VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Kiril Rajamäki

SD-WAN-TEKNOLOGIAN KÄYTTÖÖNOTTO TYÖYMPÄRISTÖSSÄ

Tekniikka
2025

VAASAN AMMATTIKORKEAKOULU
Tietotekniikka

TIIVISTELMÄ

Tekijä	Kiril Rajamäki
Opinnäytetyön nimi	SD-WAN-teknologian käyttöönotto työympäristössä
Vuosi	2025
Kieli	suomi
Sivumäärä	59 + 1 liitettä
Ohjaaja	Antti Virtanen

Tämän opinnäytetyön tavoitteena oli tutkia SD-WAN-teknologian käyttöönottoa työympäristössä ja sen vaikutuksia organisaation verkkoinfrastruktuuriin. SD-WAN (Software-Defined Wide Area Network) tarjoaa modernin tavan hallita ja optimoida yrityksen verkkoyhteyksiä perinteiseen WAN-verkkoon verrattuna. Työn tavoitteena oli suunnitella ja toteuttaa SD-WAN-ratkaisu, joka parantaa verkon suorituskykyä, joustavuutta ja tietoturvaa.

Työssä tarkasteltiin SD-WAN-teknologian keskeisiä ominaisuuksia, kuten dynaamista reititystä, keskitettyä hallinta ja tietoturvamekanismeja. Tutkimuksessa käytettiin Fortinet FortiGate 40F -palomuuria, joka tukee SD-WAN-toimintoja. Konfiguroinnin ja testauksen avulla analysoitiin, kuinka SD-WAN voidaan integroida organisaation verkkoon. Testauksessa hyödynnettiin muun muassa PING-menetelmää verkkoyhteyksien toimivuuden varmistamiseksi.

Projektin tulokset osoittavat, että SD-WAN tarjoaa merkittäviä etuja perinteisiin WAN-ratkaisuihin verrattuna. Sen avulla voidaan tehokkaasti hallita verkon suorituskykyä, priorisoida liikennettä ja parantaa tietoturvaa. Koska testausympäristössä ei ollut käytettävissä internet-yhteyttä tai oikeita operaattoriyhteyksiä, suorituskyvyn todellista vaikutusta ei voitu täysin havainnollistaa.

Avainsanat SD-WAN, Fortinet, palomuuri, lähiverkko

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietotekniikka

ABSTRACT

Author	Kiril Rajamäki
Title	Implementation of SD-WAN in the Work Environment
Year	2025
Language	Finnish
Pages	59 + 1 Appendix
Name of Supervisor	Antti Virtanen

The aim of this thesis was to investigate the implementation of SD-WAN technology in a work environment and its effects on the network infrastructure of an organization. Software-Defined Wide Area Network (SD-WAN) offers a modern way to manage and optimize a company's network connections compared to a traditional WAN network. The aim of the work was to design and implement an SD-WAN solution that improves network performance, flexibility and security.

The thesis examined the key features of SD-WAN technology, such as dynamic routing, centralized management and security mechanisms. The research used a Fortinet FortiGate 40F firewall that supports SD-WAN functions. Through configuration and testing, it was analysed how SD-WAN can be integrated into the organization's network. The testing utilized, among other things, the PING method to ensure the functionality of network connections.

The project results show that SD-WAN offers significant advantages compared to traditional WAN solutions. It can be used to effectively manage network performance, prioritize traffic and improve security. Because there was no internet connection or real carrier connections available in the testing environment, the actual performance impact could not be fully illustrated.

Keywords SD-WAN, Fortinet, Firewall, Local Area Network

SISÄLLYS

KUVALUETTELO

LYHENTEET

5G	Viidennen sukupolven mobiiliverkko
AH	Authentication Header, Todentaa viestien eheyttä
AS	Autonomous System, Autonominen järjestelmä
BGP	Border Gateway Protocol, Internetin reititysprotokolla
CIDR	Classless Inter-Domain Routing, Luokaton reititys
ESP	Encapsulating Security Payload, Salaa viestien eheyttä
DH	Diffie Hellman, Salausprotokolla
DHCP	Dynamic Host Configuration Protocol, Jakaa IP-Osoitteet verkkolaitteille
DNS	Domain Name Server, Nimipalvelujärjestelmä
FMG-ACCESS	FortiManager, Salli FortiManagerin ja FortiGate-laitteiden välinen tiedonsiirto
FTM	FortiToken Mobile, Todennusjärjestelmä
FTP	File Transfer Protocol, Tiedostonsiirto kahden tietokoneen välille
GRE	Generic Routing Encapsulation, IP-tunnelointiprotokolla
HMAC	Hash-Based Message Authentication Codes, Viestin todennuskoodi
HTTP	Hypertext Transfer Protocol, Hypertekstin siirtoprotokolla
HTTPS	Hypertext Transfer Protocol Secure, Salattu hypertekstin siirtoprotokolla
ICV	Integrity Check Value, Eheystarkistusarvo

IKE	Internet Key Exchange, Avaintenvaihtoprotokolla
IP	Internet Protocol, Internet-protokolla
IPAM	IP Address Management, IP-osoitteiden hallinta
ISAKMP	Internet Security Association and Key Management Protocol, Internet- turvallisuusyhteys ja avaintenhallintaprotokolla
IPsec	IP Security, Laitteiden välisten yhteyksien suojaus
L2TP	Layer 2 Tunneling Protocol, IP-tunnelointiprotokolla
LAN	Local Area Network, Lähiverkko
LLDP	Link Layer Discovery Protocol, Linkkikerroksen etsintäprotokolla
Loopback	Sisärakennettu silmukka
LTE	Long Term Evolution, Neljännen sukupolven langaton tiedonsiirtotekniikka
MPLS	Multiprotocol Label Switching, Reititystekniikka
NTP	Network Time Protocol, Internetin aikaprotokolla
Oakley	Oakley Key Determination Protocol, Avainsopimusprotokolla
Overlay	Peittoverkko, Virtuaalinen verkko
Palomuuri	Firewall, Valvoo verkkoliikennettä
PING	Testaa verkkoyhteyden saatavuutta
PPP	Point-to-Point Protocol, Tietokoneviestintäprotokolla
PPPoE	Point-to-Point Protocol over Ethernet, Kapseloi PPP-kehykset Ethernet-kehyksiin

PPTP	Point-to-Point Tunneling Protocol, VPN-tunnelointiprotokolla
QoS	Quality of Service, Tietoliikenteen luokittelu ja priorisointi
RADIUS	Remote Authentication Dial In User Service, Valtuuttaa ja todentaa käyttäjiä.
RIB	Routing Information Base, Reititystietokanta
SA	Security Association, Turvallisuusyhteys
SASE	Secure Access Service Edge, Ohjelmistopohjaisen suuralueverkon (SD-WAN) ja Zero Trust -suojausmalliratkaisu
SD-WAN	Software-Defined Wide Area Network, Ohjelmistopohjainen verkkopalvelu
SKEME	Secure Key Exchange Mechanism, Turvallinen avaimenvaihtomekanismi
SLA	Service Level Assurance, Palvelutason varmistus
SLIP	Serial Line Internet Protocol, SLIP-toiminnot kapseloivat IP-paketit sarjaliikennelinjan yli
SNMP	Simple Network Management Protocol, Verkonhallintaprotokolla
SSH	Secure Shell, Salattu tietoliikenneprotokolla
SSL	Secure Sockets Layer, Tietoverkkosalausprotokolla
TCP	Transmission Control Protocol, Yhteydellinen tiedonsiirtoprotokolla
TELNET	Telecommunications network, Etäyhteys muodostaminen
TLD	Top-Level Domain, Ylätason verkkotunnus

TLS	Transport Layer Security, Kuljetuskerroksen suojaus
UDP	User Datagram Protocol, Yhteydetön tiedonsiirtoprotokolla
VDOM	Virtual Domains, Virtuaalinen verkkotunnus
VLAN	Virtual LAN, Virtuaalilähiverkko
VPN	Virtual Private Network, Virtuaalinen erillisverkko
WAN	Wide Area Network, Suuralueverkko
WWAN	Wireless Wide Area Network, Langaton laajaverkko
ZTP	Zero Touch Provisioning, Automaattinen hallintamekanismi

LIITELUETTELO

1 JOHDANTO

SD-WAN (Software-Defined Wide Area Network) on moderni verkkoratkaisu, jonka avulla yritykset voivat optimoida tietoliikenneverkkonsa suorituskykyä ja kustannustehokkuutta yhdistämällä perinteisen WAN-verkkoarkkitehtuurin ja pilvipohjaisen hallinnan. SD-WAN-teknologian keskeinen tavoite on tarjota joustava ja keskitetysti hallittava ratkaisu, joka vastaa nykyaikaisen digitaalisen työympäristön tarpeisiin, kuten etätyön ja hajautettujen toimipisteiden yleistymiseen.

Tässä opinnäytetyössä tutkitaan, miten SD-WAN voidaan ottaa käyttöön työympäristössä sekä mitä hyötyjä sen käyttöönotolla voidaan saavuttaa. SD-WAN parantaa verkon suorituskykyä ja tietoturvaa, mahdollistaa tehokkaamman hallinnan ja tukee organisaatioita, jotka pyrkivät laajentamaan etäyhteyksiä ja hyödyntämään pilvipalveluita entistä kattavammin (Palo Alto Networks, 2025).

Työn toimeksiantajana toimii 2M-IT Oy, joka on hyvinvointialueelle tietoliikennepalveluja tarjoava organisaatio. Se tavoittelee tehokkaampaa verkon hallintaa ja kapasiteetin optimointia. Tässä tutkimus keskittyy selvittämään, miten SD-WAN voidaan käytännössä toteuttaa ja konfiguroida vastaamaan organisaation tarpeisiin. Työssä käsitellään teknisiä toteutustapoja, laitteiden määrityksiä sekä SD-WAN-teknologian vaikutuksia nykyiseen verkkoarkkitehtuuriin.

2 KEHITTÄMISPROJEKTIN TARKOITUS, TAVOITTEET JA TARVEANALYYSI

SD-WAN on verkkoprotokollana vielä uusi käsite, mutta se yleistyy jatkuvasti, erityisesti etätyön ja hajautettujen toimipisteiden tarpeisiin. Se tarjoaa aiempaa tehokkaamman, turvallisemman ja joustavamman tavan hallita tietoliikenneverkkoja hyödyntäen keskitettyä pilvihallintaa. Tässä kehittämisprojektissa tarkoituksena on ottaa SD-WAN käyttöön työympäristössä, mutta sitä ei oteta tuotantokäyttöön asiakkaalle. Tämä johtuu aikataulun tiukkuudesta ja siitä, että oppimisen näkökulmasta toteutus jäisi tällöin liian suppeaksi.

Kehittämisprojektin tavoitteena on suunnitella ja toteuttaa SD-WAN-ratkaisu, joka optimoi organisaation verkkoinfrastruktuurin parantamalla suorituskykyä, verkon joustavuutta ja tietoturvaa. Verkon työympäristö sisältää Fortinet FortiGate 40F -palomuurin, tietokoneita, tulostimia, loopbackin sekä operaattoriyhteyksiä (operaattori1 ja operaattori2). Verkkoteknologiassa käytetään VLANeja, DHCP- ja DNS-palvelimia, BGP-reitityksiä, IPSec VPN:ää, palomuurisääntöjä sekä SD-WANia.

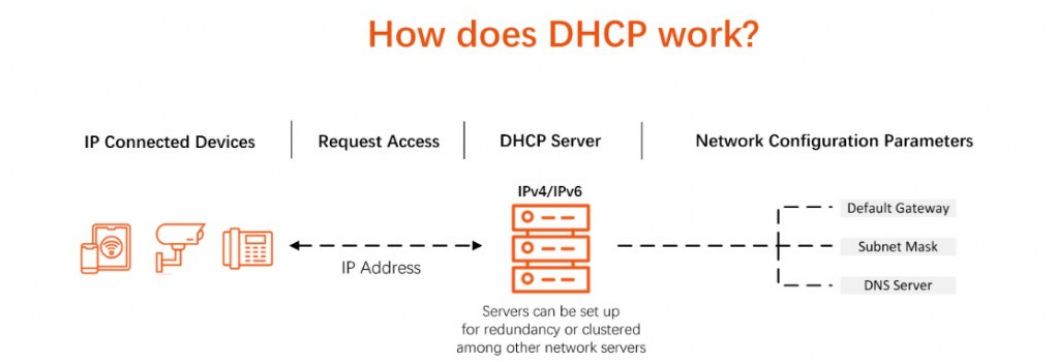
SD-WANin keskeiset hyödyt ovat keskitetty hallinta, dynaaminen reititys sekä kustannustehokkaiden yhteyksien käyttö. Teknologian avulla organisaatio voi saavuttaa paremman hallittavuuden ja suorituskyvyn, mikä tukee sekä nykyisiä että tulevaisuuden toimintatavoitteita. Tämä projekti tarjoaa mahdollisuuden oppia SD-WANin teknisestä toteutuksesta ja konfiguroinnista sekä arvioida sen käytännön soveltuvuutta organisaation tarpeisiin.

3 VERKKOPROTOKOLLAT

3.1 DHCP

DHCP (Dynamic Host Configuration Protocol) on verkkoprotokolla, joka jakaa IP-osoitteet automaattisesti verkoissa oleville laitteille. DHCP määrittää yksikertaisesti IP-osoitteet tietokoneille tai muille laitteille sekä muut tarvittavat verkkoparametrit, kuten aliverkon maskin, oletusyhdyskäytävän ja DNS-palvelimen. Lisäksi DHCP voi automaattisesti lisätä tai poistaa verkossa olevia laitteita ilman, että niitä tarvitsee konfiguroida manuaalisesti. (Ali, 2023.)

Kuvassa 1 näkyy DHCP:n palvelinjärjestelmä. Laite lähettää verkkoon DHCP-pyynnön, johon DHCP-palvelin vastaa tarjoten IP-osoitteet. DHCP vastaa pyyntöön tarjousviestillä, jossa sisältää määritetyn IP-osoitteen. Palvelin lähettää lopuksi takaisin DHCP-kuittausviestin laitteelle, ja viestintä voi alkaa. (Ali, 2023.)

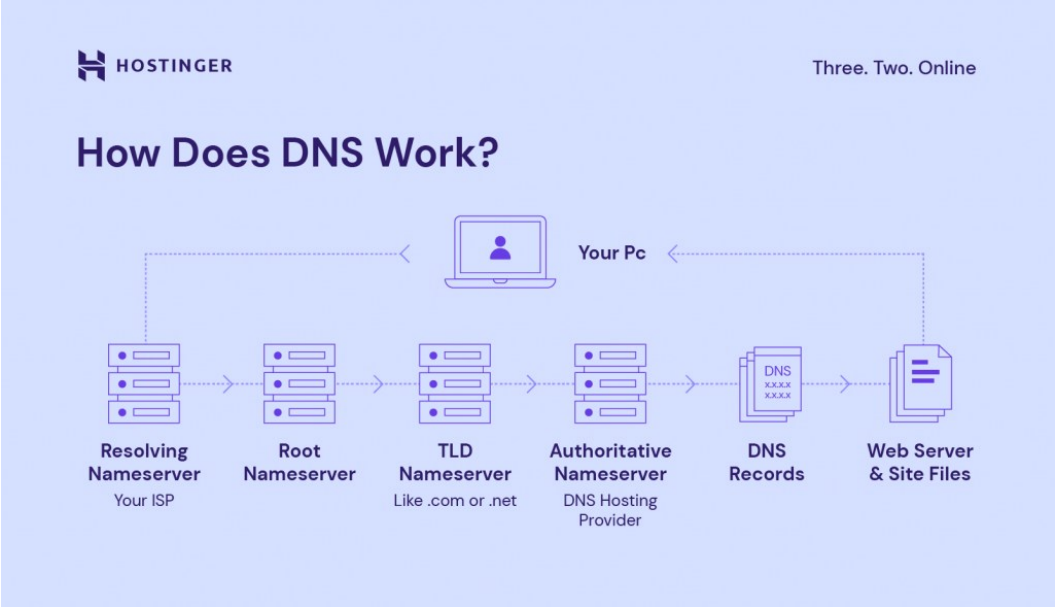


Kuva 1. DHCP:n palvelinjärjestelmä. (Ali, 2023)

3.2 DNS

DNS (Domain Name Server) on nimipalvelujärjestelmä, joka kääntää verkkotunnuksen IP-osoitteiksi. DNS:n avulla verkkosivustoon pääsee paikallisesti selaimella ilman, että käyttäjän tarvitsee muistaa pitkää IP-osoitetta ja se helpottaa käyttäjien selaamista ja verkkopalveluiden käyttöä. DNS:n tehtävä koostuu useista vaiheista, jotka tunnetaan nimellä DNS-selvitysprosessi.

Kuvassa 2 on DNS-selvitysprosessista, kun käyttäjä yrittää päästä verkkosivulle. Jos kone ei löydä IP-osoitteesta isäntien tietoja, se lähettää DNS-kyselyjä tai -pyyntöjä. (Hasna, 2024.)



Kuva 2. DNS-selvitysprosessi toiminnasta. (Hasna, 2024)

1. Resolving Nameserver (Rekursiivinen nimipalvelin): Toimii välikätenä tietokoneille ja muiden DNS-palvelimien välillä. Palvelin etsii ensin IP-osoitetta välimuististaan, ja jos osoite löytyy, se palauttaa osoitteen käyttäjälle. Muuten palvelin ohjaa pyynnön seuraavalle palvelimelle Root Nameserverelle.
2. Root Nameserver (Juurinimipalvelin): DNS-hierarkian ylin taso, joka toimii ohjauspisteenä. Ei sisällä itse IP-osoitetta, mutta ohjaa resolverin oikeaan TLD-palvelimeen (Top-Level Domain) verkkotunnuksen päätteen (esim. .com, .net) perusteella.
3. TLD Nameserver (TLD-nimipalvelin): Hallinnoi tietyn TLD:n (esim. .com, .net) verkkotunnuksia. Ohjaa resolverin eteenpäin Authoritative Nameserveriin, joka sisältää tarkan IP-osoitteen.

4. Authoritative Nameserver (Auktoritatiivinen nimipalvelin): DNS-hakujen viimeinen vaihe, joka sisältää kaikki tiedot verkkotunnuksesta, mukaan lukien sen IP-osoitteen. Palauttaa IP-osoitteen resolverille, joka välittää sen käyttäjälle.
5. DNS Records: Verkkotunnusten ja IP-osoitteiden yhdistäminen. Ne ohjaavat liikenteen oikeisiin palvelimiin.
6. Web Server & Site Files: Verkkosivuston sisällön palveleminen. Verkkopalvelin vastaanottaa pyynnön ja lähettää sivuston tiedostot käyttäjän selaimelle.

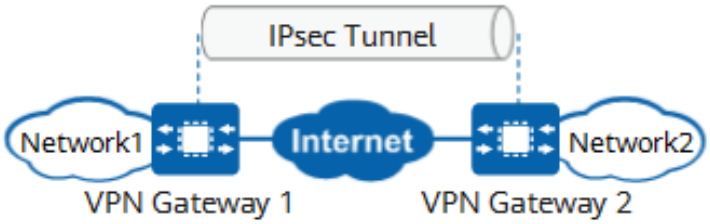
(Hasna, 2024.)

3.3 IPsec VPN

IPsec VPN on virtuaalinen yksityinen verkko (VPN) -verkkoprotokolla, joka käyttää IPseciä (Internet Protocol Security) varmistaakseen IP-pakettien turvallisen siirron julkisissa verkoissa, kuten Internetissä. Se korjaa IP-pakettien luontaisia haavoittuvuuksia, kuten tietojen väärentämistä, varkautta ja peukalointia, luomalla salattuja IPsec-tunneleita. (Youyuan, 2024.)

