

## **Lähiverkon optimointi avoimen lähdekoodin laitteilla**



Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutus

kevät, 2022

Tuukka Haapakoski

Tietojenkäsittelyn koulutus

Tekijä Tuukka Haapakoski

Työn nimi Lähiverkon optimointi avoimen lähdekoodin laitteilla

Ohjaaja Ismo Turve

Tiivistelmä

Vuosi 2022

---

## TIIVISTELMÄ

Opinnäytetyön tarkoituksena oli luoda turvallinen koko asunnon kattava langaton lähiverkko yksityishenkilön käyttöön. Lähiverkko toteutettiin hyödyntämällä 5G-yhteyttä, jonka sijainnin optimoinnilla saatiin vakautta verkon toimintaan. Lisäksi työn tarkoituksena oli muodostaa yksityishenkilön käyttöön tietoturvallinen verkkoympäristö, jonka avulla voidaan suojautua verkon uhilta.

Opinnäytetyössä käytettiin hyödyksi avoimen lähdekoodin ohjelmistoja reitittimen ja wlan-tukiasemien osalta. Reitittimeen asennettiin pfSense-käyttöjärjestelmä ja wlan-tukiasemaan OpenWrt-käyttöjärjestelmä. Tietoturvan osalta pfSense-järjestelmään asennettiin tunkeutumisenestojärjestelmä Snort, jonka lisäksi otettiin käyttöön salattu DNS-yhteys.

Opinnäytetyössä tutkittiin, mitä hyötyä on avoimen lähdekoodin ohjelmistostoista sekä miten nämä parantavat tietoturvaa. Lisäksi kartoitettiin, miten tehdään koko asunnon kattava wlan-verkko. Verkon toiminnallisen toteuttamisen kautta saatiin tulokseksi, että paras tapa toteuttaa kattava langaton lähiverkko on käyttää useampaa tukiasemaa. Näin wlan-verkon kantama ja nopeus kasvavat. Työn tulosten pohjalta voidaan tulevaisuudessa tutkia, miten Wi-Fi 6 vaikuttaa langattoman verkon nopeuteen ja verkon kattavuuteen.

Avainsanat Lähiverkko, 5G, avoin lähdekoodi, tietoturva, tukiasemat

Sivut 57 sivua ja liitteitä 1 sivua

Degree Programme in Business Information Technology

Author Tuukka Haapakoski

Subject Local network optimization with open source devices

Supervisors Ismo Turve

Abstract

Year 2022

---

## ABSTRACT

The aim of the thesis was to implement a secure apartment-wide wireless local area network for private use. The network was implemented by utilizing a 5G base station and the position of the base station was optimized in order to ensure the stable operation of the network. The network was also secured against network attacks. The network was secured by installing open-source software pfSense and OpenWrt to the router and the wlan base station respectively. In addition, the router was configured with the intrusion prevention system Snort and encrypted DNS connection.

The research questions of this thesis were the benefits of using open-source software alongside their effectiveness in providing network security. Optimal usage and placement of the wlan stations for covering the entire apartment were also investigated. It was concluded that the best way to implement an apartment-wide network is to use several base stations, increasing the network's range and speed.

This thesis can be developed further by researching how Wi-Fi 6 affects the speed and coverage of the network.

Keywords Local area network, 5G, open source, information security, base station

Pages 57 pages and appendices 1 pages

## Sanasto

5G	Viidennen sukupolven tiedonsiirtoprotokolla
DNS	Domain Name Server (nimipalvelujärjestelmä)
IOT	Internet of Things (esineiden internet)
DOT	Dns over TLS (TLS salatut DNS kyselyt)
WLAN	Wireless local arena network (langaton lähiverkko)
DHCP	Dynamic Host Configuration Protocol (jakaa IP-osoitteet)
VLAN	Virtual LAN (virtuaalinen verkko)
IDS	Intrusion Detection System (tunkeutumisen havaitsemin järjestelmä)
IPS	Intrusion Prevention System (tunkeutumisen estojärjestelmä)

## Sisällys

1	Johdanto .....	1
2	Turvallinen kotiverkko .....	2
2.1	5G .....	3
2.2	Saunalahti mobiililaajakaista 5G .....	3
2.3	DNS & DOT .....	4
2.4	Tunkeutumisen estojärjestelmä .....	5
2.5	Wi-Fi 5 (802.11ac) .....	6
2.6	Fast BSS Transition (802.11r) .....	7
3	Järjestelmät ja laitteet .....	8
3.1	pfSense .....	8
3.2	OpenWrt .....	9
3.3	Rufus .....	9
3.4	Putty .....	9
3.5	Huawei 5G CPE Pro 2 -reititin .....	10
3.6	APU4D4-järjestelmäpiiri .....	11
3.7	TP-link Archer C6 -reititin .....	12
4	Toteutus .....	13
4.1	Huawei 5G CPE Pro 2 -reitittimen määrytykset .....	13
4.1.1	Julkisen IP-osoitteen asettaminen .....	13
4.1.2	Siltatila .....	15
4.2	pfSense-palomuurin asennus ja määrytykset .....	16
4.2.1	DHCP .....	27
4.2.2	DOT & DNS resolver .....	28
4.2.3	Snort (IDS/IPS protection) .....	31
4.2.4	UPnP .....	38
4.2.5	pfSense ongelmia .....	39
4.3	OpenWrt-ohjelmiston asennus .....	41
5	Johtopäätökset ja pohdinta .....	51
5.1	Verkkotopologia .....	51
5.2	Mittaustulokset .....	52
5.3	Hinnat .....	52
5.4	NMAP-porttiskannaus .....	53
5.5	Snort testaus ja pohdinta .....	54

6 Yhteenveto .....	56
Lähteet.....	58

## Kuvat, ohjelmakoodit ja taulukot

Kuva 1 Suojaamaton DNS (Cloudflare, 2022) .....	5
Kuva 2 Huawei 5G CPE Pro2 (Elisa, 2022a).....	10
Kuva 3 Lähin tukiasema (CellMapper, 2022) .....	11
Kuva 4 APU4D4-järjestelmäpiiri .....	12
Kuva 5 Huawei hallintasivu .....	13
Kuva 6 Huawei profiiliasetukset .....	14
Kuva 7 Huawei profiilit .....	14
Kuva 8 Myip.fi (Myip.fi, n.d.) .....	15
Kuva 9 Huawei Wi-Fi perusasetukset .....	15
Kuva 10 Huawei siltatila .....	16
Kuva 11 Komentokehote,” ipconfig” .....	16
Kuva 12 pfSense asennusmedian lataus .....	17
Kuva 13 Rufus-osiointityökalu .....	18
Kuva 14 PuTTY Configuration .....	18
Kuva 15 Asennusmedia ja sarjaliikennekaapeli kiinnitettynä reitittimeen .....	19
Kuva 16 Sarjaliikennekaapeli ja USB-DB9 adapteri .....	19
Kuva 17 Windows-laitehallinta.....	20
Kuva 18 Select boot device.....	20
Kuva 19 Console Type.....	21
Kuva 20 Käyttöehdot .....	21
Kuva 21 Kielen valinta.....	22
Kuva 22 Osiointi .....	22
Kuva 23 Levyaseman tyyppi .....	23
Kuva 24 Looginen asema .....	23
Kuva 25 Valmiit asetukset .....	24
Kuva 26 Asennus käynnissä .....	24
Kuva 27 Asennus valmis .....	25

Kuva 28 pfSense ensimmäinen käynnistys.....	25
Kuva 29 IP-asetukset .....	26
Kuva 30 pfSense kirjautuminen.....	27
Kuva 31 pfSense DHCP server .....	28
Kuva 32 pfSense DNS-asetukset.....	29
Kuva 33 Enable DNS resolver.....	29
Kuva 34 DNS Resolver.....	30
Kuva 35 Diagnostics - States.....	30
Kuva 36 Package Manager.....	31
Kuva 37 Package Installer .....	31
Kuva 38 Package Installer Progress .....	32
Kuva 39 Snort Oinkcode .....	32
Kuva 40 Snort Global Settings .....	33
Kuva 41 Snort Global Settings 2 .....	33
Kuva 42 Snort Updates .....	34
Kuva 43 Rules Update Task.....	34
Kuva 44 Rule Update Task Success.....	34
Kuva 45 Snort Interface .....	35
Kuva 46 Wan - Interface Settings .....	35
Kuva 47 WAN - Interface Settings 2 .....	36
Kuva 48 Interface luotuna .....	36
Kuva 49 Settings - WAN Categories.....	37
Kuva 50 Block Settings.....	37
Kuva 51 WAN Preprocs.....	38
Kuva 52 UPnP.....	39
Kuva 53 Gateways .....	40
Kuva 54 Gateways Edit .....	40
Kuva 55 User Forced Disabled Rules .....	40
Kuva 56 Ipconfig .....	41
Kuva 57 TP-Link kirjautuminen .....	42
Kuva 58 TP-Link salasanan vaihto.....	42
Kuva 59 TP-Link Quick Setup .....	42

Kuva 60 TP-Link Advanced.....	43
Kuva 61 Firmware Upgrade .....	43
Kuva 62 OpenWrt kirjautuminen.....	44
Kuva 63 OpenWrt etusivu.....	44
Kuva 64 OpenWrt ajan asettaminen .....	45
Kuva 65 OpenWrt interfaces .....	45
Kuva 66 Staattinen osoite.....	46
Kuva 67 OpenWrt custom dns.....	46
Kuva 68 OpenWrt Firewall Settings.....	47
Kuva 69 OpenWrt DHCP .....	47
Kuva 70 Interfaces-määrittäminen valmis.....	47
Kuva 71 Wireless Overview .....	48
Kuva 72 General Setup .....	49
Kuva 73 Interface Configuration.....	50
Kuva 74 Interface Advanced Settings .....	50
Kuva 75 Lähiverkon dokumentaatio.....	51
Kuva 76 Mittaustulokset.....	52
Kuva 77 NMAP .....	53
Kuva 78 ICMP-sääntö.....	55
Kuva 79 Snort Alerts .....	55
 Taulukko 1 laitteiston hinnat.....	 52

## Liitteet

Liite 1	Aineistonhallintasuunnitelma
---------	------------------------------



## 1 Johdanto

Opinnäytetyön idea syntyi tarpeesta toteuttaa tietoturallinen lähiverkko kotiin ottamalla huomioon nykyajan vaatimukset. Nykypäivänä yhä useammat laitteet tarvitsevat langattoman pääsyn internettiin, esimerkiksi älyvalot, -kellot, -jääkaapit jne. Tämä asettaa myös haasteita niin langattoman verkon rakentamiselle kuin tietoturvalle. Opinnäytetyössä käsitellään, kuinka rakennetaan kattava langaton lähiverkko omakotitaloon. Verkkolaitteiden valinnassa pyritään käyttämään avoimen lähdekoodin ohjelmistoja tukevia laitteita, jolloin laitteen koko elinkaari saadaan pidemmäksi tietoturva- ja järjestelmäpäivitysten osalta. Näin ollen myös toimintavarmuus ja vikasietoisuus laitteissa paranee.

Opinnäytetyö pyrkii vastaamaan seuraaviin tutkimuskysymyksiin:

- 1) Mitä hyötyä on avoimen lähdekoodin ohjelmistoista ja miten nämä parantavat tietoturvaa?
- 2) Miten tehdään koko asunnon kattava langaton lähiverkko?

