiin käyttäen esijaettua avainta ja tunnelin toisen pään IP-osoitetta. Lisäksi kahden Fortigate palomuurin välille tulevaan tunneliin piti määrittää paikallinen aliverkko sekä tunnelin toisen pään aliverkko. Muita määrityksiä ei kahden Fortigate palomuurin välillä tarvita määrittää.

VPN-tunneli vaati toimiakseen vielä staattisen reitityksen määrityksen Kuopiosta Iisalmeen sekä Iisalmesta Kuopioon. Kuopion palomuuriin määritettiin staattinen reitti kulkemaan Iisalmen osoitteeseen portista WAN1 ja Iisalmessa tehtiin palomuuriin samat määritykset.

3.2.2 Viitasaari

Viitasaarella ei varsinaista palomuuria entuudestaan ollut. VPN-tunneli oli määritetty Ubiquity Edgerouter X -reitittimeen. Myös Viitasaaren suuntaan toteutettiin VPN-tunneli aluksi vanhaan laitteeseen. Myös Viitasaaren vanha palomuuri korvattiin Fortigate 40F-palomuurilla. VPN-tunnelin määritykset tehtiin samalla periaatteella kuin Iisalmeen. VPN-tunneli määritettiin käyttämällä esijaettua avainta sekä VPN-tunnelin toisen pään julkista IP-osoitetta. Lisäksi määritettiin palomuureihin staattiset reititykset samalla periaatteella Kuopion ja Iisalmenkin välillä.

4 LOPPUTULOS

Opinnäytetyöni tavoitteena oli uusia ja yhtenäistää verkkolaitteet ITC-Solution Groupille. Työn toteutus pysyi hyvin aikataulussa ja työn tilaaja oli työhön tyytyväinen. Työn pohjalta usealle yrityksen asiakkaalle onkin onnistuttu tarjoamaan Fortinetin verkkolaitekokonaisuuksia. Laitteiden uusinnan myötä ongelmat verkossa katosivat ja langattomien verkkojen laatu parani huomattavasti. Laitekanta yrityksen toimipisteiden välillä saatiin halutusti yhtenäistettyä.

Työssä pääsin kerryttämään arvokasta tietoa Fortinetin verkkoratkaisuista. Lisäksi pääsin toteuttamaan itselleni entuudestaan tuntemattomia tekniikoita kuten käyttäjien autentikointia LDAP:lla. Työn valmistuttua verkossa esiintyi joitakin ongelmia, joita jouduin selvittämään itse työn jälkeen.

Työtä on mahdollista jatkokehittää esimerkiksi palomuurien kahdennuksella. Tällöin jokaisella palomuurille olisi identtinen laite, jonka kautta liikenne alkaisi kulkea, jos yhteys päälaitteessa katkeaa tai yhteyden laatu heikkenee huomattavasti. Näin yhteyksistä saataisiin entistä vakaammat. Tulevaisuudessa myös loput Kuopion toimipisteen kytkimistä, sekä Iisalmen ja Viitasaaren kytkimet ja tukiasemat tullaan uusimaan Fortinetin tuotteilla.

5 LÄHDELUETTELO

Fortinet. (30.3.2021). *ACME certificate support.* Haettu 8.9.2021 osoitteesta docs.fortinet.com:

https://docs.fortinet.com/document/fortigate/7.0.0/new-features/822087/acme-certificate-support

Cloudflare. (ei pvm). *What is IPsec?* / *How IPsec VPNs work.* Haettu 25.8.2021 osoitteesta www.cloudflare.com:

https://www.cloudflare.com/learning/network-layer/what-is-ipsec/

Let's Encrypt. (18.9.2019). *How it works.* Haettu 8.9.2021 osoitteesta letsencrypt.org:

https://letsencrypt.org/how-it-works/

Fortinet. (30.3.2021). *SSL VPN with LDAP user authentication.* Haettu 9.9.2021 osoitteesta docs.fortinet.com:

https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/115783/ssl-vpn-with-ldap-user-authentication

Fortinet. (30.3.2021). *SSLVPN tunnel mode host check.* Haettu 15.9.2021 osoitteesta docs.fortinet.com:

https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/179703/ssl-vpn-tunnel-mode-host-check

Cisco. (ei pvm). *What is a VPN? – Virtual Private Network.* Haettu 25.9.2021 osoitteesta www.cisco.com:

https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

Cloudflare. (ei pvm). *What is SSL?* Haettu 25.9.2021 osoitteesta www.cloudflare.com:

https://www.cloudflare.com/learning/ssl/what-is-ssl/