VPN:t luovat yksityisiä, loogisia verkkoja julkiseen infrastruktuuriin, mikä mahdollistaa turvallisen tietoliikenteen. Toisin kuin perinteiset yksityiset verkot, jotka perustuvat fyysisiin linkkeihin, VPN:t käyttävät virtuaalisia yhteyksiä. Yleisiä VPN-protokollia ovat IPsec, SSL (Secure Sockets Layer), GRE (Generic Routing Encapsulation), PPTP (Point-to-Point Tunneling Protocol) ja L2TP (Layer 2 Tunneling Protocol), ja IPseciä käytetään laajasti sen vankan suojauksen vuoksi. (Youyuan, 2024.)

IPsec VPN mahdollista etäkäytön ja IPsec-tunnelin muodostamisen kahden tai useamman yksityisen verkon välille julkisessa verkossa ja salaus- ja todennusalgoritmien käyttämisen VPN-yhteyksien turvallisuuden varmistamiseksi (Kuva 3). (Youyuan, 2024.)



Kuva 3. IPsec VPN. (Youyuan, 2024)

IPsec VPN toimii IP-kerroksessa salaamalla ja todentaen datapaketteja suojellakseen isäntien tai verkon suojausyhdyskäytävien, kuten (reitittimet ja palomuurit) välistä point-to-point-viestintää. Vaikka IPsec VPN tarjoaa turvallisemman suojauksen muihin VPN-tekniikoihin verrattuna, vaatii se monimutkaisempaa konfigurointia ja verkkokäyttöönottoa. (Youyuan, 2024.)

3.3.1 IPsec-protokollat

IKE (Internet Key Exchange) on UDP-pohjainen sovelluskerroksen protokolla, joka on suunniteltu SA-neuvotteluun ja avainten hallintaan. Sillä on kaksi versiota, joissa IKEv2 tarjoaa parannettua turvallisuutta, tehokkuutta ja yksinkertaistettua neuvottelua IKEv1:een verrattuna. (Youyuan, 2024.)

IKE on myös hybridiprotokolla, jossa yhdistyvät Internet Security Association ja Key Management Protocol (ISAKMP), Oakley ja SKEME. Oakleyn ja SKEME:n käyttävät Diffie-Hellman (DH) -algoritmia avainten turvalliseen jakeluun, todentamiseen ja tiedonsiirron suojaukseen. IKE SA:iden ja IPsec SA:iden salaus- ja varmennusavaimet luodaan ja niitä voidaan dynaamisesti päivittää DH-algoritmin avulla. (Youyuan, 2024.)

AH:lla (Authentication Header) voidaan todentaa datan lähettäjä ja varmistaa IP-pakettien eheyden tarkistamiseen. AH ei salaa tietoja, mutta se liittää AH-otsikon jokaisen paketin IP-otsikkoon ja tarkistaa koko IP-paketin eheyden. (Youyuan, 2024.)

ESP:llä (Encapsulating Security Payload) tieto salataan ja tarjoaa tietolähteen autentikoinnin sekä ja IP-pakettien eheyden varmistamisen. ESP-otsikko liitetään IP-otsikkoon jokaisessa datapaketissa, ja ESP Trailer- ja ESP Auth -datakentät liitetään myös jokaiseen datapakettiin. Siirtotilassa ESP ei kuitenkaan tarkista IP-otsikoiden eheyttä, mikä tekee otsikoista alttiita muutoksille. AH ja ESP voi käyttää joko itsenäisesti tai yhdessä. (Youyuan, 2024.)

3.3.2 IPsecin toimintavaiheista

IPsecin toiminta koostuu neljästä vaiheesta, jotka ovat liikenteen tunnistaminen, turvallisuusyhdistelmien (Security Association, SA) neuvottelutiedonsiirto ja lopuksi tunnelin purkaminen. (Youyuan, 2024.)

Ensimmäinen vaihe on kiinnostavan liikenteen tunnistaminen. Kun verkkolaite vastaanottaa paketin, vertaa se paketin 5 osaa tietorakenteista määritettyyn IP-sec-käytäntöön määrittääkseen, vaatiiko paketti lähettämistä IPsec-tunnelin kautta. IPsec-tunnelin kautta siirrettävää liikennettä kutsutaan kiinnostavaksi liikenteeksi. (Youyuan, 2024.)

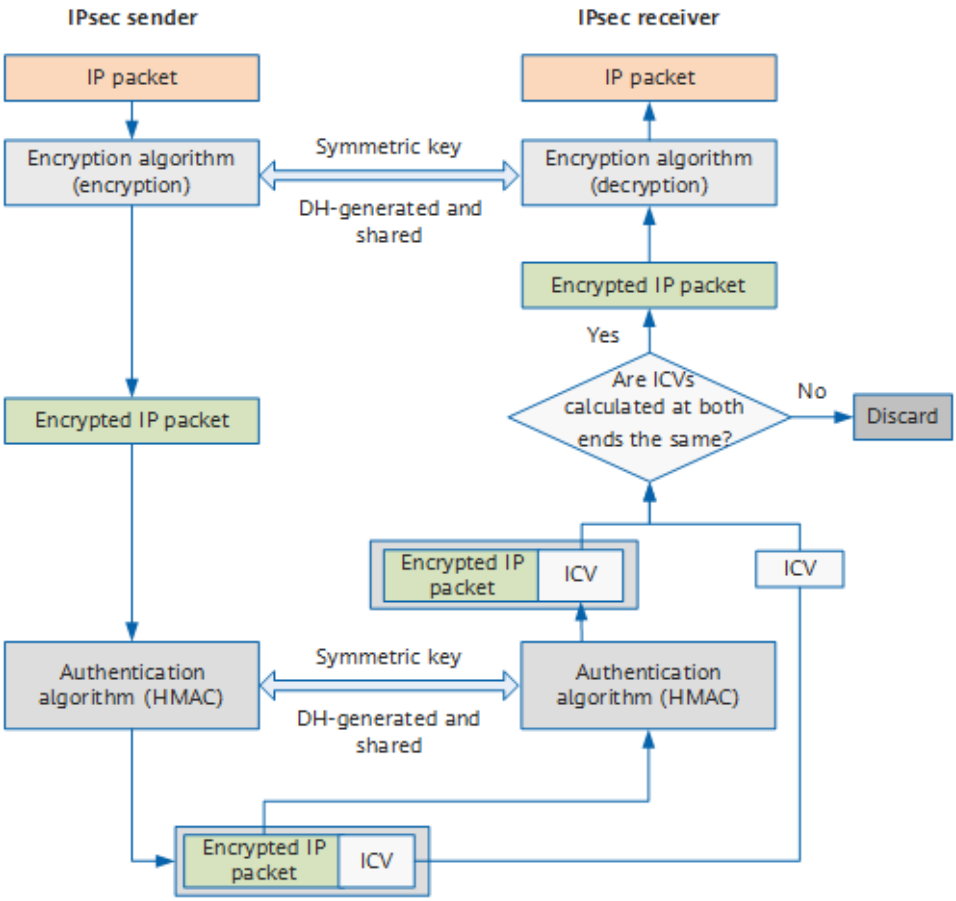
Toinen vaihe on neuvottelut (Security Association, SA). SA määrittää tarvittavat parametrit osapuolten välistä suojattua viestintää varten. Näitä ovat suojausprotokollat, kapselointitilatiedot, salaus- ja todennusalgoritmit sekä tiedonsiirrossa käytettävät avaimet. (Youyuan, 2024.)

Kun kiinnostava liikenne on tunnistettu, aloittaa paikallinen verkkolaite SA-neuvottelun vertaisverkkolaitteen kanssa. Tämän prosessin aikana IKE (Internet Key Exchange) -protokollaa käytetään luomaan IKE SA:ita identiteetin todentamista ja suojattua avainten vaihtoa varten. IKE SA:iden pohjalta luodaan IPsec SA:t, jotka mahdollistavat suojatun tiedonsiirron. (Youyuan, 2024.)

Kolmas vaihe on tiedonsiirto. Kun IPsec-suojausyhteydet (SA:t) on muodostettu, suojattu tiedonsiirto lähettää IPsec-tunnelin kautta. Tietojen salaamiseen ja to-

dentamiseen käytetään AH (Authentication Header) -autentikointia ja ESP (Encapsulating Security Payload) -salausta avulla. Salausmekanismi varmistaa tietojen luottamuksellisuuden ja estäen sieppauksen lähetyksen aikana. Todennus vahvistaa tietojen eheyden ja luotettavuuden varmistaen, että tietoja ei peukaloida tai väärennetä. (Youyuan, 2024.)

Kuvassa 4 IPsec-lähettäjä salaa IP-paketin käyttämällä salausalgoritmia ja salausavainta kapseloimalla alkuperäiset tiedot. Sitten lähettäjä ja vastaanottaja käyttävät samaa todennusalgoritmia ja todennusavainta salattujen pakettien käsittelemiseen saadakseen eheystarkistusarvon (ICV). Jos ICV:t täsmäävät molemmissa päissä, paketin katsotaan olevan ehjä ja vastaanotin purkaa paketin sen salauksen. Jos ICV:t eroavat toisistaan, vastaanotin hylkää paketin. (Youyuan, 2024.)



Kuva 4. IPsec-salaus ja -todennusprosessi. (Youyuan, 2024)

Viimeinen vaihe on tunnelin purkaminen. Tunnelin purkaminen tapahtuu, kun tiedonvaihto kahden kommunikoivan viestintäosapuolen välillä on valmis. Tämä tapahtuu tyypillisesti istunnon ikääntymisen vuoksi, jolloin istunto katkeaa tietyn tyhjäkäynnin aikakatkaisujakson jälkeen. Järjestelmäresurssien säästämiseksi IPsec-tunneli puretaan automaattisesti, kun sitä ei enää käytetä aktiivisesti. (Youyuan, 2024.)

3.4 Suuralueverkko

3.4.1 WAN

Wide Area Network (WAN) on laajaverkko, joka kattaa laajoja maantieteellisiä alueita ja mahdollistaa datan, äänen ja videon siirron kaupunkien, maiden tai maanosien välillä. Se toimii maailmanlaajuisten yhteyksien selkärankana, joka yhdistää laitteita ja järjestelmiä tietoliikenneverkkojen kautta. (GeeksforGeeks, 2023.)

WAN-verkot mahdollistavat saumattoman viestinnän ja resurssien jakamisen kaukaisten paikkojen välillä, mikä tarjoaa skaalautuvuuden kasvaakseen käyttäjien tai maantieteellisten tarpeiden mukaan. Ne sisältävät edistyneitä suojaustoimenpiteitä, kuten salauksen ja palomuurit, jotka takaavat tietosuojan. Keskitetty hallinta yksinkertaistaa valvontaa, kun taas luotettavat, korkealaatuiset viestintäyhteydet ylläpitävät johdonmukaista yhteyttä. (GeeksforGeeks, 2023.)

WAN-verkkojen käyttöönotto ja ylläpito voi olla kallista, mikä edellyttää erikoistunutta infrastruktuuria ja teknistä asiantuntemusta. Kaistanleveyden rajoitukset voivat vaikuttaa suorituskykyyn pitkillä etäisyyksillä, ja riittämättömät suojatoimenpiteet voivat altistaa verkot tietomurroille. Lisäksi WAN-verkot vaativat säännöllistä huoltoa optimaalisen toiminnan varmistamiseksi. (GeeksforGeeks, 2023.)

3.4.2 WWAN

WWAN (Wireless Wide Area Network) on langaton laajaverkko, joka yhdistää laitteita laajoilla maantieteellisillä alueilla. Toisin kuin perinteiset WAN-verkot, jotka

voivat käyttää sekä langallisia että langattomia yhteyksiä, WWAN-verkot käyttävät vain langattomia yhteyksiä. WWAN käyttää ensisijaisesti matkapuhelinverkkoihin, kuten 3G, 4G ja 5G, siirtääkseen dataa, ääntä ja videota pitkiä matkoja. (GeeksforGeeks, 2023.)

WWAN tarjoaa liikkuvuutta, helppokäyttöisyyttä ja laajaa saatavuutta hyödyntäen olemassa olevia matkapuhelinverkkoja. Se on kustannustehokas ratkaisu erityisesti pienyrityksille ja yksityiskäyttäjille, ja sen laaja kattavuus mahdollistaa yhteydet alueilla, joissa muut verkot eivät ole käytettävissä. (GeeksforGeeks, 2023.)

WWANilla on kuitenkin rajoituksia, kuten verkon ruuhkautumisesta ja signaalihäiriöistä johtuvat hitaammat nopeudet sekä heikentynyt suorituskyky. Tietoturvariskit, kuten salakuuntelu, tietoliikenteen sieppaus ja hakkerointi kasvavat, jos asianmukaista suojausta ja ylläpitoa ei tehdä. Kaistanleveyden rajoitukset alueilla, joissa verkossa on heikko tai ruuhkainen, mikä vaikuttaa suorituskykyä ja käyttökokemuksia. Datarajoitukset voivat myös rajoittaa käyttöä ja lisätä kustannuksia, jos ne ylittyvät. (GeeksforGeeks, 2023.)

3.5 BGP

Border Gateway Protocol (BGP) on yhdyskäytäväprotokolla, jonka avulla Internet voi vaihtaa reititystietoja autonomisten järjestelmien (AS) välillä. Kun eri verkot ovat vuorovaikutuksessa, ne tarvitsevat tavan kommunikoida keskenään. BGP tekee tämän mahdollistamalla ”peeringin” eli verkkojen välisen yhteyden. Ilman BGP:tä verkot eivät pystyisi lähettämään tai vastaanottamaan tietoja keskenään. (Fortinet, 2024.)

Kun verkkoreititin yhdistyy muihin verkkoihin, se ei tiedä, mihin verkkoon tiedot on paras lähettää. BGP ottaa huomioon kaikki reitittimen käytettävissä olevia peering-vaihtoehdot ja valitsee optimaalisen reitin, usein lähimpänä reitittimen sijainnin perusteella. Jokainen vertaisverkko (peer) jakaa omat reititystietonsa, jotka

tallennetaan reititystietokantaan RIB (Routing Information Base). BGP käyttää näitä tietoja valitakseen parhaan peering-vaihtoehdon. (Fortinet, 2024.)

3.5.1 BGP:n ominaisuudet

BGP mahdollistaa autonomisten järjestelmien välisen kommunikoinnin. BGP tukee next-hop periaatetta, joka tarkoittaa, että jokainen reitityspäätös perustuu seuraavan "hyppäyksen" (next hop) osoitteeseen. Tämä osoite kertoo, mihin verkkolaitteeseen tai reitittimeen tietyn verkon liikenne ohjataan. Next-hop auttaa BGP:tä valitsemaan parhaan reitin tiedonsiirtoon ja parantaa verkon suorituskykyä. Se voi koordinoida useita BGP-osapuolia, analysoida reititysvaihtoehtoja ja hyödyntää polkutietoja reittien valinnassa. (Fortinet, 2024.)

BGP tarjoaa järjestelmänvalvojille mahdollisuuden määrittää reitityskäytäntöjä ja hallita liikennettä joustavasti. TCP-yhteensopivuutensa ansiosta se toimii luotettavasti Internetin ja suojausprotokollien, kuten SSL, VPN ja TLS kanssa. Lisäksi BGP tukee CIDR:ää, mikä varmistaa IP-osoitteiden tehokkaan käytön, jonka avulla ei häiritse IP-osoitteiden määrittämistä tai hallintaa. Vaikka BGP:llä ei ole varsinaisia suojausominaisuuksia, se tukee suojaustyökaluja ja -protokollia, mikä mahdollistaa järjestelmänvalvojat pystyvät suojamaan verkkonsa ja käyttää BGP:tä samanaikaisesti. (Fortinet, 2024.)

3.5.2 BGP:n toiminnot

BGP varmistaa tehokkaan ja luotettavan verkkotoiminnan hallitsemalla vertaisjärjestelmien välisiä yhteyksiä. Se identifioi, todentaa ja yhdistää kumppanit ja varmistaa näiden yhteyksien kunnon. BGP välittää saavutettavuustietoja reitityksen optimoimiseksi ja virheellisten yhteyksien estämiseksi. (Fortinet, 2024.)

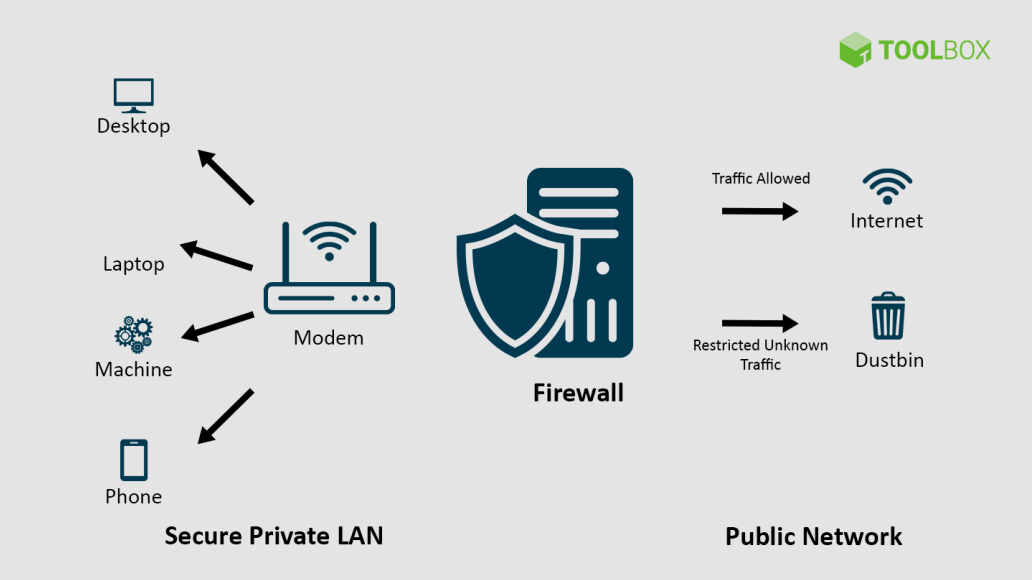
BGP:n reittien hallintaan kuuluu reititystietojen tallentaminen tietokantoihin, reititystaulukoiden päivittäminen ja vain parhaiden reittien mainostaminen vertaisille, mikä varmistaa verkon optimaalisen suorituskyvyn. (Fortinet, 2024.)

Sisäinen BGP on mekanismi, jota käytetään järjestelmässä reititystietojen jakamiseen sisäisten reitittimien kesken. Se käyttää mesh-topologiaa, joka varmistaa, että yhdeltä sisäiseltä BGP-naapurilta vastaanotettuja reittejä ei mainosteta muille, mikä estää tehokkaasti reitityssilmukat. Tämä rakenne eroaa ulkoisesta BGP:stä, jossa reitityssilmukat ovat todennäköisempiä, koska ne eivät käyttää samalaista verkkotopologiaa. (Fortinet, 2024.)

Autonominen järjestelmä (AS) on joukko toisiinsa yhdistettyjä verkkoja, jotka toimivat yhdellä hallinnolla ja käyttävät samoja BGP-protokollia reitittämiseen. Näitä järjestelmiä hallinnoivat yksi järjestelmänvalvoja tai taho. Tämä voi olla yritys, yliopisto tai muu taho, joka käyttää valittua joukkoa reititysprotokollia. (Fortinet, 2024.)

