Laajamittainen Fortinetin palomuurien käyttöönotto

Lappeenrannan–Lahden teknillinen yliopisto LUT

Tietotekniikan diplomityö

2022

Ville Tele

Tarkastaja(t): Apulaisprofessori Jussi Kasurinen, TkT

DI Ville Hapuoja

TIIVISTELMÄ

Lappeenrannan–Lahden teknillinen yliopisto LUT

LUT Teknis-luonnontieteellinen

Tietotekniikka

Ville Tele

Laajamittainen Fortinetin palomuurien käyttöönotto

Tietotekniikan diplomityö

2022

65 sivua, 29 kuvaa, ja 1 liite

Tarkastaja(t): Apulaisprofessori Jussi Kasurinen, TkT ja DI Ville Hapuoja

Avainsanat: FortiGate, ZTP, SD-WAN, FortiManager, Fortinet, deploy

Tässä työssä tutkitaan eri tapoja konfiguroida ja käyttöönottaa suuri määrä Fortinetin palomuureja mahdollisimman helposti ja nopeasti. Normaalisti palomuurit esikonfiguroidaan ennen asennusta. Esikonfiguroinnin jälkeen laitteet lähetetään asennettaviksi asiakkaalle. Tämän jälkeen asentaja suorittaa asennuksen loppuun tarvittaessa konfiguroijan avustuksella.

Uusia tapoja käyttäen on mahdollista vähentää esiasennuksen tarvetta esimerkiksi fyysisen laitepääsyn osalta, jolloin ennakkon valmsiteltu konfiguraatio voidaan hakea asennuksen yhteydessä pilvestä. Parhaimmillaan tämä mahdollistaa asennuksen jopa ilman asentajaa, jos asiakkaalla on mahdollisuus liittää laite verkkoon.

FortiGaten Zero-Touch Provisioning toimi testeissä hyvin, ja mahdollisti nopean ja tehokkaan asennuksen verrattuna klassiseen tapaan suoriutua konfiguroinnista ja asennuksesta. Rajoitteina tässä toimi IP-osoitteen saanti operaattorilta DHCP:llä, sillä ilman sitä laite ei osaa yhdistää automaattisesti itseään internettiin, ja hakea omaa konfiguraatiotaan pilvestä. Lisäksi laitteen konfiguraation toimivuutta ei voida varmistaa, sillä se ajetaan palomuuriin vasta asennushetkellä. Tästä muodostuvaa riskiä voidaan kuitenkin hallita erilaisia pohjia hyödyntämällä.

Sisällysluettelo

Liitteet

1 Johdanto

Tämän tutkimuksen tarkoitus on selvittää, miten Fortinetin palomuureja käyttämällä on helpointa saada konfiguroitua suuri määrä laitteita ilman esiasennusta, tai mahdollisimman pienellä työllä. Muutamien laitteiden kohdalla manuaalinen konfigurointi on järkevää, mutta isoissa määrissä työmäärät kasvavat suuriksi logististen syiden, mutta myös heikon tehokkuuden takia. Ratkaisu tähän on ZTP, Zero Touch Provisioning. Tämän avulla laitteille voidaan luoda konfiguraatio pohjia hyödyntäen etäyhteydellä, minimaalisella konfiguroinnilla.

Vaikka ZTP ei ole uusi juttu, sen toiminta on vaihtelevaa ja käyttötapauskohtaista. Tarkoitus on tutkia ZTP:n soveltuvuutta Elisan käyttötapaukseen, jossa halutaan tuotteistaa SD-WAN (Software Defined Wide Area Network) palomuuriratkaisu mahdollisimman pitkälle, jotta toimitusprosessi saadaan mahdollisimman nopeaksi, helpoksi ja tehokkaaksi. Tutkimuksessa vertaillaan eri tapoja luoda laitteeseen konfiguraatio, joka sisältää hallintayhteydet, SD-WAN- liitännän, sekä laitteen muut perustiedot. Tutkimuksen tavoite ei ole luoda kaiken kattavaa pohjaa tai konfiguraatiota, eikä ottaa kantaa tarkemmin laitteen ominaisuuksiin tai asiakaskohtaisiin asetuksiin.

Tutkimuksessa käydään aluksi läpi käsitteet ja teknologiat, joita työssä käytetään, sekä syitä aiheen valinnalle. Tämän jälkeen luodaan konfiguraatio, joka toimii tavoitetilana testeissä. Lopuksi testataan eri tapoja tuoda konfiguraatio laitteille mahdollisimman vähäisellä vaivalla. Tämän jälkeen tulee johtopäätökset ja yhteenveto.

2 Teoria

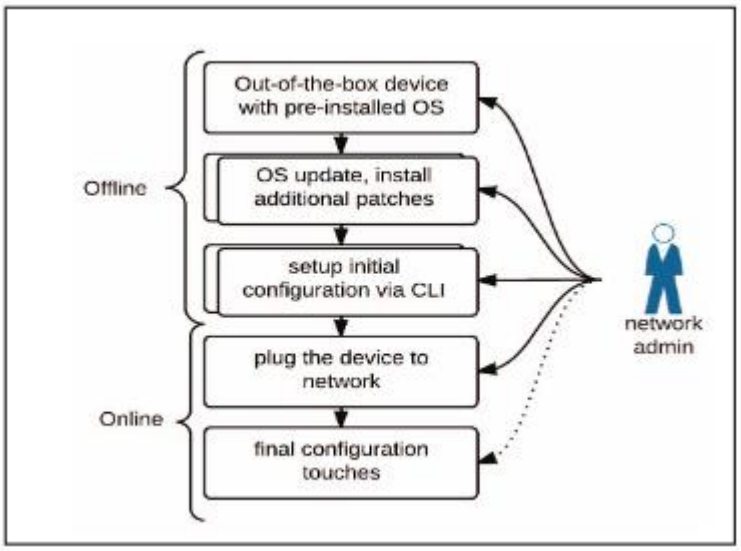
Viimevuosina toistettavien prosessien automatisointi on noussut pinnalle. Automatisoinnilla tarkoitetaan manuaalisen työn korvaamista tässä tapauksessa tietokoneella suoritetulla automaattisella työllä. Tällä säästetään työaikaa, ja sitä kautta rahaa. Lisäksi vakioidut prosessit takaavat samanlaisen lopputuloksen riippumatta niiden käyttäjästä, eikä virheiden mahdollisuus ole läheskään yhtä suuri.

Verkkolaitteita on pitkään konfiguroitu käsin – aluksi asiakkaiden tiloissa, nykyään esiasennuksessa ennen asiakkaalle lähettämistä. Jokatapauksessa konfiguraatiotyö on työlästä ja vaatii laitteiden purkamista ja pakkaamista yksitellen jokaisen konfiguroinnin yhteydessä. Tekniikan, varsinkin pilvipalveluiden, kehittyessä pinnalle on noussut ns. ZTP eli Zero Touch Provisioning. Tällä tarkoitetaan verkkolaitteiden konfigurointia täysin ilman fyysisen läsnäolon tarvetta. ZTP:n toiminnasta lisää myöhemmin, olennaista tässä on ihmisen läsnäolon poistaminen laitteen luota konfiguraatiota asennettaessa. Tavoitetilassa siis koko konfigurointi voidaan tehdä etäyhteydellä.

Tämä mahdollistaa parhaimmillaan prosessien kehittämistä suoraviivaisemmiksi ja nopeammiksi, sekä antaa mahdollisuuden konfiguroida suuria määriä laitteita hyvinkin lyhyessä ajassa, ainoana ehtona toimiva verkkoyhteys hallintaa varten. (Chai, C, 2015)

Yrityksille ZTP konseptina on kiinnostava, sillä se mahdollistaa kustannussäästöjen ja virheiden karsimisen lisäksi paljon paremman skaalautuvuuden laitteiden valmistelulle (provisioning). Tämä mahdollistaa yhä suurempien laitemäärien konfiguroinnin ilman työmäärän merkittävää kasvua, sillä provisioinnissa voidaan käyttää erilaisia skriptejä ja pohjia automaattisesti.

Kuten Demchenko et al. Kuvassaan 1 esittää, laitteiden konfigurointi ilman ZTPtä on monivaiheinen manuaalinen prosessi, mikä vie aikaa, mutta myös tilaa. Työntekijän ajan lisäksi logistiikan tarve on suurempi, sillä laitteet tulee ensin kuljettaa esiasennukseen, josta ne lähetetään vasta asiakkaalle.



Kuva 1 Laitteiden konfigurointi ilman ZTPtä (Demchenko, Filiposka, S., Tuminauskas, R., Mishev, A., Baumann, K., Regvart, D., & Breach, T. (2015))

ZTPllä käytännössä osa prosessista voidaan ohittaa, ja laitteet toimittaa suoraan asiakkaille. Konfiguraatio tapahtuu parhaimmillaan täysin etäyhteydellä, eikä laitetta tarvitse konfiguroida fyysistä läsnäoloa vaativasti.

Oman haasteensa tähän tuo yhtälailla viimevuosina suosiotaan kasvattanut SD-WAN (Lampimäki S., 2021), joka mahdollistaa erilaisten underlay yhteyksien käyttäminen verkoissa samanaikaisesti. Tämän seurauksena esimerkiksi palomuuripalveluntarjoaja ei voi kontrolloida kaikkea verkkoyhteyksiin liittyvää, sillä käytössä saattaa olla hyvinkin erilaisia verkkoyhteyksiä muilta operaattoreilta. Tämä tuo oman haasteensa yllä mainittuun ZTP:iin, joskaan se ei sitä estä.

Kuten ZTP, SD-WAN:in mahdollistamat underlay-yhteydet tuovat käyttäjille kustannussäästöjä (Kuismala L., 2021), sillä he eivät välttämättä enää tarvitse kalliita MPLS-yhteyksiä. Sen sijaan he voivat käyttää edullisempia yritysliittymiä, tai jopa mobiiliratkaisuja. Myös nykyisellä pilviarkkitehtuurien aikakaudella mukaan voidaan lisätä dedikoituja pilviyhteyksiä, kuten esimerkiksi Azuren ExpressRouteja tai muita vastaavia yhteyksiä rinnalle. Tällä saavutetaan aiempaa vikasietoisempia ja kustannustehokkaampia verkkoja, joiden suorituskyky on erinomainen. (Yang, Z., Cui, Y., Li, B., Liu, Y., & Xu, Y. 2019).

Yritysten kiinnostus SD-WANia kohtaan on myös valtavaa. Pandian, A. P., Fernando, X., & Islam, S. M. S. (2021) kertoo, että lähes 40% yrityksistä käyttää tai on ottamassa käyttöön

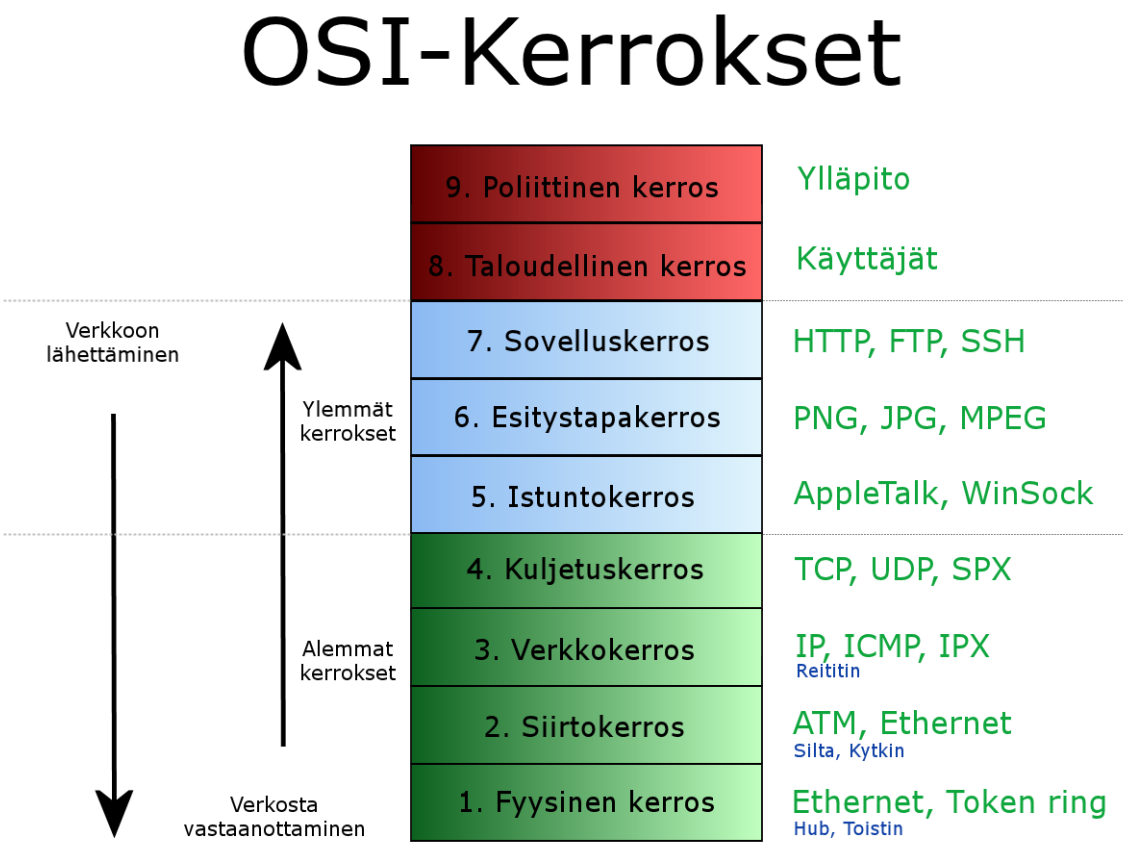
SD-WANia. Lisäksi 83% yrityksistä on joko kiinnostuneita tai aikovat ottaa SD-WAN:in käyttöön. Nämä numerot ovat valtavia, eikä kysynnän uskota laantuvan tulevaisuudessa, päin vastoin. Tämän takia on tärkeää, että palveluntarjoajat pystyvät vastaamaan kysyntään, ja tarjoamaan luotettavaa ja tehokasta palvelua kysynnän kattamiseksi.

Näiden hyötyjen, mahdollisuuksien ja tarpeiden pohjalta tässä työssä tutkitaan, kuinka hyvin SD-WAN:in ja ZTP:n yhteyskäyttö onnistuu Fortinetin palomuureilla. Tavoitteena on verrata erilaisia tapoja viedä laitteen konfiguraatio palomuuriin täysin etänä, tai pienellä fyysisellä konfiguroinnilla. Työssä tutkitaan eri toimintatapojen hyötyjä ja etuja, sekä käytännön toimivuutta. Tarkoituksena on löytää tapa, joka voidaan viedä tuotantoon edellä mainittujen hyötyjen saavuttamiseksi.

Aihetta on tutkittu jonkinverran aiemmin, esimerkiksi Oskar Louko (Zero-Touch Deployment of Fortinet Devices, 2021) tutki samaa ongelmaa Fortinetin laitteilla vuosi ennen tätä tutkimusta. Hänen tutkimus ei ollut kovin kattava, eikä hän testannut varsinaista ZTP-konfikuraatiota vedoten siihen, että FortiDeploy ei olisi käytettävä paikallisen FortiManagerin kanssa. Myöskään SD-WAN ei ollut mukana, vaan testattavana oli yleisellä tasolla ZTPn käyttökelpoisuus ainoana kriteerinä lisäämisen onnistuminen FortiManageriin. Tässä työssä perehdytään aiheeseen tarkemmin, monipuolisemmin ja syvällisemmin, sekä otetaan mukaan SD-WAN. FortiManager on Fortinetin hallintaportaali, johon tutustutaan lyhyesti myöhemmin tässä työssä.

2.1 OSI-malli lyhyesti

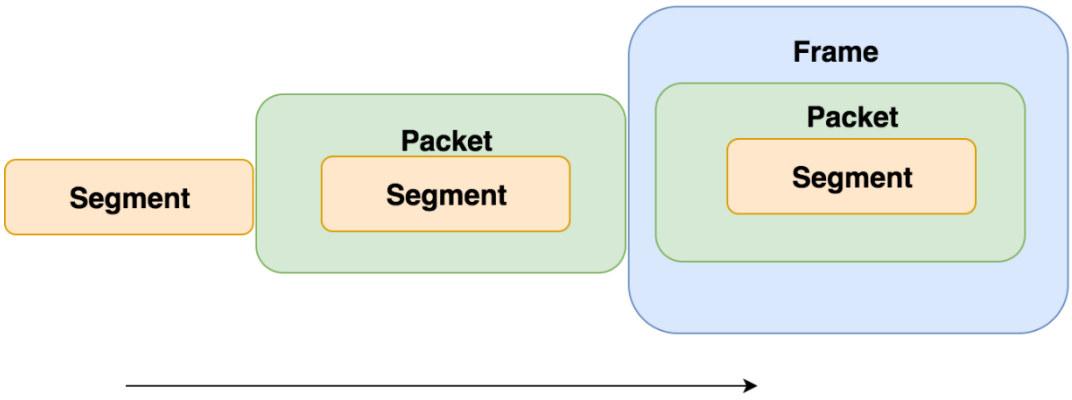
OSI-malli (Open Systems Interconnection Reference Model) on verkkotekniikassa käytetty 7-kerroksinen esitys tiedonsiirtoprotokollista. Alin kerros kuvaa fyysistä yhteyttä ja vastaavasti ylin kuvaa sovellusta. Välissä on kerroksia, jotka liittyvät mm. reititykseen tai istuntoihin.



Kuva 2 - OSI-malli (Malino, 2006)

Tämän työn kannalta oleellisimmat kerrokset ovat 2 ja 3, eli siirtokerros ja verkkokerros. Näistä käytän myöhemmin työssä lyhenteitä L2 ja L3 (Layer 2 ja Layer 3). Siirtokerros on kytkentäistä verkkoa, ja se toimii MAC (Media Access Control)-osoitteilla. L2-verkoissa liikenne tapahtuu yhden aliverkon sisällä, eikä reitittimelle ole tarvetta. Vastaavasti L3 verkoissa liikenne on verkkojen välistä, ja verkkojen väliseen siirtymään tarvitaan jokin reitittävä laite väliin. Tällöin IP-osoitteet ovat tapa päästä määränpäähän.

4. kerros on kuljetuskerros, mihin liittyy vahvasti esimerkiksi TCP- ja UDP-liikenne, tai portit (esimerkiksi HTTPS liikenne käyttää porttia 443). Näitä protokollia ei tässä työssä sen tarkemmin käsitellä läpi, mutta on hyvä tietää näiden sijainti OSI-mallissa.



Kuva 3 Segmentti, paketti, kehys (Pillai S. 2017)

Yllä oleva kuva kuvastaa, miten kuljetuskerrokselta valuva valuva segmentti ensin paketoidaan, ja lopuksi kehystetään lähetystä varten. Kun tämä kehys liikkuu verkossa, löytyy kehyksestä aina kohdelaitteen MAC-osoite. Jos verkosta ei löydy kyseistä MAC-osoitetta, siirtyy paketti yhdyskäytävään. Oletusyhdyskäytävänä oleva laite purkaa kehyksen, ja tarkistaa omasta reititystaulusta mistä portista IP-osoite löytyy. Jos IP-osoitteen verkko ei ole tiedossa, lähettää tämä reititin paketin eteenpäin kehystäen sen uudestaan omalle yhdyskäytävälleen. Tätä jatkuu, kunnes paketti löytää perille, tai sen TTL (Time to Live) loppuu, ja paketti poistetaan verkosta.