Hyvä lähiverkko yksinomaan ei takaa vielä hyvää käytettävyyttä, sillä näiden lisäksi tarvitaan vakaa ja nopea internetyhteys. Opinnäytetyössä oleva kiinteistö sijaitsee taajamassa, eikä sinne aikaisemmin ole ollut tarjolla kuin hidas ADSL-yhteys tai ilta-aikaan ruuhkainen 4G-yhteys. Tekniikan kehittyttyä tarjolle on tullut 5G-verkko, jota hyödynnetään opinnäytetyössä. Lisäksi opinnäytetyö pyrkii tarjoamaan tietoa, kuinka 5G-reititin asennetaan optimaaliseen sijaintiin ja miten reitittimestä otetaan kaikki palvelut käyttöön, kuten julkinen IP-osoite.

Opinnäytetyön loppuosuudessa kuvannetaan tilanne ennen ja jälkeen sekä esitellään mittaustulokset lähiverkon ja internetyhteyden osalta. Lähiverkon tietoturva painottuu opinnäytetyössä pfSense-ohjelmistoon. Opinnäytetyössä rakennetaan pfSense-reititin, johon asennetaan tietoturvaa parantavia lisäominaisuuksia, kuten tunkeutumisen estojärjestelmä (IPS).

## 2 Turvallinen kotiverkko

Kotiverkko pitää sisällään laajan kirjon kaikista kodin laitteista, kuten tietokoneet, puhelimet, tabletit ja tulostimet. Se jakautuu yleensä langalliseen kiinteään verkkoon ja langattomaan verkkoon. Riippuen käytettävästä verkosta ja laitteesta asettaa se erilaisia haasteita loppukäyttäjälle. Hakkerit voivat käyttää hyökkäyksiin haavoittuvia laitteita, joiden tietoturva ei ole ajan tasalla. Yleisimpiä riskejä ovat erilaiset haittaohjelmat, henkilötietojen ja datan varastaminen tai kodin verkkolaitteen, esimerkiksi reitittimen liittäminen osaksi bottiverkkoa. (Kaspersky Lab, n.d.)

Verkkorikollisilta suojautumisen peruslähtökohtana on riittävän turvallisen modeemin tai reitittimen valinta. Verkkouhkien kehittyessä kehittyvät myös verkkolaitteet ja niiden ominaisuudet. Mikäli käyttäjällä on käytössään vuosia vanha laite, tulisi käyttäjän harkita laitteen päivittämistä uuteen. (Malmelin, 2021) Uusikaan verkkolaite ei vielä pelasta uhilta, sillä käyttäjän tulisi vielä huolehtia päivityksen ajantasaisuudesta säännöllisesti. Tietoturvaa voidaan parantaa entisestään vaihtamalla verkkolaitteen oletus-IP-osoite ja salasana sekä kytkeä laitteen palomuri päälle. Lisäksi modeemin tai reitittimen etäkäyttöasetus kannattaa sammuttaa. (Kaspersky Lab, n.d.)

Kotiverkkoon liitettävien laitteiden määrä kasvaa tulevaisuudessa, sillä yhä useampi laite tarvitsee toimiakseen internetyhteyttä esimerkiksi älykaiuttimet (Amazon Echo ja Google Home), älykellot ja -jääkapit. Näistä muista verkon fyysisistä laitteista käytetään nimeä IoT, eli Internet of Things. IoT-esineet vaikuttavat merkittävästi verkon tietoturvaan, sillä mitä useampi laite on internetissä, tarjoaa se hakkereille uusia mahdollisuuksia hyväksikäyttää haavoittuvuuksia. Myöskään kaikki IoT-laitteet eivät täytä turvallisuusvaatimuksia ja ohjelmistojen päivityselinkaari on lyhyt. Käyttäjä voi parantaa tietoturvaa jakamalla kotiverkkonsa virtuaaliverkkoihin, eli vlaneihin. Verkon osioimisella pyritään pitämään IoT-laitteet omassa yksityisessä verkossaan, jolloin niillä ei ole yhteyttä kodin muihin laitteisiin, esimerkiksi tietokoneisiin. (Kaspersky Lab, n.d.)

Langattoman wlan-verkon suojaamiseen liittyy myös omat haasteensa. Wlan-verkon nimi ja oletussalasana kannattaa vaihtaa alkuperäisistä. Nykyaikaisten suositusten mukaan hyvässä salasanassa on vähintään 12 merkkiä tai enemmän. Mikäli hakkerilla on tiedossaan wlan-

reittimen malli, voidaan oletussalasana arvata nopeasti ja kotiverkko altistuu hyökkäykselle. Wlan-verkon salaus tulisi olla vähintään WPA2 tasolla. Vanhemmat WPA ja WEP suojaustasot ovat alttiita salasanan arvaukselle ns. ”Brute Force”-tekniikalla, jossa hakkeri arvaa salasanan tietokoneohjelmalla. (Kaspersky Lab, n.d.) Uudemmatkaan suojausmenetelmät eivät korvaa hyvää salausavainta, tästä esimerkkinä sanakirjahyökkäys. Sanakirjahyökkäyksessä hakkeri käyttää ennalta määrättyä sanakirjaa, joka sisältää erilaisia ennalta määriteltäviä mahdollisia salasanoja, joiden toimivuutta testataan verkon murtamiseksi. (Delgado, 2017) Wlan-reitittimen mac-suodatus on myös hyvä keino rajoittaa langattoman verkon laitteita. Mac-suodatusta käyttämällä vain tietyn mac-osoitteen omaavat laitteet saavat liikennöidä internettiin. Vierailijoita varten tulisi luoda oma Guest-verkko (vierailijaverkko), jolloin vierailijoiden laitteilla ei ole suoraa pääsyä kodin verkkolaitteisiin. Syynä Guest-verkon luomiseen ei ole niinkään vierailijoiden epärehelliset aiheet, vaan heidän käyttämänsä laitteisto, jossa voi olla viruksia tai muita haittaohjelmia. Tietoturvaa voidaan parantaa vielä hieman sammuttamalla kodin wlan-verkko, kun käyttäjä ei ole itse paikalla. Näin pienennetään hakkerin toiminta-aikaa verkkohyökkäystä valmisteltaessa. (Kaspersky Lab, n.d.)

## 2.1 5G

5G on nimensä mukaisesti viidennen sukupolven tiedonsiirtoprotokolla. Ensimmäinen 1G yhteys esiteltiin vuonna 1980 ja se tarjosi väylän siirtää analogista ääntä. 1990-luvulla esiteltiin 2G, jossa siirrettiin jo digitaalista ääntä. 3G saapui 2000-luvun alussa mahdollistaen jouhevan tavan siirtää mobiilidataa verkossa. 2010-luvulla saapui 4G ja kansan kielessä ”mokkulat”, jotka aloittivat mobiililaajakaistojen täysin uuden aikakauden. (Qualcomm Technologies, 2022)

## 2.2 Saunalahti mobiililaajakaista 5G

Tässä työssä käytettäväksi palveluntarjoajaksi valikoitui Elisa johtuen tukiaseman maantieteellisestä sijainnista asuinkiinteistöön nähden. Käyttäjäprofiloinnin jälkeen päädyin Saunalahti 5G mobiililaajakaistaliittymään, jonka teoreettinen maksiminopeus on 300Mbps.

Operaattori ilmoittaa yhteyden vaihteluväliksi 5G verkossa 10-300Mbps ja 4G-verkossa 5-300Mbps. (Elisa, 2022c)

Elisan mobiililiittymissä käytetään pääsääntöisesti NAT-osoitteenmuutosta IPv4-osoitteille, mikä johtuu IPv4-osoitteiden vähydestä. Tämä tarkoittaa, että tietyt palvelut toimivat heikosti. Syynä on, että portteja ei voida avata verkkoliikenteelle, joita käyttävät esimerkiksi riistakamerat tai verkkopelit. (Elisa, 2022b) Ostettaessa mobiililaajakaistaa näihin ominaisuuksiin on kiinnitettävä erityisiä huomioita, mikäli yhteyttä käytetään normaalin kiinteän yhteyden tavoin talouden ainoana liittymänä. Elisan mobiililiittymiin on mahdollista saada julkinen IP-osoite, jolloin mobiililiittymään saadaan kaikki samat palvelut käyttöön kuin kiinteässä verkossa. Julkinen IP-osoite on saatavilla kaikille Elisan mobiililaajakaistaliittymille. Julkisen IP-osoitteen voi aktivoida omaelisasta. (Elisa, 2022b)

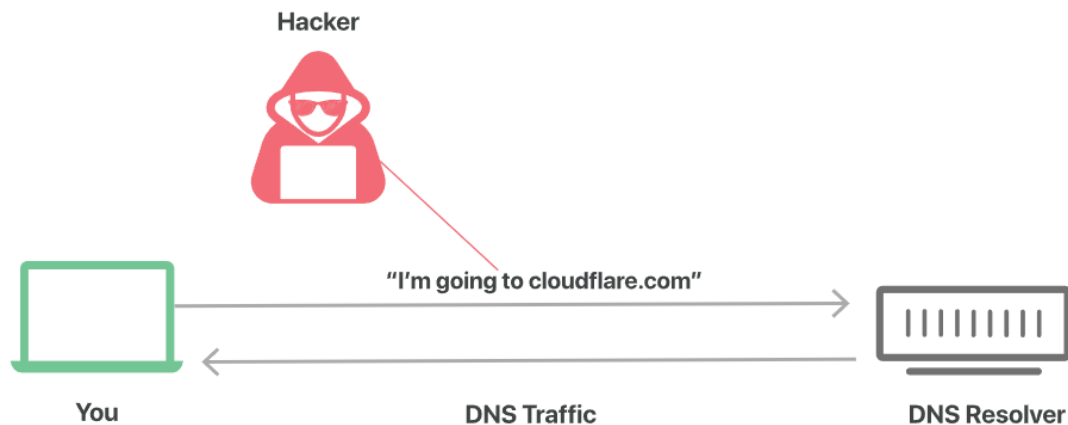
Tietoturvan näkökulmasta julkista IP-osoitetta käytettäessä on panostettava tietoturvaan. Julkinen IP-osoite mahdollistaa yhteydet avaamisen internetin suunnassa (sisäänpäin), joten on tärkeä huolehtia tietoturvapalveluiden ajantasaisuudesta sekä vaihdettava verkkolaitteiden oletussalasanat. (Elisa, 2022b)

## 2.3 DNS & DOT

DNS lyhenne muodostuu sanoista Domain Name System. DNS-palvelua voidaan pitää internetin puhelinluettelona, joka pitää sisällään listauksen sivustojen nimistä esimerkiksi [www.google.fi](http://www.google.fi). DNS-Resolver -palvelinten ansiosta käyttäjän ei tarvitse tietää sivuston fyysistä IP-osoitetta, sillä heidät ohjataan nimikyselyn perusteella oikealle sivustolle.

DNS over TLS (DOT) protokollalla DNS-kyselyt salataan päätelaitteelta DNS-palveluntarjoajalle. Tämä parantaa tietoturvaa käyttäjän näkökulmasta luoden ylimääräisen kerroksen turvallisuuteen. Yleensä normaalit DNS kyselyt lähetetään selkokielenä sanomana, jolloin operaattori tai kuka tahansa pystyy seuraamaan liikennettä. Asia havainnollistettuna kuvassa 1.