3.6 Palomuuri

Palomuuri on kyberturvallisuustyökalu, joka valvoo verkkoliikennettä ja sallii tai estää tietopaketteja ennalta määritettyjen sääntöjen perusteella. Sen ensisijainen tehtävä on estää haitalliset datapaketit ja sallia vain luvallinen liikenne, mikä auttaa suojaamaan verkkoa ulkoisilta hyökkäyksiltä. Palomuuria käytetään erityisesti verkon solmujen eristämiseen ja poisto- sekä sisääntuloliikenteen hallintaan tai tietyistä sovelluksista. Liikennettä valvotaan tietokoneen sisääntulopisteissä eli portti, jossa tietoja pyritään vaihtamaan ulkoisten laitteiden kanssa. Esimerkiksi jos lähdeosoitteen '198.21.1.1' sallitaan kommunikoida määränpään '198.21.2.1' kanssa portin 22 kautta, palomuuri varmistaa, että portti on suojattu tunkeutumisilta. Kuva 5 havainnollistaa palomuurin toimintaa yksikertaisuudessa. (Kanade, 2022.)



Kuva 5. Palomuuriarkkitehtuuri. (Kanade, 2022)

Palomuurin toimintaa voi ymmärtää vertaamalla sitä taloon, jossa IP-osoitteet ovat taloja ja porttien numerot vastaavat huoneita. Vain luotetut lähteet (henkilöt) voivat päästä taloon (kohdeosoitteeseen), ja heidän liikkumistaan talon sisällä (porttien välillä) rajoitetaan sääntöjen mukaisesti. Talon omistaja voi kulkea vapaasti mihin tahansa huoneeseen, kun taas vieraat pääsevät vain tiettyihin huoneisiin. Näiden sääntöjen avulla palomuuri valvoo tehokkaasti verkkoliikennettä ja varmistaa järjestelmän turvallisuuden. (Kanade, 2022.)

3.6.1 Palomuurin keskeiset osat

Palomuuriarkkitehtuurilla on neljä tärkeää pääkomponenttia, joita ovat verkkosääntö, edistynyt todennus, pakettisuodatus ja sovellusyhdyskäytävä. (Kanade, 2022.)

Palomuurin suunnitteluun, asennukseen ja käyttöön verkossa perustuu kahteen verkkopolitiikan tasoon: ylemmän tason politiikkaan ja alemman tason politiikkaan. Ylemmän tason keskittyy verkkokäytön sääntöihin. Se määrittelee tarkasti, mitkä palvelut ovat sallittuja tai kiellettyjä, miten niitä käytetään ja millä ehdoilla poikkeuksia sallitaan. Alemman tason konkretisoi ylemmän tason ohjeet ja määrittelee, miten palomuuri käytännössä hallitsee liikennettä, suodattaa palveluita

ja rajoittaa pääsyä. Näistä kaksi keskeistä asiaa liittyvät palvelujen käyttöpolitiikkaan ja palomuurin suunnittelupolitiikkaan. (Kanade, 2022.)

Palvelun käyttöpolitiikka keskittyy Internet-kohtaisiin käyttöongelmiin ja ulkoisiin verkkoyhteyksiin (eli puhelinsoitto, SLIP- ja PPP-yhteydet). Jotta palomuuri voidaan toteuttaa tehokkaasti, käytännön on oltava realistinen ja järkevä, ja se on tehtävä ennen palomuurin käyttöottoa. Realistinen käytäntö varmistaa, että se tarjoaa tasapainon verkon suojauksen välillä tunnetuilta riskeiltä ja että myös käyttäjillä on mahdollisuus päästä verkkoresursseihin. Palomuurin suunnittelupolitiikka määrittelee säännöt, joilla palvelun käyttöoikeuskäytäntö pannaan täytäntöön, ottaen huomioon palomuurin ominaisuudet, TCP/IP-uhat ja haavoittuvuudet. Palomuurilla on kaksi yleistä lähestymistapaa: kaikkien palvelujen salliminen (permit), ellei niitä nimenomaisesti kielletä, ja kaikkien palvelujen kieltäminen (deny), ellei niitä ole nimenomaisesti sallittu. (Kanade, 2022.)

Edistyneet todennusmenetelmät, kuten älykortit, todennustunnukset, biometriset tiedot ja ohjelmistopohjaiset ratkaisut, korjaavat perinteisten salasanojen heikkouksia. Nämä menetelmät luovat ainutlaatuisia, kertaluonteisia salasanoja, joita hyökkääjät eivät voi käyttää uudelleen, vaikka yhteyttä valvottaisiin. Palomuurit, joista puuttuu kehittyneet todennusominaisuudet, katsotaan vanhentuneiksi nykyaikaisissa Internet-ympäristöissä. Kertakäyttöiset salasanajärjestelmät, kuten älykortteja tai tunnuksia käyttävät järjestelmät, toimivat yhdessä isäntäkoneen ohjelmiston tai laitteiston kanssa luodakseen yksilöllisiä vastauksia jokaiselle kirjautumiselle, mikä parantaa turvallisuutta ja estää luvattoman käytön. (Kanade, 2022.)

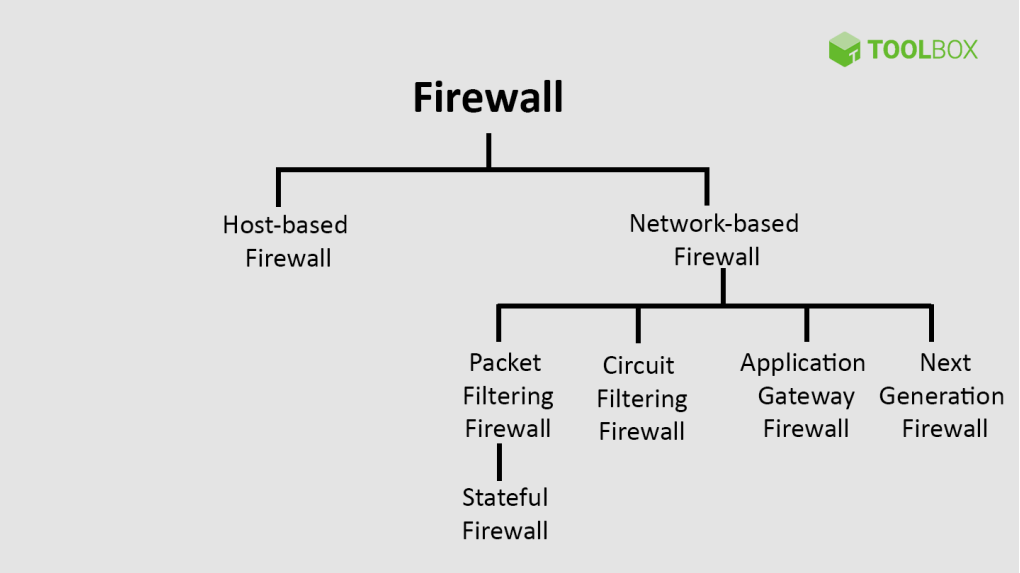
IP-paketti suodatuksen suorittaa pakettisuodatusreititin, joka tarkistaa ja suodattaa pakettien kulkiessa reitittimen rajapintojen välillä. Suodattimet perustuvat tyypillisesti kriteereihin, kuten lähde- ja kohde-IP-osoitteet, TCP/UDP-lähdeportin tai kohdeportit. Kaikki reitittimet eivät tällä hetkellä tue suodatusta lähde-

TCP/UDP-porttien mukaan. Tätä ominaisuutta otetaan käyttöön yhä enemmän. Lisäksi jotkut reitittimet tutkivat tiettyä verkkoliitäntää, jonka kautta paketti saapuu, ja on osana lisäsuodatusehtona. (Kanade, 2022.)

Sovellusyhdyskäytävät eli välityspalvelimet tarjoavat lisäturvaa suodattamalla tiettyjen palveluiden, kuten TELNET:n ja FTP:n, liikennettä. Ne korjaavat pakettisuodatuksen heikkouksia tarjoamalla ohjelmistotason hallinnan ja suojauksen. (Kanade, 2022.)

3.6.2 Palomuurityypit

Palomuurityypit voidaan jakaa kahteen tyyppiin, isäntä- ja verkkopohjaisiin palomuureihin (Kuva 6). Niillä on eri käyttötarkoitus palomuurin toiminnassa. (Kanade, 2022.)



Kuva 6. Palomuurityypit. (Kanade, 2022)

Isäntäpohjainen palomuuri on yksittäisiin verkkolaitteisiin asennettu ohjelmistosovellus, joka valvoo ja ohjaa kaikkea saapuvaa ja lähtevää paketteja. Se suojaa isäntäkonetta luvattomalta käytöltä ja haitallisilta hyökkäyksiltä toimien lisäsuojauskerroksena laitetasolla. (Kanade, 2022.)

Verkkopalomuurit toimivat verkkotasolla. Ne käyttävät tyypillisesti useita verkkoliitäntäkortteja (NIC) suodattamaan tulevaa ja lähtevää liikennettä ennalta määritettyjen sääntöjen perusteella. Nämä palomuurit ovat usein omistettuja järjestelmiä, joissa on oma ohjelmisto. Ajan myötä on kehittynyt useita erilaisia palomuuriluokkia:

1. Pakettisuodatuspalomuuri: Toimii verkkoliittymissä ja tarkastaa paketteja sellaisten kriteerien kuten IP-osoitteiden, porttien ja protokollien perusteella. Se pudottaa epäilyttäviksi merkittyjä paketteja.

2. Piiritason yhdyskäytävä: Valvoo TCP-kättelyjä ja istunnon aloitusviestejä varmistaakseen yhteyksien laillisuuden tarkastamatta yksittäisiä paketteja.

3. Tilallinen tarkastuspalomuuri: Seuraa aktiivisia verkkoistuntoja ja tarkastaa paketit näiden istuntojen yhteydessä tarjoten parannettua suojausta, mutta se heikentää verkon suorituskykyä. Toinen tilallisen tarkastuksen variantti on monikerroksiset tarkastuspalomuurit, jotka analysoivat tapahtumia useiden OSI-kerrosten välillä.

4. Sovellustason yhdyskäytävä: Kutsutaan myös välityspalvelimeksi tai välityspalvelinpalomureiksi, ja niissä yhdistyvät pakettisuodatus ja piiritason yhdyskäytäväominaisuudet, jotka tarkastavat paketteja aiotun palvelun esim. HTTP ja muiden ominaisuuksien perusteella.

5. Uuden sukupolven palomuuri (NGFW): Integroi tilallisen tarkastuksen syvälliseen pakettitarkistukseen ja lisätietoturvaominaisuuksiin, kuten tunkeutumisen havaitsemiseen/estoon, haittaohjelmien suodatukseen ja virustorjuntaan. NGFW:t analysoivat todelliset datahyötykuormat paketeissa ja varmistavat, että ne muodostavat oikeita vastauksia, kuten kelvollista HTML-sisältöä.

Näillä palomuuriluokat parantavat verkon turvallisuutta torjumalla erilaisia uhkia eri tasoilla ja verkkotoiminnan tyypeissä. (Kanade, 2022.)

3.7 SD-WAN

SD-WAN (Software-defined Wide Area Network) on ohjelmistopohjainen verkkoratkaisu, joka yksinkertaistaa yritysten verkkojen hallintaa eri sijaintien välillä. SD-WAN tarjoaa organisaatioille joustavamman ja kustannustehokkaamman tavan hallita ja optimoida verkkoyhteyksiä ratkaisuihin. Se mahdollistaa liikenteen reitittämisen useiden yhteystyyppien, kuten MPLS (Multiprotocol Label Switching), laajakaistan, LTE/5G ja pilvipalveluiden, kautta, mikä parantaa verkon suorituskykyä ja luotettavuutta. Reaaliaikainen verkon seuranta ja sovellusten priorisointi takaavat optimaalisen tiedonsiirron ja vähentävät häiriöitä. (Yelland, 2024.)

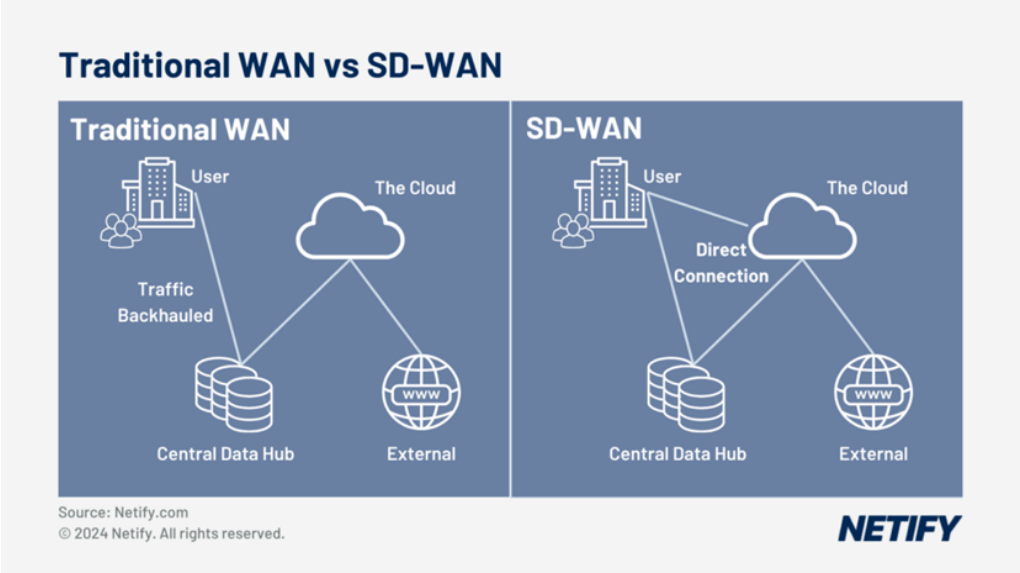
Kustannussäästöjä syntyy erikoistuneiden ja kalliiden MPLS-piirien tarpeen vähenemisestä sekä virtualisoinnin hyödyntämisestä, joka korvaa fyysisiä verkkolaitteita ohjelmistopohjaisilla ratkaisuilla. Tämä mahdollistaa muun muassa palomuurien ja WAN-optimointiohjainten keskitetyn hallinnan ilman ylimääräisiä laitehankintoja. (Yelland, 2024.)

SD-WAN yksinkertaistaa verkon hallintaa keskitetyn hallinta- ja orkestrointijärjestelmän avulla, mahdollistaen nopean käyttöönoton ja skaalautuvuuden. Lisäksi palvelun laadunhallinta QoS (Quality of Service) optimoi verkon suorituskyvyn luokittelemalla liikennettä, ja integroidut tietoturvaratkaisut, kuten SASE (Secure Access Service Edge)-kehys, takaavat yhtenäisen ja ajan tasalla olevan suojauspolitiikan. (Yelland, 2024.)

Standardointi ja yhteentoimivuus eri valmistajien ratkaisujen välillä varmistavat, että SD-WAN voidaan ottaa käyttöön ilman yhteensopivuusongelmia. Kaiken kaikkiaan SD-WAN mahdollistaa yrityksille tehokkaamman, turvallisemman ja skaalautuvamman verkkoratkaisun, joka tukee liiketoiminnan kasvua ja digitalisaatiota. (Yelland, 2024.)

3.7.1 SD-WANin toiminnat

SD-WAN hyödyntää ohjelmistopohjaista hallintaa liikenteen ohjaamiseen ja optimointiin yrityksen eri sijaintien, kuten sivukonttoreiden ja etäkäyttäjien, sekä keskusresurssien, kuten datakeskusten ja pilvipalveluiden, välillä. Perinteisessä WAN-verkossa liikenne kulkee vain datakeskuksen kautta, mikä aiheuttaa viivettä ja kuormittaa verkkoa (Kuva 7). (Yelland, 2024.)



Kuva 7. WAN vs. SD-WAN arkkitehtuuri. (Yelland, 2024)

Yritykset hyötyvät yhä enemmän julkisen internetin käytöstä, joka mahdollistaa työntekijöille joustavan pääsyn liiketoimintakriittisiin järjestelmiin mistä tahansa laitteesta ja sijainnista. SD-WAN-arkkitehtuuri koostuu kahdesta keskeisestä komponentista: reunalaitteista ja yhdyskäytäväohjaimista. (Yelland, 2024.)

SD-WAN reunalaitteet sijaitsevat sivukonttoreissa tai etätoimipisteissä ja muodostavat suojatun yhteyden SD-WAN-verkkoon. Ne vastaavat liikenteen priorisoinnista, tietoturvasta ja reitityksestä, ja niihin voidaan integroida lisäominaisuuksia, kuten palomuurit ja WAN-optimointi. (Yelland, 2024.)

SD-WAN yhdyskäytäväohjaimet sijaitsevat datakeskuksissa tai pilviympäristöissä ja tarjoavat skaalautuvuutta sekä mahdollistavat palveluketjun hallinnan. Ne vastaavat verkon suorituskyvyn seurannasta, käytäntöjen jakamisesta reunalaitteisiin ja dynaamisesta reitityksestä. Ohjaimet hallitaan keskitetysti orkestrointi- ja hallinta-alustan kautta. (Yelland, 2024.)

SD-WAN reititystä voi optimoida liikennevirrat valitsemalla älykkäästi ja dynaamisesti parhaan mahdollisen datapolun reaaliaikaisten verkko-olosuhteiden perusteella. Yritykset siirtävät yhä enemmän sovelluksia julkisiin pilvipalveluihin, kuten Google Cloudiin, Microsoft Azureen ja Amazon Web Servicesiin (AWS), tarjotakseen etäkäyttäjille turvallisen ja luotettavan pääsyn liiketoimintakriittisiin resursseihin. SD-WAN mahdollistaa suoran ja optimoidun yhteyden näihin pilvipalveluihin, mikä parantaa suorituskykyä ja vähentää viiveitä. Lisäksi SD-WAN integroi pilvipalveluiden tietoturvaominaisuudet, kuten liikenteen salauksen ja sovellustason suojaukset, varmistaen tietojen turvallisuuden ja eheyden koko verkon laajuudelta. (Yelland, 2024.)

3.7.2 SD-WAN tulevaisuudessa

SD-WAN on tuonut merkittäviä parannuksia perinteisiin WAN-verkkoihin lisäämällä ominaisuuksia, kuten reaaliaikaisen reitityksen, sisäänrakennetut turvatoiminnot ja automaattisen käyttöönoton ZTP (Zero Touch Provisioning). Teknologian kehittyessä ja yleistyessä yritysten keskuudessa SD-WANin mahdollisuudet laajenevat useille alueille:

1. Pilvipohjaisten ratkaisujen kasvu: Pilvipalveluiden käytön kasvaessa yhä useammat yritykset hyödyntävät pilvipohjaisia SD-WAN-palveluja. Tämä mahdollistaa joustavan ja suorituskykyisen yhteyden pilveen ja sovelluksiin, parantaen verkon saavutettavuutta ja luotettavuutta. SD-WAN palveluiden kehittyessä on yleistymässä täysin pilvipohjainen hallinta, mikä vähentää tarvetta fyysiselle laitteistolle yrityksen toimitiloissa.