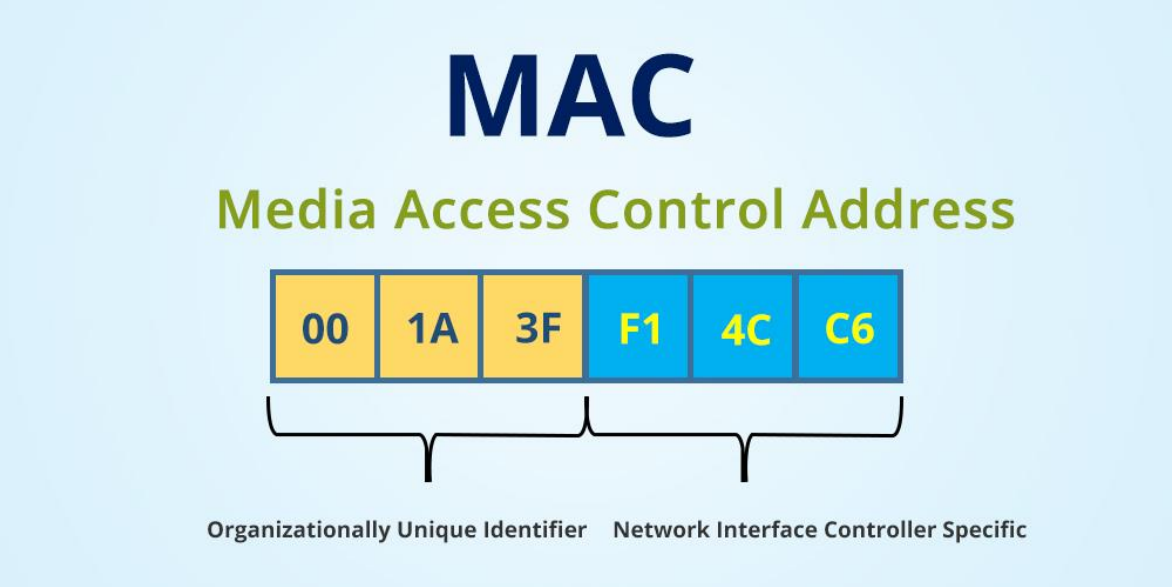
Kantava teema OSI-mallissa on se, että jokainen kerros käyttää alemman kerroksen palveluja, ja vastaavasti tarjoaa niitä ylemmälle kerrokselle. Esimerkiksi 2. kerros, eli siirtokerros käyttää ensimmäisen kerroksen palveluja, eli fyysistä reittiä, ja vastaavasti tarjoaa kehyksiä verkkokerrokselle välitettävksi.

2.2 Ethernet

Nykyisissä tietoverkoissa hyödynnetään kahta erillistä teknologiaa, Ethernettiä sekä

IP:tä (Internet Protocol). Ethernet on matalamman tason kehyspohjainen teknologia, ja sen avulla liikennöidään samassa verkkosegmentissä. Liikennöinti tapahtuu laitteiden MAC-osoitteilla (Media Access Control Address). Nämä ovat 48-bittisiä yksilöllisiä osoitteita, ja ne ovat osoitettu jokaiselle verkkolaitteelle. Itse osoitteessa on 2 osaa, alun

organisaatiotunniste, sekä lopun yksilöllinen osoite. Eri organisaatioille jaetaan tietty määrä alun organisaatiotunnisteita, joiden perään he voivat vapaasti luoda uniikkeja yksilöllisiä osoitteita. Näinollen MAC-osoitteesta voi nähdä, kuka sen on luonut.



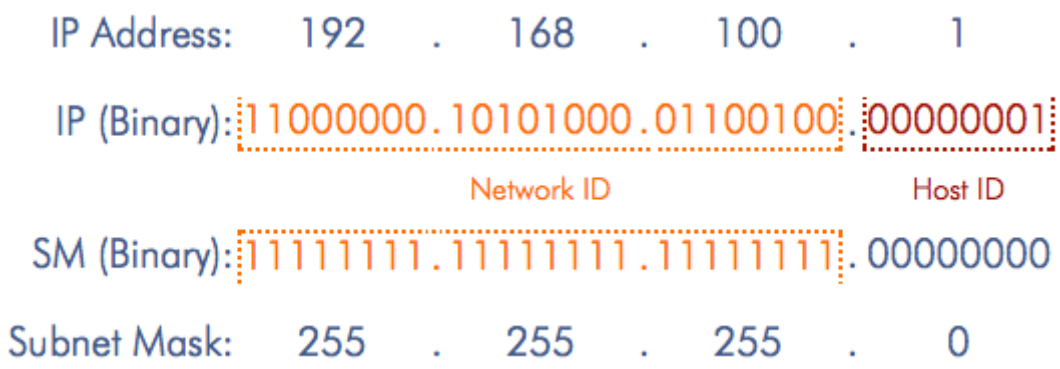
Kuva 4 MAC-osoite. Irving (2021)

2.3 IP-osoitteet, aliverkot ja oletusyhdyskäytävä

IP-osoite (Internet Protocol address) on neljästä pisteellä erotetusta luvusta koostuva osoite, jolla yksilöidään verkossa olevat laitteet. Jokainen numero on 8-bittinen, eli sen arvo voi olla mitä tahansa 0 ja 255 väliltä. Toki nykyään on myös uudempi IPv6- standardi, jossa osoitteet näyttävät hieman erilaisilta, mutta tässä työssä käsitellään vain edellä kuvattua vanhempaa IPv4-standardia. Laitteiden IP-osoitteiden tulee olla uniikkeja jokaisessa erillisessä verkossa, jotta IP-paketit löytävät perille. Tämä tarkoittaa sitä, että IP-osoitteita voidaan kierrättää täysin erillississä yksityisissä verkoissa, esimerkiksi eri yritysten sisäverkoissa, mutta yhden yrityksen sisäverkossa ei saa olla päällekkäisiä osoitteita. Vastaavasti jos yritysten välille tehdään VPN-yhteyksiä, tulee välitettävien verkkojen olla uniikkeja. VPN:stä lisää myöhemmin.

Käytännössä nykyään kaikki verkkoliikenne pohjautuu IP-verkkoihin ja liikennöinti tapahtuu IP-osoitteiden avulla. IP-osoitteisiin liittyy varsin läheisesti myös maski tai aliverkon peite. Tällä määritellään yksittäisten aliverkkojen suuruus. Merkintätapa maskille

on suhteellisen samanlainen kuin varsinaisille IP-osoitteille, pisteillä eroitetut 4 kappaletta 8-bittistä numeroa. Käyttötapa on kuitenkin hyvin erilainen: siinä missä IP-osoite kuvaa yksittäistä osoitetta tietylle laitteelle, maski kuvaa aliverkon suuruutta, sekä osoiteavaruuden alku- ja päätepistettä. Esimerkiksi IP-verkossa 192.168.1.0 (bitteinä 11000000.10101000. 00000001.00000000), jonka maski on 255.255.255.0 (bitteinä 11111111.11111111. 11111111.00000000) voidan käyttää koko viimeisen oktetin verran osoitteita. Helpoissa tapauksissa siis verkon suuruus on edellisen esimerkin kuvaama 256 osoitetta (0-255 on 256 uniikkia numeroa). Toki tästä ensimmäinen numero varataan verkon osoitteeksi (192.168.1.0), sekä viimeinen broadcast eli yleislähetys-osoitteeksi (192.168.1.255). Loput 254 osoitetta ovat käytännössä vapaasti sijoitettavia verkon laitteille, mukaanlukien yhdyskäytävälle (gateway).



Kuva 5Kuva 4Yllä oleva kuva näyttää, miten aliverkon bitit kertovat käytettävissä olevien bittien määrän itse IP-osoitteessa. Connected Dots Online, (2022)

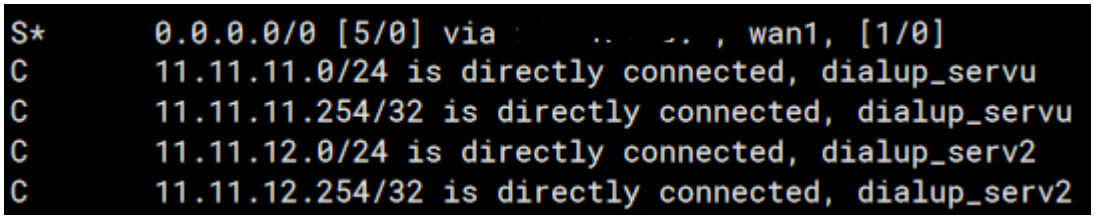
Vaikka aliverkon peite voidaan kuvata yllä kuvatulla tavalla muodossa xxx.xxx.xxx.xxx, se voidaan ilmaista myös lyhyemmin CIDR (Classless Inter-Domain Routing)-notaatiolla. Tällöin kerrotaan merkitsevät, eli arvon 1 saavat bitit. Esimerkiksi verkko 192.168.1.0 255.255.255.0 voidaan kuvata CIDR-notaatiolla muodossa 192.168.1.0/24. Käytännössä tällöin 24 ensimmäistä bittiä maskista ovat ykkösiä, loput nollia. Tällöin saadaan binäärimuodossa peite 11111111.11111111. 11111111.00000000, joka voidaan myös ilmaista muodossa 255.255.255.0.

Hieman epänormaalimmissa tai haastavammissa aliverkoissa verkon koko voidaan laskea helposti biteistä. Esimerkiksi verkko 192.168.0.0 255.255.248.0, eli 192.168.0.0/21 sisältää 2046 osoitetta. Tämä tarkoittaa binäärimuodossa 11111111.11111111.11111000.00000000. 2^11 (11 on lopun nollien määrä) on 2048. Jos maskin kääntäminen binäärimuotoon on hankalaa, voi ”haastavammat” oktetit järkeillä näin: 248 ja 255 (suurin mahdollinen numero)

väli sisältää yhteensä 8 numeroa. 8 saadaan 2:n potenssina 3:lla, eli 2^3. Tästä tiedetään, että kolmannessa oktetissa on 3 0:aa lopussa, eli kolmas oktetti on 11111000. Saadusta 2048:sta osoitteesta vähennetään verkon osoite sekä yleislähetysosoite, jolloin saadaan 2046 IP-osoitteen kokoinen verkko. Verkon osoite on siis 192.168.0.0/21, ja yleislähetys-osoite on 192.168.7.255.

Aliverkot ovat tietoliikenteessä erittäin oleellisia. Ensinnäkin samassa aliverkossa olevat laitteet voivat keskustella suoraan keskenään. Tämä toki olettaa, että laitteet ovat kytkettynä fyysisesti samaan verkkoon asianmukaisesti. Jos siis yllä olevassa verkossa olisi tietokone IP-osoitteella 192.168.1.48, ja toinen tietokone osoitteella 192.168.6.4, voisivat tietokoneet keskustella keskenään ilman suurempia murheita esimerkiksi kytkimen kautta, tai suoraan toisiinsa kytkettyinä.

Jos oletetaan rinnalle toinen aliverkko, esimerkiksi 192.168.8.0/24, jossa on tietokone IP-osoitteella 192.168.8.60. Jotta aikaisempi 192.168.1.48-osoitteen saanut tietokone voisi tähän ottaa yhteyttä, vaaditaan siirtymä aliverkosta toiseen. L2-, eli kytkentäisessä verkossa tämä ei ole mahdollista, joten väliin tarvitaan jokin L3-kyvykäs laite, eli reititin. Reititin pitää kirjaa eri verkoista, sekä mistä portista ne löytyvät. Koska tietokone 192.168.1.48 huomaa, että kohdetietokone 192.168.8.60 ei ole enää samassa aliverkossa, lähettää tietokone paketin oletusyhdyskäytävälle. Tämä on monesti verkon ensimmäinen vapaa osoite, eli esimerkiksi 192.168.0.1. Tämä laite on edellämainittu L3-kyvykäs reitittävä laite, joka osaa katsoa kohdeosoitteen IP-paketista. Koska reititin pitää yllä reittitaulua, se osaa lähettää paketin oikeasta portista ulos, jotta se saapu verkolle 192.168.8.0/24. Vastaanottava kytkentäinen laite osaa toimittaa kehykseksi puretun paketin perille, sillä tässä vaiheessa kehys on saapunut oikeaan L2-verkkoon.



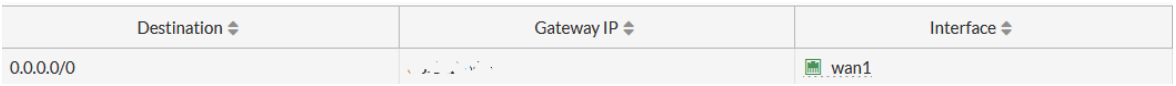
Kuva 6 Reittitauluesimerkki FortiGaten CLI:stä

Jotta edellinen järjestely toimii, tulee reitittimellä olla reittitaulu, ja se pitää olla ajantasalla. Reittejä voidaan jakaa monella tavalla, esimerkiksi staattisilla reiteillä, tai BGP:llä.

2.4 Staattiset ja dynaamiset reitit

2.4.1 Staattiset reitit

Staattiset reitit sisältävät tiedon liitännästä, jota kyseinen reitti käyttää. Tämän lisäksi tarvitaan tieto, mitä sen takaa löytyy. Se voi olla yksittäinen pieni verkko, esimerkiksi 192.168.1.0/24, mutta kyseessä voi olla myös nk. oletusreitti, eli 0.0.0.0/0. Pienemmän verkon kohdalla reititin tietää, että kyseisestä liitännästä löytyy jokin aliverkko, kun taas nollareitin kohdalla liikenteeseen lähetetään kaikki liikenne, joka ei osu muihin reitteihin. Käytännössä tämä tarkoittaa usein yhteyttä runkoverkkoon. Jos kohdeosoite osuu moneen reittiin, se lähetään siihen suuntaan, missä yhteneväisyys reitin kohdeverkon kanssa on suurin. Kolmas tieto on mahdollinen kohdereitittimen IP-osoite. Jos liitäntä ohjaa suoraan kohti kytkintä, tämä tieto voidaan jättää tyhjäksi. Jos kuitenkin reitti menee kohti runkoa tai toista reititintä, täytetään tähän nk. Next hop, eli seuraava hyppy, joka tarkoittaa seuraavan reitittimen IP-osoitetta.



Kuva 7 Esimerkkikuva FortiGaten staattisesta reitistä GUI:sta

Yhteenvetona, jos kohdeosoite on samassa aliverkossa, kytkimen pitäisi osata lähettää kehys oikeaan suuntaan. Jos kohdeosoite on eri verkossa, lähetetään paketti yhdyskäytävälle, joka toivonmukaan tietää mihin paketti pitää lähettää. Se, onko kohdeosoite samassa aliverkossa, nähdään omasta kohde-IP-osoitteesta ja maskista, sekä kohde-IP-osoitteesta.

2.4.2 Dynaamiset reitit

Dynaamisia reititysprotokollia on useita, ja niiden tärkein piirre on nimensä mukaisesti niiden dynaaminen eli muuttuva luonne. Tässä työssä käytetään kevyesti BGP:tä. BGP (Border Gateway Protocol) on aiheena valtava (Hu B. 2021) ja tässä teoriaosuudessa sitä sivutaan ohitse vain soveltuvin osin työn kannalta.

BGP:llä mainostetaan Dial-up VPN:llä yhteyden ottavien muurien takana olevat verkot. Käytännössä siis luotuaan VPN-tunnelin palomuuri kertoo keskitetylle palomuurille, mitä IP-verkkoja kyseisen tunnelin takaa löytyy. Tämä mahdollistaa sen, että uusien yhteyksien

myötä jokaiselle tunnelille ei tarvitse tehdä omia staattisia reittejä, vaan niitä voidaan lisätä BGP:tä käyttäen dynaamisesti tarpeen mukaan. Tämä vähentää konfiguraation tarvetta palomuurien määrän kasvaessa, sekä helpottaa ylläpitoa, sillä reittejä ei tarvitse poistaa tai muuttaa keskitetyltä muurilta, jos VPN-tunneleita poistetaan käytöstä. Kappaleessa 3.2.2 käydään läpi työssä käytetty BGP-konfiguraatio.

2.5 DHCP

Edellisessä kappaleessa puhuttiin IP-osoitteesta hyvin yleisesti. IP-osoitteet voidaan jakaa laitteille manuaalisesti, jolloin ne ovat staattisia. Tämä jako voidaan tehdä joko laitteelta itseltään, tai DHCP-palvelimelta (Dynamic Host Configuration Protocol). DHCP-palvelin vastaa IP-osotteiden jakelusta laitteille, jotka kytketään samaan verkkoon. Palvelimelle määritellään osoiteavaruus, josta osoitteita voidaan jakaa.

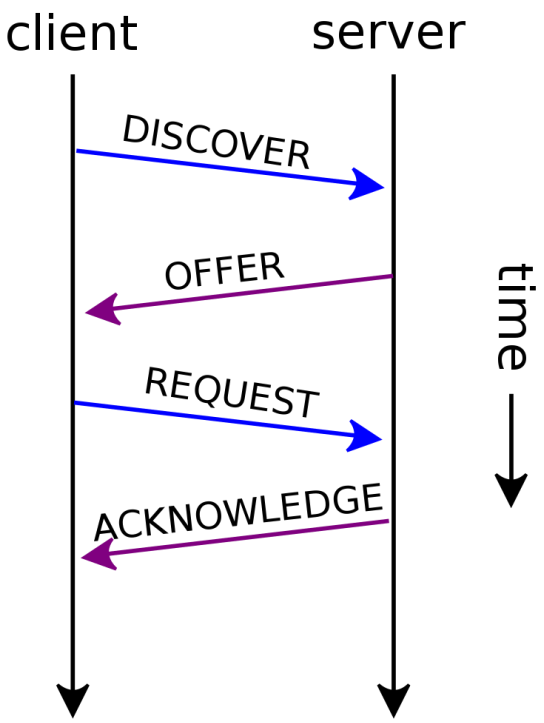
Kun verkkoon kytketään uusi laite, se lähettää niin sanotun DHCPDISCOVERY viestin koko verkolle broadcastinä, eli yleislähetyksenä (Deland H., eross-msft, v-kents. 2021). Koska se lähetetään jokaiselle verkossa olevalle laitteelle, tulee se myös verkossa olevalla DHCP-palvelimelle. Viestistä käy ilmi lähettävän laitteen fyysinen osoite, eli MAC-osoite. Viestiin merkattu lähetys IP-osoite on 0.0.0.0.

Kun viesti saapuu DHCP-palvelimelle, se vastaa tähän DHCPOFFER viestillä. Viestin lähde IP-osoite on DHCP-palvelin, mutta kohde on edelleen yleislähetysosoite, sillä DHCP-palvelin ei varsinaisesti osaa kohdentaa sitä osoitetta kysyneelle laitteelle. Viesti sisältää ehdotuksen IP-osoitteesta, sekä kysyvän laitteen MAC-osoitteen, jotta yleislähetyksenä lähetty paketti voidaan tunnistaa kohdistetuksi nimenomaan IP-osoitetta kyseneelle laitteelle. Lisäksi tämä viesti sisältää lähtökohtaisesti verkon maskin, sekä oletusyhdyskäytävän osoitteen.

Kun DHCP-tarjous saavuttaa IP-osoitetta kysyneen laitteen, se vastaa tähän DHCPREQUEST viestillä. Tämän viestin lähdeosoite on edelleen 0.0.0.0, koska IP-osoitetta ei ole vielä lyöty lukkoon. Lisäksi kohdeosoite on yleislähetysosoite, jotta mahdolliset muut osoitteita tarjonneet DHCP palvelimet saavat tiedon, että heidän tarjoamaansa osoitetta ei oteta käyttöön, ja tarjotut osoitteet voidaan vapauttaa seuraaville kysyjille. Viesti sisältää kuitenkin hyväksytyn tarjoajan IP-osoitteen.

Kun DHCP-palvelin saa edellisen pyyntöpaketin, lähettää se vielä lopuksi DHCPACK viestin. Lähetysosoite on DHCP-palvelimen IP-osoite, kohdeosoite yleislähetysosoite. Viestissä on lisäksi kysyjän MAC-osoite, sekä sille annettu IP-osoite.

Kun kysyjä saa tämän kuittauksen, ottaa se käyttöön sovitun IP-osoitteen, sekä annetun maskin ja verkon oletusyhdyskäytävän. Jatkossa liikennöinti tapahtuu näitä osoitteita käyttäen.