Kuva 1 Suojaamaton DNS (Cloudflare, 2022)



Euroopan unioni on myös havahtunut, miten merkittävä asia DNS-palvelu on verkon infrastruktuurin ja yksityisyyden kannalta. Tällä hetkellä DNS-palvelimet ovat keskittyneet pienelle joukolle palveluntarjoajia, jotka toimivat EU:n ulkopuolella. (Brunoli, 2022)

Euroopan komissio on julkaissut virallisen selvityksen DNS4EU-hankkeen aloittamiseksi. DNS4EU tulisi olemaan eurooppalainen DNS-resolver ja suunnattu palvelemaan kaikkia EU:n alueella asuvia käyttäjiä kunnioittaen yksityisyyttä ja tarjoten tietoturvallisen tavan käyttää internetin palveluita. DNS4EU:n keskiössä yksityisyyden lisäksi on myös kyberturvallisuus, joka suojaa käyttäjiä haittaohjelmilta, tietojenkalastelulta sekä muilta uhilta. (Brunoli, 2022)

## 2.4 Tunkeutumisen estojärjestelmä

IPS (Intrusion Prevention System) on verkon tietoturvaauhkien estotekniikka. IPS-järjestelmä monitoroi aktiivisesti verkkoliikennettä paljastaen ja estäen haavoittuvuuksien käyttämisen. IPS-järjestelmä on yleensä sijoitettu heti palomuurin jälkeen, jolloin kaikki liikenne ohjataan sen muodostaman analytiikkakerroksen lävitse. Mikäli järjestelmä havaitsee poikkeavaa liikennettä, ryhtyy se aktiivisesti toimenpiteisiin, jotka voivat olla esimerkiksi haitallisten pakettien pudottaminen pois liikenteestä, liikenteen estäminen kohdeosoitteeseen tai jopa koko yhteyden katkaiseminen. Kaikista poikkeamista ilmoitetaan järjestelmänvalvojalle. IPS-järjestelmää voidaan pitää aktiivisena järjestelmänä verrattuna vanhempaan IDS-järjestelmään (Intrusion Detection System). IDS-järjestelmä toimii passiivisesti tarjoten järjestelmänvalvojalle ilmoituksen epäilyttävästä liikenteestä, mutta järjestelmä ei suorita

ehkäiseviä toimenpiteitä, vaan nämä jäävät järjestelmänvalvojalle. (Palo Alto Networks, 2022)

IPS-järjestelmän havainnointikyky perustuu ennalta määriteltyihin sääntöihin. Nämä säännöt pitävät sisällään tietoja tunnetuista haavoittuvuuksista. Haavoittuvuudella tai haittaohjelmalla on ennalta profiloitu käytösmalli tai digitaalinen allekirjoitus, joiden perusteella järjestelmä osaa etsiä ja reagoida uhkiin. Näiden lisäksi IPS-järjestelmä etsii tilastollisesti poikkeavaa verkkoliikennettä parametrien avulla. Verkon analysointi tapahtuu tunnistamalla verkkoprotokollan epätavallinen käyttäytyminen sen tunnetusta käytösmallista. Esimerkiksi jos verkon perussuorituskyky muuttuu epätavalliseksi, järjestelmä ryhtyy toimenpiteisiin tilanteen palauttamiseksi. (Palo Alto Networks, 2022)

## **2.5 Wi-Fi 5 (802.11ac)**

Wi-Fi järjestelmä käyttää standardia IEEE 802.11, jonka avulla päätelaitteet voivat viestiä langattomissa verkoissa. Standardin on määritellyt Institute of Electrical and Electronics Engineers -järjestö. IEEE 802.11 standardista on useita sukupolvia ja uudistusten myötä tiedonsiirtonopeus ja käytettävissä oleva kaista kasvaa. Ensimmäinen Wi-Fi standardi IEEE 802.11 julkaistiin vuonna 1997. 802.11 standardi sisälsi 2,4Ghz kaistan, jolla saavutettiin 1–2 Mbps:n nopeus. Seuraavat standardit tulivat vuosina: 1999 IEEE 802.11b (Wi-Fi 1), 2003 IEEE 802.11g (Wi-Fi 3), 2009 IEEE 802.11n (Wi-Fi 4) ja vuonna 2013 IEEE 802.11ac (Wi-Fi 5). Tällä hetkellä uusin kaupallinen standardi on IEEE 802.11ax, joka tuotiin markkinoille 2019. (SignalBoosters, 2020)

IEEE 802.11ac standardi mahdollistaa optimaalisissa olosuhteissa jopa 1300Mbps – 2300Mbps tiedonsiirtonopeudet. Todellisuudessa tiedonsiirtonopeuksiin vaikuttavat ympäristötekijät, esimerkiksi seinien rakennusmateriaalit, ovet ja huonekalut. IEEE 802.11ac standardista on olemassa versiot Wave 1 ja Wave 2. Wave 2 toi mahdollisuuden käyttää MU-MIMO (Multi-User Multiple-Input Multiple-Output) -tekniikkaa. MU-MIMO-tekniikalla reititin voi kommunikoida ja lähettää paketteja useammalle laitteelle saman aikaisesti, jolloin verkon viive laskee ja suorituskyky paranee. Aikaisemmassa Wave 1 versioissa käytettiin SU-MIMO (Single-User Multiple-Input Multiple-Output) -tekniikkaa. Tämän takia laitteet

joutuivat jonottamaan paketteja, sillä reititin pystyi kommunikoimaan vain yhden laitteen kanssa kerrallaan.

## **2.6 Fast BSS Transition (802.11r)**

Fast BSS Transition tunnetaan myös nimellä Fast transition (FT). Tämä on protokolla, jonka avulla voidaan lyhentää merkittävästi sitä aikaa, jolloin yhteys katkeaa laitteen ja Wi-Fi-tukiaseman välillä laitteen muodostaessa yhteyttä uuteen tukiasemaan.

Tästä on erityisesti hyötyä käytettäessä suojatussa wlan-verkossa reaaliaikaisia palveluita, kuten Teams-palaveria. 802.11r-standardia käytettäessä päätelaite muodostaa yhteyden uuteen tukiasemaan ”Make before break”-periaatteella eli päätelaite autentikoi yhteyden ennen vanhan yhteyden katkaisua. 802.11r-standardin avulla wlan-tukiaseman vaihto onnistuu ilman häiriötä ja viivettä käytettävään palveluun. Esimerkiksi käyttäjä voi kävellä kiinteistön päästä päähän yhteyden katkeamatta, vaikka käyttäjä matkansa aikana liittyisi useampaan tukiasemaan. Ilman 802.11r-standardia käyttäjä olisi autentikoitava itsensä aina uuden tukiaseman kohdalla uudelleen verkkoon, jolloin myös käytettävässä palvelussa esiintyisi katkos. (Huotari, 2015)

### 3 Järjestelmät ja laitteet

Luvussa 3 käsitellään opinnäytetyössä käytettävät ohjelmistot. Opinnäytetyössä käsitellään vain avoimenlähdekoodin ohjelmistoja, sillä ne ovat ilmaisia ja kaikkien saatavilla kotikäyttöön. Palomuuriohjelmistoksi valikoitui arvostelujen ja aktiivisen käyttäjäkunnan vuoksi pfSense. Kodin langattoman lähiverkon ohjelmistoksi valikoitui OpenWrt, sillä tämä ohjelmisto on mahdollista asentaa useamaan reitittimeen alkuperäisen ohjelmiston päälle. Myös päivitystuki on todella hyvä.

Ohjelmistojen asentamiseen tarvitaan myös avoimen lähdekoodin sovelluksia. Esimerkiksi pfSensen asennus tapahtuu käyttäen sarjaliikenneporttia, jolloin tarvitaan Putty-etähallintatyökalua, jolloin voidaan käyttää sarjaliikenneporttia. Lisäksi asennettavia ohjelmistoja varten tulee luoda asennusmedia USB-muistitikulle. Tätä käyttötarkoitusta varten työssä käytetään Rufus Flash-työkalua. Näiden lisäksi kappaleessa esitellään opinnäytetyössä käytettävä laitteisto.

#### 3.1 pfSense

pfSense on ilmainen palomuri- ja reititinohjelmisto, joka pohjautuu FreeBSD ohjelmistoalustaan. pfSensen hallinta on toteutettu selainpohjaisesti ja ohjelmistossa on paketinhallintajärjestelmä, josta käyttäjä voi ladata sekä ottaa käyttöön laajennuksia pfSense-ohjelmistoon. pfSense-ohjelmisto on avointa lähdekoodia ja käyttää Apache 2.0 Open Source -lisenssiä. (Electric Sheep Fencing, 2022). Apache 2.0 -lisenssillä tarkoitetaan, että käyttäjä voi vapaasti käyttää, muokata, jakaa ja myydä Apache-lisenssillä lisensoituja ohjelmistoja henkilökohtaiseen tai kaupalliseen käyttöön. (Rami, 2021)

pfSense on myös varustettu laajalla kirjolla ominaisuuksia. Sovelluskaupasta voidaan asentaa lukuisia lisäosia esimerkiksi Snort, joka toimii IPS-järjestelmänä. pfSensessä on myös sisäänrakennettu tuki OpenVPN-yhteyksille, jonka avulla voidaan ottaa suojattu VPN-yhteys kotiverkkoon mistäpäin maailmaa tahansa. Verkonhallinnassa pfSense tarjoaa lukemattomia vaihtoehtoja, miten verkko määritellään, kuten esimerkiksi virtuaaliset verkot (vlan) ja aikarajoitukset. pfSensen etuihin voidaan myös laskea, että sen voi asentaa omalle raudalle. Tämä mahdollistaa oikean mitoituksen ostettaessa laitteistoa. Esimerkiksi IPS-järjestelmän ajaminen edellyttää järjestelmältä paljon enemmän kuin normaali palomuurikäyttö. pfSense



tukee myös useampaa WAN-yhteyttä kerrallaan. Tämä mahdollistaa hyvän häiriönhallinnan. Mikäli pääyhteys katkeaa, voidaan siirtyä saumattomasti käyttämään varayhteyttä. pfSensellä on myös suuri keskustelufoorumi, missä käyttäjät jakavat vinkkejä aktiivisesti. (HomeTechHacker, 2018)

### 3.2 OpenWrt

OpenWrt on avoimen lähdekoodin Linux-käyttöjärjestelmä, joka on tarkoitettu sulautettuihin järjestelmiin. OpenWrt:n kehittämisestä vastaa laaja yhteisö kehittäjiä. OpenWrt:n tehtävänä on tarjota vaihtoehtoinen käyttöjärjestelmä laitevalmistajan oman järjestelmän tilalle esimerkiksi wlan-reitittimiin. OpenWrt sisältää laajan pakettihallinnan, jonka avulla käyttöjärjestelmään voidaan asentaa lisäosia. OpenWrt:n käyttäjät uskovat käyttöjärjestelmän olevan vakaampi kuin useimpien laitevalmistajien omat järjestelmät. Lisäksi OpenWrt jatkaa laitteen elinkaarta tarjoten paremman päivitettävyyden kuin useimmat laitevalmistajat. Tämä parantaa myös laitteen tietoturvaa. (Openwrt.org, 2021)

### 3.3 Rufus

Rufus on GPL3-lisensoitu työkalu, joka on suunniteltu boottaavien usb-muistitikkujen luomiseen. Rufusta käytetään silloin, kuin halutaan luoda USB-asennusmedia esimerkiksi Windows- tai Linux-käyttöjärjestelmälle. Rufuksella voidaan myös tehdä boottaava asennusmedia laitteiden firmware tai bios-päivitystä varten. Rufusta itsessään ei tarvitse asentaa laitteistolle, sillä se voidaan suorittaa ladatusta exe-tiedostosta käyttäen järjestelmänvalvojan oikeuksia. Rufus on myös tutkitusti nopeampi, kuin useimmat kilpailijansa. (Batard, 2021)