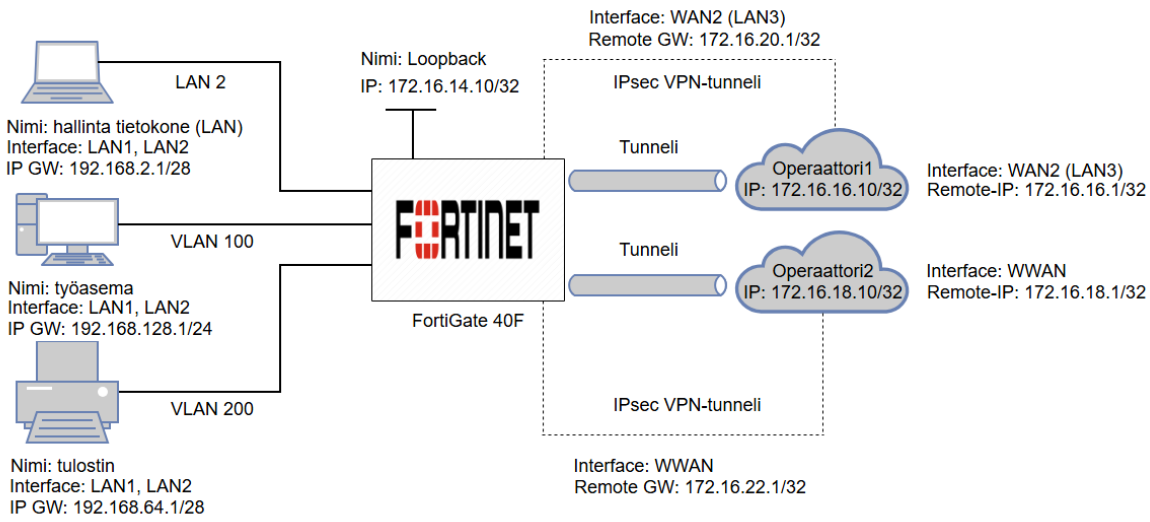
2. Tekoälyn ja koneoppimisen hyödyntäminen: Tekoäly ja koneoppiminen tarjoavat uusia mahdollisuuksia SD-WAN-verkkojen optimointiin. Ne mahdollistavat verkon suorituskyvyn jatkuvan parantamisen, automaattisen ongelmanratkaisun ja paremman turvallisuuden. Näiden teknologioiden avulla voidaan tunnistaa poikkeamia liikenteessä ja reagoida mahdollisiin uhkiin nopeammin.
3. Tietoturvan kehitys: Tulevaisuudessa yhä suurempi painotus on kattavissa suojausratkaisuissa, kuten SASE, palomuureissa ja VPN-yhteyksissä. Näiden avulla voidaan yksinkertaistaa järjestelmäarkkitehtuuria ja parantaa järjestelmän hallintaa.

(Yelland, 2024.)

4 SD-WANIN SUUNNITTELU JA KONFIGUROINTIVAIHEET

4.1 Suunnittelu

Tässä opinnäytetyössä pyrittiin suunnittelemaan mahdollisimman yksinkertainen ja joustava verkkoratkaisu. Verkko rakennettiin palomuurin ja hallintatietokoneen väliseksi yhteydeksi, mutta internet-yhteys jätettiin pois käytöstä tietoturvan ja olemassa olevia IP-osoitteiden suojelun vuoksi. Tässä työssä ei käytetä muita fyysisiä laitteita, verkko on jaettu VLAN (Virtual Local Area Network) -verkkoihin työasemalle ja tulostimille. Operattorille1 ja operattorille2 on luotu tunneli, joka mahdollistaa erillisen verkkoyhteyden. Lisäksi käytössä on Loopback-verkko (Kuva 8).



Kuva 8. Verkkokuva.

4.2 Fortinet FortiGate 40F -palomuuri

Työssä käytetään Fortinet FortiGate 40F -palomuuria, koska se tukee SD-WAN-toimintoa ja tarjoaa laajan valikoiman verkkoprotokollaominaisuuksia sekä sopii erinomaisesti pienille -ja keskikokoisille yritysverkoille.

Verkkokortista löytyy yksi USB-portti, konsoliportti, Gigabit Ethernet RJ45 WAN -portti, Gigabit Ethernet RJ45 FortiLink -portti sekä kolme Gigabit Ethernet RJ45 Ethernet -porttia.

Tässä työssä käytetään verkkokorteista kahta Ethernet-porttia LAN1 ja LAN2, kolmas Ethernet-portti (LAN3) konfiguroidaan WAN2-yhteyttä varten. WAN-portti ja FortiLink-portti A pysyvät oletusasetuksessa.

4.3 Konfigurointivaiheet

Tässä luvussa käydään läpi palomuurin eri konfigurointivaiheet. Konfigurointikomennot sisältävät muun muassa DHCP:n, DNS:n, BGP:n, VPN IPsecin, Palomuurisäännöt sekä muita komentoja. Ensimmäisessä vaiheessa varataan IP-osoitteet loopbackille, overlay operattorille1 ja operattorille2, työasemalle, tulostimille ja hallintaverkoille. Seuraavaksi määritetään yhdyskäytävä (gateway) työasemalle, tulostimille ja hallintaverkoille. Lisäksi laitteelle annetiin nimi SD-WAN-Labra. Työasemalle ja tulostimille määritettiin nimet työasemaverkko ja tulostinverkko.

Tämän jälkeen Fortinet FortiGate 40F -palomuurilaite konfiguroitiin käyttämällä SD-WAN-konfigurointipohjaa, joka on esitetty liitteessä 1. Konfigurointipohja saatiin 2M-IT:n toiselta tietoliikenneasiantuntijalta, ja sitä on muokattu tähän opinnäytetyöhön sopivaksi siten, ettei se sisällä tietoturvariskejä. Kaikki asetukset tehtiin suoraan tämän konfiguraatiopohjan mukaisesti. Konfigurointi voidaan tehdä joko Putty-ohjelman kautta tai Fortinet FortiGaten omalla komentokehotteella, mutta tässä työssä konfigurointi suoritettiin Putty-ohjelmalla.

4.4 Fortinet FortiGate -hallintapaneeli

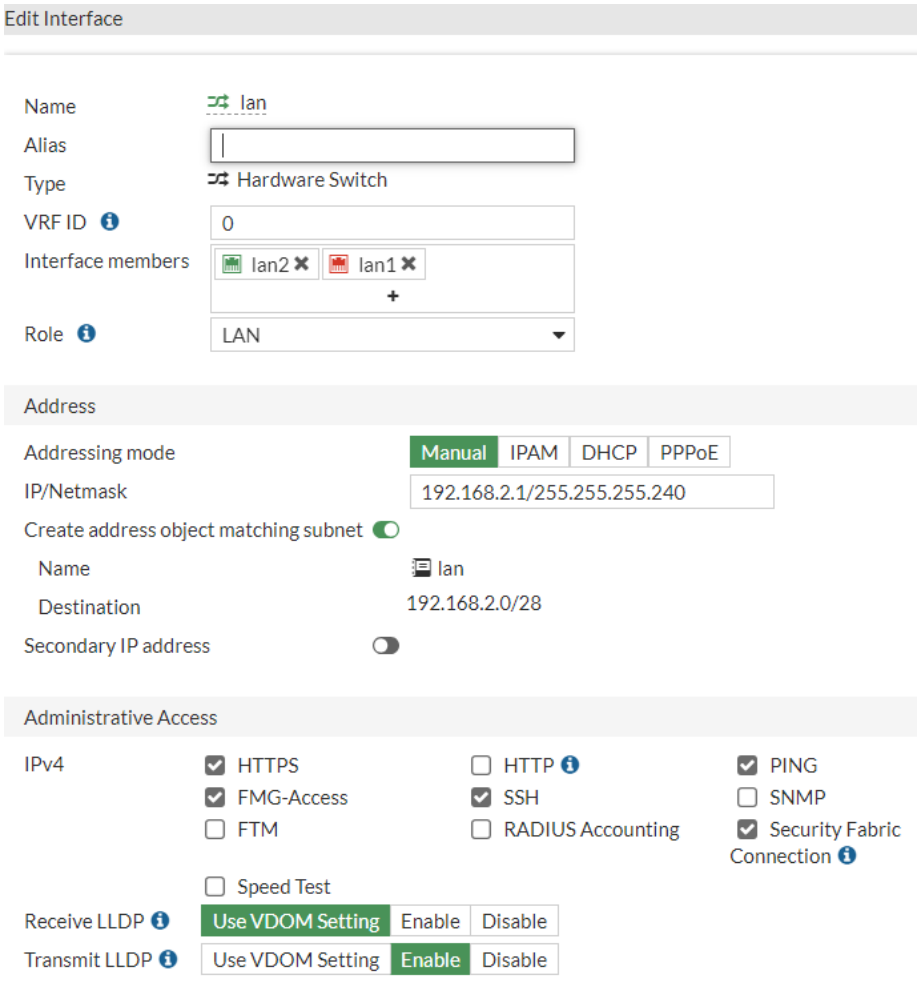
Kun palomuurilaite on saatu konfiguroitua, käydään läpi tärkeimmät vaiheet Fortinet FortiGaten hallintapaneelissa tehdyt asetukset ja lopuksi testataan verkon toimivuus.

Fortinet Fortigate -hallintapaneelin tarjoaa käyttäjälle selkeän ja informatiivisen näkymän laitteen asetuksiin ja tilaan. Hallintapaneeli on web-pohjainen ja sen kautta voidaan tehdä kaikki laitteeseen liittyvät määritykset ja tarkistukset. Se tarjoaa kattavan valikoiman työkaluja, joilla hallita palomuurin toimintaa, liikennettä, käyttäjiä ja monia verkkoturvallisuuden osa-alueita.

4.4.1 Käyttöliittymät

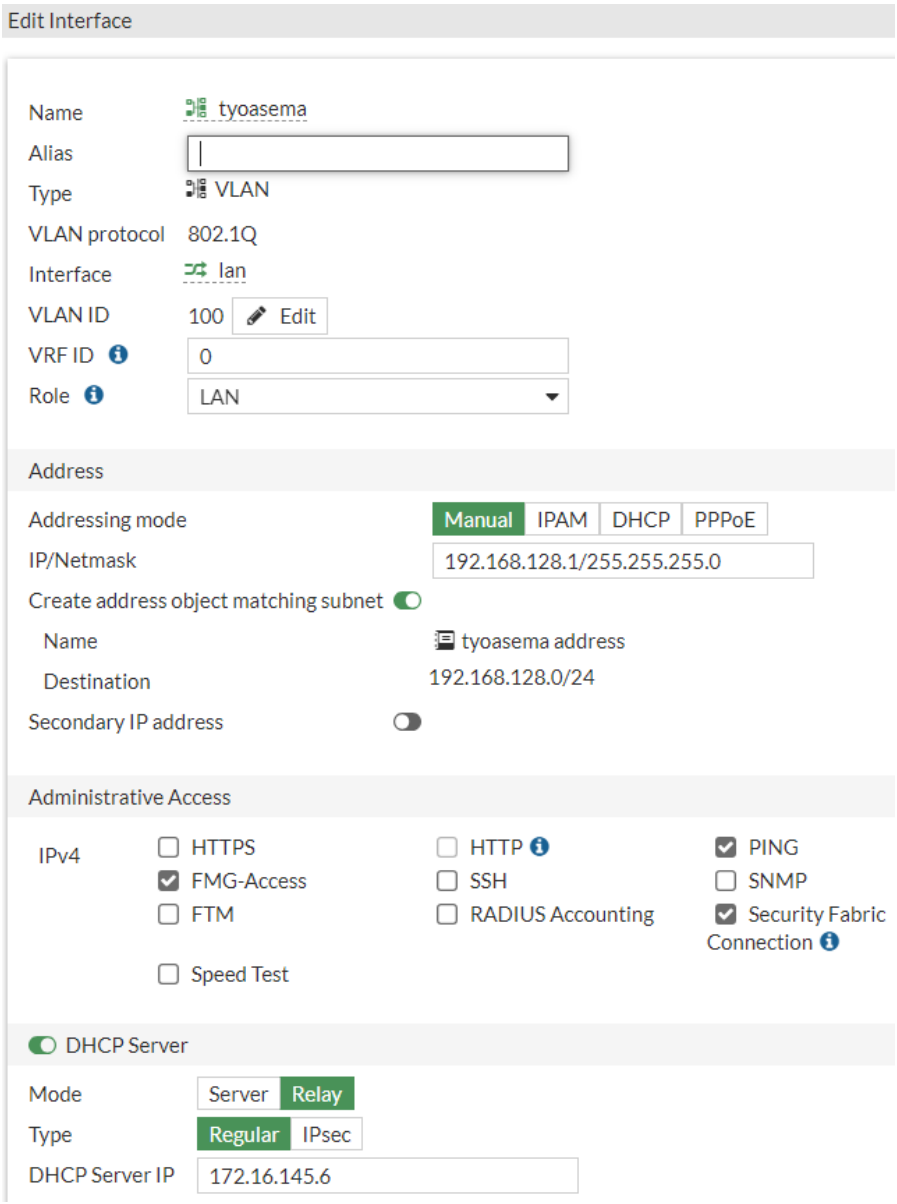
Kuvassa 9 on hallintaverkon käyttöliittymän muokkaustila. Liittymä nimettiin ”lan” ja se kuuluu paikallisverkon LAN-liittymään. Se käyttää ”Hardware Switch” kytkintä, mikä tarkoittaa, että se toimii sekä kytkimenä että palomuurina. Tämä liittymä kostuu kahdesta fyysisestä portista (LAN1 ja LAN2), joista tässä tapauksessa LAN2 on käytössä. IP-osoite määriteltiin manuaalisesti osoitteeseen 192.168.2.1 ja aliverkkomaskiksi 255.255.255.240, jolloin verkkoalueeksi muodostuu 192.168.2.0/28. Hallinnollinen käyttöoikeus määrittää, mitkä hallintayhteydet ovat sallittuja IPv4-verkon kautta. Siinä asetukset sisältävät HTTPS:n, HTTP:n, PING, FMG-ACCESS:n, SSH:n, SNMP:n, FTM:n, RADIUS Accountingin, Security Fabric Connectionin ja Speed Testin. LLDP (Link Layer Discovery Protocol) vastaanottaa ja lähettää liikennettä käyttäen VDOM (Virtual Domains)-asetuksia.

VDOM on Fortinetin käyttämä virtuaalinen verkkotunnus, jonka tehtävänä on jakaa useimpiin laitteelle virtuaalisiksi yksiköiksi. Jokainen VDOM toimii itsenäisenä yksikkönä omilla asetuksillaan, reitityksellään, palomuurisäännöillään ja hallintaoikeuksillaan. (Fortinet, 2025.)



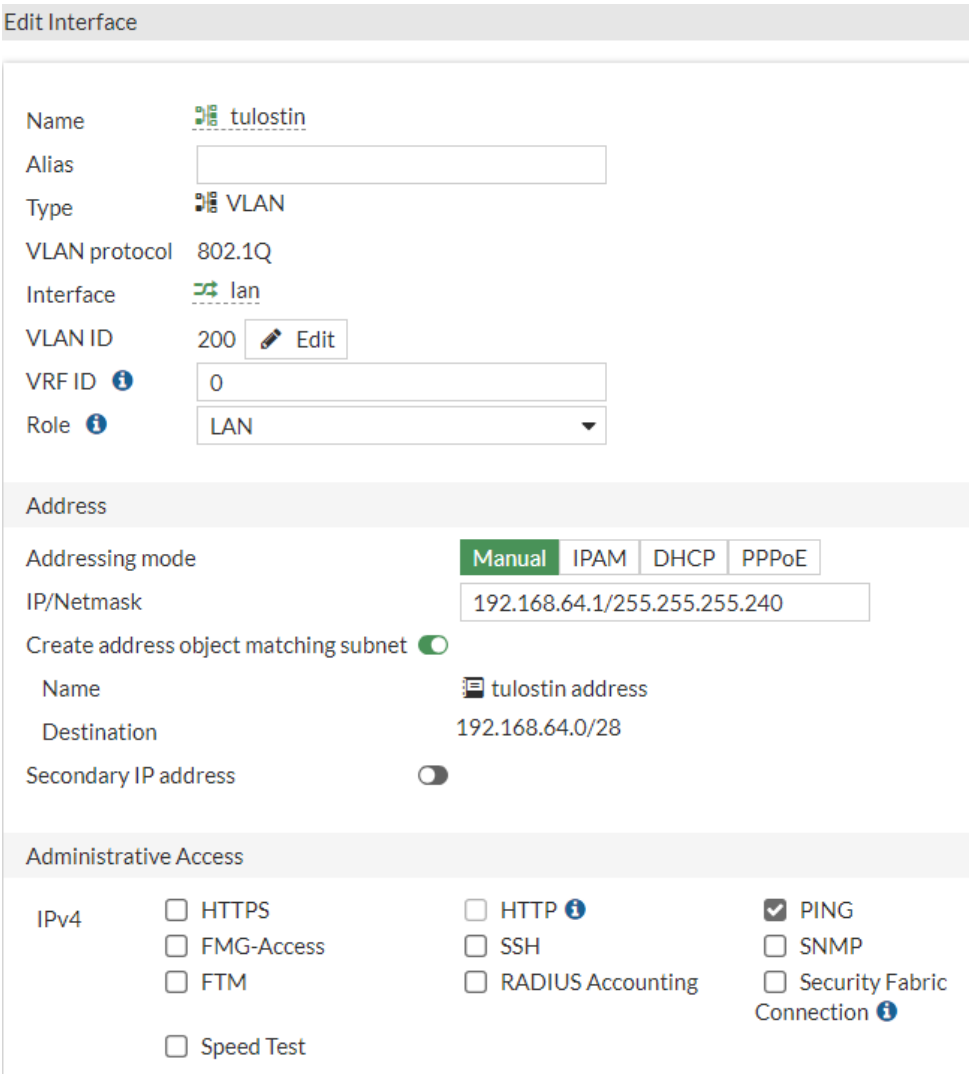
Kuva 9. Hallintaverkon käyttöliittymä.

Kuvassa 10 on työasemaverkon käyttöliittymän muokkaustila. Liittymä nimettiin "työasema" ja se kuuluu työasemaverkon VLAN-liittymään. VLAN-protokollana käytetään 802.1Q, mikä mahdollistaa liikenteen tunneloimisen VLAN-tageilla. Tämä VLAN-liittymä on yhdistetty "LAN"-rajapintaan ja kuuluu VLAN 100 ryhmään, toimien LAN-verkon yhteytenä. IP-osoite määriteltiin manuaalisesti osoitteeseen 192.168.128.1 ja aliverkonmaskiksi 255.255.255.0, jolloin verkkoalueeksi muodostuu 192.168.128.0/24. Liittymä toimii myös DHCP Relaynä, mikä tarkoittaa, että DHCP-pyynnöt välitetään eteenpäin varsinaiselle DHCP-palvelimelle. DHCP-määritettiin normaalisen toiminnantilassa ja DHCP-palvelimen IP-osoitteeksi asetettiin 172.16.145.6.