Kuva 8 DHCP sessio, Gelmo96 (2015)

DHCP-palvelimelle jaettavaksi annettu osoiteavaruus ei välttämättä ole koko käytettävissä olevan aliverkon kokoinen. Monesti verkon alku- tai loppupäähän jätetään varausta staattisille IP-osoitteille, joka mahdollistaa kiinteämpien laitteiden sijoittamisen verkkoon. Nämä voivat olla esimerkiksi palvelimia tai tulostimia. Näiden laitteiden osoitteet eivät vaihdu, ja ne ovat lähtökohtaisesti aina verkossa. Siispä osoitteen antaminen DHCP:llä ei kävisi järkeen, sillä huonoimmillan osoite vaihtuisi, eikä resurssi enää löytyisi tutulla IP-osoitteella.

2.6 Se ei ole aina DNS – paitsi että on

DNS tulee sanoista Domain Name System. Sen tarkoitus on tarjota jotain helpompaa kuin IP-osoitteet normaaleille käyttäjille. Tietokoneisiin on yksinkertaista tallentaa IP-osoitteita, mutta ihmisten on niitä vaikea muistaa ja erottaa. Jos haluaa mennä Googleen etsimään tietoa jostain asiasta, on helppoa kirjoittaa selaimessa osoitteeksi https://www.google.fi, tai nykyään google.fi. Tietokone osaa automaattisesti ottaa yhteyttä DNS-palvelimeen, joka muuntaa pyynnön helposti muistettavasta osoitteesta IP-muotoon.

DNS:ää käytetään julkisissa verkko-osoitteissa, mutta sitä voidaan käyttää myös yritysten sisäverkoissa. Esimerkiksi palvelimella tai tulostimelle voidaan antaa hostname, jolla laitteeseen päästään käsiksi. Jos siis verkossa 192.168.1.0/24 olisi tulostin, jolle on asennettu staattinen IP-osoite 192.168.1.2, voidaan siihen ohjata hostname ”tulostin”. Näin IP-osoitteen sijaan tulostimeen päästään käsiksi hostnamella, mikä on helpompi muistaa. Jos tulostimen IP-osoite ei kuitenkaan olisi staattinen, saattaisi sen IP-osoite vaihtua, ja edellä mainittu IP-osoite 192.168.1.2 saatettaisiin antaa jollekkin toiselle laitteelle. Tällöin hostname ei enää ohjaisi tulostimeen. Tämän vuoksi staattisen IP-osoitteet ovat tärkeitä verkoissa. DHCP:n jakamat dynaamiset IP-osoitteet tarjoavat helppoutta muuttuvalle laitekannalle, kun taas staattisen IP-osoitteet ja hostnamet tarjoavat pääsyn haluttuihin resursseihin aina samoilla osoitteilla pienellä ylläpidollisella vaivalla.

2.7 NAT

NAT, eli osoitteenmuunnos (Network Address Translation) tarkoittaa toimenpidettä, jossa yleensä julkisten IP-osoitteiden taakse sisällytetään useita käyttäjiä. Kuten aiemmin todettiin, jotta IP-verkoissa voidaan liikennöidä, tulee jokaisella laitteella olla verkolle uniikki IP-osoite. Internet on kuitenkin laajentunut alkuajoistaan paljon, eikä vanhempia IPv4 osoitteita enää riitä jokaiselle kytketylle laitteelle. Tässä mukaan astuu osoitteenmuunnos. Esimerkiksi kotikäytössä monella on operaattorin toimittama modeemi tai reititin. Normaalisti jokainen tämän takana oleva laite saisi oman uniikin IP-osoitteen, jolla laitteisiin saataisiin yhteys. Osoitteenmuunnoksella operaattorin tarvitsee luovutta vain 1 IP-osoite reitittimelle. Kaikki tämän takana olevat laitteet ”natataan”, eli piilotetaan tämän yhden julkisen osoitteen taakse. Tällä säästetään IPv4-osoitteita, mutta myös parannetaan verkon tietoturvaa, sillä laitteet eivät ole suoraan saavutettavissa internetistä –

oletusarvoisesti julkinen IP-osoite kohdistuu reitittimelle, joka hoitaa myös jollain tasolla palomuurausta ja muuta tietoturvaa.

Nattaava laite luo NAT-taulun, joka pitää yllä kirjaa NATin takana olevista laitteista. Staattisessa NAT:issa sisäverkon osoitteet ohjataan 1:1 ulkoverkon laitteiden kanssa. Jos siis operaattorilta saataisiin esimerkiksi verkko 193.100.100.0/29 käyttöön, tarkoittaisi se 6 osoitetta laitteiden käyttöön. Tällöin sisäverkosta 6 laitetta voitaisiin NATata näiden 6:n julkisen osoitteen taakse suhteellisen loogisesti:

Sisäverkon osoite	ulkoverkon osoite
192.168.1.1	193.65.76.1
192.168.1.2	193.65.76.2
…	
192.168.2.1	193.76.77.1

Kuva 9 Esimerkki staattisesta NATista Wikipedia (2022)

Jos sisäverkon laitemäärä kasvaisi yli kuuden, osoitteet loppuisivat, eikä uusia staattisia NATteja voisi enää luoda. Tätä varten tarvittaisiin lisää IP-osoitteita operaattorilta.

Dynaamisessa NATissa homma toimii lähes samalla tavalla, ulkoverkon osotteita otetaan käyttöön sitä mukaa, kun sisäverkon laitteet niitä tarvitsevat. Jos osoitteet loppuvat, ei uudet laitteet enää pääse julkiverkkoon, sisäverkossa ne toki voivat liikennöidä. Esimerkki toteutuksesta:

Sisäverkon osoite	ulkoverkon osoite
192.168.1.17	193.65.76.2
192.168.1.22	193.65.76.3
192.168.1.29	193.65.76.4
…	

Kuva 10 Esimerkki dynaamisesta NATista Wikipedia (2022)

Porttimuunnos on kolmas tapa NATata laitteita reitittimen taakse. Tällöin reititin tarvitsee operaattorilta vain yhden IP-osoitteen. Kaikki tarvittava ohjaus sisäverkon laitteile tehdään tarvittaessa porttien avulla.

Sisäverkon osoite	sisäverkon portti	ulkoverkon osoite	ulkoverkon portti
192.168.1.1	1111	193.65.76.1	1025
192.168.1.1	1112	193.65.76.1	1026
192.168.1.2	2001	193.65.76.1	1027
192.168.1.1	1113	193.65.76.1	1028
...			

Kuva 11 Esimerkki porttimuunnoksesta Wikipedia (2022)

Tässä työssä ei perehdytä varsinaisesti NATin toimintaan, mutta sen aiheuttamat rajoitteet on hyvä tietää. Jos jokin laite on NATin takana, ei siihen voida suoraan ottaa ulkoverkosta yhteyttä, sillä laitteella ei ole julkista IP-osoitetta. NAT-tyypistä riippuen yhteydenotto vaatii erinäköistä konfiguraatiota NATtaavaan laitteeseen. NAT ei kuitenkaan estä yhteyksiä sisäverkosta ulospäin, sillä monesti kohdeosoite johon halutaan ottaa yhteyttä omaa julkisen IP-osoitteen. Tällöin yhteys muodostuu laitteiden välille normaalisti, ja tallentuu reitittimen sessiotauluun. Tämän ansiosta session muodostuttua yhteydet onnistuvat molempiin suuntiin.

2.8 MPLS

MPLS, eli MultiProtocol Label Switching on tekniikka, jolla voidaan kuljettaa normaaleja IP-paketteja nopeasti ja luotettavasti paikasta toiseen. Tämä on mahdollista, sillä paketteja ei tarvitse reitittää aktiivisesti matkan varrella. MPLS-verkon reitit ja reititykset ovat tietyllä tavalla esimääriteltyjä, eli liikenne menee paikasta A paikkaan B aina samaa reittiä (Josh Fruhlinger, 2022). Kun uusi MPLS-verkkoon saapuva paketti lähtee matkaan, matkan varrella olevat solmut osaavat automaattisesti laittaa sen eteenpäin kohdeosoitteen perusteella. Tällä saavutetaan pienemmät vasteajat, minkä lisäksi internetistä irrallaanolon vuoksimyös tietoturvaa. Vaikka liikennettä ei varsinaisesti salata, se liikkuu kuitenkin yksityisessä verkossa. Näiden lisäksi verkon suorituskykyä voidaan seurata, sillä se on kokonaan palveluntarjoajan hallussa. Näin olleen esimerkiksi palvelun laadun tarjoaminen on mahdollista.

2.9 VPN

VPN, eli virtuaalinen erillisverkko (Virtual Private Network) tarkoittaa tapaa, jolla voidaan loogiesti yhdistää kaksi fyysisesti erillään olevaa verkkoa toisiinsa. Jos yrityksellä on vain yksi toimipiste, ja siellä on useita aliverkkoja eri laitteille, mutta verkot ovat saman palomuurin tai reitittimen takana, ei VPN:lle ole tarvetta, sillä verkkojen välillä liikennöinti onnistuu reitittimen kautta. Jos yrityksellä on kuitenkin useita toimipisteitä, ja tahtotila on liikennöidä näiden välillä käyttäen yrityksen omia sisäisiä verkkoja, tulee eri toimipisteiden välille rakentaa VPN-tunneli. VPN voi tarkoittaa yleisesti nk. Site-to-site yhteyttä, eli tunnelia toimipisteiden välille. Se voi tarkoittaa myös esimerkiksi client VPN:ää, joka on usein point-to-site- tyylinen. Tällöin käyttäjän kone luo yhteyden saitille. VPN-tunneleita on myös muunlaisia, mutta tässä työssä käsitellään site-to-site tunneleita, joten emme käy sen tarkemmin läpi muita VPN-ratkaisuja.

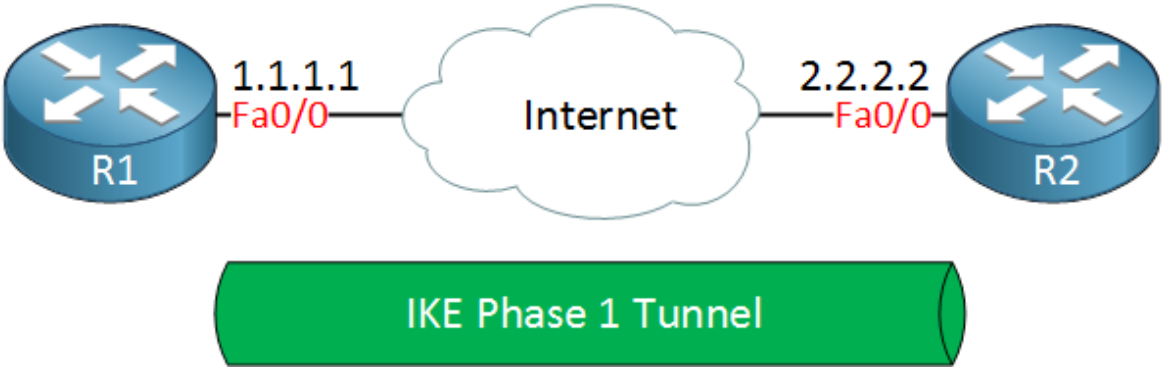
Tunnelit luodaan nykyään yleensä käyttäen joko IPSec:iä (IP Security Architecture) tai SSL(Secure Sockets Layer)-VPN:ää. IPSec on tietoliikenneprotokolla, joka on luotu verkkoyhteyksien suojaamiseen. Vastaavasti SSL-VPN käyttää yhteyden salaamiseen SSL-protokollaa. Tämän työn Site-to-Site VPN-tunnelit luodaan käyttäen IPSec-protokollaa.

Site-to-site tunnelit luodaan kahden L3 laitteen välille, jotka ovat usein palomuureja. Jotta tunneli saadaan muodostettua, tulee luonnollisesti asetukset konfiguroida molemmille muureille. Oleellista on tietää vastapuolen IP-osoite, sekä vaaditut asetukset tunnelin muodostumiseksi. Jos asetukset eivät ole keskenään yhteensopivia, ei tunneli nouse pystyyn.

Varsinainen tunneli muodostetaan käyttäen IKE-protokollaa (Internet Key Exchange). IKE vastaa tunnelia muodostettaessa viestien vastaanottamisesta, sekä niihin vastaamisesta. IKE:stä on 2 versiota, IKEv1 ja IKEv2, joista jälkimmäinen on nykyään suositeltavampi tietoturvan takia.

VPN-tunnelin ensimmäisessä vaiheessa aluksi osapuolet neuvottelevat käytettävät salaus- ja tiivistealgoritmit (Kaarnalehto M. 2011), sekä Diffie-Hellman ryhmän (DH-group). Lisäksi päätetään, käytetäänkö autentikointiin salasanaa (PSK, Pre Shared Key) vai sertifikaattia. Lopuksi sovitaan tunnelin elinikä, luonnollisesti lyhyempi elinikä on pääsääntöisesti turvallisempi, sillä salausavaimet tunneliin vaihtuvat useammin. Kun asetuksista on päästy sopuun, vaihdetaan DH-avaimet. Lopuksi vastapouolet autentikoivat toisensa käyttämällä

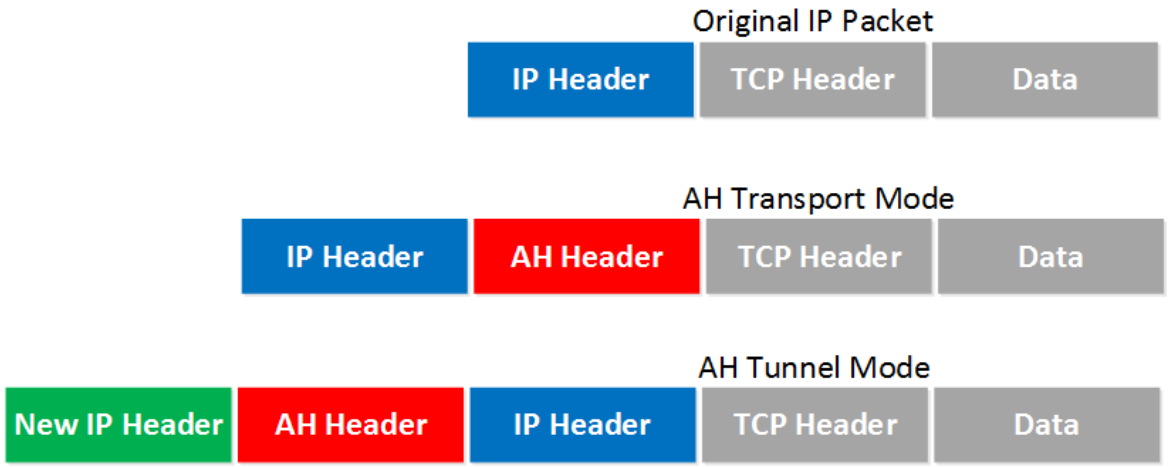
aiemmin sovittuja autentikointivaihtoehtoja. Tämän seurauksena saadaan pystyyn 1. vaiheen tunneli.



Kuva 12 IKE tunneli 1. vaihe ReneMolenaar (2022)

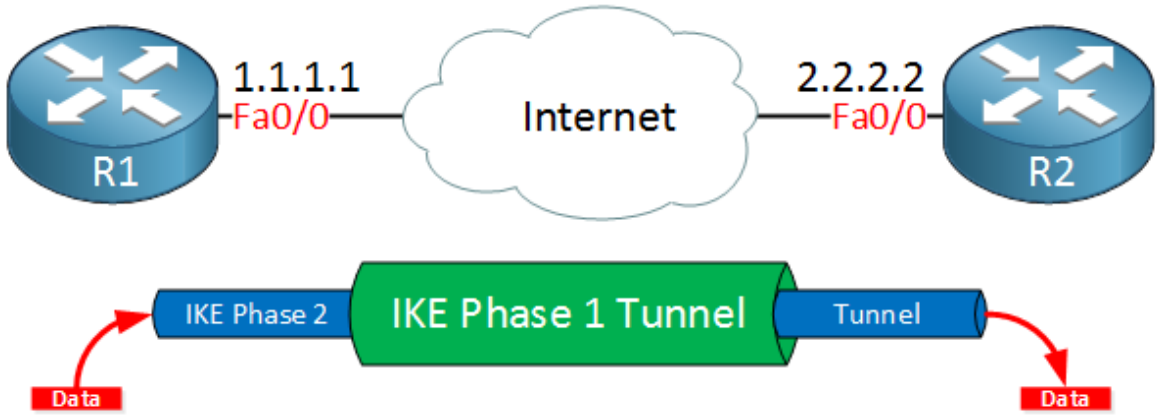
1. vaiheen tunneli ei liikuta varsinaista liikennettä tunnelin päiden välillä, vaan sen tarkoitus on puhtaasti luoda salattu ja turvallinen hallintatunneli jatkoa varten. Valittujen asetusten ”kokoelmaa” kutsutaan SA:ksi (Security Association).

2. vaiheen tunneli, eli IPSec- tunneli luodaan 1. vaiheen tunnelissa, ja sen tarkoitus on siirtää varsinainen data tunnelin päiden välillä. Kuten 1. vaiheen tunnelissa, tässäkin osapuolet ensin neuvottelevat käytettävistä asetuksista. Oleellisia valintoja ovat IPSec-protokollaan liittyvä valinta AH:n (Authenticating Headers) ja ESP:n (Encapsulating Security Payload) välillä, liikenteen kapselointitapa, salaus- sekä autentikointialgoritmit, tunnelin elinikä, sekä DH-ryhmät. IPSecin tukemat AH ja ESP mahdollistavat joko tunneli- tai kuljetusmuodon salauksessa. Tunnelissa koko IP-paketti salataan, ja sen eteen luodaan uusi IP-otsikko. Kuljetusmuodossa vain sisältö salataan, ja alkuperäinen IP-otsikko jätetään salaamattomaksi paketin eteen.



Kuva 13 Tunnelointivaihtoehdot ReneMolenaar (2022)

Jos kaikki asetukset ovat samalla tavalla, myös 2. vaihe nousee pystyyn, ja sitä kautta itse tunneli aloittaa toimintansa. Oikeasti toimiakseen tunneli tarvitsee toki palomuurisääntöjä, sekä reitit tunneliin, jotta relevantti liikenne saadaan ohjattua sinne.



Kuva 14 IKE tunneli 2. vaihe ReneMolenaar (2022)

Käytämme tässä työssä Dial-up VPN-tunneleita. Nämä eroavat normaaleista tunneleista siten, että keräävä pää ei tiedä mihin se muodostaa tunnelin. Siihen konfiguroidaan yleiset asetukset, ja se asetetaan vastaanottamaan yhteyspyyntöjä julkiverkosta. Tämä mahdollistaa sen, että uusia VPN-tunneleita ei tarvitse joka kerta konfiguroida keräävälle muurille. Tämän lisäksi tunnelit voidaan luoda myös NATin takaa tulevilta laitteilta, sillä vastapään IP-osoitetta ei tarvita. Eri valmistajilla on omat toteutukset tähän, ja työn osalta konfiguraatio käydään läpi myöhemmin tässä työssä.