### 3.4 Putty

PuTTY on etähallintatyökalu, joka tukee SSH-, Telnet-, Rlogin- ja SUPDUP-verkkoprotokollia. Näitä käytetään etäistuntojen suorittamiseen asiakaspäätelaitteelta palvelimelle. Näin ollen PuTTY itsessään ei suorita paikallisesti prosesseja, vaan toteuttaa ainoastaan asiakaspäätteen istunnon palvelimelle. PuTTY käyttää MIT-lisenssiä, jolloin ohjelmistoa

voidaan käyttää vapaasti myös kaupallisiin tarkoituksiin. PuTTyn kehittäjät eivät tosin ota vastuuta, mikäli ohjelma käyttäytyy ei toivotulla tavalla sulautettuna osaksi kaupallista järjestelmää. (Chiark.greenend.org.uk, 2022)

### 3.5 Huawei 5G CPE Pro 2 -reititin

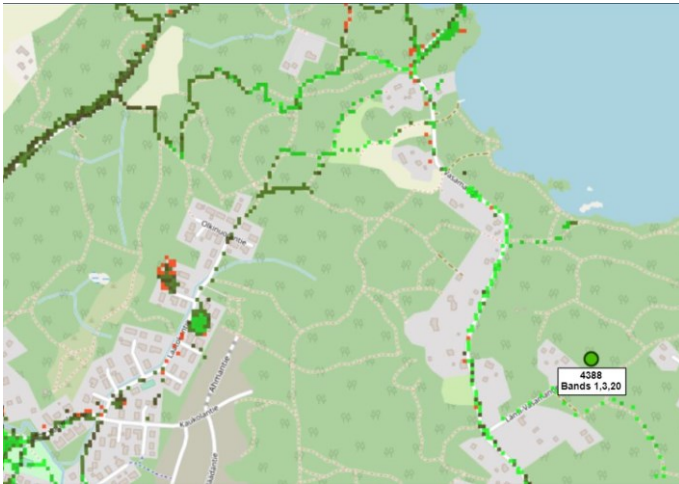
Opinnäytetyössä käytettäväksi 5G-verkkolaitteeksi valikoitui palveluntarjoajan valikoimiin kuuluva Huawei 5G CPE Pro 2 (kuvassa 2). Laite toimii 5G-verkossa saavuttaen parhaimmillaan 3,6Gbps latausnopeuden ja 250Mbps lähetysnopeuden. Lisäksi myös vanhempi 4G-verkko on tuettuna, jossa saavutetaan 1,6Gbps latausnopeus ja 150Mbps lähetysnopeus. Langaton lähiverkkoyhteys on toteutettu uusimmalla Wi-Fi 6 standardilla (Wi-Fi 802.11ax 2x2) ja laitteesta löytyy kaksi kappaletta gigabitin nopeudella varustettua rj45-porttia. (Elisa, 2022a)

Kuva 2 Huawei 5G CPE Pro2 (Elisa, 2022a)



Asennettaessa 5G-sisäyksikköä on asennuspaikkaa mietittävä tarkoin. Laite tulisi ensisijaisesti asentaa avaralle paikalle ikkunan läheisyyteen. (Telia, 2022b) Myös operaattorin tukiaseman sijainti tulisi kartoittaa mahdollisimman tarkasti parhaan verkonviiveen ja laadun varmistamiseksi. Tukiaseman sijaintia voi tiedustella omalta operaattorilta. Saatavilla on myös hyvä palvelu nimeltään Cellmapper, josta voi hakea osoitteella oman operaattorinsa lähimmät tukiasemat. (CellMapper, 2022)

Kuva 3 Lähin tukiasema (CellMapper, 2022)



Kuvassa 3 nähdään lähin tukiasema, joka sijaitsee kiinteistön läntisellä puolella. Tässä tapauksessa 5G-reitittimen sijainniksi valikoitui olohuone, jonka laakeat ikkunat osoittavat länteen. Tämä mahdollistaa esteettömän näkymän tukiasemalle. Huaweiin 5G-reitittimen valot indikoivat vihreällä led-valolla suuntauksen onnistuneen ja signaalin olevan hyvä. (Telia, 2022a)

### 3.6 APU4D4-järjestelmäpiiri

Opinnäytetyössä käytetään pfSensen alustaratkaisuna PC Enginesin Taiwanissa valmistettua APU4D4-järjestelmäpiiriä. Laite on varustettu AMD GX-412TC-prosessorilla ja 4 GB DRAM-keskusmuistilla. Lisäksi laitteesta löytyy paikka mSATA SSD-kiintolevylle, johon asennettiin 16GB:n SSD-kiintolevy. Laitteessa on neljä kappaletta yhden gigabitin verkkoportteja, jotka ovat Intelin valmistamat (i211AT). Näiden lisäksi on sarjaliikenneportti ja kaksi kappaletta USB3-portteja. Laite käyttää 12 v(voltin) tasajännitettä ja toimii 6–12 W (watin) tehoalueella riippuen laitteen kuormituksesta. (PC Engines GmbH, 2022)

Kuvassa 4 nähdään APU4D4-järjestelmäpiiri asennettuna sille erikseen tilattuun koteloon. Kuvassa myös SSD-kiintolevy asentumassa paikoilleen vasemmalla puolella.

Kuva 4 APU4D4-järjestelmäpiiri



### 3.7 TP-link Archer C6 -reititin

Opinnäytetyössä käytettävä langaton lähiverkkoyhteys toteutetaan käyttämällä kahta TP-Link Archer C6 wlan-reititintä.

TP-Link Archer C6 reititin on varustettuna Qualcommn QCA9563 järjestelmäpiirillä, jolla laitteen teoreettinen tiedonsiirtonopeus 5Ghz verkossa on 867Mbps ja 2,4Ghz verkossa 300Mbps. Laite tukee WPA/WPA2 salausteknologioita sekä uusinta WPA3 versiota. Lisäksi laitteessa on neljä kappaletta gigabitin Ethernet-portteja. Laite toimii reitittimenä sekä tukiasemana (accesspoint) ja tukee MU-MIMO sekä beamforming-lähetystekniikkaa. TP-Link suosittelee laitetta maksimissaan kolmen makuuhuoneen kokoisiin asuntoihin. (TP-Link Corporation Limited, 2022)

## 4 Toteutus

Luvussa 4 käydään läpi opinnäytetyön tekninen osuus. Luvussa tutustutaan, kuinka Huaweiin reititin asetetaan siltatilaan sekä miten julkinen IP-osoite asetetaan. Lisäksi käymme läpi pfSensen käyttöönoton ja OpenWrt:n asennuksen wlan-reittimiseen.

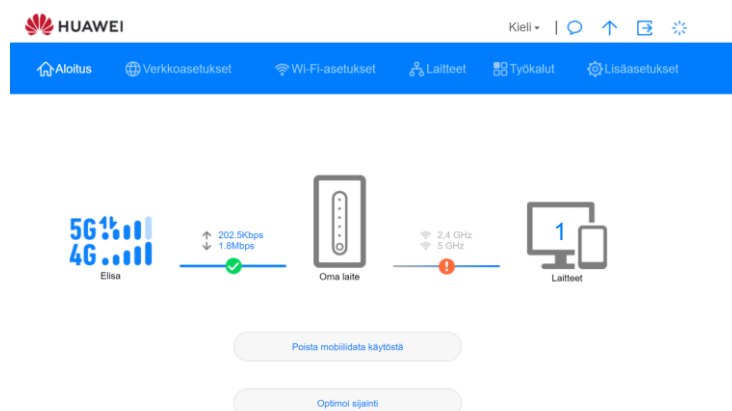
### 4.1 Huawei 5G CPE Pro 2 -reitittimen määrittelykset

Tässä luvussa käydään läpi Huawei 5G CPE Pro 2 määrittelykset. Oletuksena Huawei 5G CPE pro 2 sisältää kaikki palvelut, jotka kotireititin tarvitsee, esimerkiksi DHCP palvelu, palomuuuri ja langatonlähiverkko (wlan). Tämä mahdollistaa, että laite on suoraan käyttöönottokelpoinen kotikäyttäjälle. Opinnäytetyön tarkoituksena on luoda lähiverkko käyttäen avoimen lähdekoodinpalveluita, joten nämä Huaweiin reitittimen tarjoamat oletuspalvelut kytketään pois päältä muuttamalla laite käyttämään siltatilaa. Siltatilassa laite toimii vain 5G-modeemina ottamatta kantaa verkon muuhun toimintaan. Tämän lisäksi laitteessa otetaan käyttöön julkinen IP-osoite, jolloin kaikki verkon portit ja palvelut saadaan käyttöön.

#### 4.1.1 Julkisen IP-osoitteen asettaminen

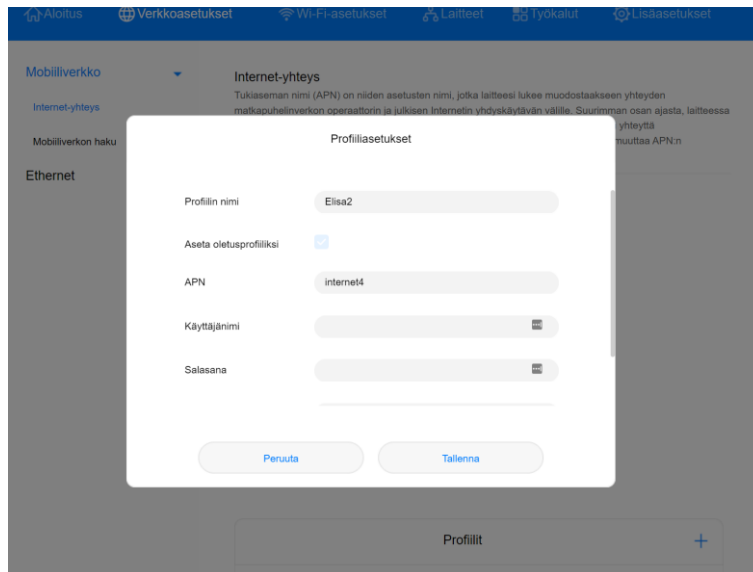
Julkinen IP-osoite asetetaan seuraavasti. Aluksi kirjaudutaan sisään Huaweiin hallintasivulle osoitteella: 192.168.8.1. Käyttäjätunnus ja salasana löytyvät laitteen pohjasta olevasta tarrasta.

Kuva 5 Huawei hallintasivu



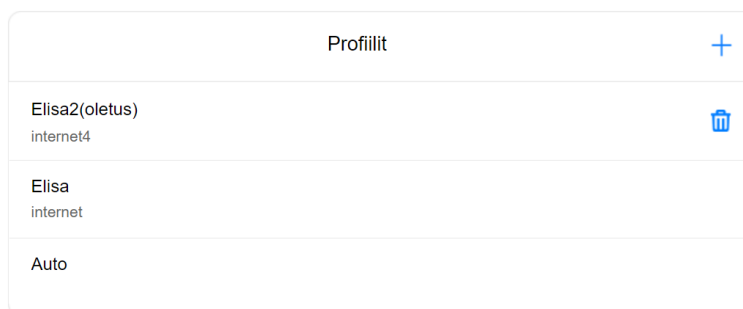
Seuraavaksi siirrytään kuvan 5 näkymästä kohtaan verkkoasetukset ja sieltä internetyhteys.