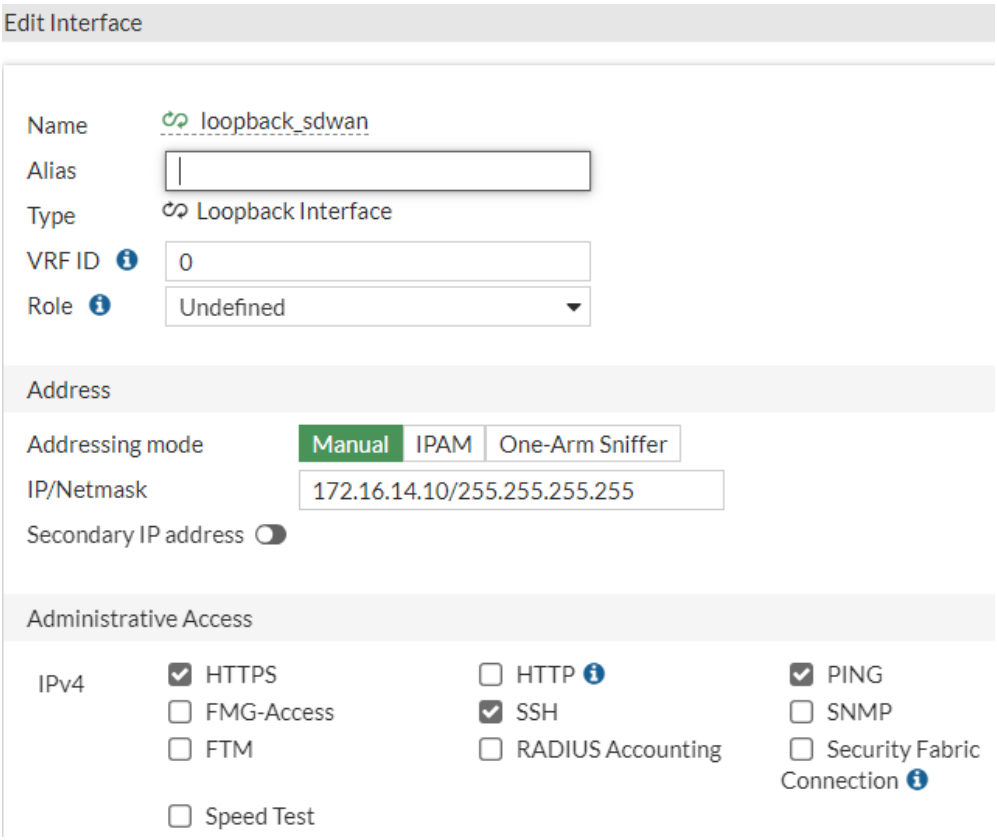
Kuva 10. Työasemaverkon käyttöliittymä.

Kuvassa 11 on tulostinverkon käyttöliittymän muokkaustila. Liittymä nimettiin "tulostin" ja se kuuluu tulostinverkon VLAN-liittymään. VLAN-protokollana käytetään samaa kuin työasemaverkko ja se käyttää myös samaa ”LAN”-rajapintaa, toimien LAN-verkon yhteytenä. Tulostinverkko kuuluu kuitenkin VLAN 200 ryhmään. IP-osoite määriteltiin osoitteeseen manuaalisesti 192.168.64.1 ja aliverkonmaskiksi 255.255.255.240, jolloin verkkoalueeksi muodostuu 192.168.64.0/28.



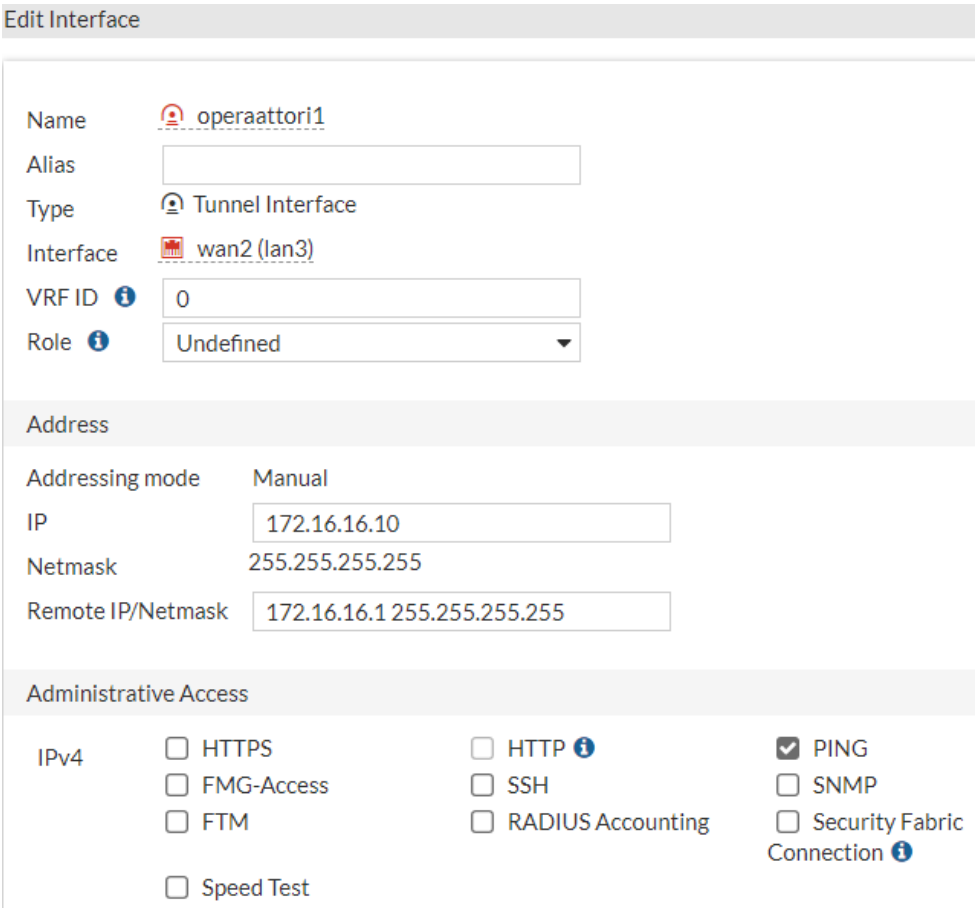
Kuva 11. Tulostinverkon käyttöliittymä.

Kuvassa 12 on Loopback-käyttöliittymän muokkaustila. Loopback liittymä on nimetty ”loopback_sdwan” ja se on virtuaalinen verkkorajapinta, joka ei ole sidottu fyysiseen porttiin. Sitä käytetään SD-WAN-konfiguraatiossa reitityksen, tunnistautumisen tai liikenteen hallinnan tukena. IP-osoite on määritelty manuaalisesti osoitteeseen 172.16.14.10 ja aliverkkomaskiksi 255.255.255.255, mikä tarkoittaa, että Loopback-liittymä käyttää yksityisverkon osoitetta.



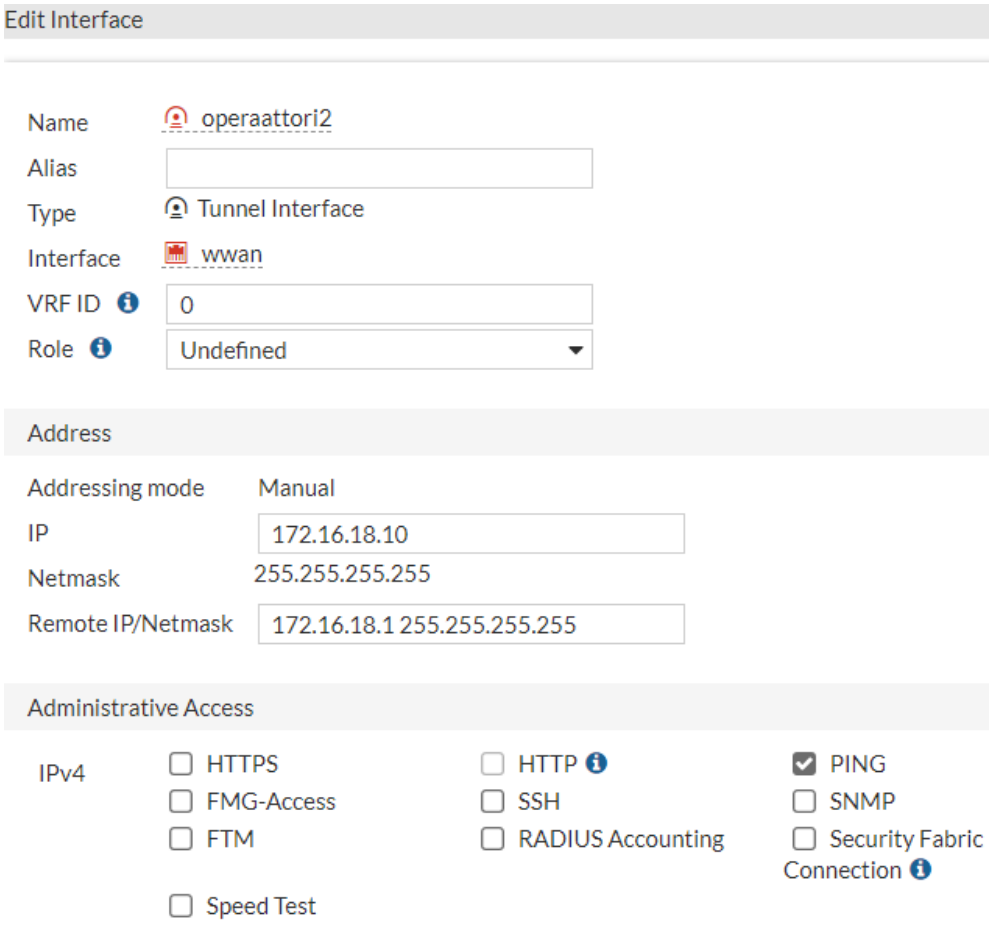
Kuva 12. Loopback-käyttöliittymä.

Kuvassa 13 on operaattori1-käyttöliittymän muokkaustila. Liittymän nimettiin "operaattori1" ja se kuuluu tunneliliittymään. Tämä liittymä on liitetty fyysiseen rajapintaan WAN2 (LAN3), mikä tarkoittaa, että WAN2 käyttää laajaverkkoa LAN3 portissa. IP-osoite määriteltiin manuaalisesti osoitteeseen 172.16.16.10 ja aliverkonmaskiksi 255.255.255.255. Etä-IP-osoitteena käytetään 172.16.16.1 ja verkkomaskiksi 255.255.255.255, mikä tarkoittaa, että liittymä on osa kahden pisteen välistä tunneliyhteyttä.



Kuva 13. Operaattori1-käyttöliittymä.

Kuvassa 14 on operaattori2-käyttöliittymän muokkaustila. Liittymä nimettiin "operaattori2" ja se kuuluu tunneliliittymään. Tämä liittymä on liitetty fyysiseen rajapintaan WWAN, joka käyttää langatonta verkkoa. IP-osoite määriteltiin manuaalisesti osoitteeseen 172.16.18.10 ja aliverkonmaskiksi on 255.255.255.255. Etä-IP-osoitteena käytetään 172.16.18.1 ja verkkomaskiksi 255.255.255.255.

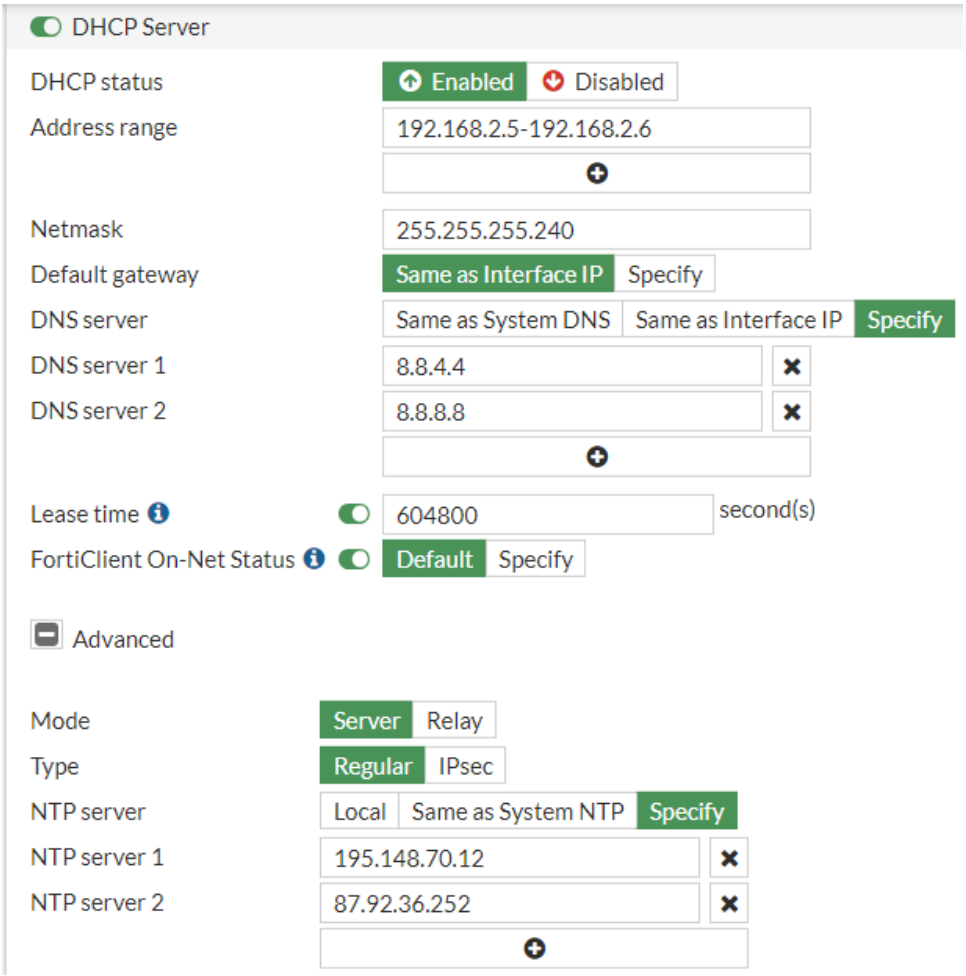


Kuva 14. Operaattori2-käyttöliittymä.

4.4.2 DHCP- ja DNS-palvelimen asetukset

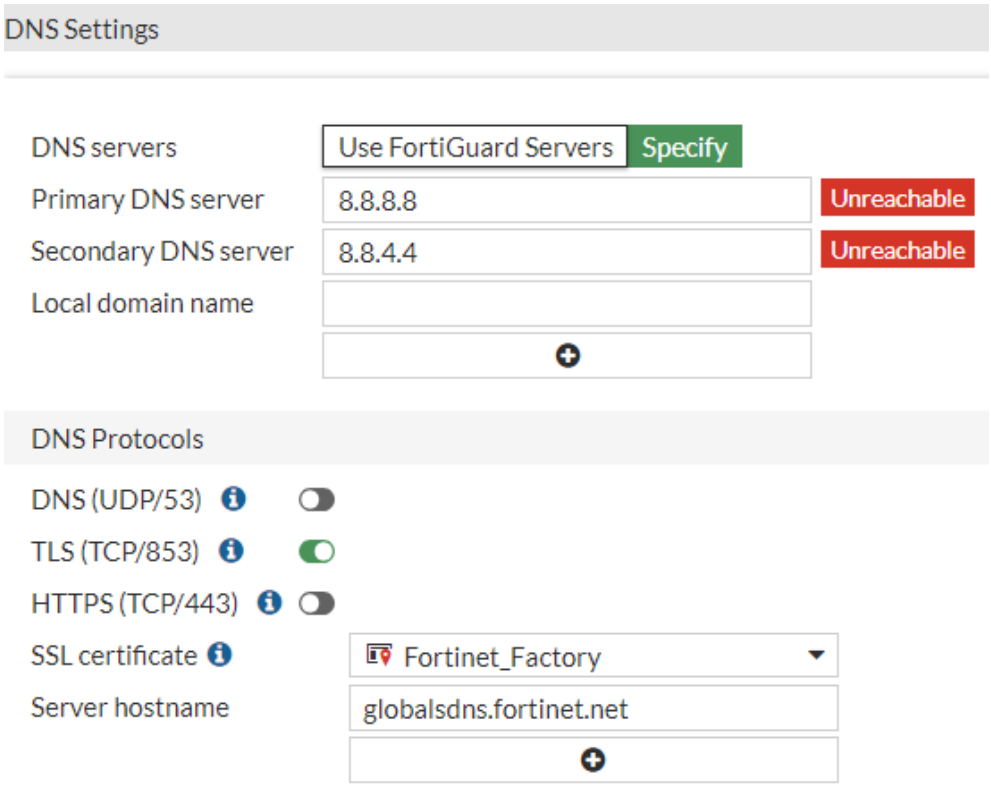
Kuvassa 15 on DHCP-palvelimen asetukset. DHCP jakaa kahta IP-osoitetta 192.168.2.5–192.168.2.6 ja aliverkkomaskiksi 255.255.255.240. Tämä käyttää samaa oletusyhdyskäytävää kuin hallintaverkko eli 192.168.2.1 osoitetta. DNS-palvelin määriteltiin manuaalisesti ja se käyttää Googlen julkisia DNS-palvelinosoitteita 8.8.4.4 ja 8.8.8.8. IP-osoitteiden vuokra-aika on asetettu 604800 sekuntiin (7 päivään), eli asiakas säilyttää saamansa IP-osoitteen viikon ajan ennen uusimistarvetta. NTP (Network Time Protocol) on määritelty kaksi palvelinta 195.148.70.12 ja 87.92.36.252, jotka molemmat ovat julkisia aikapalvelimia.

NTP on aikapalvelinprotokolla, jolla synkronoidaan laitteiden kelloja verkossa. Sen avulla varmistetaan, että kaikki verkkoon liitetyt laitteet, kuten palvelimet, reitittimet ja tietokoneet, käyttävät samaa ja tarkkaa aikaa. Tämä on tärkeää lokitietojen analysoinnissa, tietoturvassa ja verkkohallinnassa. (Spiceworks, 2025.)



Kuva 15. DHCP-palvelimen asetukset.

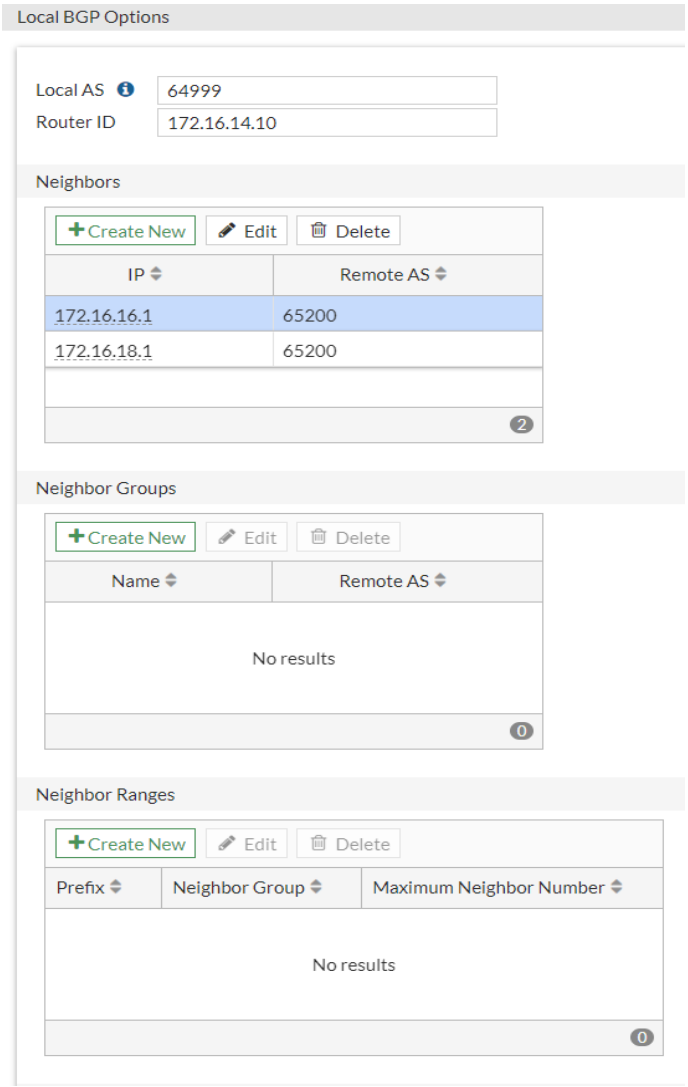
Kuvassa 16 on DNS-palvelimen asetukset. DNS-palvelin käyttää ensisijaisesti osoitetta 8.8.8.8 ja toissijaisesti 8.8.4.4. DNS-protokollassa käytetään TLS:ää (TCP/853), mutta tarvittaessa voidaan käyttää joko DNS:ää (UDP/53) tai HTTPS:ää (TCP/443). SSL-sertifikaatti on oletuksena käytössä Fortinetin tehdasasetuksissa ja palvelimen isäntänimenä käytetään globalsdns.fortinet.net.