2.10 SD-WAN

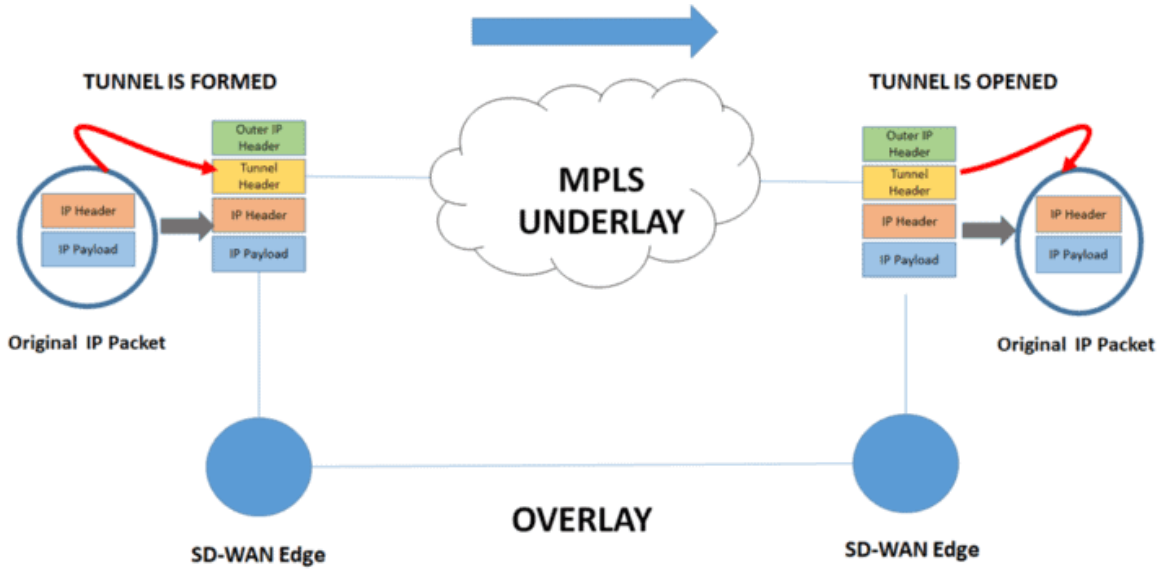
Viime vuosina SD-WAN on kasvattanut suosiotaan suuresti. Tämä tarkoittaa ”software defined” WANia, mikä käytännössä tarkoittaa sitä, että palomuuri osallistuu aktiivisesti reititykseen ohjelmistollaan. Tämä on mahdollista, sillä SD-WAN:issa varsinaiset verkkoyhteydet ovat niinkutsuttuja ”underlay”- yhteyksiä, joiden päälle rakentuu palomuurin toimesta ”overlay”:ksi SD-WAN.

2.10.1 Underlay

Underlay yhteydet voivat olla periatteessa mitä vain. Aikaisemmin yritysten toimipisteiden välillä on käytetty paljon MPLS-yhteyksiä, mutta SD-WANin alapuolella voi olla myös esimerkiksi normaaleja valokuitu internetliittymiä, Azure ExpressRoute tai vaikka 4G/5G mobiililiittymiä. Varsinainen yhteys ei rajoita juurikaan toiminnallisuuksia, sillä lähes kaikki äly löytyy overlaysta. Tämä mahdollistaa kustannussäästöjä, sillä liikennettä voidaan jakaa halvemmille linkeille ilman esimerkiksi tietoturvan unohtamista.

2.10.2 Overlay

Overlayna toimii SD-WAN, joka luo eräänlaisia virtuaalisia tunneleita toimipisteiden väleihin. Nämä tunnelit muodostuvat käytettyjen underlay-yhteyksien päälle, ja kaikki niissä liikkuva liikenne pakataan ja puretaan tunneleiden päissä. Overlay ei siis varsinaisesti tiedä matkan aikana mitään käytetystä underlay-yhteydestä, sillä se kulkee tunneloituna.



Kuva 15 SD-WAN yhteys MPLS underlaylla

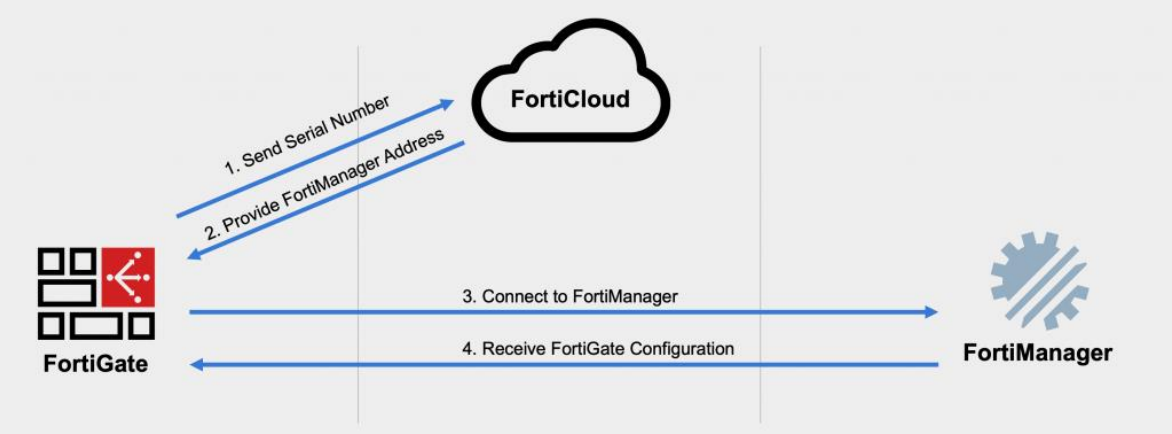
Luonnollisesti palomuurin tulee jollain tavalla päättää, mitä linkkiä käytetään kulloisenkin paketin kohdalla. SD-WANissa palomuuri pystyy monitoroimaan ja seuraamaan eri linkkejä, sekä niiden suorituskykyä. Tämän avulla se pystyy tekemään kulloinkin parhaan mahdollisen päätöksen, jotta paketit saadaan perille halutuilla parametreillä. Priorisoitavana voi olla esimerkiksi vasteaika, tai vaikka kaistanleveys. (Uppal, S., Woo, S. & Pitt, D. 2018.). Palomuuri pystyy poimimaan esimerkiksi liikenteestä Teams-palaverit, jotka voidaan lähettää matalan vasteajan yhteyteen, kun taas kaistaa vaativa tiedostojen lataus voidaan lähettää toista yhteyttä pitkin maailmalle. Näin saadaan kokonaisuudessa mahdollisimman nopea ja kustannustehokas verkko, jonka käyttöaste on mahdollisimman korkea – Miksi maksaa kuukausimaksua yhteydestä, joka on pelkkä varayhteys suurimman osan ajasta?

SD-WAN mahdollistaa myös puhtaissa mobiilitoteutuksissa paremmat yhteydet, sillä eri operaattorien mobiiliyhteyksiä voidaan käyttää saumattomasti yhden palomuurin edessä. Tällöin liikenne menee kulloinkin parhaan mobiiliyhteyden omaavan operaattorin verkossa (Mohamed A., 2019), eikä katvealueita käyttäjän näkökulmasta ole samalla tavalla, kuin vain yhteen operaattoriin turvauduttaessa.

2.11 ZTP

Zero Touch Provisioning tarkoittaa tapaa saattaa laitteita kentälle ”ilman yhtäkään kosketusta”. Tällä viitataan siihen, että laitteen konfiguraatio ei vaadi fyysistä pääsyä laitteeseen. Kaikki vaadittava asetukset voidaan siis määritellä etäyhteydellä, esimerkiksi pilven kautta Fortinetin tapauksessa.

Eri valmistajilla on omat työkalut ZTP:n mahdollistamiseen, Fortinetillä se on FortiDeploy. FortiDeploy mahdollistaa konfiguraation ajamisen laitteeseen FortiManagerista. Kun palomuuri laitetaan päälle konfiguroimatta ja siihen yhdistetään verkkojohto, palomuuri pyrkii saamaan IP osoitteen operaattorin DHCP palvelimelta. Jos tämä onnistuu, palomuuri lähettää kyselyn DNS:n avulla Fortinetin palvelimille FortiCloudiin selvittääkseen onko sen sarjanumerolla FortiDeploy avainta. Jos myös tämä avain löytyy, FortiCloud antaa palomuurille sille osoitetun FortiManagerin IP-osoitteen. Tämän jälkeen palomuuri ottaa yhteyttä tähän FortiManageriin, josta käsin muuri voidaan autorisoida ja yhdistää sen hallintaan. FortiManagerista konfiguraatio voidaan ajaa laitteeseen ilman fyysistä läsnäoloa laitteen luona, mikä tarjoaa varsinaisen ZTP-kyvykkyyden.



Kuva 16FortiDeployn toiminta Travis A. (2021)

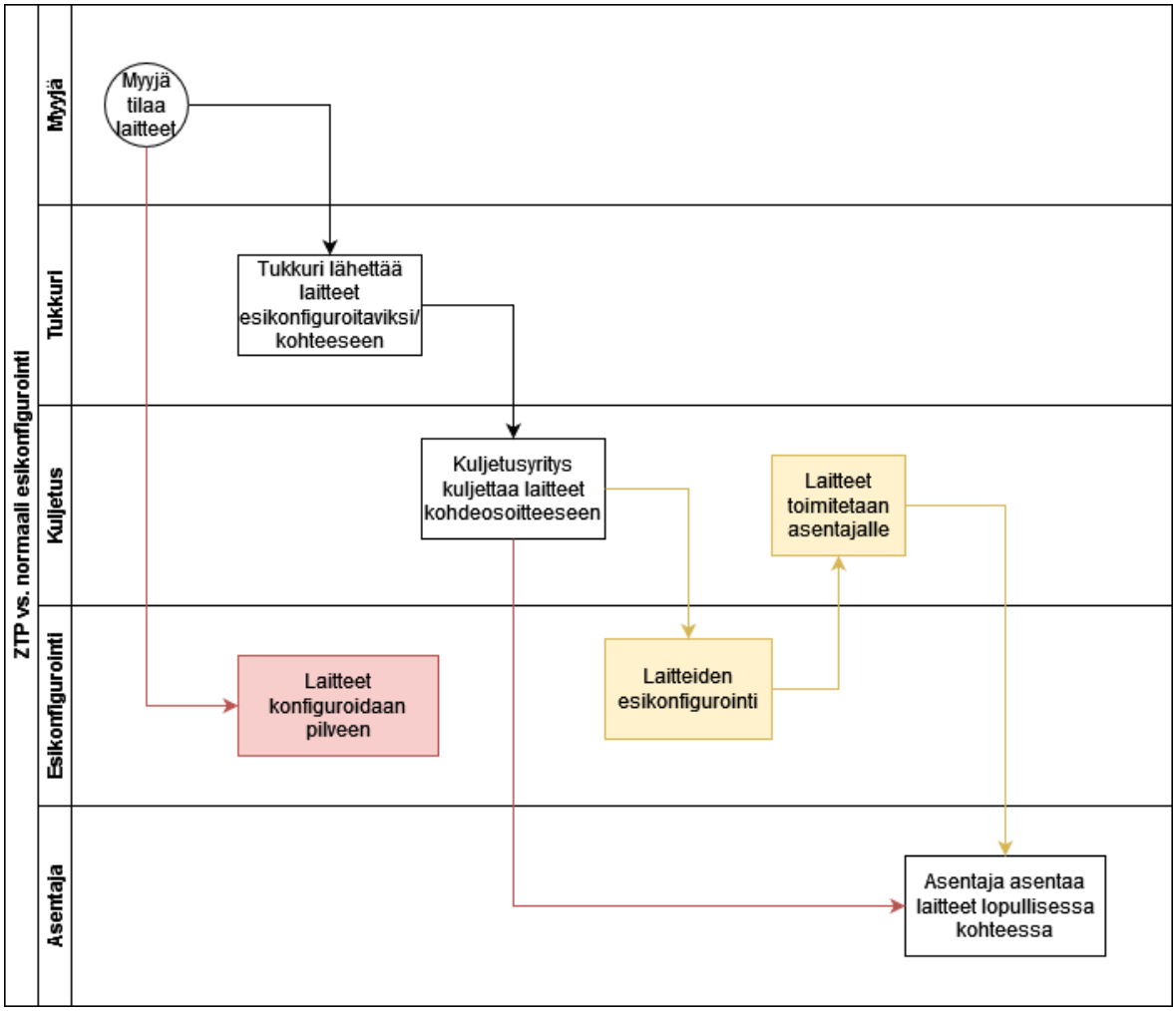
Taka-ajatuksena ZTP:issa on laitteiden helpompi asennettavuus, sekä ylimääräisten ja työläiden työvaiheiden poisto prosesseista. Laitteita ei tarvitse esiasentaa ennakkoon, vaan ne voidaan toimittaa suoraan perille asiakkaalle. Parhaimmillaan kytkennät voi tehdä jopa asiakas, sillä varsinkin pienemmissä toteutuksissa pelkkä verkkoon kytkeminen ja virtajohdon kiinnittäminen riittää asennukseksi. Myös konfigurointiprosessia voidaan

automatisoida, sillä laitteiden korfiguraatio voidaan jakaa keskitetystä paikasta, Fortinetin tapauksessa FortiManagerista.

3 Testattavat laitteet ja testit

Aikaisemmin palomuurien ja muiden verkkolaitteiden konfiguraatio tehtiin asennuksen yhteydessä paikanpäällä. Työvälineiden kehityttyä siirryttiin esikonfiguraatioon, jolloin laite konfiguroidaan ennen asennusta niin pitkälle, kuin mahdollista. Tämä mahdollistaa työn teon joustavammin, sillä konfiguraatio voidaan tehdä aikataulun mukaan sopivassa välissä, eikä kiinteästi asennuksen yhteydessä. Tämän lisäksi mahdollisiin ongelmiin konfiguraatiossa voi tarttua jo hyvissä ajoin ennen käyttöönottoa, konfiguraation edetessä.

Ongelmana molemmissa näissä tavoissa on se, että ne vaativat manuaalista ja fyysistä työtä tekijältä. Varsinaista asennusta varten laitteita on turha purkaa laatikoista esiasennettavaksi, sillä ne joudutaan kuitenkin pakkaamaan niihin uudestaan lähetystä varten. Lisäksi konfiguroijan tulee monesti olla fyysisesti kiinni laitteessa, jotta konfigutointi voidaan suorittaa. Tässä työssä ja siihen liittyvissä testeissä on tarkoitus testata erilaisia tapoja konfiguroida palomuuri käyttövalmiiksi tietyn pohjakonfiguraation osalta etänä. Tarkoitus on saada prosesseista nopeampia ja suoraviivaisempia, ja pyrkiä säästämään työaikaa skripteillä. Tiukemmat prosessit myös tukevat yhtenäisempää konfiguraatiota, sillä mahdollisuus konfiguroida laitteita keskenään eri tavalla pienenee. Myös logistiikka helpottuu, sillä laitteet voidaan toimittaa parhaimmassa tapauksessa suoraan asiakkaalle, eikä kolmannen osapuolen asentajaa välttämättä tarvita laitteiden asennukseen.

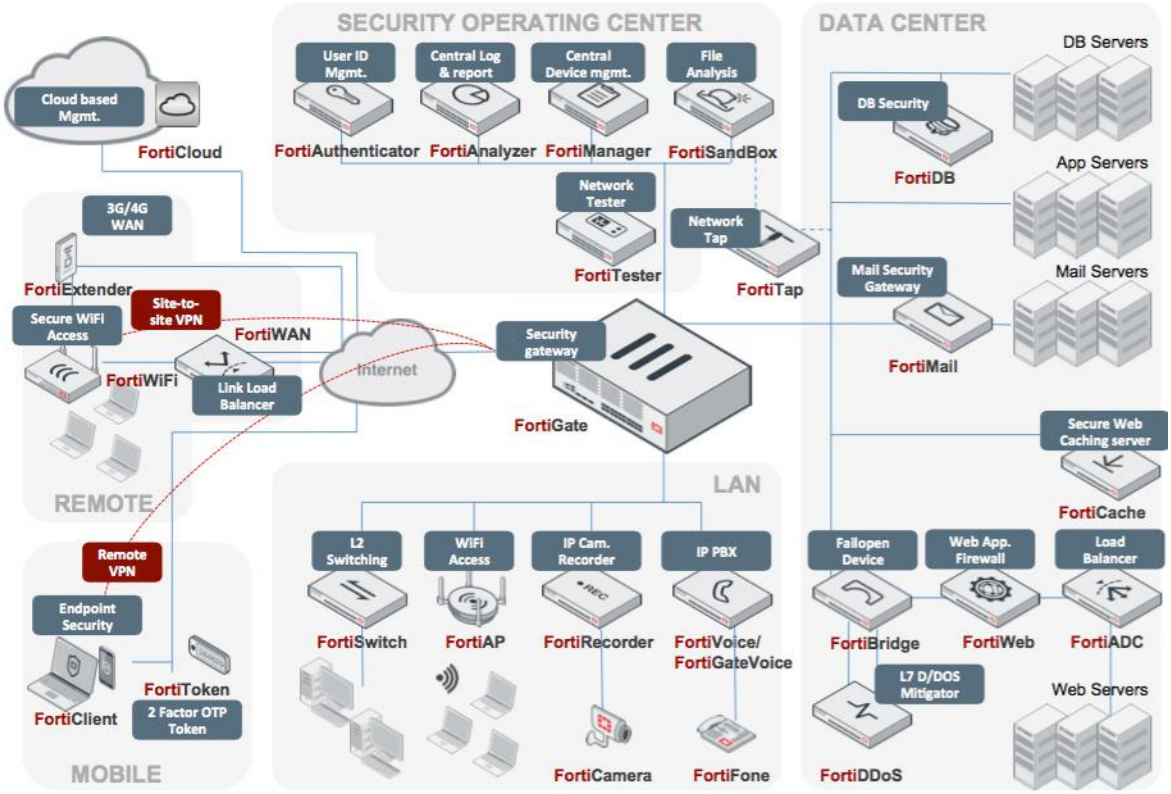


Kuva 17 ZTP vs. normaali esikonfigurointi

Kuvasta 17 nähdään, miten ZTP eroaa logistiikan osalta klassisesta tavasta esikonfiguroida laitteet. Aikaisemmin tukkuri toimitti laitteet palveluntarjoajalle, joka konfiguroi laitteet, ja lähetti eteenpäin loppuasiakkaalle. ZTP:n avulla laitteet voidaan konfiguroida laitevalmistajan pilveen jo toimituksen aikana, minkä lisäksi laitteet voidaan toimittaa suoraan kohdeosoitteeseen. Tämä mahdollistaa pienemmän määrän työvaiheita, minkä lisäksi tyovaiheita voidaan suorittaa rinnakkain. Lisäksi prosessin läpimenoaika pienenee ja ennakoitavuus paranee pienemmän kuljetusmäärän ansiosta. Kuvassa mustavalkoiset kohdat suoritetaan molemmissa toimintatavoissa, punaiset ZTP:tä käytettäessä, ja keltaiset normaalia esikonfiguraatiota käytettäessä.

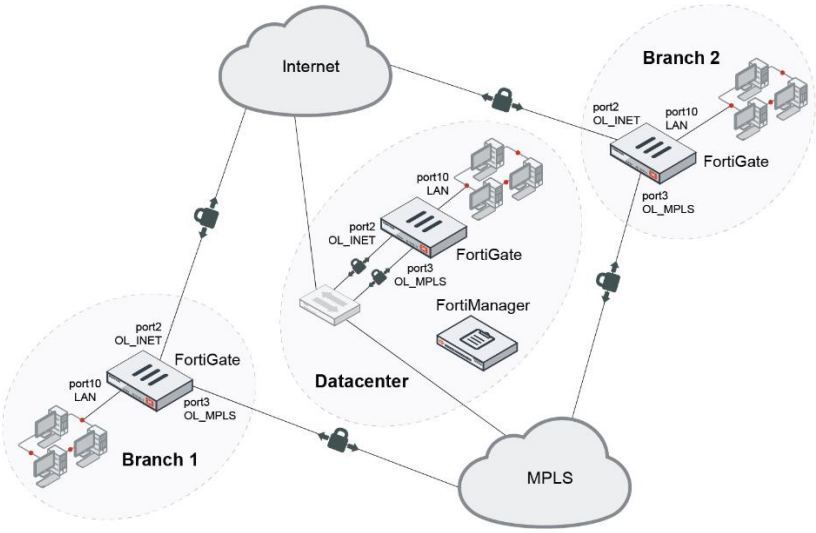
3.1 Testikokoonpano

Koska tämä työ toteutetaan Fortinetin laitteilla, on syytä käydä nopeasti läpi Fortinetin ekosysteemi, ja miten testikokoonpano tulee siihen sijoittumaan.