Kuva 6 Huawei profiiliasetukset



Valitaan (kuvassa 6) sivun alareunasta kohta ”profiilit” ja painetaan plusmerkkiä. Aukeavaan profiiliasetukset-ikkunaan syötetään haluttu nimi uudelle profiilille, esimerkiksi elisa2. APN-riville kirjoitetaan julkisen IP-osoitteen APN-nimi, joka on ”internet4”.(Elisa, 2022b) Lisäksi laitetaan raksi kohtaan ”aseta oletusprofiiliksi”. Seuraavaksi hyväksytään muutokset painamalla ”tallenna”. Kuvassa 7 nähdään, että profiilit välilehdelle on tullut tekemämme muutokset oletusprofiiliksi. Lopuksi suositeltavaa on käynnistää reititin uudelleen.

Kuva 7 Huawei profiilit



Seuraavaksi tarkistetaan, että muutos on onnistunut. Ensimmäisenä täytyy selvittää oma julkinen IP-osoite. Tämä käy kätevästi esimerkiksi sivustolta: <http://myip.fi>.

Kuva 8 Myip.fi (Myip.fi, n.d.)

IP-osoite	
Isäntänimi (hostname)	.elisa-mobile.fi

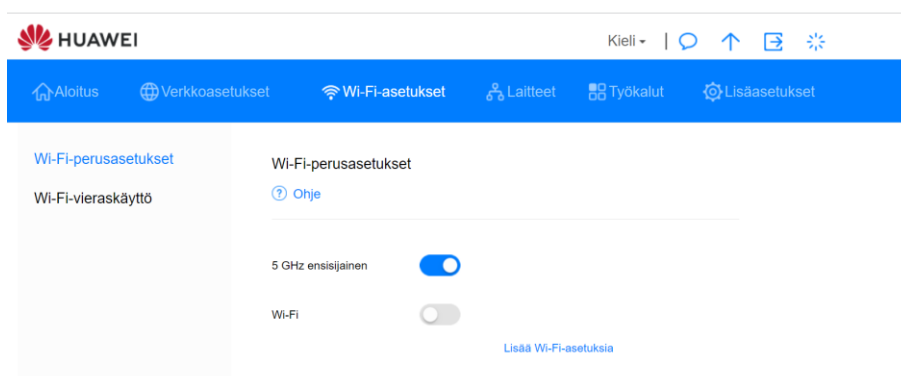
Kuvassa 8 näkyvässä kohdassa ”isäntänimi” (Hostname) tulisi lukea osoitteen perässä: `elisa-mobile.fi`. Mikäli osoitteen loppuosa on muotoa: `nat.elisa-mobile.fi`, ei muutos ole onnistunut ja IP-osoite on edelleen Elisan nat-palvelun takana.(Elisa, 2022b)

#### 4.1.2 Siltatila

Huawei 5G CPE Pro 2 5G -reititin sisältää monenlaisia palveluita esimerkiksi: DHCP, palomuuuri ja wlan-tukiasema. Huaweiin omat toiminnallisuudet eivät ole opinnäytetyön kannalta oleellisia ja kaikki nämä palvelut otetaan käyttöön myöhemmissä kappaleissa avoimen lähdekoodin pfSense ja OpenWrt-alustoilla. Huaweiin reitittimen tehtäväksi jää toimia siltatilassa linkkinä julkiseen verkkoon, joten ylimääräiset palvelut karsitaan pois päältä.

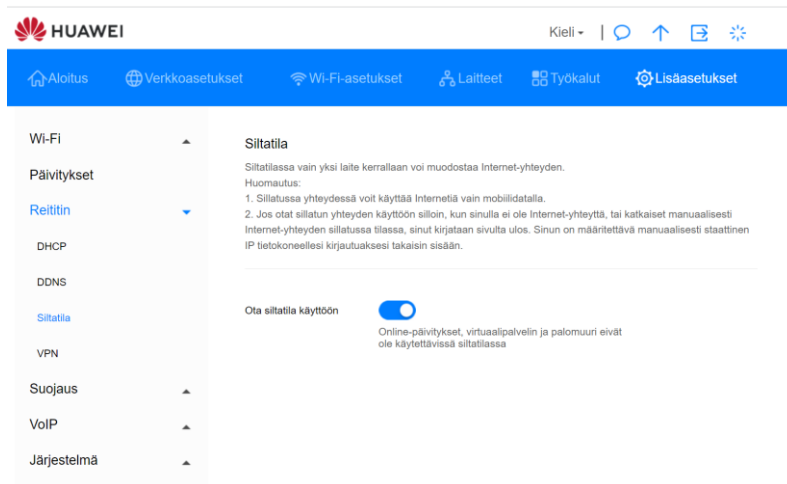
Aluksi laitteeseen kannattaa kytkeytyä Ethernet-kaapelilla, joka menee suoraan tietokoneeseen. Muita laitteita ei saa olla kytkettynä. Seuraavaksi kirjaudutaan Huaweiin hallintaosoitteeseen: `192.168.8.1`. Käyttäjätunnus ja salasana löytyvät laitteen pohjasta olevasta tarrasta. Etusivulta siirrytään kohtaan ”Wi-Fi asetukset” ja otetaan valinta ”Wi-Fi” pois (kuvassa 9).

Kuva 9 Huawei Wi-Fi perusasetukset



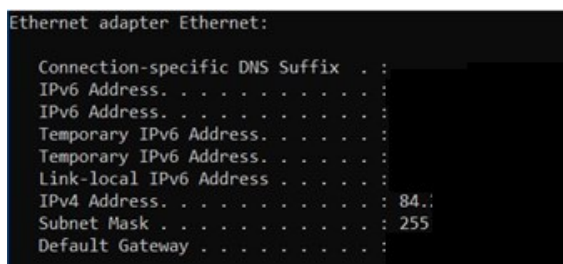
Seuraavaksi siirrytään lisäasetuksiin, jonka jälkeen valitaan reititin ja siltatila (kuvassa 10). Avautuvasta valikosta otetaan liukukytkintä näpäyttämällä siltatilakäyttöön ja hyväksytään varoitus painamalla ”ok”. Tämän jälkeen laite käynnistyy uudelleen ja yhteys laitteelle menetetään. Laitteeseen pääsee kirjautumaan jatkossa asettamalla tietokoneelle kiinteän IP-osoitteen, mikäli tulee tarve muuttaa laitteen asetuksia.

Kuva 10 Huawei siltatila



Lopuksi todennetaan vielä muutosten toimivuus. Windows työasemissa painetaan näppäinyhdistelmää ” lippu + r ”ja kirjoitetaan aukeavaan suoritaikkunaan ”cmd”. Tämän jälkeen kirjoitetaan komentokehoteeseen: ”ipconfig” ja verrataan tuloksia kuvan 8 näkymään. IP-osoitteiden tulisi nyt olla täysin identtiset, kuten kuvassa 8 ja kuvassa 11, eli työasema saa julkisen IP-osoitteen.

Kuva 11 Komentokehote,” ipconfig”




## 4.2 pfSense-palomuurin asennus ja määrittelyt

pfSensen asentaminen alkaa lataamalla oikea asennusmedia valmistajan sivuilta. Työssä käytettävä versio on pfSense Community Edition 2.5.2. Arkkitehtuuriksi valitaan AMD64 (64-



bit) (kuvassa 12). Asennusmediaksi valitaan ”USB Memstick Installer”. Asennuksessa käytettäväksi konsolityypiksi valitaan ”Serial”.

Kuva 12 pfSense asennusmedian lataus



The screenshot shows the 'Select Image To Download' interface on the pfSense website. It includes several dropdown menus for configuration: Version (2.5.2), Architecture (AMD64 (64-bit)), Installer (USB Memstick Installer), Console (Serial), and Mirror (New York City, USA). A blue 'DOWNLOAD' button is prominently displayed. To the right, it says 'Supported by' followed by the Netgate logo. At the bottom, a SHA256 checksum is provided for the compressed file.

Select Image To Download

Version: 2.5.2


Architecture: AMD64 (64-bit) ⓘ

Installer: USB Memstick Installer ▾

Console: Serial ▾

Mirror: New York City, USA ▾

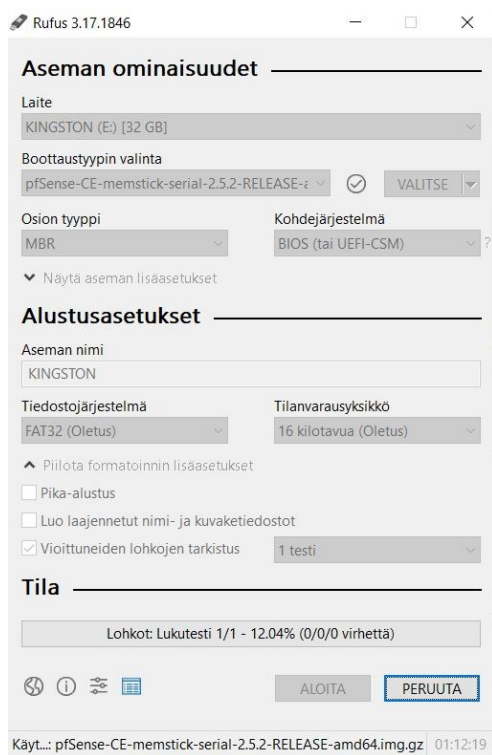
[SHA256 Checksum](#) for compressed (.gz) file:  
bb5287e52a01a67ba72d4685401799e5e1ada10c5e8d29c32f0b7a09d58d70d6

Supported by 

pfSensen sivuilta ladattu asennusmedia täytyy vielä saattaa asennettavaan muotoon tekemällä boottaava muistitikku. Työssä käytetään Kingstonin valmistamaa 32gb:n USB3-muistitikkoa.

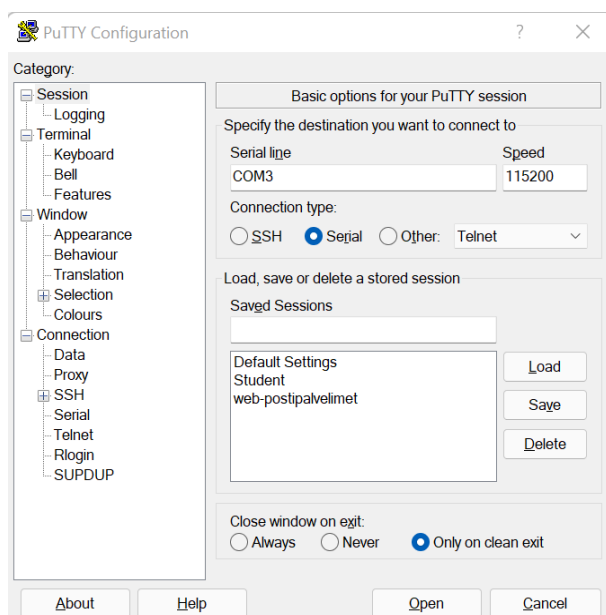
Boottaavan USB-muistitikun luominen tapahtuu avaamalla Rufus-sovellus ja valitsemalla oikea asennusmedia ja haluttu levynkuva (image) (kuvassa 13). Rufus täyttää muut tiedot automaattisesti. Ajan säästämiseksi on hyvä käyttää pika-alustusta USB-muistitikun formatoimisessa ja lisäksi on suositeltavaa tarkistaa USB-muistitikun lohkojen tila ainakin yhdellä testillä, mikäli kyseessä on ns. epämääräinen tallennusmedia.