Kuva 16. DNS-palvelimen asetukset.

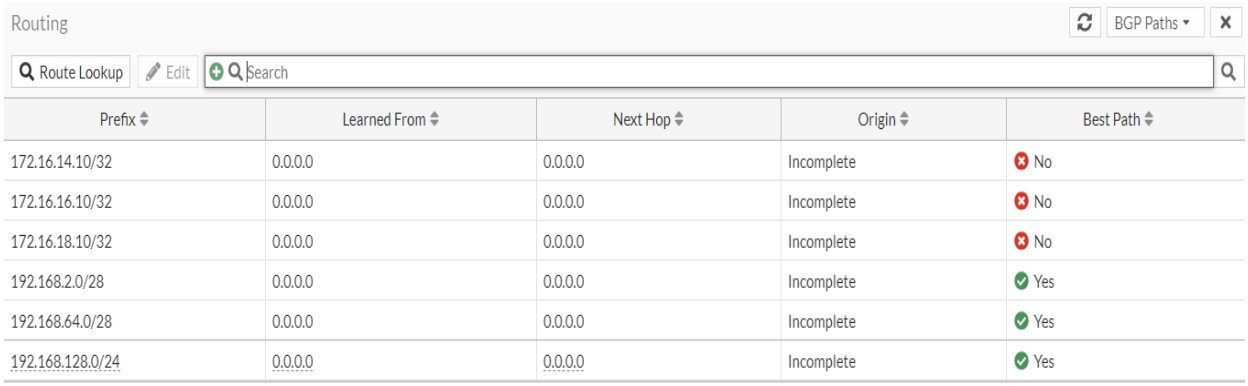
4.4.3 BGP-asetukset

Kuvassa 17 on paikalliset BGP-asetukset. Määriteltiin paikallinen autonominen järjestelmä (Local AS) arvoksi 64999 ja reitittimen tunniste (Router ID) IP-osoitteeseen 172.16.14.10. Kahdelle naapurille on lisätty osoitteet 172.16.16.1 ja 172.16.18.1 sekä niiden Remote AS -arvoksi 65200, mikä tarkoittaa, että laite vaihtaa BGP-reitti-informaatiota näiden kahden naapurin kanssa. Naapuriryhmät (Neighbor Groups) ja naapureiden alueet (Neighbor Ranges) -osiot ovat tyhjiä, mutta niihin voidaan luoda uusia ryhmiä ja alueita.



Kuva 17. Paikalliset BGP-asetukset.

Kuvassa 18 on BGP-reititystaulu, joka näyttää reititystiedot BGP-protokollan kautta. Reititystaulussa esiintyvät verkot 172.16.14.10/32, 172.16.16.10/32, 172.16.18.10/32, 192.168.2.0/28, 192.168.64.0/28 ja 192.168.128.0/24, joista ensimmäiset kolme eivät ole saatavilla parhaan BGP-reitityksen mukaisesti (Best Path = No, punainen rasti), kun taas jälkimmäiset kolme ovat saatavilla parhaan BGP-reitityksen (Best Path = Yes, vihreä merkki) mukaisesti. Kaikkien reittien Next Hop ja Learned From -arvot ovat 0.0.0.0, mikä tarkoittaa, ettei laite ole oppinut reittejä aktiivisilta BGP-naapureilta. Lisäksi Origin-tilana näkyy "Incomplete", mikä tarkoittaa, että reitit eivät ole peräisin suoraan BGP-naapureilta, vaan ne on määritelty manuaalisesti.



Prefix	Learned From	Next Hop	Origin	Best Path
172.16.14.10/32	0.0.0.0	0.0.0.0	Incomplete	No
172.16.16.10/32	0.0.0.0	0.0.0.0	Incomplete	No
172.16.18.10/32	0.0.0.0	0.0.0.0	Incomplete	No
192.168.2.0/28	0.0.0.0	0.0.0.0	Incomplete	Yes
192.168.64.0/28	0.0.0.0	0.0.0.0	Incomplete	Yes
192.168.128.0/24	0.0.0.0	0.0.0.0	Incomplete	Yes

Kuva 18. BGP-reititystaulu.

4.4.4 IPsec VPN-tunnelin asetukset

Kuvassa 19 ja 20 on IPsec VPN-tunnelin asetukset, jossa tunneli on nimetty "operaattori1 ja operaattori2". Molemmat käyttävät IPv4-protokollaa. Etäkohteen (Remote Gateway) IP-osoitteeksi on määritelty:

- operaattori1: 172.16.20.1 ja liikenne kulkee liittymän WAN2 (LAN3) kautta.
- operaattori2: 172.16.22.1 ja liikenne kulkee liittymän WWAN kautta.

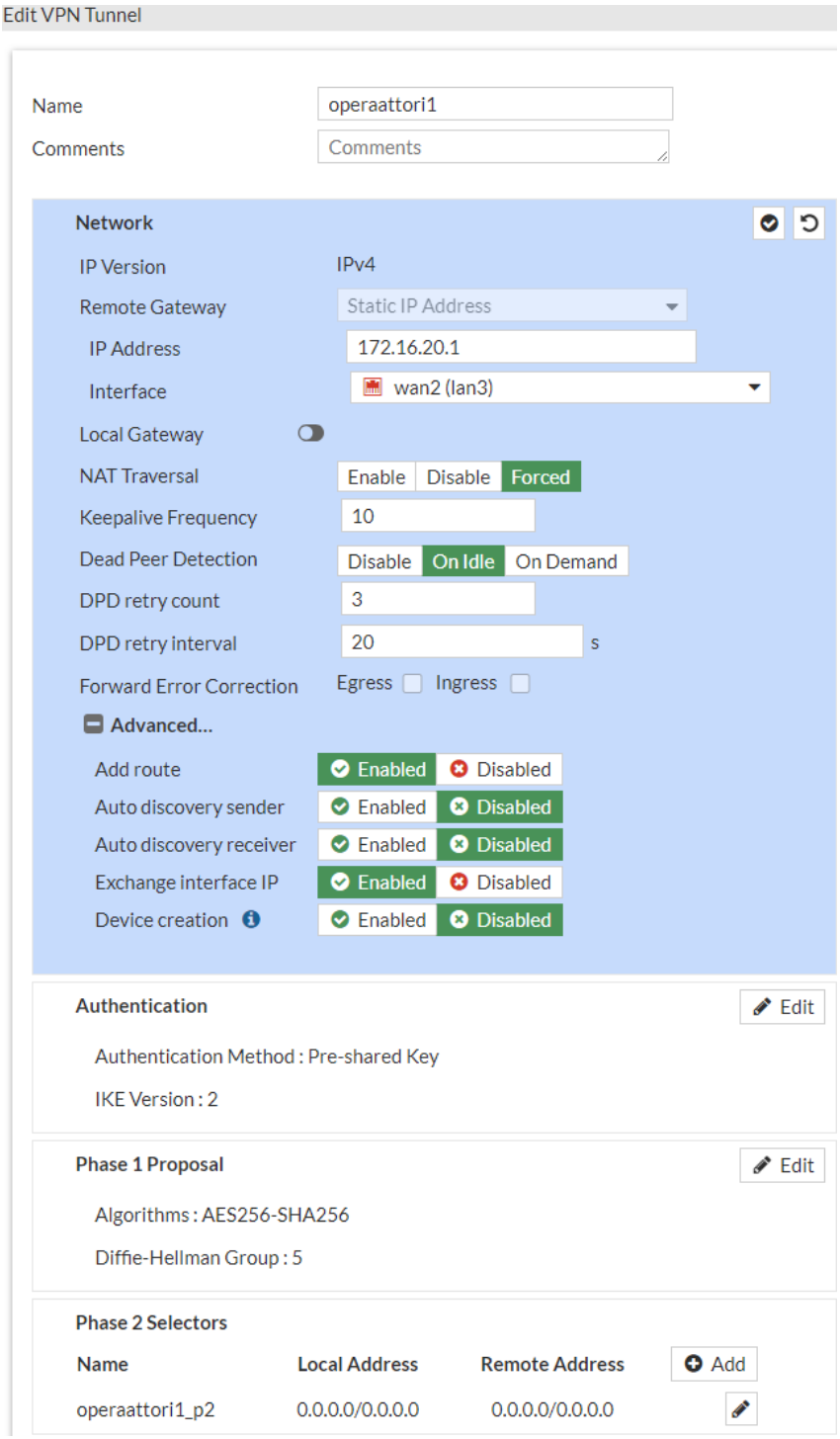
VPN-asetuksissa NAT Traversal on pakotettu (Forced) operaattori1-tunnelissa, kun taas operaattori2-tunnelissa on normaalisti päällä (Enable).

Muut asetukset ovat molemille tunneleille samat:

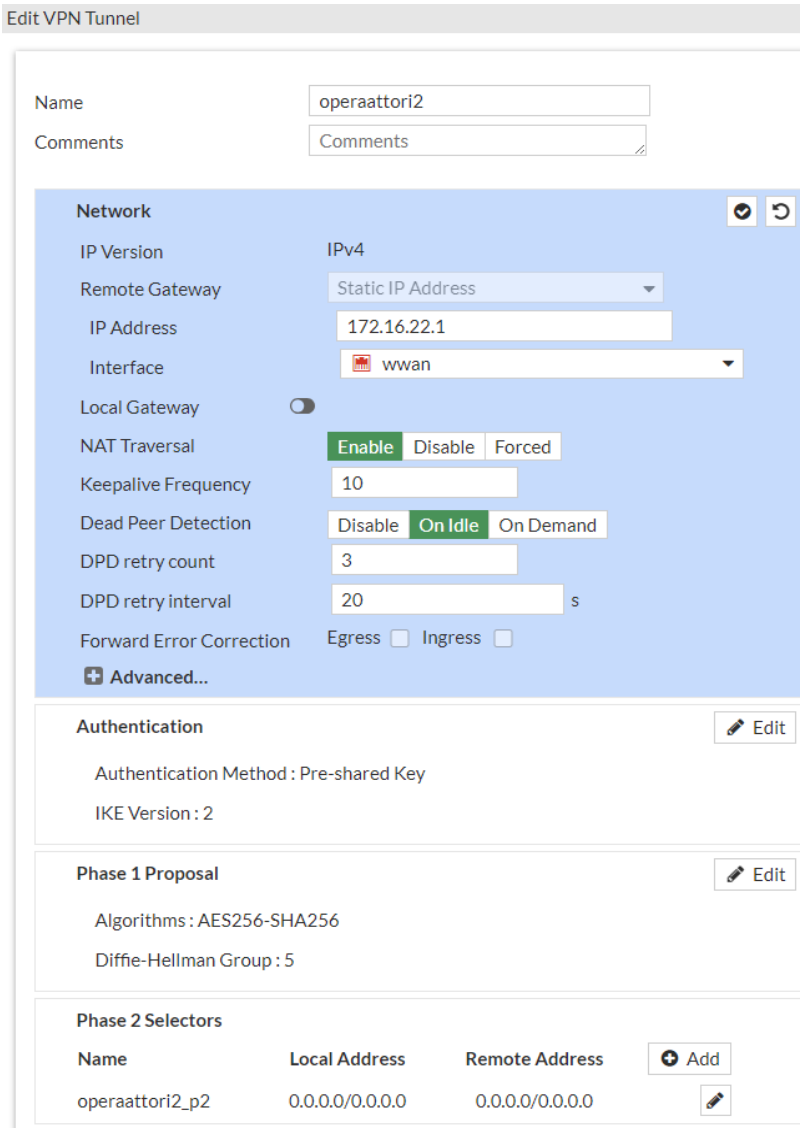
- Keepalive -viestit lähetetään 10 sekunnin välein.
- Dead Peer Detection (DPD) on asetettu ”On Idle”, mikä tarkoittaa, että yhteys tarkistetaan vain, kun liikennettä ei ole.
- DPD-asetuksissa on määritelty kolme yritystä 20 sekunnin välein.
- Lisäasetuksista reititys, automaattinen havaitseminen ja laitteiden luonti ovat käytössä.

Autentikointina operaattori1 ja operaattori2 käyttävät IKEv2-protokollaa ja esijaettua avainta (Pre-shared Key). Salauksessa käytetään AES256-SHA256-algoritmia

ja Diffie-Hellman-ryhmää 5. Toiseen vaiheen asetuksissa (Phase 2) tunnelit on nimetty ”operaattori1_p2 ja operaattori2_p2” ja molemmissa sekä paikallinen että etäosoitealue on 0.0.0.0/0.0.0.0, mikä sallii kaiken liikenteen VPN-tunnelin kautta.



Kuva 19. Operaattori1:n IPsec VPN-tunnelin asetukset.



Kuva 20. Operaattori2:n IPsec VPN-tunnelin asetukset.

4.4.5 Palomuurisäännön hallintanäkymä

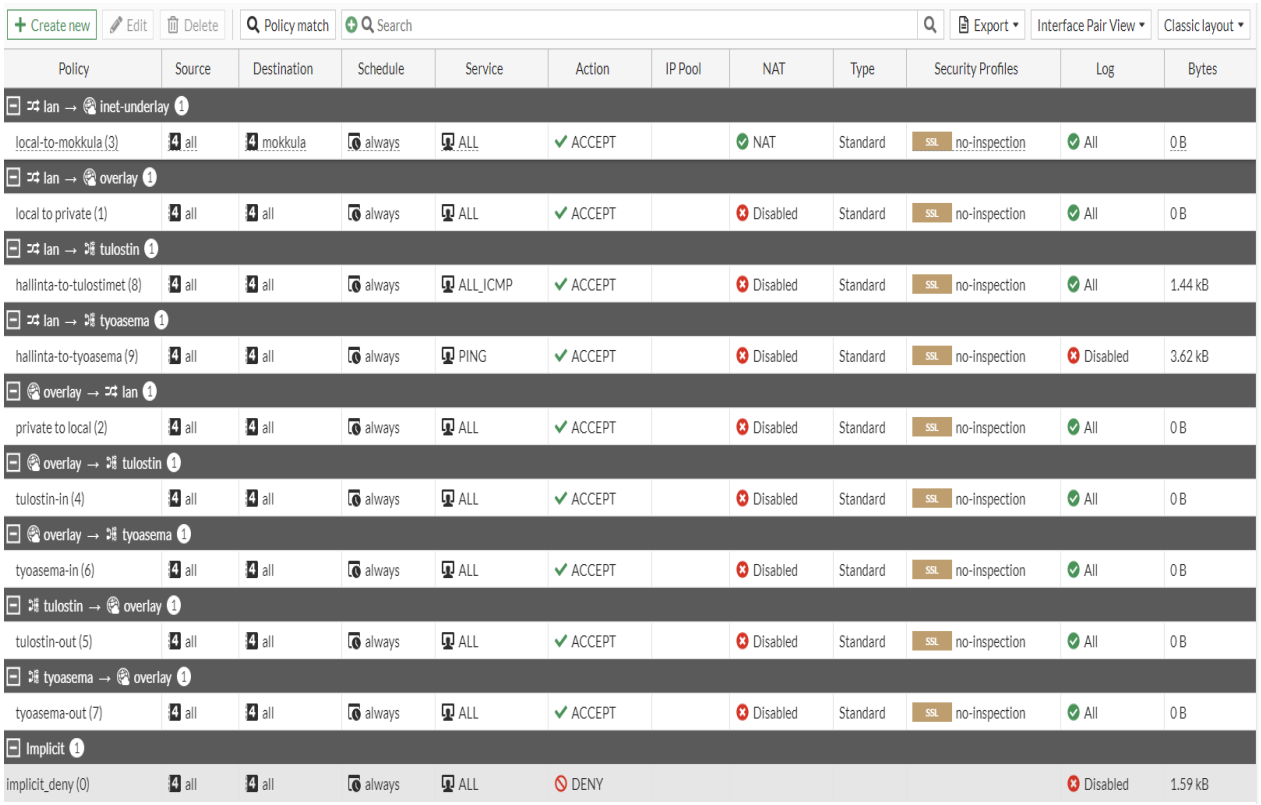
Kuvassa 21 on palomuurisääntöjen hallintanäkymä, jossa määritellään sallittu ja estetty verkkoliikenne eri verkkoalueiden välillä. Tämä on keskeistä verkon suojauksen ja liikenteen hallinnan kannalta.

Kuvan 21 taulukossa on luettelo erilaisista määritellyistä palomuurisäännöistä:

- ”**local-to-mokkula**” sallii kaiken liikenteen lähteestä ”all” kohteeseen ”mokkula” NATin kautta.

- ”**local to private**” sallii kaiken liikenteen lähteestä ja kohteeseen ilman NAT:n.
- ”**hallinta-to-tulostimet**” sallii kaiken ICMP-liikenteen.
- ”**hallinta-to-tyoasema**” sallii kaiken PING-liikenteen.
- Muut säännöt, kuten ”**private to local**”, ”**tulostin-in**”, ”**tyoasema-in**”, ”**tulostin-out**” ja ”**tyoasema-out**”, sallivat kaiken liikenteen ilman NATia.

Viimeisenä sääntönä on ”**implicit deny**”, joka estää kaiken liikenteen, jota aiemmat säännöt eivät salli. Tämä on erittäin tärkeää tietoturvan kannalta, sillä ilman sitä kaikki liikenne menisi läpi, mikä olisi merkittävä tietoturvariski.



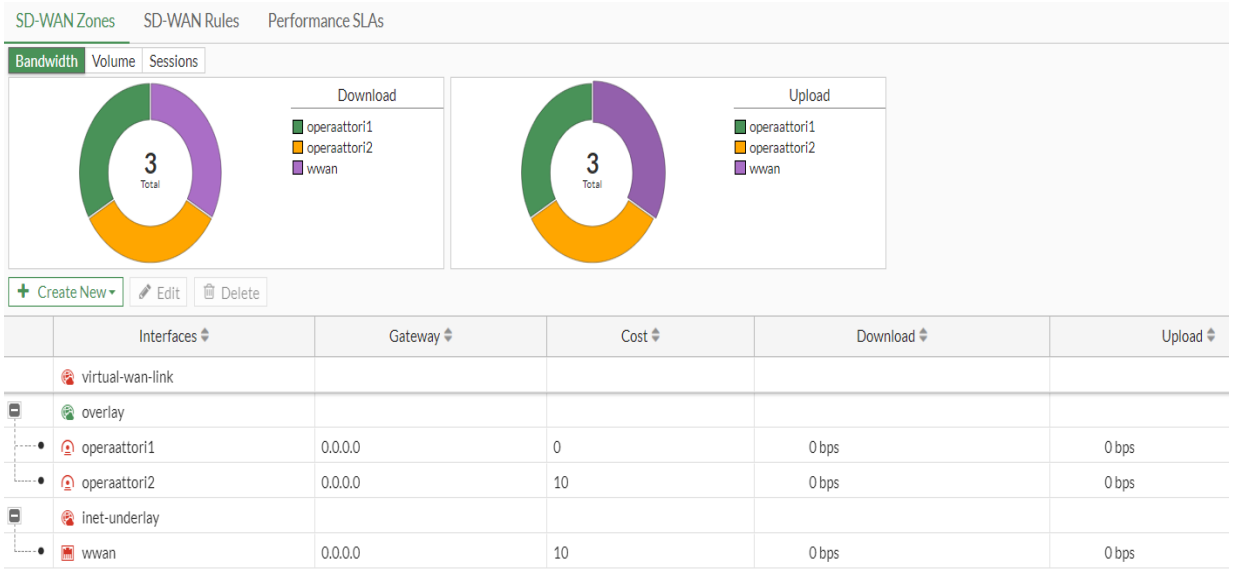
Kuva 21. Palomuurisääntöjen hallintanäkymä.