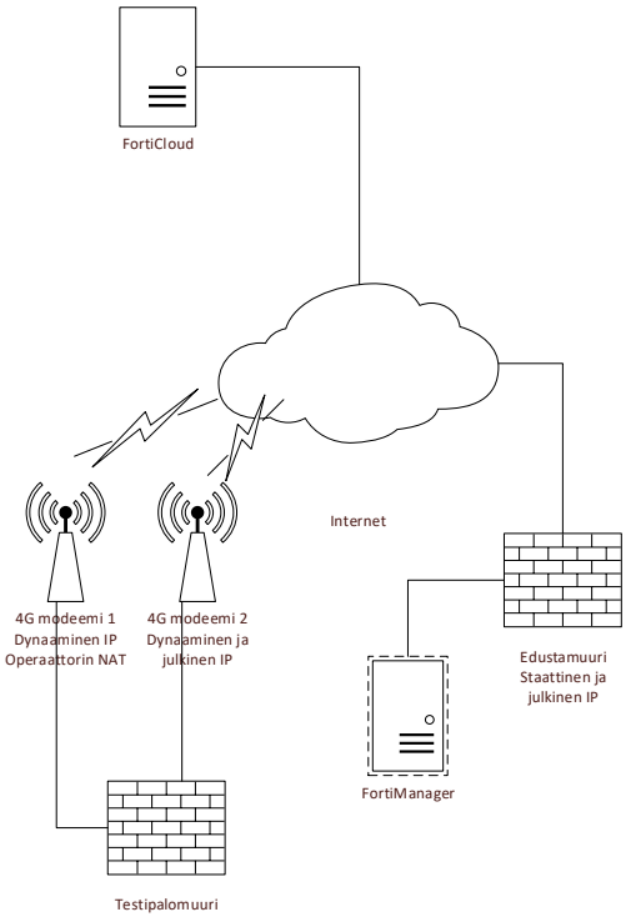


Kuva 18 FortiNetin ekosysteemi. Altaware

Kuvan ”Remote site”:ssä oleva FortiWiFi kuvastaa testattavaa palomuuria, jota pyritään saattamaan konfiguroituun tilaan erilaisilla keinoilla. Keskellä kuvaa oleva FortiGaten kuvastaa palomuuria, johon luodaan VPN yhteydet, ja security operating centerissä näkyvä FortiManager toimii hallintapisteenä muureille. Karsitumpi kuva kokoonpanosta voisi näyttää tältä:



Kuva 19 Fortinetin esimerkki ADVPN topologiasta. Fortinet



Kuva 20 Varsinainen kuva testiympäristöstä

Kuva 20 hahmottaa, miten varsinainen testiympäristö muodostuu. FortiCloud on toteutuksessa mukana niiden testien osalta, jossa sitä käytetään, muutoin testit ovat hyvin pitkälti testipalomuurin ja FortiManagerin välisiä.

Testipalomuurina toimii Fortinetin FortiWiFi 40F-3G4G (jatkossa 40F yksinkertaisuuden vuoksi). Laite eroaa 40F-perusmallista siten, että siinä on sisäänrakennettu modeemi 3G- tai 4G-liittymälle, sekä sisäänrakennettu langaton tukiasema. Tämä edustaa pienen toimipaikan mahdollista esimerkkikokoonpanoa hyvin, sillä erillisiä laitteita eri toiminnoille ei välttämättä tarvita. Suuremmat laitteet tarjoavat enemmän ominaisuuksia, joten toiminta pienellä ”all-in-one” laitteella on hyvä varmistaa käyttöönoton skaalautumiseksi kaikille laitteille.

Tässä kyseisessä työssä ei kuitenkaan hyödynnetä laitteen sisäänrakennettuja mobiili- tai WiFi yhteyksiä, sillä ne eivät vaikuta laitteen konfigurointiin, hallintayhteyksiin tai SD-WAN:iin

40F edustaa uuden sukupolven palomuureja (NGFW, Next Gen Firewall)[https://www.fortinet.com/blog/business-and-technology/redefining-next-generation-firewalls]. Tämä tarkoittaa aikaisempiin palomuureihin verrattuna sitä, että liikennettä voidaan tutkia, nähdä ja suodattaa OSI-mallin korkeammilla tasoilla. Laite siis osaa ottaa kantaa paketteihin sisällön lisäksi sormenjälkien ja muiden tunnisteiden avulla, jotta isoa liikennemäärää ja poikkeuksia voidaan käsitellä kokonaisuuksina.

Tässä työssä palomuurisäännöt eivät hyödynnä NGFW-ominaisuuksia, sillä työn tarkoitus ei ole tutustua erilaisiin palomuurisääntöihin. Palomuurisäännöt ovat mahdollisimman yksinkertaisia työn ymmärrettävyyden kannalta

Palomuurin lisäksi testikokoonpanoon kuuluu 2 kappaletta ZTE:n MF286D 4G-modeemeja. Erillisten 4G-modeemien käyttämisessä on monta monta syytä: Ensinnäkin internet saadaan palomuurille ethernetillä verkkojohtoa pitkin, minkä ansiosta testi pätee myös kuitu, VDSL tai muille langallisille yhteyksille. Toiseksi, tämä mahdollistaa testin pätevyyden myös laitteisiin, joissa ei ole sisäänrakennettua 3G/4G-modeemia. Kolmanneksi, tällä tavalla saadaan käyttöön 2 eri yhteyttä, jotta liiketoiminnalta saatu vaatimus SD-WAN:in käytöstä toteutuu.

Laitteisiin on testiä varten hankittu 3 erilaista Elisan 4G-liittymää: Ensimmäinen liittymä on dynaamisella IP-osoitteella operaattorin NAT:n takana. Tämä edustaa halvinta mahdollista

liittymätyyppiä, eikä mahdollista IP-osoitteen esikonfigurointia verkkolaitteeseen, koska IP saadaan operaattorilta DHCP:llä. Toinen liittymätyyppi on vastaava Elisan 4G liittymä dynaamisella IP-osoitteella, mutta se ei sisällä NAT:ia, eli IP-osoite on julkinen. Tämän pitäisi mahdollistaa paremmin yhteydenotto laitteeseen. IP-osoite on kuitenkin myös tässä liittymässä dynaaminen, eli sitä ei voida konfiguroida staattisesti palomuurille. Kolmas liittymä on Elisan 4G julkisella kiinteällä IP-osoitteella. Tämä mahdollistaa tarpeen mukaan IP-osoitteen konfiguroinnin staattisesti palomuurille, jos käyttö sitä vaatii. Tämä liittymä on myös kallein, joten sen käyttö on suotavaa vain tarpeen niin vaatiessa.

Tukemassa konfiguraatiota on käytössä myös FortiManager, mikä on asennettu virtuaalialustalle. Tämän edessä on 61F palomuuri, jota käytetään lähinnä liikenteen ohjaamiseen FortiManagerille hallintayhteyttä varten.

3.2 Konfiguraatio

Pelkät laitteet eivät kuitenkaan riitä, vaan ne tulee konfiguroida testiä varten. Seuraavaksi käydään läpi testissä käytettyjen laitteiden konfigurointi ja konfiguraatiot. Konfiguraatiot on pyritty pitämään mahdollisimman yksinkertaisina, ja keskittyä testin kannalta oleellisiin asioihin. Tuotantokäytössä tarvitaan huomattavasti enemmän työtä, mutta nämä jätetään pois tästä työstä, sillä ne eivät liity työn aiheeseen.

3.2.1 ZTE MF286D

ZTE:n 4G-modeemia käytetään vakioasetuksilla siltaavassa tilassa. Tämä mahdollistaa langattoman mobiiliyhteyden muuntamisen langalliseen muotoon siten, että palomuuri saa suoraan IP-osoitteen operaattorilta ilman välissä olevaa 4G-reititintä. Tuotantokäytössä yhteys voi olla myös esimerkiksi kuituyhteys, tai toisen operaattorin yhteys, eikä varsinainen media ole oleellista tämän työn kannalta. Testeissä kokeillaan myös NAT:in takana dynaamisella IP-osoitteella olevat yhteydet, sillä ne ovat niin sanotusti pahin mahdollinen skenaario verkon osalta. Kiinteällä ennalta tiedetyllä IP-osoitteella voidaan tehdä erilaisia toteutuksia josutavammin, mutta natattu dynaaminen IP-ei mahdollista yhteyden luontia hallintapalvelimelta laitteeseen IP-osoitteella. Tämä johtuu siitä, että IP-osoite ei ole tiedossa

sen dynaamisen luonteen vuoksi. Toiseksi NAT estäisi laitteeseen yhteyden muodostamisen ilman ylimääräistä konfiguraatiota.

Siltaavassa tilassa laite tarjoaa langallisen yhteyden portista WAN/LAN1, eikä muut portit ole käytettävissä.

3.2.2 FortiGate 40F

40F:n konfiguraatio voidaan jakaa karkeasti kolmeen osaan. Ensimmäinen osa kattaa laitteen perustiedot, kuten hostnamen. Toinen osa kattaa SD-WAN- konfiguraation, jonka avulla voidaan käyttää molempia kytkettyjä internet-yhteyksiä samanaikaisesti halutun säännöstön mukaan. Kolmas osa sisältää laitteen hallintayhteyden Elisan hallintatyökaluihin, jotta laitteisiin päästään kiinni etänä hallintaa ja seurantaa varten.

Testilaitteen versio oli toimituksessa 6.2.5, mikä ei edusta uusimpia päivityksiä. Ennen konfiguraatiota laite päivitettiin uusimpaan saatavilla olevaan (16.2.2022) versioon 6.4. julkaisusta, joka oli 6.4.8.

Testilaitteen hostnameksi valitaan ”elisa-sd-wan-fw1”. Testien yhteydessä nimestä pyritään mahdollisuuksien mukaan vaihtamaan numero, mikä mahdollistaa kohteiden nimeämisen loogisesti. Samalla aikavyöhykkeeksi valitaan Suomen aika.

```
config system global
    set hostname "elisa-sd-wan-fw1"
    set timezone 35
end
```

Laitteen käynnistämiseen liittyvistä asetuksista otetaan sekä ”detect configuration”, että “detect firmware” pois päältä. Näillä asetuksilla laite voidaan joko konfiguroida tai päivittää USB-portin kautta, jos laitteeseen päästään fyysisesti käsiksi. Laitteiden hallinta tapahtuu joko hallintayhteyden yli, tai lokaalisti konsoliyhteydellä, joten tälle ominaisuudelle ei ole tarvetta.

Oletusarvoisesti laitteessa on vain 1 konfiguroitu WAN-portti. Portit 1-3 ovat virtuaalisena kytkimenä, ja portti a on tarkoitettu fortilinkille, jos halutaan käyttää fyysisiä Fortinetin laitteita kuten kytkimiä palomuurin perässä. Jotta SD-WAN:ia varten saadaan myös toinen

WAN-portti, tulee oletuskonfiguraatiosta poistaa lan-portti virtuaalisen kytkimen osalta. Tämä tapahtuu cli:n kautta seuraavilla komennoilla:

```
config system virtual-switch
    edit "lan"
        config port
            delete lan2
            delete lan3
        end
    end
end
```

Nämä komennot poistavat lan2 ja lan3 -portit virtuaalisesta kytkimestä, jotta niitä voidaan käyttää internetyhteyteen. Tässä työssä näistä vain lan2 tullaan ottamaan käyttöön WAN-yhteyksille.

SD-WAN-konfiguraatio porteille WAN ja lan2 luodaan SD-WAN-zoneista. Oletusarvoisesti laitteessa on SD-WAN-zone nimeltä ”virtual-wan-link”, mikä käy hyvin nimeksi. Virtuaalisesta kytkimestä irrotettu lan2-portti voidaan lisätä suoraan zoneen jäseneksi, mutta wan-portin lisääminen vaatii oletusarvoisten palomuurisääntöjen poistamista. Normaalisti palomuureissa on vain deny sääntö, mutta testikäytössä olevassa WiFi + 4G -mallissa wan-portti on osallisena sisäverkkoa koskevissa säännöissä. Kun kaikki ylimääräiset säännöt on poistettu, voidaan wan-portti lisätä toiseksi jäseneksi SD-WAN-zoneen.

```
Config system sdwan
    Set status enable
    Set load-balance-mode measured-volume-based
    Config members
        Edit 0
            Set interface “lan2”
        next
        Edit 0
```

```
            Set interface “wan”
        Next
    End
End
```

Lisäksi tarvitaan staattinen reitti SD-WAN liitännälle.

```
config router static
    edit 1
        set distance 1
        set sdwan enable
    next
end
```

Tässä työssä varsinaiseen SD-WAN-säännöstöön ei perehdytä sen tarkemmin, joten kuormanjako ja linkkien käyttö jätetään automaattisille asetuksille. Reaalimaailmassa näitä asetuksia muokattaisiin asiakkaan toiveiden mukaisesti. Sekä käytettävissä olevien yhteyksien ja yhteystyyppien perusteella. Portit jätetään ilman staattista IP-osoite-konfiguraatiota. DHCP määritellään päälle, jotta laitteeseen saadaan yhteys testatessa. Jos liittymät tarjoavat kiinteitä IP-osotteita, voidaan konfiguraatiolla ajaa nämä laitteelle staattisia reittejä unohtamatta.

Internetyhteyksiin WAN-portin lisäksi valikoitui LAN2 seuraavana vapaana porttina. Lopullisessa tuotantokäytössä käytetyt portit tulee suunnitella ratkaisun mukaisella tavalla porttien, sekä porttimäärän osalta.

Testimuurille tulee seuraavaksi konfiguroida dial up VPN -tunneli, jotta muuriin päästään käsiksi hallintaverkosta, ja se voidaan lisätä valvontaan. Tunneli on asetettu välittämään lokaali verkko (192.168.1.0/24 tässä testissä) FortiManagerin edustamuurille ja sitä kautta FortiManagerille, mutta tämä tulee allokoida toimipistekohtaisesti tuotannossa. Tunnelit on luotu testimuurilla molemmille nettiliittymille (ADVPN with BGP as the routing protocol, 2020)

Dial up tunnelit luodaan testimuurin molempiin 4G underlay yhteyksiin erikseen, eli muurille tulee 2 dial up VPN:ää. Dial up palvelimen, eli edustamuurin asetukset:

Dial up clientin, eli testimuurin asetukset:

```
config vpn ipsec phase1-interface
    edit "dialup_vpn_w"
        set interface "wan"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device disable
        set proposal aes256-sha256
        set localid "dialup_peer"
        set dhgrp 21
        set remote-gw <remote ip>
        set tunnel-search nexthop
        set psksecret <salasana>
    next
    edit "dialup_vpn_l"
        set interface "lan2"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device disable
        set proposal aes256-sha256
        set localid "dialup_pee2"
        set dhgrp 21
        set remote-gw <remote ip>
```

```
        set tunnel-search nexthop
        set psksecret <salasana>
    next
end
config vpn ipsec phase2-interface
    edit "dialup_vpn_w"
        set phase1name "dialup_vpn_w"
        set proposal aes256-sha256
        set dhgrp 21
        set keylifeseconds 3600
    next
    edit "dialup_vpn_l"
        set phase1name "dialup_vpn_l"
        set proposal aes256-sha256
        set dhgrp 21
        set keylifeseconds 3600
    next
end
```

Aluksi tunnelit terminoitiin yhteen dial-up-VPN-yhdyskäytävään, mutta ongelmaksi muodostui tunneleiden ”lepattaminen” ylös ja alas. Ongelma korjattiin luomalla kaksi erillistä dial-up-VPN-yhdyskäytävää edustamuurille. Testilaitteen underlay-yhteyksien tunnelit muodostetaan kumpaankin yhdyskäytävään siten, että wan1-portin yhteys kohdistetaan gatewayhin 1, ja lan2-portin yhteys kohdistetaan yhdyskäytävään 2. Tällöin tunnelit pysyivät ylhäällä, ja näiden molempien kautta pystyttiin välittämään testissä liikennettä.

```
config system interface
    edit "dialup_client_w"
        set vdom "root"
        set ip 11.11.11.1 255.255.255.255
        set type tunnel
```

```
        set remote-ip 11.11.11.254 255.255.255.0
        set snmp-index 0
        set interface "wan"
    next
    edit "dialup_vpn_1"
        set vdom "root"
        set ip 11.11.12.1 255.255.255.255
        set type tunnel
        set remote-ip 11.11.12.254 255.255.255.0
        set snmp-index 0
        set interface "lan2"
    next
end
```

Lisäksi reititys hoidetaan BGP:llä.

```
config router bgp
    set as 65412
    config neighbor
        edit "11.11.11.254"
            set advertisement-interval 1
            set link-down-failover enable
            set remote-as 65412
        next
        edit "11.11.12.254"
            set remote-as 65412
        next
    end
    config network
        edit 1
            set prefix 192.168.1.0 255.255.255.0
        next
```

```
    end
end
```

Näissä asetuksissa verkot 11.11.11.0/24 sekä 11.11.12.0/24 ovat käytössä toimipistemuureille. Tuotantokäytössä nämä alueet tulee suunnitella tarpeen mukaan niin avaruuden, kuin verkon suuruuden osalta. Aliverkkojen viimeiset osoitteet, eli .254 on varattu FortiManagerin edustamuurille, johon tunnelit terminoidaan. Toimipisteiden numerointi alkaa osoitteista 11.11.11.1 ja 11.11.12.1.