Kuva 13 Rufus-osiointityökalu



Asennus aloitetaan kytkemällä sarjaliikennekaapeli kiinni USB-adapterilla tietokoneeseen ja pfSense reitittimeen kuvan 15 ja kuvan 16 mukaisesti. Rufuksella luotu USB-muistitikku kiinnitetään laitteen USB-porttiin (kuvassa 15). Seuraavaksi käynnistetään PuTTY-sovellus ja tehdään tarvittavat perusmääritykset (kuvassa 14).

Kuva 14 PuTTY Configuration



Ensimmäisenä selvitetään Windowsin laitehallinnasta sarjaliikennekaapelin virtuaalisen portin tunnus kohdasta "portit" (COM ja LPT), (kuvassa 17). Seuraavaksi kirjoitetaan Serial Line -riville oikea virtuaalisen portin tunnus, joka on tässä tapauksessa "COM3".

Sarjaliikenneportin nopeudeksi asetetaan 11500 (Electric Sheep Fencing LLC and Rubicon Communications LLC, 2022). Yhteyden tyyppiä valitaan "Serial" ja käytettäväksi protokollaksi Telnet. Lopuksi valitaan Open ja PuTTY käynnistää terminaali-istunnon.

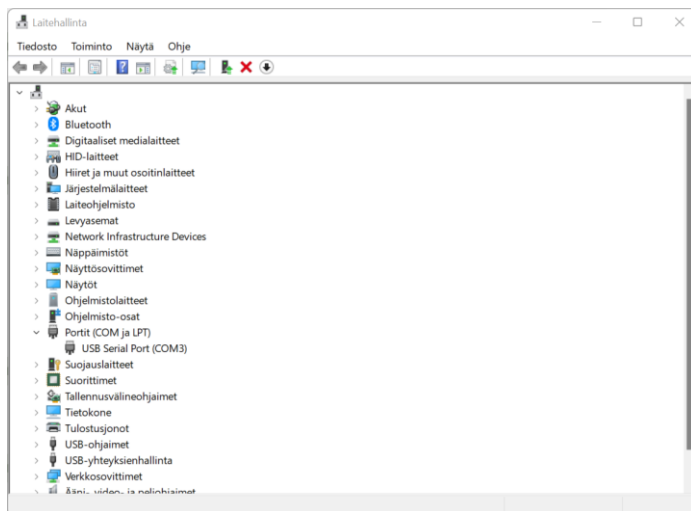
Kuva 15 Asennusmedia ja sarjaliikennekaapeli kiinnitettynä reitittimeen



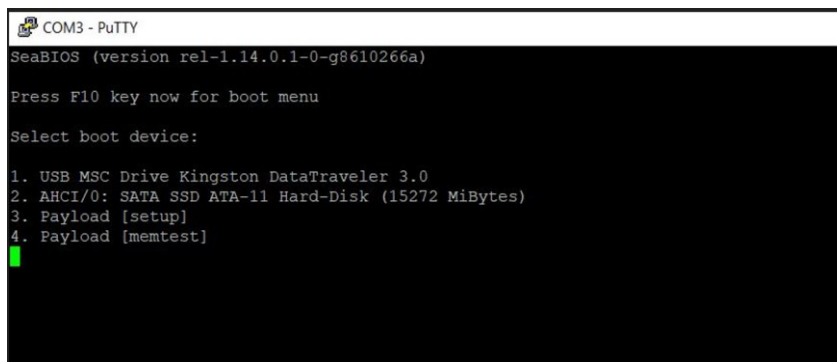
Kuva 16 Sarjaliikennekaapeli ja USB-DB9 adapteri



Kuva 17 Windows-laitehallinta



Kuva 18 Select boot device

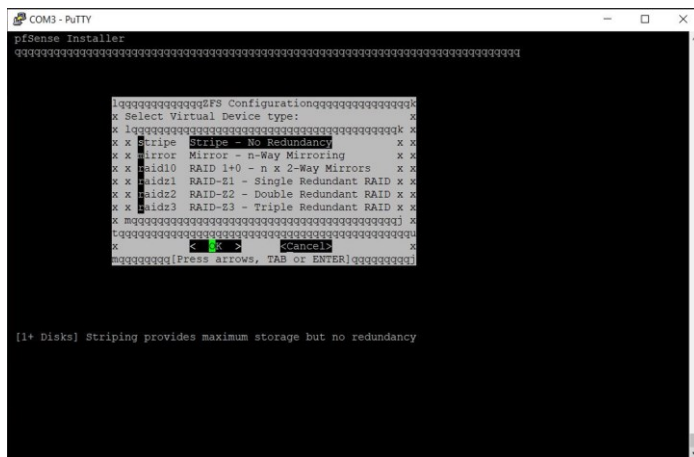


Valitaan, miltä loogiselta asemalta halutaan laitteen käynnistyvän. Tässä tapauksessa valitaan 1) USB MSC Drive Kingston DataTravel 3.0 (kuvassa 18).



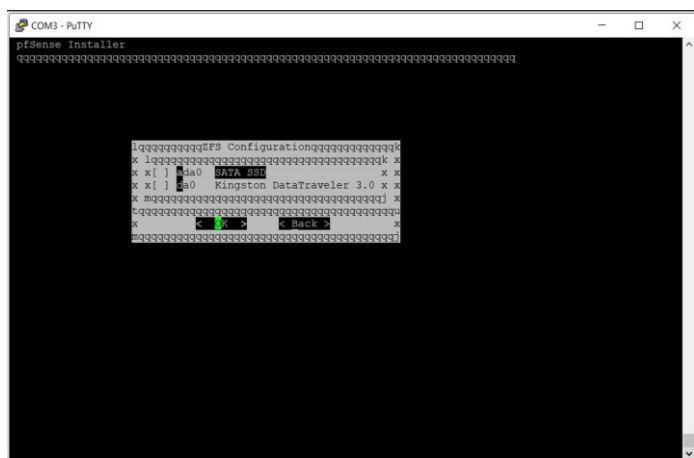


Kuva 23 Levyaseman tyyppi



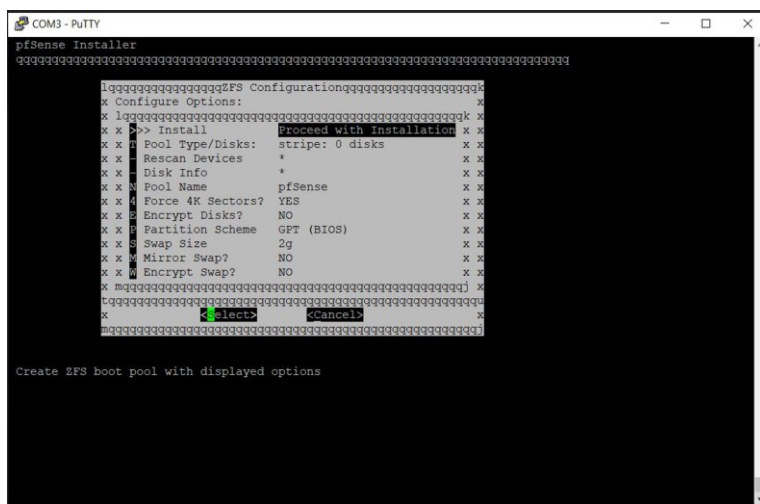
Valitaan levyaseman tyyppi. Työssä ei ole käytössä kuin yksi looginen asema, joten valitaan "Stripe" (kuvassa 23).

Kuva 24 Looginen asema



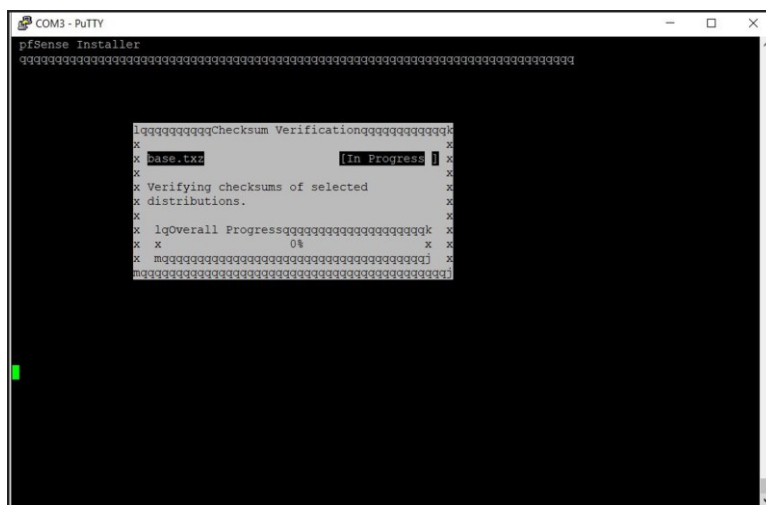
Valitaan haluttu looginen asema, eli "ada0, SATA SSD" (kuvassa 24).

Kuva 25 Valmiit asetukset



Asetukset ovat nyt valmiit ja voidaan valita Install-valikosta ”Proceed with Installation” painamalla Enter-näppäintä (kuvassa 25)

Kuva 26 Asennus käynnissä



pfSensen asennus käynnissä (kuvassa 26).





Kuva 29 IP-asetukset

```

COM3 - PuTTY
5) Reboot system          14) Enable Secure Shell (sshd)
6) Halt system            15) Restore recent configuration
7) Ping host              16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:
1 - WAN (igb0 - dhcp, dhcp6)
2 - LAN (igb1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.0.0.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 23

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.0.0.2
Enter the end address of the IPv4 client address range: 10.0.1.254
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 10.0.0.1/23
You can now access the webConfigurator by opening the following URL in your web
browser:
        https://10.0.0.1/

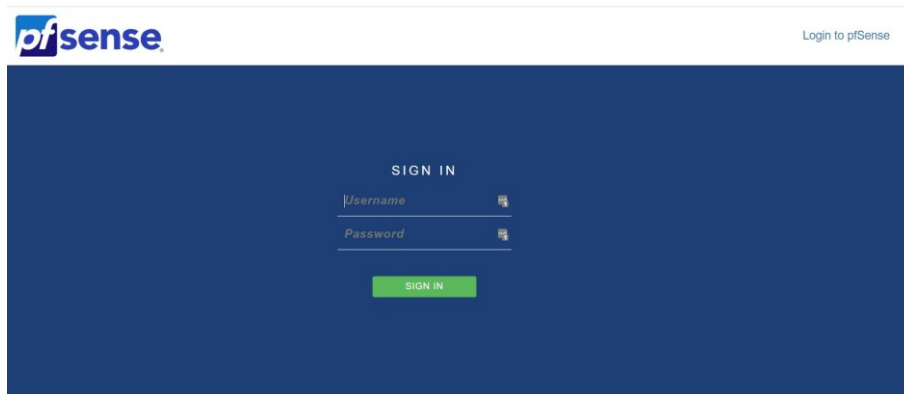
Press <ENTER> to continue.

```

Valitaan optio 2 (kuvassa 29), kun halutaan määrittää LAN-puolen IP-alue. Seuraavaksi annetaan yhdyskäytävän eli verkon ensimmäinen osoite, joka on 10.0.0.1. Sitten määritellään maski, joka on tässä tapauksessa 23. IPv6-asetuksia ei määritellä tässä tapauksessa ja siirrytään eteenpäin painamalla Enter-näppäintä. Seuraavaksi pfSense tiedustele, halutaanko käynnistää ”dhcp”, johon valitaan kyllä (y) ja painetaan Enter. Lopuksi pfSense ilmoittaa verkon olevan 10.0.0.1/23 ja hallintaliittymä löytyy osoitteesta 10.0.0.1.