4.4.6 SD-WANin asetukset

Kuvassa 22 on SD-WAN Zones -näkymä, jossa SD-WANissa on määritelty kolme yhteyttä: operaattori1, operaattori2 ja WWAN. Näiden yhteyksien liikennettä ja kustannuksia hallitaan dynaamisesti. SD-WANin kaistanlevynäkymä (Bandwidth)

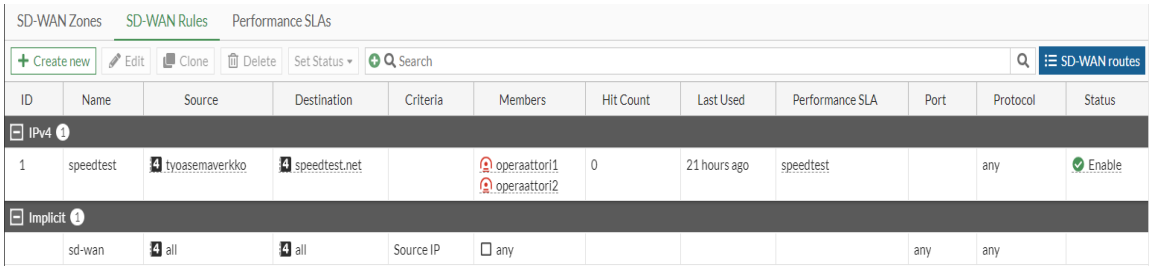
esittää, että tällä hetkellä kaikki kolme yhteyttä ovat aktiivisia mutta niiden lataus- ja lähetysnopeudet ovat 0 bps, mikä tarkoittaa, ettei niillä ole tällä hetkellä liikennettä, tämä vaikuttaa, kun internet-yhteyttä ei ole käytössä. Oletuskäytäväosoitteet ovat 0.0.0.0, mikä viittaa siihen, että laite ei ole oppinut reitittimiltä.

Lisäksi operaattori1:llä on kustannusarvo 0, kun taas operaattori2:lla ja WWAN:lla kustannusarvo on 10, mikä tarkoittaa, että FortiGate suosii ensisijaisesti operaattori1-yhteyttä, ellei SLA-sääntöjen mukaiset suorituskyky- tai häiriörajoitukset vaadi yhteyden vaihtamista. (Fortinet, 2025.)



Kuva 22. SD-WAN Zones -näkymä.

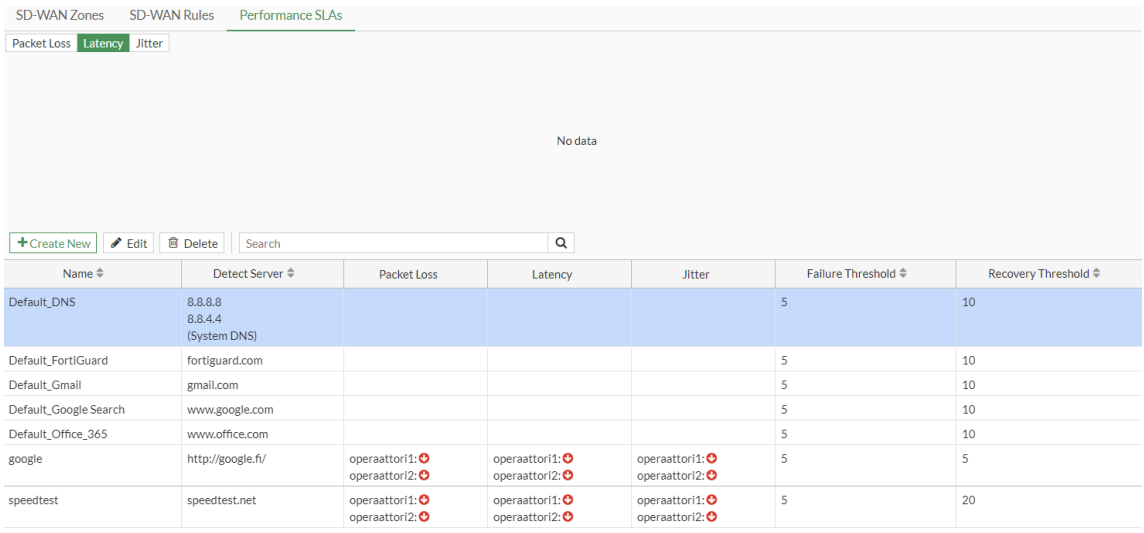
Kuvassa 23 on SD-WAN Rules -näkymä, jossa määritellään liikenteen reititys SD-WAN-yhteyksien välillä. Speedtest reititetään työasemaverkosta speedtest.net-osoitteeseen suuntautuva liikenne operaattori1- ja operaattori2-yhteyksien kautta Performance SLA -säännön mukaisesti, mutta koska Hit Count -arvo on 0, sääntöä ei ole vielä käytetty tai liikenne ei ole osunut siihen viimeaikaisesti. Implisiittinen (Implicit) SD-WAN-sääntö mahdollistaa kaiken muun liikenteen reitittämisen SD-WAN-yhteyksien kautta ilman erityisiä ehtoja. Tämä tarkoittaa, että speedtest.net-liikenne ohjataan optimaalisimman yhteyden kautta ja muu liikenne kulkee oletussäännön mukaisesti.



Kuva 23. SD-WAN Rules -näkymä.

Kuvassa 24 on SD-WAN Performance SLA -asetukset, joilla seurataan eri palveluiden, kuten Googlen ja Speedtestin, suorituskykyä SD-WAN-yhteyksien kautta. Packet Loss, Latency ja Jitter -mittareiden perusteella operaattori1- ja operaattori2-yhteyksillä on ongelmia, sillä ne näyttävät punaisia rasteja, mikä johtuu internet-yhteyden puuttumisesta. Failure Threshold ja Recovery Threshold -arvot määrittävät, milloin yhteys merkitään vialliseksi tai palauteta käyttöön, ja ne ovat pääosin 5 ja 10, paitsi Speedtest-palvelulle, jossa palautuskynnys on 20. Tämä tarkoittaa, että SD-WAN voi siirtää liikenteen toiseen yhteyteen vikatilanteessa.

Vaikka tässä työssä ei näy SD-WANin suorituskyky toiminnassa, on se tärkeä työkalu verkkoliikenteen seuraamiseen, toimivuuden arviointiin ja käytössä olevien yhteyksien hallintaan.

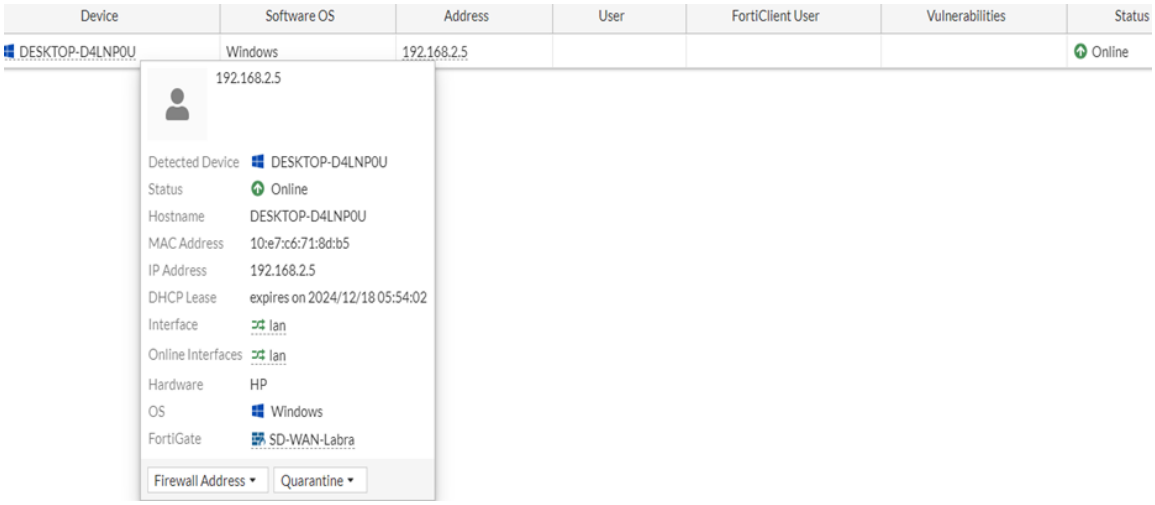


Kuva 24. SD-WAN Performance SLA -näkymä.

5 TULOKSET

Tässä työssä testauksessa käytettiin PING-menetelmää verkkoyhteyden toiminnan tarkistamiseksi sekä palomuurin toimivuuden varmistamiseksi.

Kuvassa 25 näkyvät verkkoon liitetyn laitteen tiedot, jotka sisältävät laitteen nimen, käyttöjärjestelmän, IP -ja MAC-osoitteet, tilan, DHCP Lease eli vuokra-ajan, käyttöliittymän (Interface), laitteistotiedot sekä FortiGate-laitteen nimen. Voidaan huomata, että hallintatietokone on saanut IP-osoitteen 192.168.2.5 DHCP-palvelimelta ja vuokra-aika päättyy tiettynä ajankohtana. Tässä on myös mahdollisuus määrittää palomuuri osoitteita (Firewall Address) ja siirtää laitetta karanteeniin (Quaratine) tarvittaessa.



Kuva 25. Verkkoon liitetyn laitteen tiedot.

Taulukossa 1 on esitetty ping-testin tulokset. Hallintatietokone toimi lähtölaitteena kaikissa ping-testeissä, koska muita koneita ei ollut käytettävissä.

Ping-testien perusteella lähes kaikki testit onnistuivat, paitsi loopback ping-testi, joka epäonnistui. Työasema, tulostin ja loopback käydä erikseen läpi ping-testien sekä palomuurin toiminnan osalta näiden välillä.

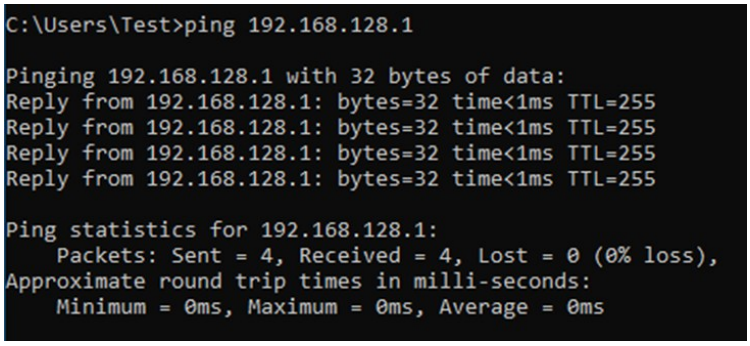
Taulukko 1. Ping-testin tulokset.

Lähdelaite	Kohdelaite	Lähdeosoitteet	Kohdeosoitteet	Testi tulos
Hallintatietokone	Palomuuri (DHCP-palvelin)	192.168.2.5	192.168.2.1	Ping OK
Hallintatietokone	Työasema GW	192.168.2.5	192.168.128.1	Ping OK
Hallintatietokone	Tulostin GW	192.168.2.5	192.168.64.1	Ping OK
Hallintatietokone	Loopback	192.168.2.5	172.16.14.10	Ping Fail
Hallintatietokone	Operaattori1	192.168.2.5	172.16.16.10	Ping OK
Hallintatietokone	Operaattori2	192.168.2.5	192.16.18.10	Ping OK

Hallintatietokone on saanut IP-osoitteen DHCP-palvelimelta, kuten edellisessä kuvassa 25 on esitetty. Tämä tarkoittaa, että hallintatietokone on onnistuneesti pyytänyt ja vastaanottanut IP-osoitteen DHCP-palvelimen kautta. Lisäksi ping-testi osoittaa, että yhteys tietokoneen ja DHCP-palvelimen välillä toimii.

Ping-testit osoittavat, että operaattori1- ja operaattori2-osoitteet vastasivat, mutta tunnelin toista päätä ei testattu, joten yhteyden toimivuus päästä päähän jäi vahvistamatta.

Kuvassa 26 näkyy työasemanverkon osoite, johon ping-testi onnistui. Tämä tarkoittaa, että hallintatietokoneen ja työasemanverkon välillä on toimiva VLAN-yhteys ja palomuuri on sallinut niiden välisen liikenteen.

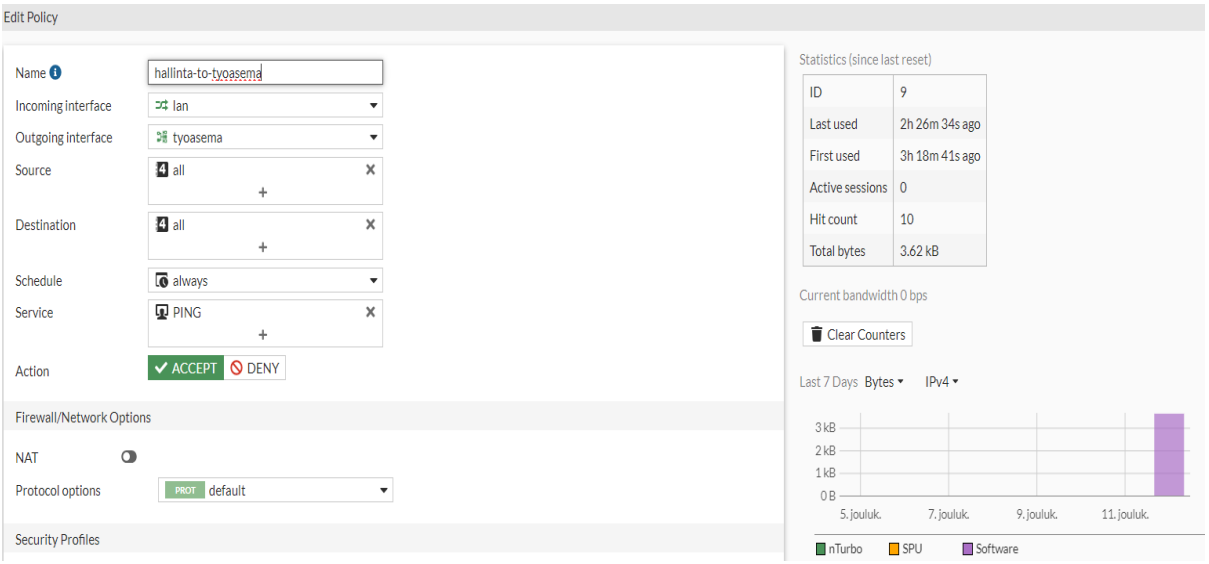


Kuva 26. Työasemanverkon osoitenäkymä.

Kuvassa 27 on palomuurisäännön muokkausnäkymä, jossa voidaan määritellä palomuurisääntöjä hallintayhteyden ja työasemaverkon väliselle liikenteelle. Liikenne tulee LAN-verkosta ja se ohjataan työasemaverkkoon, koskien kaikkia lähde- ja kohdeosoitteita. Sääntö on aina voimassa ja sallii ainoastaan PING-liikenteen.

Oikeassa reunassa näkyvät verkkoliikennetilastot osoittavat, että viimeksi verkkoliikennettä oli 2 tuntia 26 minuuttia 34 sekuntia sitten ja ensimmäistä kertaa verkkoliikennettä otettiin käyttöön 3 tuntia 18 minuuttia 41 sekuntia sitten. Osumien määrä oli yhteensä 10 kertaa, eli tässä tapauksessa PING-paketit ovat osuneet liikenteessä oli 10 kertaa ja näiden pakettien datamäärä oli yhteensä 3,62 kilotavua.

Lisäksi näkyy viimeisen 7 päivän liikennemäärät tavuina, jotka ovat kulkenet ohjelmistopohjaisen palomuurin kautta. Vaikka tässä työssä liikennettä on ainoastaan yhden päivän ajalta, tämä mahdollistaa verkkoliikenteen seuraamisen, kuten minkä tyyppistä tietoa on liikennöity, kuinka paljon dataa on kulunut ja onko liikennettä ollut tiettyinä päivinä lainkaan.



Kuva 27. Hallintayhteyteen työasemaan palomuurisäännön näkymä.

Kuvassa 28 näkyy tulostinverkon osoite, johon ping-testi onnistui. Tämä tarkoittaa, että hallintatietokoneen ja tulostinverkon välillä on toimiva VLAN-yhteys ja palomuuri sallinut näiden liikenne välillä.

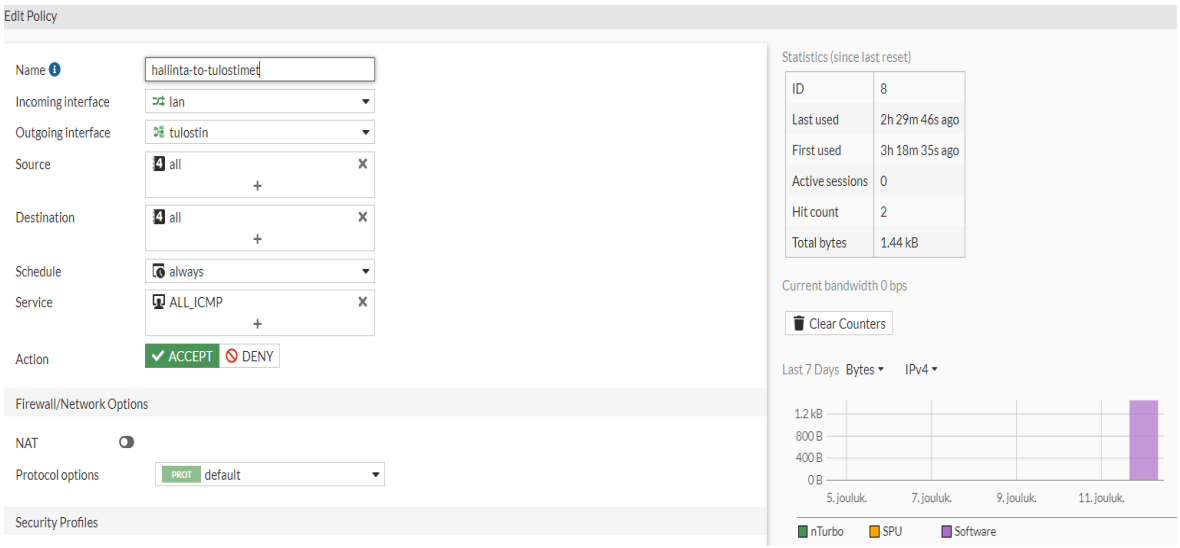
```
C:\Users\Test>ping 192.168.64.1

Pinging 192.168.64.1 with 32 bytes of data:
Reply from 192.168.64.1: bytes=32 time<1ms TTL=255
Reply from 192.168.64.1: bytes=32 time<1ms TTL=255
Reply from 192.168.64.1: bytes=32 time<1ms TTL=255
Reply from 192.168.64.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.64.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Kuva 28. Tulostinverkon osoitenäkymä.

Kuvassa 29 on palomuurisäännön muokkausnäkymä, jossa voidaan määritellä palomuurisääntöjä hallintayhteyden ja tulostinverkon väliselle liikenteelle. Liikenne tulee LAN-verkosta ja ohjataan tulostinverkkoon, koskien kaikkia lähde- ja kohdeosoitteita. Sääntö on aina voimassa ja sallii kaiken ICMP-liikenteen.

Oikeassa reunassa näkyvät verkkoliikennetilastot osoittavat, että viimeksi verkkoliikennettä oli 2 tuntia 29 minuuttia 46 sekuntia sitten ja ensimmäistä kertaa verkkoliikennettä otettiin käyttöön 3 tuntia 18 minuuttia 35 sekuntia sitten. Osumien

määrä oli yhteensä 2 kertaa, eli tässä tapauksessa ICMP-paketit ovat osuneet liikenteessä oli 2 kertaa ja näiden pakettien datamäärä oli yhteensä 1,44 kilotavua.



Kuva 29. Hallintayhteyteen tulostimen palomuurisäännön näkymä.

Kuvassa 30 näkyy loopback-osoite, johon ping-testi ei mennyt läpi. Tämä tarkoittaa, että hallintatietokoneen ja loopback-verkon välillä ei ole toimivaa yhteyttä, koska palomuurisäännössä ei ole määritelty liikennettä.

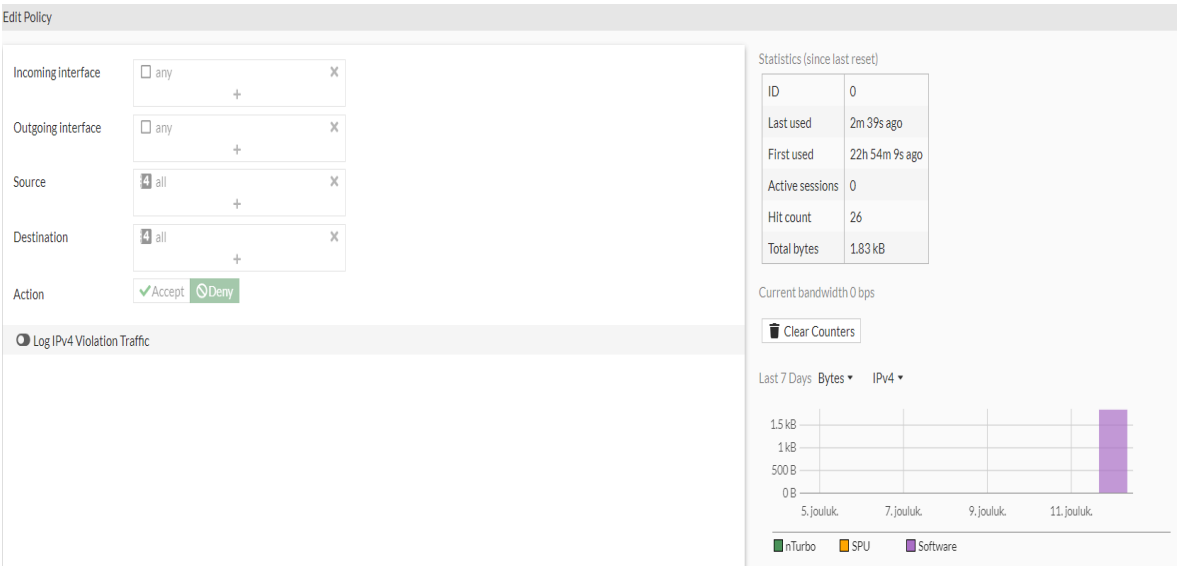
```
C:\Users\Test>ping 172.16.14.10