Palomuurisäännöt

Palomuurisäännöt eivät ole tämän työn ydin, mutta FortiGate vaatii VPN-tunneleille vähintään yhden säännön, jotta ne voivat nousta ylös. Tämän vuoksi luodaan seuraavat säännöt testejä varten.

```
config firewall policy
    edit 0
        set name "netti"
        set uuid dfa1fc0c-8f2f-51ec-cf03-57afe7c81461
        set srcintf "internal"
        set dstintf "virtual-wan-link"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
    edit 0
        set name "dialup"
        set uuid eea4858e-b9dd-51ec-82eb-671c2e558586
        set srcintf "dialup_vpn_w"
        set dstintf "internal"
        set srcaddr "all"
        set dstaddr "all"
```

```
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 0
        set uuid 9c9acfe0-b9de-51ec-107c-1d331a6af513
        set srcintf "internal"
        set dstintf "dialup_vpn_w"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 0
        set name "dialup_vpn_l"
        set uuid 525bf8ea-b9df-51ec-0381-145dcc2b6bb5
        set srcintf "dialup_vpn_l"
        set dstintf "internal"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 0
        set uuid 56a9393a-b9df-51ec-7395-0af854ccc0b2
        set srcintf "internal"
        set dstintf "dialup_vpn_l"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

Säännöt siis käytännössä sallivat kaiken liikenteen FortiManagerin verkosta toimipisteverkkoon, sekä toisin päin.

3.3 FortiManager

Koska testattavan konfiguraation tarkoitus on jäljitellä realimaailman ympäristöä, tulee testitoimipiste liitettäväksi FortiManageriin. FortiManager on Fortinetin työkalu, jolla voidaan hallita suurta määrää laitteita. FortiManager voi olla fyysinen laite, mutta myös palvelimelle asennettava järjestelmä. Tässä työssä käytössä on VMWaren päälle asennettu FortiManager 6.4.7., mikä edusti uusinta versiota 6.4. ohjelmistojulkaisusta asennushetkellä (31.3.2022).

Itse FortiManagerissa ei ole kovin kummoista konfiguraatiota, sillä se ei ole tämän työn aihe. Kuitenkin eri konfiguraatiotapojen tulee saada yhteys FortiManageriin, jotta tuotantokäytössä ne olisivat realistisia vaihtoehtoja. Myös osa konfiguraatioista vaatii FortiManageria, jolloin sinne asetetaan vaaditut pohjat.

Testimuuri asetetaan ottamaan yhteys FortiManagerin edustamuurin IP-osoitteella, josta DNATilla (Virtual IP, Destination NAT) liikenne ohjataan FortiManagerille. Kun testimuuri on lähettänyt pyynnön rekisteröityä FortiManageriin, tulee käyttäjän hyväksyä se Managerin käyttöliittymästä. Tämän jälkeen laitetta voi konfiguroida yksilönä tai ryhmän kautta FortiManagerista, mikä mahdollistaa esimerkiksi ennakkoon luodun konfiguraation tiputtamisen laitteelle. Laitetta ei voida lähtökohtaisesti lisätä FortiManagerista käsin, sillä liittymät ovat monesti NATin takana, joten niihin ei voida ottaa suoraa yhteyttä IP-osoitteella.

Tässä työssä osassa ratkaisumalleja käytetään Fortimanageria konfiguraation toimittamiseen palomuurille. Konfiguraatio tulee kuitenkin luoda, sillä osa konfiguraatiosta on aina toimipistekohtaista. Tätä varten FortiManageriin voidaan luoda sktriptejä, joihin asetetuilla muuttujilla toimipisteen konfiguraatio voidaan luoda automaattisesti laitteelle toimitettavaksi. Lisäksi muut ominaisuudet, joita tässä työssä ei käsitellä, kuten langaton verkko, voidaan määritellä kätevästi ryhmien avulla ilman suurempia haasteita.

3.4 Testattavat konfigurointitavat

Työn tarkoitus on testata palomuurin konfigurointia mahdollisimman nopeasti ja tehokkaasti siten, että se on mahdollista skaalata isoihin määriin. Konfigurointiin käytetään seuraavia tapoja: laitteen fyysinen konfigurointi konfiguraatiopohjan avulla, laitteen konfigurointi asennuspaikalla muisitikun avulla, laitteen konfiguraation jakaminen FortiManagerista, sekä laitteen konfiguraation jakaminen Fortinetin ZTP-lisenssillä.

3.4.1 Konfigurointi manuaalisesti

Konfiguraatio manuaalisesti voidaan tehdä komentorivin tai graafisen käyttöliittymän kautta muuttamalla halutut asetukset toimipistekohtaiseksi. Tällöin laitteelle tulee ensin ladata jokin pohjakonfiguraatio, jotta universaalit asetukset saadaan käyttöön. Konfiguraatiopohja voidaan tiputtaa laitteelle käyttöliittymän kautta. Kun laitteella on muutettu toimipistekohtaiset muuttujat, voidaan laite pakata ja lähettää asennukselle.

Toinen vaihtoehto on muokata konfiguraatiopohjaa sopivalla tekstieditorilla, esimerkiksi Notepad++:lla, ja luoda siihen suoraan toimipistekohtainen konfiguraatio. Tällöin konfiguraatio voidaan tiputtaa suoraan laitteelle. Toimipistekohtaiset konfiguraatiomuutokset voidaan myös ajaa tiedostoon skriptillä, mikä nopeuttaa prosessia.

3.4.2 Konfigurointi kentällä muistitikulla

Oletusarvoisesti Fortinetin palomuurit tukevat käynnistyksen yhteydessä päivittymistä sekä konfiguraation lataamista muistitikulta. Nämä ominaisuudet voi ottaa väärinkäytön ehkäisemiseksi pois päältä konfiguraatiossa, mutta niitä voi hyödyntää asennuksessa.

Tässä vaihtoehdossa laitteelle ei tehdä esiasennusta, vaan se lähetetään suoraan asentajalle kohteeseen. Kun asentaja asentaa laitetta, hän liittää palomuuriin muistitikun, johon on tallentanut saamansa konfiguraation asennuksen tukihenkilöltä. Tämä konfiguraatio tulee toki luoda etukäteen, mutta se ei vaadi fyysistä laitetta. Kun asentaja laittaa laitteeseen virrat päälle, palomuuri lataa konfiguraation muistitikulta.

Käytännössä tämä vaihtoehto on hyvin samanlainen kuin edeltävä, mutta laitetta ei esiasenneta operaattorin toimesta. Tämä helpottaa logistiikkaa, mutta toisaalta laitteiden toimintaa ja konfiguraation oikeellisuutta ei voida varmistaa ennakkoon.

3.4.3 Konfigurointi FortiManagerin kautta

Konfiguroinnissa Fortimanagerin kautta ideana on se, että palomuuri lisätään aluksi FortiManageriin. Tämän jälkeen laitteen konfiguraatio ajetaan FortiManagerista pohjia hyväksikäyttäen. Tässä ratkaisussa ongelmana on palomuurin yhdistäminen FortiManageriin, sillä se tarvitsee joko yhteyden manuaalisen konfiguroinnin palomuuriin, tai laitteen lisäämisen IP-osoitteella käyttäen palomuurin käyttäjätunnusta. Konfiguroimattomassa laitteessa käyttäjätunnus on tehtaalta tullessaan admin ilman salasanaa, joten palomuuria ei voida avata hallinnan osalta internettiin ilman tunnusten päivittämistä. Toki oletusarvoisesti FortiManager pääsy on sallittuna WAN-porteista.

Palomuuria ei voida myöskään lisätä hallintaan FortiManagerista käsin, jos asennettavan palomuurin yhteydet ovat NAT:in takana, tai jos laitteen IP-osoite ei ole tiedossa. Toinen rajoite näissä tavoissa on se, että jos operaattori ei tarjoa verkossaan DHCP:tä, ei palomuuri saa IP-osoitetta ilman konfiguraatiota. Tällöin IP-osoite on annettava laitteelle tavalla tai toisella, jotta se saa yhteyden internettiin.

3.4.4 Konfigurointi Fortinetin ZTP:lla

ZTP:n idea on nimensä mukaisesti Zero Touch Provisioning. Fortinetin muurien osalta tämä tarkoittaa erillistä lisenssiä, joka yhdistetään palomuurin sarjanumeroon. Kun laite laitetaan verkkoon, se soittaa Fortinetin pilveen. Pilvestä laite saa lisenssillä tiedot FortiManagerista, johon laite yhdistää, ja josta laite käy lataamassa konfiguraation.

Tässä tavassa pätee hyvin pitkälti edellisen tavan rajoitteet: Laitteen on saatava IP-osoite operaattorilta DHCP:llä, jotta se voi ottaa yhteyttä internettiin, ja yhdistää itsensä FortiManageriin.

Tämä konfigurointitapa edustaa tässä työssä kaikista automatisoiduinta tapaa tiputtaa laitteelle haluttu konfiguraatio.

4 Testit

4.1 Manuaalinen konfigurointi

Manuaalinen konfigurointi alkaa konfiguraatiotiedosto muokkaamisella. Testikonfiguraatiossa tämä tarkoittaa laitteen hostnamen päivttämistä, sekä laitteen VPN-tunneleiden IP-osoitteiden määrittämistä. Lisäksi paikallisten LAN-verkkojen IP-avaruus pitää muuttaa toimipistekohtaiseksi

Hostname on testimuurin tapauksessa Elisa-sd-wan-testi. Laitteiden VPN-tunneleiden IP-osoitteiksi testiä varten valitaan 11.11.11.1, sekä 11.11.12.1.

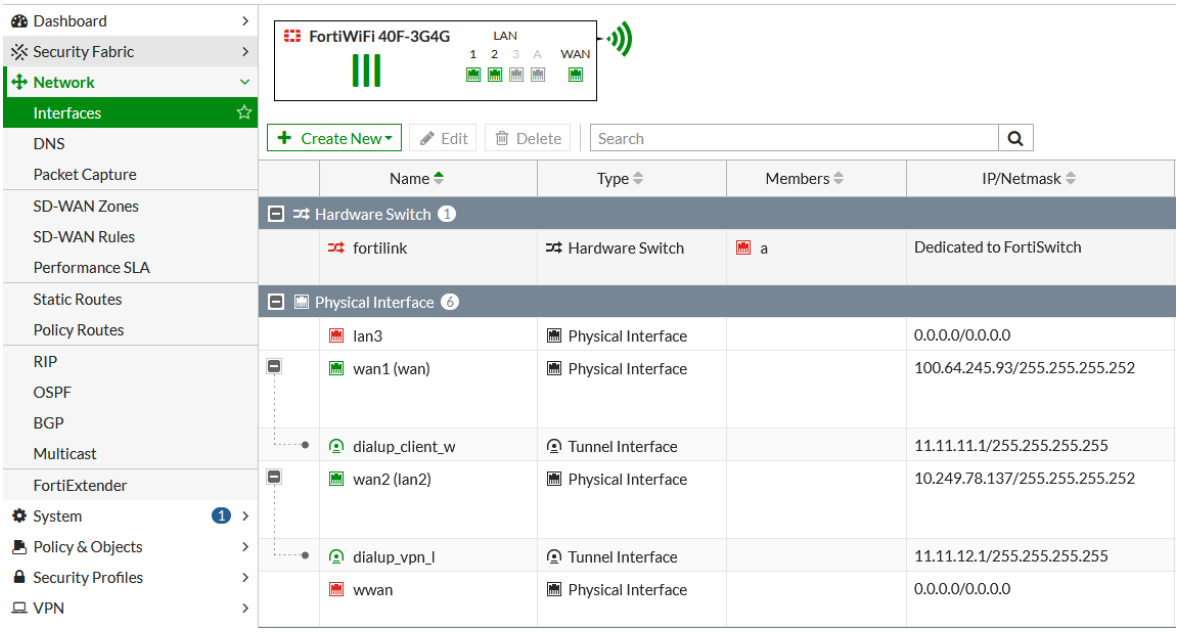
Konfigurointi tapahtuu konfiguraatiotiedostosta etsimällä kentän ”hostname”, sekä kentät ”dialup_vpn_w” ja ”dialup_vpn_l”. Kun tiedot ovat muutettu, kirjaudutaan sisään tehdasasetuksilla olevalle muurille.

Edeltävä toimenpide voidaan myös suorittaa skriptillä. Tässä työssä konfiguratio on hyvin yksinkertainen, joten skripti ei juurikaan nopeuta prosessia. Laajemmassa konfiguraatiossa tällä voidaan kuitenkin säästää aikaa, sillä esiasentajan ei tarvitse etsiä konfiguraatiosta itse muutettavia kohtia, vaan riittää, että hän kertoo skriptille esimerkiksi saitin ID:n (VPN:n IP-osoitteisiin), sekä hostnamen.

Yhdistäminen konfiguraation luonnin jälkeen tapahtuu rj45-kaapelilla, mikä liitetään palomuuriin porttiin 1 (lan1). Toinen pää liitetään kannettavaan tietokoneeseen, jolla palomuuria konfiguroidaan. Palomuuri antaa oletusarvoisesti portista 1 IP-osoitteen DHCPllä, joka on aliverkosta 192.168.1.0/24. Palomuurin IP-osoite on 192.168.1.99. Tässä testissä IP otetaan DHCP:llä, mutta konfiguroija voisi valita oman IP-osoitteen myös staattisesti edeltävästä aliverkosta. Syöttämällä selaimeen osoitteen https://192.168.1.99 päästään palomuurin kirjautumissivulle. 6.2.x edeltävissä versioissa toimii oletustunnukset admin/<blank>, uudemmissa versioissa tunnusten syöttämisen jälkeen kysytään uutta salasanaa. Testiä varten valitaan salasanaksi ”testimuuri”. Valinnalla ei ole juurikaan merkitystä, sillä laite ei ole vielä verkossa, ja siihen tallennettava konfiguraatio tulee ylikirjoittamaan valitun salasanan.

Muurille päästyä laite päivitetään ensin uuteen versioon, tässä työssä 6.4.8. Päivitys tapahtuu klikkaamalla graafisessa käyttöliittymässä ruudun ylä oikeasta laidasta ”admin”, jonka takaa avautuvasta valikosta ”system” ja ”firmware”. Tämän jälkeen valitaan koneelta tiedosto, jolla päivitys suoritetaan. Päivityksen jälkeen laitteelle viedään konfiguraatiotiedosto. Tämä tapahtuu samalla tavalla yläoikeasta laidasta ”admin” valikon takaa, josta löytyy ”configuration” ja ”restore”. Konfiguraation lisäämisen jälkeen palomuuri käynnistää itsensä uudestaan, ja on valmis liitettäväksi verkkoon. Laitteen porteihin wan, sekä lan2 liitetään 4G-modeemit, jotka jakavat porteille IP-osoitteet DHCP:llä.

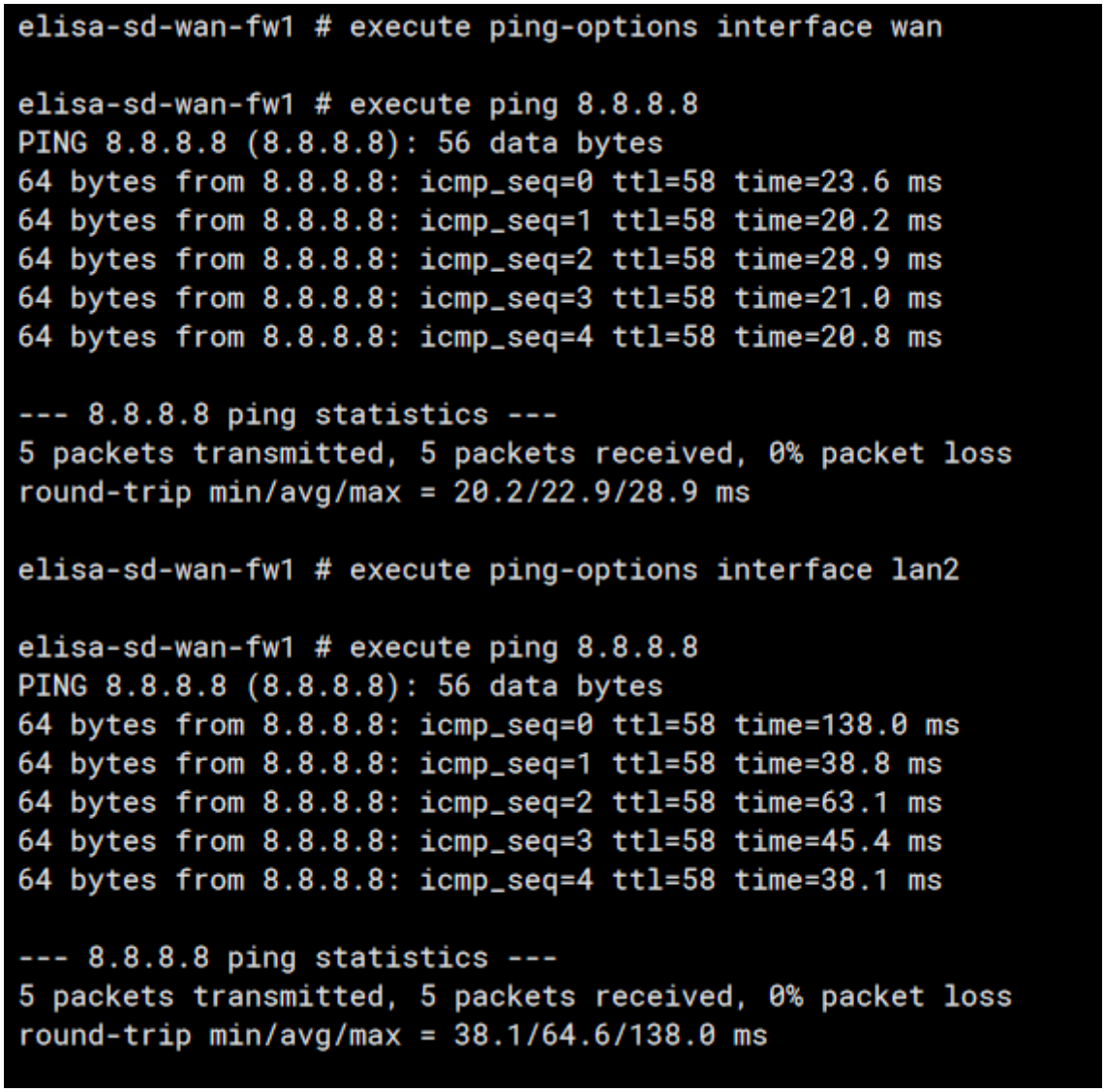
Kun palomuuri on kytketty verkkoon, tarkistetaan, että molemmat portit saavat IP-osoitteet, ja VPN-tunnelit ovat ylhäällä. Tämä nähdään Interfaces-välilehdestä.



Kuva 21palomuurin liitännät

Tämän jälkeen testataan verkon toimivuus avaamalla konsoli selainnäkymän yläoikeasta kulmasta. Molemmat underlay-yhteydet voidaan testata esimerkiksi seuraavilla komennoilla:

```
Execute ping-options interface <nimi>
Execute ping 8.8.8.8
```



Kuva 22 Yhteystestit kummallakin underlay- yhteydellä

Seuraavaksi laite lisätään FortiManageriin. Laitteen konfiguraatio osaa automaattisesti muodostaa yhteyden, joten käyttäjän tulee tässä hyväksyä laite FortiManagerista sen jäseneksi. Tämän jälkeen laite on saatu asennettua tämän työn vaatimaan tilaan.

Manuaalinen konfiguraatiotapa toimi, ja palomuuri saatiin yhdistettyä FortiManageriin. Lisäksi testit menivät läpi. Toimintatapa on kuitenkin hyvin manuaalinen, ja vaatii laitteiden purkua pakkauksista. Tämä johtaa väistämättä tehottomaan toimintaan, sillä laitteet joudutaan pakkaamaan uudestaan asentajalle lähetettäviksi. Lisäksi logistiikka monimutkaistuu, sillä laitteita ei voida lähettää suoraan asentajalle, vaan ne tulee kierrättää esiasennuksen kautta. Tämä tapa ei myöskään skaalaudu kovin helposti, sillä mekaanista työtä on paljon.

Positiivisina huomioida laitteiden toiminta voidaan varmistaa ennen lähetystä, mikä ehkäisee DoA (Dead on Arrival)-laitteiden lähetystä asennettavaksi. Lisäksi konfiguraatio voidaan varmistaa laitteessa ennen asennusta, mikä vähentää riskiä virheistä. Mikäli esiasentajalla on myös asiakkaalle toimitettavat 4G-yhteydet käsillä, hän voi testata verkon toiminnan, sekä lisätä laitteen FortiManageriin jo ennen asennusta. Laite myös päivitetään ennen asennusta, mikä vähentää riskejä etäpäivitykseen verrattuna. Myös asennusaika asiakkaan luona pienenee, sillä konfiguraatiot on asennettu ja testattu ennakkoon.

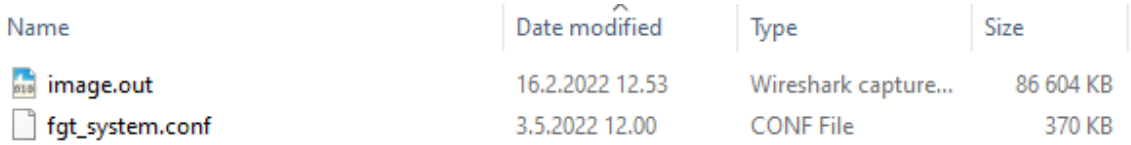
Lisäksi pidemmän konfiguraation muokkaaminen laitekohtaiseksi on aikaavievää ja itseään toistavaa puuhaa, mutta tämä voidaan kiertää luomalla skripti, joka avustaa esiasentajaa konfiguraation luonnissa. Skripti kuitenkin tulee luoda sellaiseksi, että se toimii halutuissa laitemalleissa, ja tarvittaessa myös vähän erilaisilla konfiguraatiopohjilla.

Konfiguraation luoneena sen muokkaaminen tässä testissä oli helppoa, joskin manuaalista työtä. Tuotannon esiasentajaa varten tulee kuitenkin tehdä helppolukuiset ohjeet, jotta prosessi on toistettavissa myös uusien työntekijöiden kohdalla.

4.2 Konfiguraatio USB-tikulla

USB-tikulla konfigurointi muistuttaa hyvin paljon manuaalista konfigurointia. Isoin ero tässä on muistitikun käyttö, mikä mahdollistaa palomuurin konfiguroinnin ilman minkäänlaista yhteyttä palomuuriin, oli se sitten konsolikaapelin, verkkokaapelin tai FortiManagerin välityksellä.

Tässä tavassa aluksi konfiguraatio luodaan samalla tavalla kuin aiemminkin. Tekstitiedostoa muokataan joko käsin tai skriptillä. Kun konfiguraatio on valmis, tulee se nimetä nimellä "fgt_system.conf". Tämä on palomuurin oletustiedostonimi muistitikulta haettaville konfiguraatioille. Tämän lisäksi tarvitaan haluttu versio palomuurin ohjelmistosta, tässä työssä 6.4.8. Tämä nimetään "image.out" samasta syystä. Nämä kaksi tiedostoa laitetaan sitten muistitikulle.



Kuva 23 Kongifuraatiotiedosto ja uusi laiteohjelmosto muistitikulla

Vaikka testikonfiguraatiossa otimme nämä molemmat asetukset pois käytöstä tietoturvasyistä, laitteen tehdasasetuksissa nämä ovat kuitenkin sallittuina. Se mahdollistaa tämän konfigurointitavan käyttämisen.

Kun tiedostot ovat muistitikulla, laitetaan se konfiguroimattomaan ja päivittämättömään palomuuriin kiinni. Tämän jälkeen laite kytketään verkkovirtaan ja odotetaan n. 5-10 minuuttia. Käynnistyttyään laite päivittää itsensä hakemalla muistitikulta oletustiedostonimellä uutta ohjelmistoa. Koska se löytyy, päivittyy muuri automaattisesti tähän versioon. Yhtälailla palomuuri etsii tikulta konfiguraatiotiedostoa, joka löytyy tehdasasetuksien mukaisella nimellä. Näin muuri saa myös halutun konfiguraation.

Tästä päästään tämän tavan hyötyyn: asentaja voi itse kopioida tiedostot omalle muistitikulleen, eikä konfigurointiin tarvita esiasennusta. Riittää, että joku luo konfiguraatiotiedoston, ja antaa sen asentajalle. Ohjelmistopäivitystä ei välttämättä edes joka kerralla tarvitse lähettää, sillä asentajalla saattaa olla se jo edellisistä asennuksista. Tällöin lähettettävä tiedosto on hyvin pieni, ja sen voi tehdä jopa sähköpostilla, tietoturvapolitiikkojen näin salliessa.

Loppu on täysin samanlainen, kuin manuaalisessa konfiguraatiossa. Laite autorisoidaan Manageriin, ja ajetaan halutut testit jotta voidaan varmistua verkon toimivuudesta.

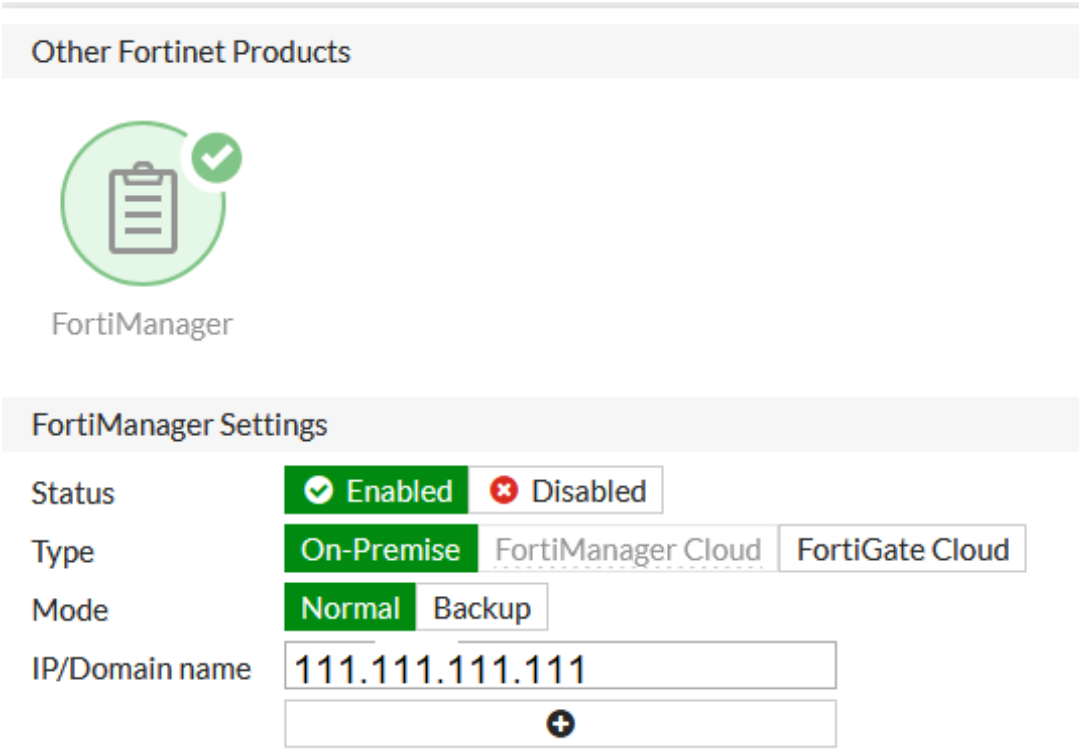
Kuten yllä todettiin, tämä tapa suoraviivaistaa logistiikkaa laitteiden osalta, sekä vähentää henkilöstötarvetta, sillä esiasennukselle ei ole tarvetta, eikä laitteita näin tarvitse myöskään purkaa laatikoistaan ennen asennusta. Haittapuolena tämä tapa vaatii asentajalta muistitikun, minkä lisäksi hänen tulee ehtiä ja osata lisätä tiedostot muistitikulle valmiiksi ennen asennusta. Konfiguraation antaminen asentajalle voi myös joissain tapauksissa olla kiellettyä tietoturvasyiden vuoksi.

4.3 Konfigurointi FortiManagerilla

Jos palomuurin internetliittymät ovat joko dynaamisilla IP-osoitteilla tai NATin takana, ei palomuuriin voida ottaa järkevästi ja/tai varmasti yhteyttä IP-osoitteella. Tällöin edellisten konfiguraatiotapojen mukaisesti palomuurin on otettava yhteyttä FortiManageriin.

Laite voidaan päivittää joko heti kättelyssä, tai FortiManagerin kautta.

Kun palomuuri on päällä ja verkossa, voidaan se lisätä FortiManageriin valitsemalla Security Fabric -> Fabric Connectors -> FortiManager (v. 6.4.8). Asetusikkunaan syötetään FortiManagerin IP-osoite ja valitaan tyypiksi On-Premise, muut asetukset jätetään oletusarvoille:



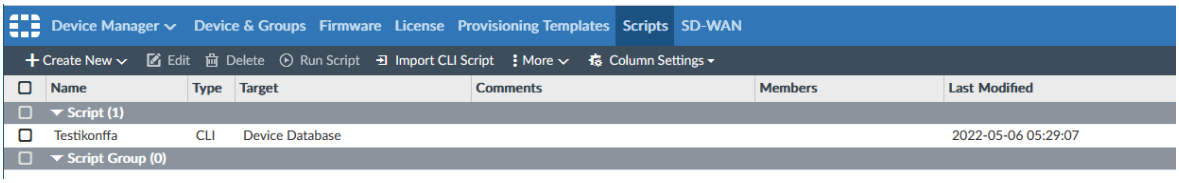
Kuva 24 FortiManagerin lisääminen palomuuriin GUI:sta

Tämän jälkeen tulee ponnahdusikkuna, joka kertoo laitteen lisäyspyynnöstä FortiManageriin. Tämän jälkeen käyttäjä kirjataan palomuurilta ulos. Sisään voi kirjautua heti vanhoilla tunnuksilla.

Tämän jälkeen palomuuri hyväksytään FortiManageriin Managerista käsin.

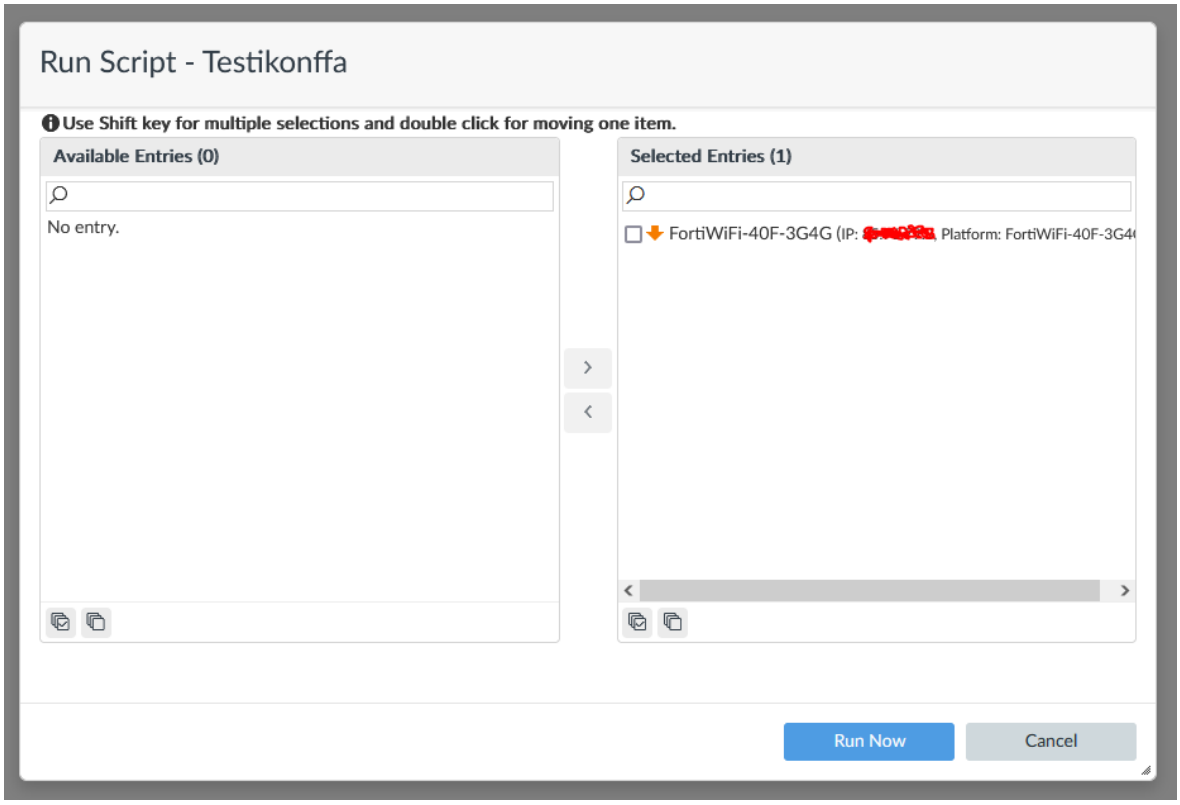
Kun laite on lisätty ForiManageriin, tulee siihen ajaa konfiguraatio. Tässä työssä tavoite ei ole FortiManager tai sen käyttäminen. Siksi konfiguraatio ajetaan sellaisenaan skriptillä. Laajemmissa toteutuksissa tietyt ominaisuudet, kuten SD-WAN- tai palomuurisäännöt, tai langattoman verkon asetukset kannattaa provisioida erillisillä pohjilla, jolloin niiden keskitetty hallinta helpottuu.

Konfiguraatio luodaan tässäkin tapauksessa ennakkoon joko manuaalisesti, tai erillisellä skriptillä, johon täytetään muokattavat tiedot. Kun tämä konfiguraatio on valmis, viedään se FortiManageriin Device Manager -> Scripts alle. Tänne luodaan uusi skripti, tai tehdään muutokset edellisen skriptin päälle.



Kuva 25 Palomuuri FortiManagerissa

Kun haluttu konfiguraatio on asetettu skriptiksi, voidaan se ajaa Scripts valikosta painamalla Run Script- nappia. Tässä vaiheessa FortiManager kysyy, mille laitteelle skripti halutaan ajaa, valitaan Manageriin lisätty uusi palomuuri ja painetaan Run Now.



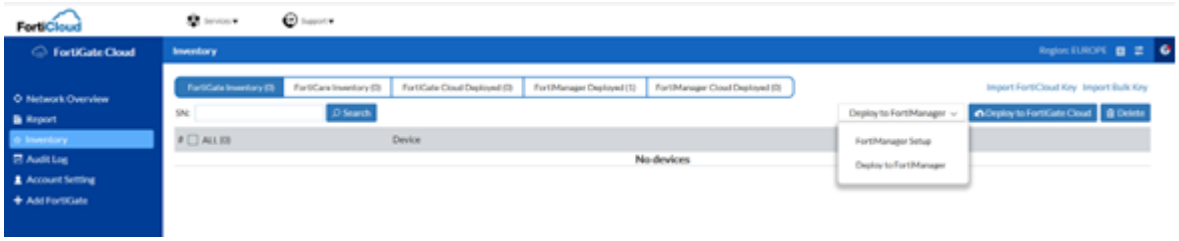
Kuva 26 Konfiguraation ajaminen skriptillä toimipistemuurille FortiManagerista

Kun skripti on onnistuneesti ajettu, on palomuurin konfiguraatio päivittynyt, ja esimerkiksi VPN-yhteyksien pitäisi muodostua automaattisesti. Tässä vaiheessa voidaan tehdä halutut testit yhteyksien ja laitteen toiminnan varmistamiseksi.

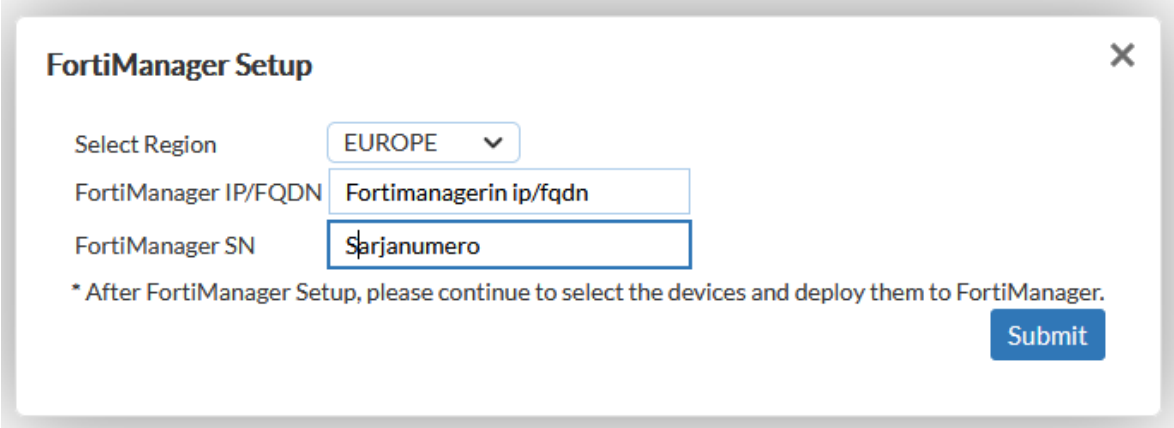
Hyötynä tässä konfiguraatiotavassa on esiasennuksen välttäminen, sillä konfiguraatio voidaan tehdä etänä. Lisäksi konfiguraatiota ei tarvitse luovuttaa esimerkiksi asentajalle, sillä se tiputetaan laitteelle etänä. Huonona puolena laitteelle tulee manuaalisesti asettaa FortiManagerin tiedot joko GUIn tai CLIn kautta, mikä tekee tästä konfiguraatiotavasta hitaamman ja työläämmän asentajalle. Toki tässäkin voidaan käyttää muistitikkua alkukonfiguraatioon, mikä taas tuo omat hyötynsä ja haittansa mukaan.

4.4 Konfigurointi Fortinetin ZTP:lla

Konfigurointi Fortinetin ZTP:lla alkaa lisäämällä FortiManagerin tiedot FortiCloudiin. Tämä sisältää IP-osoitteen, sekä sarjanumeron.

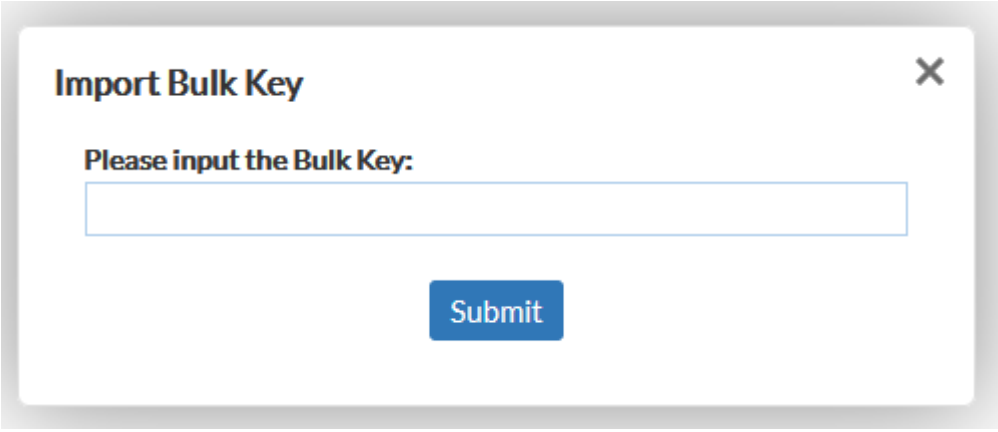


Kuva 27FortiManager-yhteyden lisääminen FortiCloudiin ZTP:tä varten



Kuva 28FortiManagerin IP-osoite ja sarjanumero

Kun FortiManagerin tiedot on lisätty, voidaan samaisesta paikasta lisätä palomuurille luotu ZTP-sarjanumero. Tässä työssä lisätään Bulk avain, mutta sen vieresetä löytyy nappula myös FortiCloud avaimelle.



Kuva 29 "Bulk key", joka mahdollistaa ZTPn käyttämisen

Tämän jälkeen palomuuri ilmestyy FortiCloudin laitelistaukseen, ja se voidaan jättää odottamaan varsinaisen laitteen kytkeytymistä verkkoon. Kun palomuuri käynnistetään ja liitetään verkkoon, se ottaa yhteyttä FortiCloudiin kysyäkseen, jos siellä olisi ZTP tietoja. Tässä tapauksessa on, ja palomuuri saa sarjanumerollansa sille osoitetun FortiManagerin

tiedot. Hetken päästä FortiManagerissa voidaan autorisoida muuri, jonka jälkeen sitä voidaan hallita FortiManagerin kautta.

Tämän jälkeen itse konfigurointi noudattaa edellisten toimintatapojen kaavaa. Konfiguraatio ajetaan laitteelle FortiManagerista, jonka jälkeen yhteydet testataan.

Hyötynä ZTP:ssä on kirjaimellisesti nollan kosketuksen provisiointi. Kenenkään ei tarvitse konfiguroida laitetta fyysisesti, vaan kaikki tarvittava voidaan tehdä etänä joko FortiCloudista tai FortiManagerista. Asentajan tarvitsee siis vain kytkeä laite verkkoon. Toki tässäkin tavassa vaatimuksena on DHCP operaattorin puolelta, sillä jos konfiguroimaton palomuuri ei saa yhteyttä internettiin, ei se pääse kysymään FortiManagerin tietoja, eikä sitä kautta myöskään saa konfiguraatiota. Lisäksi vaatimuksena on ZTP, eli FortiDeploy-lisenssi, mikä kustantaa muutaman pennin. Tämä toki on ylimääräinen kuluerä, toki se vähentää muun tuntityön määrää.

5 Johtopäätökset ja huomiot

Tämän työn tarkoitus oli löytää parhaat tavat Fortinetin palomuurien massadeployaamiseen. Eri metodeissa arvioitiin muunmuassa konfiguraation ja asennuksen nopeutta, helppoutta, sekä kustannustehokkuutta. Tämä työ ei keskittynyt itse konfiguraatiotapoihin, joskin eri asiayhteyksissä niihin saatettiin viitata.

Kaikista sulavin ja helpoin käyttää oli Fortinetin ZTP. Se mahdollisti asennuksen täysin ilman palomuuriin koskemista, pelkkä verkkoon yhdistäminen ja laitteen käynnistäminen riitti laitteen konfigurointiin etänä. Ainoa miinuspuoli tässä oli vaatimus IP-osoitteelle DHCP:llä, mikä ei välttämättä onnistu kaikissa maissa tai kaikkien operaattoreiden liittymillä. Tämä mahdollistaa laitelogistiikan suoraviivaisemman kulun, sillä laitteet voidaan toimittaa suoraan asiakkaan tiloihin mahdollistaen lyhyemmät toimitusajat asiakkaalle. Myös laitteen valmistelun kustannukset laskevat, sillä konsultin työaika kuluu käytännössä vain laitteen konfiguroimiseen, eikä esimerkiksi logistisiin tehtäviin tai laitteiden purkamiseen ja pakkaamiseen. Työn voi myös tehdä helposti pohjilla ja skripteillä, mikä myös nopeuttaa useiden laitteiden konfigurointia. Kolmas suora hyöty on

mahdollisissa vikatilanteissa laitevaihtojen helppous. Vaikka laitteita ei vikatilanteessa kierrätettäisi esiasennuksen kautta, ei uutta laitetta tarvitse konfiguroida asiakkan tiloissa paikanpäällä olevien henkilöiden avustuksella. Sen sijaan laite voidaan konfiguroida valmiiksi pilvessä, ja fyysisen laitteen vaihduttua se voidaan siirtää automaattisesti ”korvaavaksi” laitteeksi hallintaan. Näiden lisäksi laitteiden ylläpito saattaa helpottua lievästi, sillä jos kaikki kohteet ovat toteutettu saman pilvestä löytyvän pohjan avulla, konfiguraatiot ovat konsultista riippumatta samanlaisia. Jos laitteet konfiguroidaan esimerkiksi esiasennuksena, on riskinä että eri konfiguroijilla käytössä oleva pohja ei ole uusin, tai että eri konfiguroijat konfiguroivat laitteet hieman eri tavalla. Käytännössä siis hyödyt olivat suhteellisen suoraan automatisoinnista johtuvia, eikä täten varsinaisesti yllätyksellisiä. Prosessien automatisointi monesti laskee kustannuksia, tehostaa toimintaa ja auttaa skaalaamaan toimintaa ylöspäin manuaalisia prosesseja helpommin. Tämä kuitenkin vaatii sen, että prosessit ovat loppuun asti hiottuja ja suunniteltuja, jotta niitä käytettäessä ei jouduttaisi tilanteeseen, jossa joudutaan poikkemaan yleisestä prosessin toimintatavoista.

ZTP:tä hyödyntäessä esiin tulleet hyödyt eivät tulleet uusina. Šimuni´c, I. & Grgurevi´c, I (Automation of Network Device Configuration Using Zero-Touch Provisioning - A Case Study, 2021) päätyi samanlaisiin johtopäätöksiin: Mitä suuremman ympäristön konfigurointi automatisoidaan, sitä suurempia ovat saavutettavat kustannussäästöt. Heidänkin mukaan säästöt tulevat ajansäästöstä ja sitä kautta vaadittavan asiantuntijatyön lyhenemisestä, sekä konfigurointivirheiden vähenemisestä. Kokina, J.& Blanchette, S. päätyvät samaan lopputulokseen ohjelmistoautomaation saralla. Vaikka tutkimus ei koske verkkolaitteita, pätee se esimerkiksi konfiguroinnin luonnin automatisointiin. Tutkimuksessa automatisointi säästi työtunteja ja laski väliaikaistyöntekijöiden tarvetta. Lisäksi työn tehokkus nousi ja laatu parani virheiden vähentyessä. Muita hyötyjä on esimerkiksi toimitusaikojen tippuminen. Andrew Lerner (Network Equipment Lead Times, 2022) kirjoittaa blogissaan Gartnerille verkkolaitteiden tilausten läpimenoaikojen olleen n. 4-6 viikkoa ennen vallitsevaa pandemiaa. Jos oletetaan esiasennukseen ja laitteiden lähetykseen esiasennuksesta menevän 1-2 viikkoa, voidaan ZTP:tä käyttämällä fyysisen esiasennuksen sijasta nopeuttaa laitteiden toimitusprosessia noin 15-35% normaaliaikana. Nykyisten saatavuusongelmien vuoksi saavutettu hyöty ajallisesti on toki marginaalinen, mutta säästetty työ näkyy jokatapauksessa rahana. Kaikenkaikkiaan tulokset olivat myös linjassa jo aiemmin mainitun Oskar Loukon (Zero-Touch Deployment of Fortinet Devices, 2021) kanssa. Vaikka hän ei saanut ZTP:tä toimimaan täysin, hän mainitsee työssään

hyötyinä ZTP:lle helppokäyttöisyyden, virheiden vähenemisen, kevyemmän työkuorman, hallinnan helppouden ja helppokäyttöisyyden. Kustannustehokkuuteen hän ei ottanut omassa työssään kantaa, joskin tämän tutkimuksen ja logistiikan vuokaavion pohjalta voin todeta myös kustannustehokkuuden kasvavan. Kuitenkaan ennen asian tutkimista ja kokeilemista käytännössä on paha arvioida kustannussäänstöjen absoluuttista määrää.

Toinen esille nostettava tapa on palomuurin konfigurointi ja päivitys muisitikulla asentajan toimesta. Tällöin koko konfigurointi suoritetaan asennuksen yhteydessä, eikä etäkonfiguraatiolle ole tarvetta. Haittapuolina tässä konfiguraatio tulee antaa asentajalle, mikä saattaa sotia tietoturvapolitiikkoja vastaan. Lisäksi erilaisten pohjien käyttäminen FortiManagerista ei onnistu, jos konfigurointi tapahtuu suoraan laitteelta. Tällä kuitenkin saavutetaan osa edellisen tavan hyödyistä, eli esimerkiksi esiasennuksen puute, mikä näkyy suoraan kustannussäästöinä, sekä lyhyemmissä toimitusajoissa loppuasiakkaalle.

Kolmantena nostona mainittakoon laitteiden esiasennus, joka on kaikista tavoista hitain ja kallein. Tämä johtuu ylimääräisestä työvaiheesta, joka on laitteiden purkamisten ja pakkaamisten johdosta aikaa vievää ja työlästä. Positiivista tässä on kuitenkin laitteiden toiminnan varmistaminen ennen asennusta, jolloin DoA:n riski pienenee huomattavasti, ja konfiguraatio voidaan varmistaa ennen asennusta. Varsinaisia hyötyjä tällä ei muuten saavuteta, sillä tämä vaihtoehto on työssä verrokkiratkaisu – tälle siis pyritään löytämään tehokkaampia vaihtoehtoja.

Tutkimuksen pohjalta voidaan suositella ZTP:n testaamista tuotannossa. Tuotantoon vieminen kannattaa aloittaa pienimuotoisesti ja rajoitteet tiedostaen. Jos nämäkin testit tuotannossa vaikuttavat onnistuneilta, voidaan tämä tapa jalkauttaa yleisesti käytettäväksi toimintatavaksi. Lisäksi tämän työn pohjalta voidaan suorittaa jatkotutkimusta konfiguraation hallinnan suhteen. FortiManager mahdollistaa monenlaisia tapoja hallita suuria laitemääriä. Valitettavasti näitä ominaisuuksia ei aina osata tai ymmärretä käyttää mahdollisuuksien mukaisesti. Myös käytännön testi kustannussäästöjen suhteen olisi mielenkiintoinen. Valitettavasti tässä työssä ei ollut mahdollista verrata paria eri toimitustapaa toisiinsa reaalimaailman projekteissa. Tämä kuitenkin antaisi osviittaa esille nousseiden hyötyjen näkymisestä reaalimaailmassa.

6 Yhteenveto

Tässä työssä tutkittiin ZTP:n kyvykkyyksiä palomuurien laajamittaisessa SD-WANia hyödyntävässä käyttöönotossa. Syyt työn taustalla olivat tarve konfiguraatiotyön skaalautumisen parantaminen, mutta myös prosessien nopeutuminen ja kustannussäästöt. ZTP tarjoaa näitä kaikkia palveluntarjoajalle, minkä lisäksi asiakas saa ketterämmän, skaalautuvamman ja joustavamman verkkototeutuksen, mikä on valmis äkillisillekkin muutoksille liiketoiminnassa. Taustalla on lisäksi SD-WAN-verkkojen kysynnän raju kasvu, mikä mahdollistaa omalta osaltaan uusien toimintatapojen pohtimisen verkkolaitteiden konfiguroimiseksi.

Yhteenvetona voidaan todeta ZTP:n tuomien hyötyjen olevan todellisia. Tutkittavia tapauksia oli muutamia, joista erottui niiden hyödyt ja haasteet. Kaikenkaikkiaan tulokset olivat positiivisia, eikä mikään tapa konfiguraation jakamiseksi osoittautunut selkeästi huonoksi. Sen sijaan osa vaihtoehdoista oli parempia, parhaimpana Fortinetin oma ZTP.

Pelkästään yhden laitteen konfigurointi ZTP:llä nopeutui verrattuna manuaaliseen konfigurointiin. Tämä ei sisältänyt laitteen purkua ja pakkaamista, eikä ylimääräisiä logistiikasta johtuvia kuluja. Tästä huolimatta palomuuri saatiin toimintakuntoon nopeammin, minkä lisäksi pilven kautta laitteelle toimitettu konfiguraatio vähensi mahdollisuuksia virheisiin. Suuremmalla laitemäärällä hyödyt olisivat vielä isommat, sillä prosessin automatisoinnin tuomat hyödyt näkyisivät suuremmin.

SD-WAN ei tuonut testeissä lisähaasteita, sillä käytettävissä olevien nettiliittymien rajoitteet oli tiedossa jo ennen testien aloittamista. Toki tässä vaiheessa on hyvä mainita pohjatyön merkitys, sillä ZTP ei välttämättä ole mahdollinen, jos laitteet eivät pysty automaattisesti saamaan yhteyttä internettiin. Suomessa tästä tuskin muodostuu ongelmaa, mutta ulkomailla toimittaessa se on hyvä pitää mielessä.

Tietoliikenneyhteyksien siirtyessä kohti SD-WAN:ia on syytä miettiä yrityksen prosessit ja toimintatavat uudestaan, sillä tarpeet, vaatimukset ja mahdollisuudet ovat vanhoihin ratkaisuihin verrattuna erilaisia. ZTP voi olla vastaus näihin haasteisiin. Teknologioina sekä ZTP että SD-WAN ovat kuitenkin verrattain uusia, ja niiden saralla tapahtuu lähivuosina varmasti paljon kehitystä. Tämän myötä näiden kysyntä tulee todennäköisesti kasvamaan

entuudestaan. Palveluntarjoajien olisikin syytä varautua tähän ottamalla moderneja ratkaisuja käyttöön teknologioiden tarjoamisen helpottamiseksi asiakkailleen.

Toinen yleinen tutkimuksen aikana noussut havainto oli ZTP:tä koskevien tai käsittelevien tutkimusten vähyys. Työn tekemisen aikana vastaan tuli monia seuraavan sukupolven palomuureja tai SD-WAN:ia käsitteleviä tutkimuksia, diplomitöitä ja opinnäytetöitä. Kuitenkin vain harvassa oli edes käsitelty tai mainittu ZTP:tä, vaikka se on tulevissa verkoissa ja verkkolaitteissa yhä merkittävämpi ja käytetympi ominaisuus. Näkisin siis, että aihetta olisi syytä tutkia merkittävästi lisää eri näkökulmista, sillä materiaali on tällä hetkellä varsin vähäistä.

Lähteet

Demchenko, Y., Filiposka, S., Tuminauskas, R.,Mishev, A., Regvart, D., Baumann, K. & Breach, T. 2015. Enabling Automated Network Services Provisioning for Cloud Based Applications Using Zero Touch Provisioning

Chai, C. 2015. Zero Touch Provisioning can help the network world catch up to server advances. https://www.networkworld.com/article/2876096/zero-touch-provisioning-can-help-the-network-world-catch-up-to-server-advances.html (viitattu 16.8.2022)

Yang, Z., Cui, Y., Li, B., Liu, Y., & Xu, Y. 2019. Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities. 2019 28th International Conference on Computer Communication and Networks (ICCCN).

Pandian, A. P., Fernando, X., & Islam, S. M. S. (Eds.). 2021. Computer Networks, Big Data and IoT. Lecture Notes on Data Engineering and Communications Technologies. S. 297 – 304.

ADVPN with BGP as the routing protocol, 2020. https://community.fortinet.com/t5/FortiGate/Technical-Tip-ADVPN-with-BGP-as-the-routing-protocol/ta-p/192437, viitattu 16.8.2020.

Uppal, S., Woo, S. & Pitt, D. 2018. Software-Defined WAN For Dummies®, 2nd VMware Special Edition.

Louko, O., 2021, Zero-Touch Deployment of Fortinet Devices

Malino J., 2006, OSI-kerrokset (viitattu 16.8.2022), https://fi.wikipedia.org/wiki/Tiedosto:OSI-malli.png

Pillai S. 2017. Difference Between Segments, Packets and Frames (viitattu 16.8.2022), https://www.slashroot.in/difference-between-segments-packets-and-frames

Irving. 2021. Switch Mac Address: What's It and How Does it Work? (viitattu 16.8.2022), https://community.fs.com/blog/switch-mac-address-whats-it-and-how-does-it-work.html

Connected Dots Online. 2022. Techniques to master IP Subnetting - Part 1 (viitattu 16.8.2022), https://www.connecteddots.online/resources/blog/how-to-master-ip-subnetting-part-one

Gelmo96. 2015. DHCP Session (viitattu 16.8.2022), https://commons.wikimedia.org/wiki/File:DHCP_session.svg

Wikipedia. 2022. Osoitteenmuunnos (viitattu 16.8.2022), https://fi.wikipedia.org/wiki/Osoitteenmuunnos

ReneMolenaar. 2022. IPsec (Internet Protocol Security) (viitattu 16.8.2022), https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security

Travis A. 2021. FortiGate Zero Touch Provisioning (ZTP) & Low Touch Provisioning (viitattu 16.8.2022), https://andrewtravis.com/2021/11/10/fortigate-zero-touch-provisioning-ztp-low-touch-provisioning/

Altaware. Fortinet, Complete Cyber Security Solution Set (viitattu 16.8.2022),

http://www.altaware.com/v/fortinet/

Fortinet. SD-WAN with ADVPN - single hub (viitattu 16.8.2022), https://docs.fortinet.com/document/fortimanager/6.4.0/examples/380098/sd-wan-advpn-single-hub

Mohamed A. 2019. Current Trends in Using the Software-Defined WAN

Lampimäki S. 2021. SD-WAN ja sen osa nykypäivän laajaverkkoa

Kuismala L. 2021. MPLS- ja SD-WAN-verkkojen kyvykkyydet ja asema tulevaisuudessa

Hu B. 2021. BGP in a Nutshell (viitattu 16.8.2022), https://www.bo-dunhu.com/blog/posts/bgp-in-a-nutshell/

Deland H., eross-msft, v-kents. 2021. DHCP (Dynamic Host Configuration Protocol) Basics (viitattu 16.8.2022), https://docs.microsoft.com/en-us/windows-server/troubleshoot/dy-namic-host-configuration-protocol-basics

Kaarnalehto M. 2011. Salausmenetelmät: Symmetrinen, epäsymmetrinen ja tiivistealgoritmit.

Fruhlinger J. 2022. What is MPLS, and why isn't it dead yet? https://www.networkworld.com/article/2297171/network-security-mpls-explained.html (Viitattu 23.8.2022)

Šimuni´c, I. & Grgurevi´c, I., 2021. Automation of Network Device Configuration

Using Zero-Touch Provisioning - A Case Study

Lerner, A., 2022. Network Equipment Lead Times. (viitattu 26.9. 2022), https://blogs.gartner.com/andrew-lerner/2022/02/22/network-equipment-lead-times/

Kokina, J. & Blanchette, S., 2019. Kokina, J., & Blanchette, S. (2019). Early evidence of digital labor in accounting: Innovation with Robotic Process Automation.

Liite 1

FortiManagerista palomuurille puskettu konfiguraatiotiedosto