Seuraavaksi siirrytään internetselaimella osoitteeseen 10.0.0.1 ja kirjaudutaan sisään oletustunnuksilla. Käyttäjätunnus ”Admin” ja salasana ”pfsense” (kuvassa 30). Kirjautumisen jälkeen nämä kannattaa muuttaa mieleisekseen välittömästi.

Kuva 30 pfSense kirjautuminen



#### 4.2.1 DHCP

Työssä käytettävä IP-avaruus jakautuu kahteen sarjaan: kiinteä IP-osoite ja jaettavat osoitteet. Kiinteät IP-osoitteet ovat käytössä esimerkiksi tulostimille ja langattoman verkon tukiasemille. DHCP jakaa loput osoitteet automaattisesti. DHCP:n käyttöön tulevat osoitteet ovat 10.0.0.2–10.0.0.254. Kiinteässä verkossa käytetään osoitteita väliltä 10.0.1.1–10.0.1.245.

Lähiverkon IP-osoitteiden määritetään pfSensen kohdasta Services – DHCP Server – LAN (kuvassa 31). Kohdasta General Options valitaan ”Enable DHCP Server on LAN interface”. Seuraavaksi valitaan kohdasta ”Range” jaettavat IP-osoitealue. Kohtana ”From” laitetaan 10.0.0.2 ja ”To” 10.0.0.254. Kuitataan asetukset painamalla sivun alareunasta Save-näppäintä.

## Kuva 31 pfSense DHCP server

The screenshot shows the pfSense web interface for configuring the DHCP server on the LAN interface. The breadcrumb trail is Services / DHCP Server / LAN. The 'General Options' section is expanded, showing the following settings:

- Enable:** ☒ Enable DHCP server on LAN interface
- BOOTP:** ☐ Ignore BOOTP queries
- Deny unknown clients:** ☐ Deny unknown clients. When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on any scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.
- Ignore denied clients:** ☐ Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
- Ignore client identifiers:** ☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
- Subnet:** 10.0.0.0
- Subnet mask:** 255.255.254.0
- Available range:** 10.0.0.1 - 10.0.1.254
- Range:** From 10.0.0.2 To 10.0.0.254

### 4.2.2 DOT & DNS resolver

DNS asetusten määrittely tapahtuu siirtymällä ”System – General ja DNS Server Settings”.

DNS Servers riville laitetaan Cloudflaren ip-osoite, joka on 1.1.1.1 ja hostnameeksi ”cloudflare-dns.com”. Seuraavaksi määritellään toissijainen dns-osoite painamalla add dns server -näppäintä, jolloin saadaan lisäriivi. Uudelle riville laitetaan toinen Cloudflaren palvelin, jonka osoite on 1.0.0.1 ja hostnameeksi ”cloudflare-dns.com”. Tarkistetaan, että kohta ”Allow DNS Server List to be overridden by DHCP/PPP on WAN” ei ole valittuna. Seuraavaksi valitaan kohdasta DNS Resolution Behavior -liukuvalikosta ”Use local DNS (127.0.0.1)”, ”Ignore remote DNS Servers”. Lopuksi tallennetaan nämä asetukset. (kuvassa 32)

## Kuva 32 pfSense DNS-asetukset

The screenshot shows the pfSense System / General Setup page. The 'System' section includes fields for 'Hostname' (Core) and 'Domain' (vasama.lan). The 'DNS Server Settings' section shows two DNS Servers configured: 1.1.1.1 and 1.0.0.1, both pointing to cloudflare-dns.com. The 'DNS Server Override' checkbox is unchecked, and the 'DNS Resolution Behavior' is set to 'Use local DNS (127.0.0.1), ignore remote DNS Servers'.

**System**

**Hostname** Core  
Name of the firewall host, without domain part

**Domain** vasama.lan  
Do not end the domain name with 'local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternative TLDs such as 'local.lan' or 'mylocal' are safe.

**DNS Server Settings**

DNS Servers	Address	Hostname	Action
1.1.1.1	cloudflare-dns.com		Delete
1.0.0.1	cloudflare-dns.com		Delete

**Add DNS Server** + Add DNS Server

**DNS Server Override** ☐ Allow DNS server list to be overridden by DHCP/PPP on WAN  
If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.

**DNS Resolution Behavior** Use local DNS (127.0.0.1), ignore remote DNS Servers  
By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.

## Seuraavaksi siirrytään Services – DNS Resolver

Valitaan kohdasta "General DNS Resolver Options – Enable DNS resolver". Kuunneltava portti jätetään oletukseen 53 ja SSL/TLS portti jätetään myös oletukseen 853. (kuvassa 33)

## Kuva 33 Enable DNS resolver

The screenshot shows the pfSense Services / DNS Resolver / General Settings page. The 'General Settings' tab is selected. The 'General DNS Resolver Options' section shows the 'Enable' checkbox checked, 'Listen Port' set to 53, and 'Enable SSL/TLS Service' unchecked. The 'SSL/TLS Certificate' is set to 'webConfigurator default (61ebf7caac292)' and the 'SSL/TLS Listen Port' is set to 853. The 'Network Interfaces' and 'Outgoing Network Interfaces' are both set to 'All'.

**Services / DNS Resolver / General Settings**

**General Settings** Advanced Settings Access Lists

**General DNS Resolver Options**

**Enable** ☒ Enable DNS resolver

**Listen Port** 53  
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

**Enable SSL/TLS Service** ☐ Respond to incoming SSL/TLS queries from local clients  
Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.

**SSL/TLS Certificate** webConfigurator default (61ebf7caac292)  
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.

**SSL/TLS Listen Port** 853  
The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.

**Network Interfaces** All  
WAN  
LAN  
WAN IPv6 Link-Local  
LAN IPv6 Link-Local

**Outgoing Network Interfaces** All  
WAN  
LAN  
WAN IPv6 Link-Local

Siirrytään sivustolla alaspäin ja poistetaan valinta "Enable DNSSEC Support". Seuraavaksi valitaan kohdasta "DNS Query Forwarding" valinnat "Enable Forwarding Mode" ja "Use SSL/TLS for outgoing DNS Queries to Forwarding Servers" (kuvassa 34).

Lopuksi todennetaan vielä, että DNS toimii, kuten kuuluu. Avataan selain ja siirrytään sivustolle x. Siirrytään pfSensen ”Diasnoscig / States” (kuvassa 35). Kuvassa on havainnollistettuna neliön sisällä oleva DNS, jossa kysytään DNS palvelimelta 1.1.1.1 portista 853 tietoja eli liikenne kulkee nyt salattuna.

## Kuva 34 DNS Resolver

Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.

**System Domain Local Zone Type** Transparent

The local-zone type used for the pfSense system domain (System | General Setup | Domain). Transparent is the default. Local-Zone type descriptions are available in the [unbound.conf\(5\)](#) manual pages.

**DNSSEC** ☐ Enable DNSSEC Support

**Python Module** ☐ Enable Python Module  
Enable the Python Module.

**DNS Query Forwarding** ☒ Enable Forwarding Mode

If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under [System > General Setup](#) or those obtained via DHCP/PPP on WAN (if [DNS Server Override](#) is enabled there).

☒ Use SSL/TLS for outgoing DNS Queries to Forwarding Servers

When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.

**DHCP Registration** ☐ Register DHCP leases in the DNS Resolver

If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. Note that this will cause the Resolver to reload and flush its resolution cache whenever a DHCP lease is issued. The domain in [System > General Setup](#) should also be set to the proper value.

**Static DHCP** ☐ Register DHCP static mappings in the DNS Resolver

If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in [System > General Setup](#) should also be set to the proper value.

**OpenVPN Clients** ☐ Register connected OpenVPN clients in the DNS Resolver

If this option is set, then the common name (CN) of connected OpenVPN clients will be registered in the DNS Resolver, so that their name can be resolved. This only works for OpenVPN servers (Remote Access SSL/TLS or User Auth with Username as Common Name option) operating in "tun" mode. The domain in [System: General Setup](#) should also be set to the proper value.

**Display Custom Options** ☒ Display Custom Options

## Kuva 35 Diagnostics - States

**Diagnostics / States / States**

States    Reset States

### State Filter

Interface:

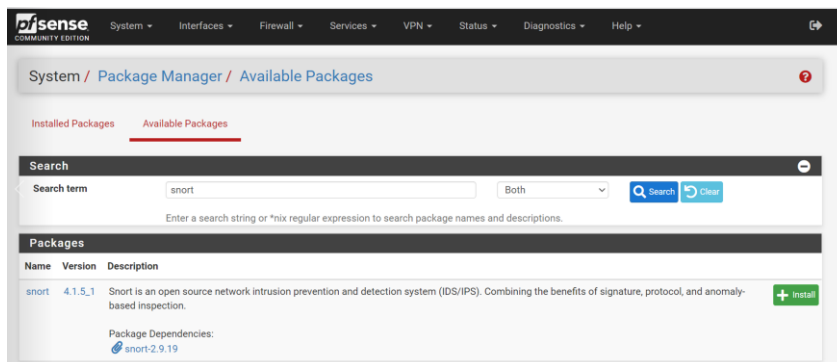
Filter expression:

Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
WAN	ipvs-icmp		NO_TRAFFIC_NO_TRAFFIC	7,856 K / 7,856 K	376 KiB / 376 KiB
WAN	icmp		0/0	7,857 K / 7,85 K	223 KiB / 222 KiB
LAN	udp		SINGLENO_TRAFFIC	484 / 0	223 KiB / 0 B
WAN	tcp	-> 1.1.1.1:853	TIME_WAIT:TIME_WAIT	13 / 11	1 KiB / 4 KiB
WAN	tcp	-> 1.1.1.1:853	TIME_WAIT:TIME_WAIT	14 / 12	1 KiB / 5 KiB

### 4.2.3 Snort (IDS/IPS protection)

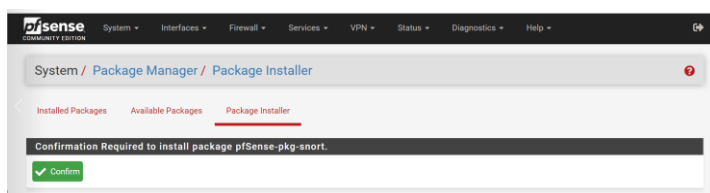
Snort-asennus aloitetaan hakemalla asennuspaketti pakettihallinnasta. Siirrytään ”System – Package Manager – Available Packages”. Haku kenttään kirjoitetaan ”Snort” ja painetaan Search-painiketta. Valitaan paketti ”Snort version 4.1.5\_1” ja painetaan ”Install” (kuvassa 36).

Kuva 36 Package Manager

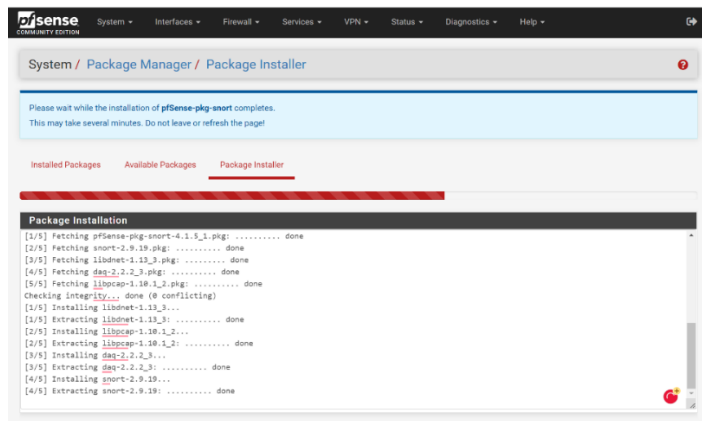


Hyväksytään paketin asennus painamalla ”Confirm”. (kuvassa 37) Seuraavaksi asennus käynnistyy (kuvassa 38).