Pinging 172.16.14.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.14.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Test>
```

Kuva 30. Loopbackin osoitenäkymä.

Kuvassa 31 on implisiittisen estokäytännön (implicit deny) muokkausnäkymä, joka estää kaiken liikenteen, jos sitä ei ole erikseen sallittu. Käytännön asetukset ovat oletusarvoisesti käytössä, mikä tarkoittaa, että käytäntöä ei voi muokata, lisätä tai poistaa.

Oikeassa reunassa näkyvät verkkoliikennetilastot osoittavat, että viimeksi verkkoliikennettä oli 2 minuuttia 39 sekuntia sitten ja ensimmäistä kertaa verkkoliikennettä otettiin käyttöön 22 tuntia 54 minuuttia 9 sekuntia sitten. Osumien määrä oli yhteensä 26 kertaa, eli tässä tapauksessa estetyt paketit ovat osuneet liikenteeseen 26 kertaa ja näiden pakettien datamäärä oli yhteensä 1,83 kilotavua.

Implisiittinen estokäytäntö varmistaa, että kaikki liikenne, joka ei ole erikseen sallittu, estetään. Tämä on keskeistä verkon turvallisuuden ja liikenteen hallinnan kannalta.



Kuva 31. Implisiittisen estokäytännön muokkausnäkymä.

6 YHTEENVETO JA POHDINTA

Opinnäytetyö keskittyi SD-WAN-teknologian käyttöönottoon työympäristössä. Tavoitteena oli suunnitella ja toteuttaa SD-WAN-ratkaisu, joka parantaa organisaation verkon suorituskykyä, joustavuutta ja tietoturvaa. Työssä käytetiin Fortinet FortiGate 40F -palomuuria, joka tukee SD-WAN-toimintoa ja tarjoaa laajan valikoiman verkkoprotokollaominaisuuksia. Projektin tavoitteet saavutettiin päänosin, vaikka SD-WAN-verkon suorituskykyä ei voitu havainnollistaa konkreettisesti, koska tietoturvasyiden vuoksi internet-yhteys ja oikeat operaattoriyhteydet eivät olleet käytössä.

Projektin tulokset osoittavat, että SD-WAN-teknologia tarjoaa merkittäviä etuja perinteisiin WAN-verkkoihin verrattuna, erityisesti keskitetyn hallinnan, dynaamisen reitityksen ja kustannustehokkaiden yhteyksien osalta. Fortinet Fortigate 40F -palomuuri osoittautui tehokkaaksi työkaluksi SD-WAN-toiminnan toteuttamiseen ja sen hallintapaneeli tarjoaa yksinkertaisen käyttöliittymän verkon seurantaan ja hallintaan.

Verkon testauksessa käytetyt PING-testit vahvistavat, että kaikki konfiguroidut yhteydet, kuten lähiverkot, VLAN-verkot ja tunnelit, toimivat odotetulla tavalla. Lisäksi palomuurisäännöt ja SD-WAN-säännöt osoittavat, että verkon liikennettä voidaan hallita ja suojata tehokkaasti.

Jatkotoimenpiteinä olisi suositeltavaa testata SD-WAN-ratkaisua todellisessa tuotantoympäristössä. Tämä mahdollistaisi paremman ymmärryksen siitä, miten SD-WAN toimii käytännössä erilaisissa verkko-olosuhteissa ja kuormitustilanteissa.

Projekti onnistui pääosin hyvin. SD-WAN tarjosi hyödyllisiä ominaisuuksia, jotka auttavat organisaatioita laajentamaan etäyhteyksiä ja hyödyntämään pilvipalveluita entistä tehokkaammin.

LÄHTEET

Ali, H. (2023). What Is DHCP? A Simple Guide To Understanding IP Address Assignment. Noudettu 8.12.2024 osoitteesta https://fiberroad.com/resources/glossary/what-is-dhcp/

Fortinet. (2024). What Is Border Gateway Protocol (BGP)? Noudettu 8.12.2024 osoitteesta https://www.fortinet.com/resources/cyberglossary/bgp-border-gateway-protocol

Fortinet. (2025). Lowest cost (SLA) strategy. Noudettu 2.4.2025 osoitteesta https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/342836/lowest-cost-sla-strategy

Fortinet. (2025). Virtual Domains. Noudettu 8.3.2025 osoitteesta https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/109991

GeeksforGeeks. (2023). Difference between WAN and WWAN. Noudettu 30.12.2024 osoitteesta https://www.geeksforgeeks.org/difference-between-wan-and-wwan/

Hasna, A. (2024). What Is DNS: A Comprehensive Guide to How It Works. Noudettu 8.12.2024 osoitteesta https://www.hostinger.in/tutorials/what-is-dns

Kanade, V. (2022). What Is a Firewall? Definition, Key Components, and Best Practices. Noudettu 9.1.2025 osoitteesta https://www.spiceworks.com/it-security/network-security/articles/what-is-firewall-definition-key-components-best-practices/

Palo Alto Networks. (2025). What Is SD-WAN? Noudettu 5.2.2025 osoitteesta https://www.paloaltonetworks.com/cyberpedia/what-is-sd-wan

Spiceworks. (10. 3 2025). What Is Network Time Protocol (NTP)? Meaning, Working, Benefits, and Challenges. Noudettu 10.3.2025 osoitteesta https://www.spiceworks.com/tech/networking/articles/what-is-network-time-protocol/

Yelland, H. (2024). What is SD-WAN? (2024 Revision). Noudettu 17.1.2025 osoitteesta https://www.netify.com/learning/what-is-sd-wan/

Youyuan, X. (2024). What Is IPsec? Noudettu 20.12.2024 osoitteesta https://info.support.huawei.com/info-finder/encyclopedia/en/IPsec.html

LIITTEET

LIITE 1. SD-WAN-konfigurointipohja.

```
Loopback verkko: 172.16.14.0/24
Overlay verkko operaattori1: 172.16.16.0/24
Overlay verkko operaattori2: 172.16.18.0/24
Työasemaverkko: 192.168.128.0/17
Tulostinverkko: 192.168.64.0/18
Hallintaverkko: 192.168.0.0/18

Loopback: 172.16.14.10/32
Overlay operaattori1: 172.16.16.10/32
Overlay operaattori2: 172.16.18.10/32
Työasemaverkko: 192.168.128.0/24
Tulostinverkko: 192.168.64.0/28
Hallintaverkko: 192.168.2.0/28

Laitteen nimi           SD-WAN-Labra
Loopback IP             172.16.14.10 255.255.255.255
Overlay Operaattori1    172.16.16.10 255.255.255.255
Overlay Operaattori2    172.16.18.10 255.255.255.255
Työasemaverkko          192.168.128.0 255.255.255.0
Työasemaverkon GW       192.168.128.1 255.255.255.0
Työasemaverkon nimi     tyoasemaverkko
Tulostinverkko          192.168.64.0 255.255.255.240
Tulostinverkon GW       192.168.64.1 255.255.255.240
Tulostinverkon nimi     tulostinverkko
Hallintaverkon GW       192.168.2.1 255.255.255.240

config system virtual-switch
    edit "lan"
        config port
            delete lan3
    end
end
config system global
    set admintimeout 30
    set alias "SD-WAN-Labra"
    set hostname "SD-WAN-Labra"
end
config system lte-modem
    set status enable
end
```

```
config system interface
    edit "wan"
        set vdom "root"
        set mode dhcp
        set allowaccess ping
        set role wan
        set defaultgw disable
        set dns-server-override disable
    next
    edit "lan3"
        set vdom "root"
        set mode dhcp
        set allowaccess ping
        set alias "wan2"
        set role wan
        set defaultgw disable
        set dns-server-override disable
    next
    edit "wwan"
        set vdom "root"
        set mode dhcp
        set allowaccess ping
        set type physical
        set role wan
        set defaultgw disable
        set dns-server-override disable
    next
    edit "loopback_sdwan"
        set vdom "root"
        set ip 172.16.14.10 255.255.255.255
        set allowaccess ping https ssh
        set type loopback
    next
end
config system dns
    set primary 8.8.8.8
    set secondary 8.8.4.4
end
```

```
config vpn ipsec phase1-interface
    edit "operaattori1"
        set interface "lan3"
        set ike-version 2
        set peertype any
        set net-device disable
        set exchange-interface-ip enable
        set proposal aes256-sha256
        set localid "SD-WAN-Labra"
        set dpd on-idle
        set npu-offload disable
        set dhgrp 5
        set nattraversal forced
        set network-overlay enable
        set network-id 222
        set remote-gw 172.16.20.1
        set psksecret 0C3GME0WDE9FMD85COVAWITGHPZIOUU
    next
    edit "operaattori2"
        set interface "wwan"
        set ike-version 2
        set peertype any
        set net-device disable
        set exchange-interface-ip enable
        set proposal aes256-sha256
        set dpd on-idle
        set localid "SD-WAN-Labra"
        set npu-offload disable
        set dhgrp 5
        set network-overlay enable
        set network-id 233
        set remote-gw 172.16.22.1
        set psksecret 11BMDPDENS2ADASNZSBTT0TBDGC3JI1
    next
end
config vpn ipsec phase2-interface
    edit "operaattori1_p2"
        set phase1name "operaattori1"
        set proposal aes256-sha256
        set pfs disable
        set replay disable
        set auto-negotiate enable
    next
    edit "operaattori2_p2"
        set phase1name "operaattori2"
        set proposal aes256-sha256
        set pfs disable
        set replay disable
        set auto-negotiate enable
    next
end
```

```
config system interface
    edit "operaattori2"
        set vdom "root"
        set ip 172.16.18.10 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 172.16.18.1 255.255.255.255
        set interface "wwan"
    next
    edit "operaattori1"
        set vdom "root"
        set ip 172.16.16.10 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 172.16.16.1 255.255.255.255
        set interface "lan3"
    next
end
config firewall address
    edit "tyoasemaverkko"
        set associated-interface "lan"
        set subnet 192.168.128.0 255.255.255.0
    next
    edit "speedtest.net"
        set subnet 151.101.2.219 255.255.255.255
    next
        edit "google.fi"
        set subnet 216.58.211.227 255.255.255.255
    next
end
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
        edit "overlay"
        next
        edit "inet-underlay"
        next
    end
    config members
        edit 1
            set interface "operaattori1"
            set zone "overlay"
        next
        edit 2
            set interface "operaattori2"
            set zone "overlay"
            set cost 10
        next
        edit 4
```

```
            set interface "wwan"
            set zone "inet-underlay"
            set cost 10
    end
config health-check
        edit "google"
            set server "google.fi"
            set protocol http
            set update-static-route disable
            set members 2 1
            config sla
                edit 1
                    set latency-threshold 80
                    set jitter-threshold 10
                    set packetloss-threshold 2
                next
            end
        next
        edit "speedtest"
            set server "speedtest.net"
            set recoverytime 20
            set update-static-route disable
            set members 2 1
            config sla
                edit 1
                    set latency-threshold 40
                    set jitter-threshold 10
                    set packetloss-threshold 2
                next
            end
        next
    end
    config service
        edit 1
            set name "speedtest"
            set load-balance enable
            set dst "speedtest.net"
            set src "tyoasemaverkko"
            config sla
                edit "speedtest"
                    set id 1
                next
            end
            set priority-members 1 2
        next
    end
end
```

```
config router prefix-list
    edit "SDBRANCH-LAN"
        config rule
            edit 10
                set prefix 192.168.0.0 255.255.0.0
                unset ge
                set le 32
            next
        end
    next
    edit "DEFAULT-ROUTE"
        config rule
            edit 1
                set prefix 0.0.0.0 0.0.0.0
                unset ge
                unset le
            next
        end
    next
end
config router community-list
    edit "PRIVATE"
        config rule
            edit 1
                set action permit
                set match "64555:4500"
            next
        end
    next
    edit "DEFAULT-ROUTE"
        config rule
            edit 1
                set action permit
                set match "64555:5500"
            next
        end
    next
end
config router route-map
    edit "REDISTRIBUTE-CONNECTED"
        config rule
            edit 5
                set action deny
                set match-interface "lan3"
            next
            edit 6
                set action deny
                set match-interface "wan"
            next
            edit 7
                set action deny
```

```
                set match-interface "wwan"
            next
            edit 10
                set match-ip-address "SDBRANCH-LAN"
            next
        end
    next
    edit "SDBRANCH_OUT"
        config rule
            edit 1
                set match-ip-address "SDBRANCH-LAN"
                set set-community "64555:3500"
            next
        end
    next
    edit "SDBRANCH_IN"
        config rule
            edit 1
                set match-ip-address "DEFAULT-ROUTE"
                set set-route-tag 5500
            next
            edit 2
                set match-community "PRIVATE"
                set set-route-tag 4500
            next
        end
    next
end
config router static
    edit 1
        set dst 172.16.20.1 255.255.255.255
        set device "lan3"
    next
    edit 2
        set dst 172.16.22.1 255.255.255.255
        set gateway 192.168.0.1
        set device "wwan"
    next
end
```

```
config router bgp
    set as 64999
    set router-id 172.16.14.10
    set bestpath-as-path-ignore enable
    set ebgp-multipath enable
    config neighbor
        edit "172.16.16.1"
            set advertisement-interval 1
            set link-down-failover enable
            set soft-reconfiguration enable
            set remote-as 65200
            set route-map-in "SDBRANCH_IN"
            set route-map-out "SDBRANCH_OUT"
            set keep-alive-timer 3
            set holdtime-timer 9
        next
        edit "172.16.18.1"
            set advertisement-interval 1
            set link-down-failover enable
            set soft-reconfiguration enable
            set remote-as 65200
            set route-map-in "SDBRANCH_IN"
            set route-map-out "SDBRANCH_OUT"
            set keep-alive-timer 3
            set holdtime-timer 9
        next
    end
    config redistribute "connected"
        set status enable
        set route-map "REDISTRIBUTE-CONNECTED"
    end
end
config system interface
    edit "lan"
        set vdom "root"
        set ip 192.168.2.1 255.255.255.240
        set allowaccess ping https ssh fgfm fabric
        set type hard-switch
        set stp enable
        set device-identification enable
        set role lan
        set interface "lan"
        set dhcp-relay-ip "172.16.145.6"
    next
```

```
    edit "tyoasema"
        set vdom "root"
        set dhcp-relay-service enable
        set ip 192.168.128.1 255.255.255.0
        set allowaccess ping fgfm fabric
        set stp enable
        set device-identification enable
        set role lan
        set interface "lan"
        set dhcp-relay-ip "172.16.145.6"
        set vlanid 100
    next
    edit "tulostin"
        set vdom "root"
        set ip 192.168.64.1 255.255.255.240
        set allowaccess ping
        set device-identification enable
        set role lan
        set interface "lan"
        set vlanid 200
    next
end
config firewall address
    edit "tulostinverkko"
        set associated-interface "lan"
        set subnet 192.168.64.0 255.255.255.240
    next
    edit "speedtest.net"
        set subnet 151.101.2.219 255.255.255.255
    next
    edit "private-192.168.net"
        set subnet 192.168.0.0 255.255.0.0
    next
    edit "mokkula"
        set subnet 192.168.0.1 255.255.255.255
    next
end
config firewall policy
    edit 1
        set name "local to private"
        set srcintf "lan"
        set dstintf "overlay"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        unset nat
    next
    edit 2
        set name "private to local"
```

```
        set srcintf "overlay"
        set dstintf "lan"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
    edit 3
        set name "local-to-mokkula"
        set srcintf "lan"
        set dstintf "inet-underlay"
        set action accept
        set srcaddr "all"
        set dstaddr "mokkula"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
    edit 4
        set name "tulostin-in"
        set srcintf "overlay"
        set dstintf "tulostin"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
    edit 5
        set name "tulostin-out"
        set srcintf "tulostin"
        set dstintf "overlay"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
    edit 6
        set name "tyoasema-in"
        set srcintf "overlay"
        set dstintf "tyoasema"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
```

```
        set logtraffic all
    next
    edit 7
        set name "tyoasema-out"
        set srcintf "tyoasema"
        set dstintf "overlay"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
    edit 8
        set name "hallinta-to-tulostimet"
        set srcintf "lan"
        set dstintf "tulostin"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL_ICMP"
        set logtraffic all
    next
    edit 9
        set name "hallinta-to-tyoasema"
        set srcintf "lan"
        set dstintf "tyoasema"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "PING"
        set logtraffic all
    next
end
```

```
config system dhcp server
    edit 1
        set default-gateway 192.168.2.1
        set netmask 255.255.255.240
        set interface "lan"
        config ip-range
            edit 1
                set start-ip 192.168.2.5
                set end-ip 192.168.2.6
            next
        end
        set dns-service specify
        set dns-server1 8.8.4.4
        set dns-server2 8.8.8.8
        set ntp-server1 195.148.70.12
        set ntp-server2 87.92.36.252
    next
end
```