```
config system global
    set hostname "elisa-sd-wan-fw1"
    set timezone 35
end

config system interface
    edit "lan2"
        set vdom "root"
        set mode dhcp
        set allowaccess ping snmp fgfm
        set type physical
        set alias "wan2"
        set lldp-reception enable
        set role wan
        set snmp-index 0
    next
    edit "dialup_client_w"
        set vdom "root"
        set ip 11.11.11.1 255.255.255.255
        set type tunnel
        set remote-ip 11.11.11.254 255.255.255.0
        set snmp-index 0
        set interface "wan"
    next
    edit "dialup_vpn_l"
        set vdom "root"
```

```
        set ip 11.11.12.1 255.255.255.255
        set type tunnel
        set remote-ip 11.11.12.254 255.255.255.0
        set snmp-index 0
        set interface "lan2"
    next
end
config system virtual-switch
    edit "lan"
        config port
            delete lan2
            delete lan3
        end
    end
end

config system admin
    edit "admin"
        set password <salasana>
    next
end
config user local
    edit "guest"
        set type password
        set passwd <salasana>
    next
    edit "vpnuser1"
        set type password
        set passwd <salasana>
    next
```

```
end

config vpn ipsec phase1-interface
    edit "dialup_vpn_w"
        set interface "wan"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device disable
        set proposal aes256-sha256
        set localid "dialup_peer"
        set dhgrp 21
        set remote-gw <ip-osoite>
        set tunnel-search nexthop
        set psksecret <salasana>
    next
    edit "dialup_vpn_l"
        set interface "lan2"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device disable
        set proposal aes256-sha256
        set localid "dialup_pee2"
        set dhgrp 21
        set remote-gw <ip-osoite>
        set tunnel-search nexthop
        set psksecret <salasana>
    next
end
```

```
config vpn ipsec phase2-interface
    edit "dialup_vpn_w"
        set phase1name "dialup_vpn_w"
        set proposal aes256-sha256
        set dhgrp 21
        set keylifeseconds 3600
    next
    edit "dialup_vpn_l"
        set phase1name "dialup_vpn_l"
        set proposal aes256-sha256
        set dhgrp 21
        set keylifeseconds 3600
    next
end


config router bgp
    set as 65412
    config neighbor
        edit "11.11.11.254"
            set advertisement-interval 1
            set link-down-failover enable
            set remote-as 65412
        next
        edit "11.11.12.254"
            set remote-as 65412
        next
    end
    config network
        edit 1
```

```
            set prefix 192.168.1.0 255.255.255.0
        next
    end
end
config firewall policy
    delete 1
    delete 2
    delete 3
end
config system sdwan
    set status enable
    set load-balance-mode measured-volume-based
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "lan2"
        next
        edit 2
            set interface "wan"
        next
    end
end
config router static
    edit 1
        set distance 1
        set sdwan enable
    next
```

```
end
config firewall policy
    edit 0
        set name "netti"
        set uuid dfa1fc0c-8f2f-51ec-cf03-57afe7c81461
        set srcintf "internal"
        set dstintf "virtual-wan-link"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
    edit 0
        set name "dialuo"
        set uuid eea4858e-b9dd-51ec-82eb-671c2e558586
        set srcintf "dialup_vpn_w"
        set dstintf "internal"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 0
        set uuid 9c9acfe0-b9de-51ec-107c-1d331a6af513
        set srcintf "internal"
        set dstintf "dialup_vpn_w"
```

```
            set srcaddr "all"
            set dstaddr "all"
            set action accept
            set schedule "always"
            set service "ALL"
            set comments " (Copy of dialuo) (Reverse of dialuo)"
        next
        edit 0
            set name "dialup_vpn_l"
            set uuid 525bf8ea-b9df-51ec-0381-145dcc2b6bb5
            set srcintf "dialup_vpn_l"
            set dstintf "internal"
            set srcaddr "all"
            set dstaddr "all"
            set action accept
            set schedule "always"
            set service "ALL"
        next
        edit 0
            set uuid 56a9393a-b9df-51ec-7395-0af854ccc0b2
            set srcintf "internal"
            set dstintf "dialup_vpn_l"
            set srcaddr "all"
            set dstaddr "all"
            set action accept
            set schedule "always"
            set service "ALL"
            set comments " (Copy of dialup_vpn_l) (Reverse of dialup_vpn_l)"
        next
    end
```