Kuva 37 Package Installer

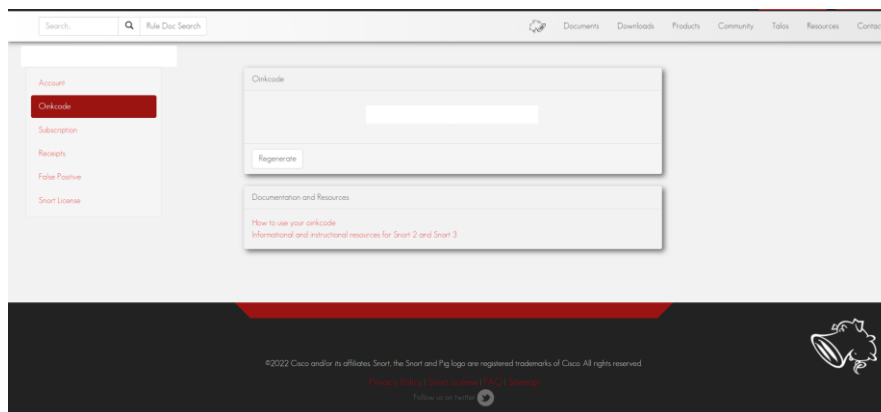


## Kuva 38 Package Installer Progress



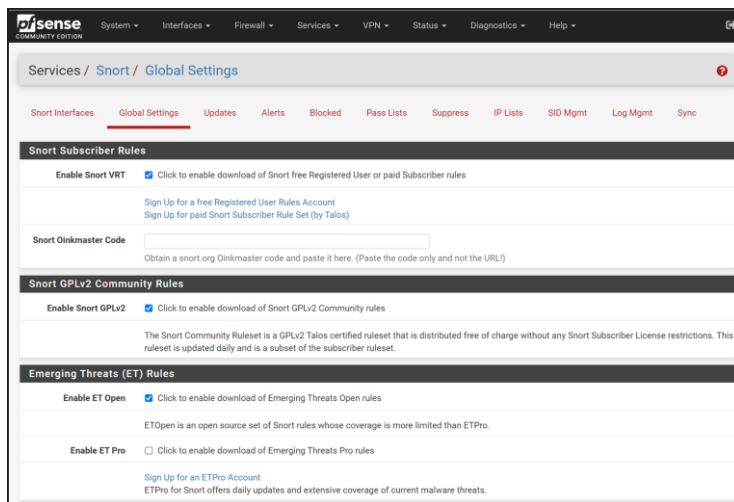
Asennuksen valmistuttua siirrytään ”Services – Snort – Global Settings” (kuvassa 40).  
 Valitaan hyperlinkki ”Sign Up for a free registered User Rules Account” ja rekisteröidytään käyttäjäksi. Sivustolle kirjautumisen jälkeen katsotaan kohdasta ”Oinkcode” henkilökohtainen tunnus järjestelmään (kuvassa 39).

## Kuva 39 Snort Oinkcode



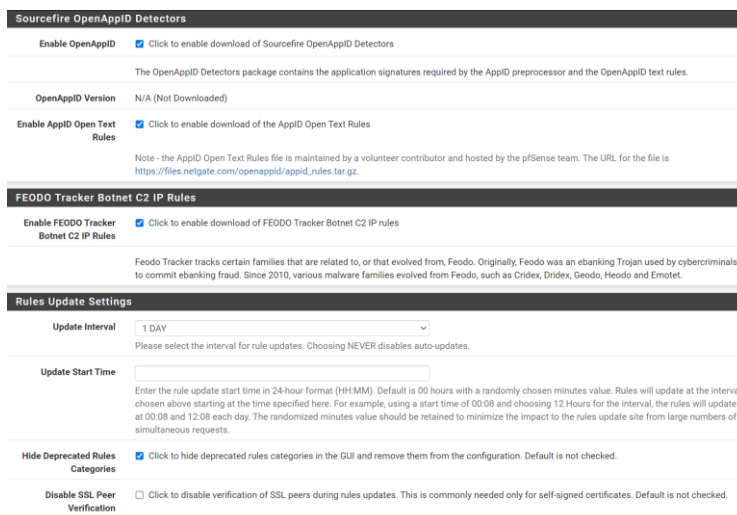


## Kuva 40 Snort Global Settings



Lähdetään ottamaan sääntöjä käyttöön valitsemalla ”Enable Snort VRT” ja kirjoitetaan (kuvassa 39) oinkcode-riville ”Snort Oinkmaster Code” (kuvassa 40). Seuraavaksi aktivoidaan ja ladataan Snort GPLv2 Community -säännöt ja ”Emerging Threats (ET) rules” (kuvassa 40). Siirrytään vielä alemmaksi sivulla ja otetaan käyttöön myös ”Sourcefire OpenAppID Detectors” ja ”FEODO Tracker Botnet c2 IP Rules”. Asetetaan päivitysväliksi yksi vuorokausi (kuvassa 41).

## Kuva 41 Snort Global Settings 2



Siirrytään ”Services – Snort – Updates” (kuvassa 42). Kohdassa ”Installed Rule Set MD5 Signature” nähdään kaikki aiemmin käyttöönotetut säännöt. Valitaan kohdasta ”Update Your Rule Set” painike ”Update Rules”. Tämän jälkeen Snort päivittää sääntöjen tietokannan

(kuvassa 43). Mikäli päivitys onnistui kohdassa ”Last Update” lukee päivämäärä ja päivityksen tila (kuvassa 44).

Kuva 42 Snort Updates

**Services / Snort / Updates**

Snort Interfaces Global Settings **Updates** Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

**Installed Rule Set MD5 Signature**

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Downloaded	Not Downloaded
Snort GPLv2 Community Rules	Not Downloaded	Not Downloaded
Emerging Threats Open Rules	Not Downloaded	Not Downloaded
Snort OpenAppID Detectors	Not Downloaded	Not Downloaded
Snort AppID Open Text Rules	Not Downloaded	Not Downloaded
Feodo Tracker Botnet C2 IP Rules	Not Downloaded	Not Downloaded

**Update Your Rule Set**

Last Update: Unknown Result: **Unknown**

Update Rules: [Update Rules](#) [Force Update](#)

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

**Manage Rule Set Log**

[View Log](#) [Clear Log](#)

The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

Logfile Size Log file is empty

Kuva 43 Rules Update Task

**Rules Update Task**

Updating rule sets may take a while ... please wait for the process to complete.

This dialog will auto-close when the update is finished.

[Close](#)

Kuva 44 Rule Update Task Success

Feodo Tracker Botnet C2 IP Rules 3d9e065ec8d06f82e8af0649920b6fab Sunday, 20-F

**Update Your Rule Set**

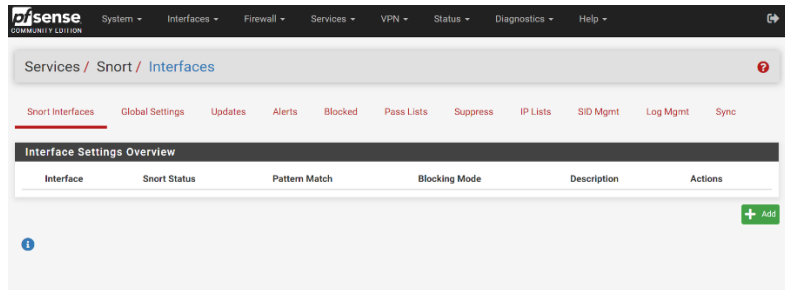
Last Update: Feb-20 2022 16:02 Result: **Success**

Update Rules: [Update Rules](#) [Force Update](#)

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

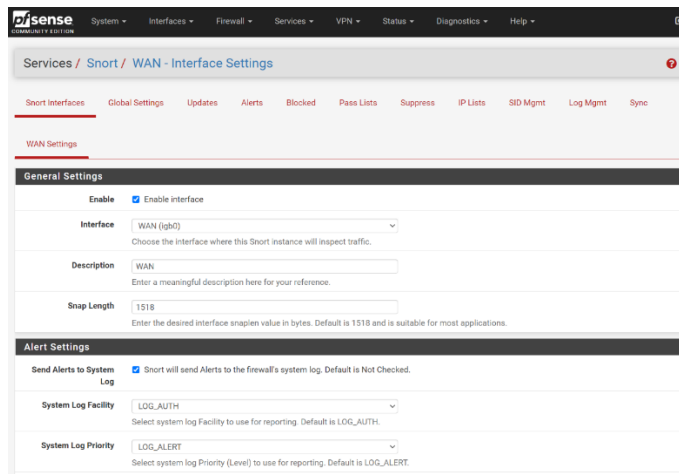
Snort Interfacen käyttöönotto tapahtuu siirtymällä ”Services – Snort – Interfaces”. Valitaan oikealta alhaalta Add-painike (kuvassa 45).

Kuva 45 Snort Interface



Valitaan kohdasta ”General Settings Enable Interface”. Interface-kohdasta valitaan se puoli, jota halutaan valvoa (WAN/LAN). Valitaan WAN (igb0). Alert Settings -kohdasta halutaan Snortin tallentavan tapahtumia palomuurin lokeihin (kuvassa 46). Siirrytään sivustolla alaspäin ja valitaan kohdasta ”Detection Performance Settings, Search Optimize” (kuvassa 47). Lopuksi tallennetaan asetukset Save-näppäimellä.

Kuva 46 Wan - Interface Settings





## Kuva 49 Settings - WAN Categories

COMMUNITY EDITION

Services / Snort / Interface Settings / WAN - Categories

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

WAN Settings **WAN Categories** WAN Rules WAN Variables WAN Preprocs WAN IP Rep WAN Logs

**Automatic Flowbit Resolution**

**Resolve Flowbits** ☒ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.  
 Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

**Snort Subscriber IPS Policy Selection**

**Use IPS Policy** ☒ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.  
 Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

**IPS Policy Selection** Balanced  
 Snort IPS policies are: Connectivity, Balanced, Security or Max-Detect.  
 Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file. Max-Detect is a policy created for testing network traffic through your device. This policy should be used with caution on production systems!

**Select the rulesets (Categories) Snort will load at startup**

Category is auto-enabled by SID Mgmt conf files  
 Category is auto-disabled by SID Mgmt conf files

Select All Unselect All Save

**Enable** **Ruleset: Snort GPLv2 Community Rules**

## Kuva 50 Block Settings

**Block Settings**

**Block Offenders** ☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

**IPS Mode** Legacy Mode  
 Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.  
 Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnx2, cc, corgbe, cxl, em, ems, ena, ice, igb, igc, ix, tgbe, tul, lem, re, vmx, vlnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

**Kill States** ☒ Checking this option will kill firewall established states for the blocked IP. Default is checked.

**Which IP to Block** BOTH  
 Select which IP extracted from the packet you wish to block. Default is BOTH.

Siirrytään kohtaan ”WAN Preprocs” ja valitaan ”Enable Performance Stats”. Lisäksi valitaan ”Auto Rule Disable” (kuvassa 51).

## Kuva 51 WAN Preprocs

**Important Preprocessor Information**  
 Rules may be dependent on enabled preprocessors! Disabling preprocessors may result in Snort startup failure unless all of the corresponding preprocessor-dependent rules are also disabled. Do not disable any default-enabled preprocessors on this page unless you are very skilled with using Snort. If you experience Snort start-up errors or failures after making changes to preprocessors, try resetting all preprocessor configurations to their defaults, and then attempt to start Snort.

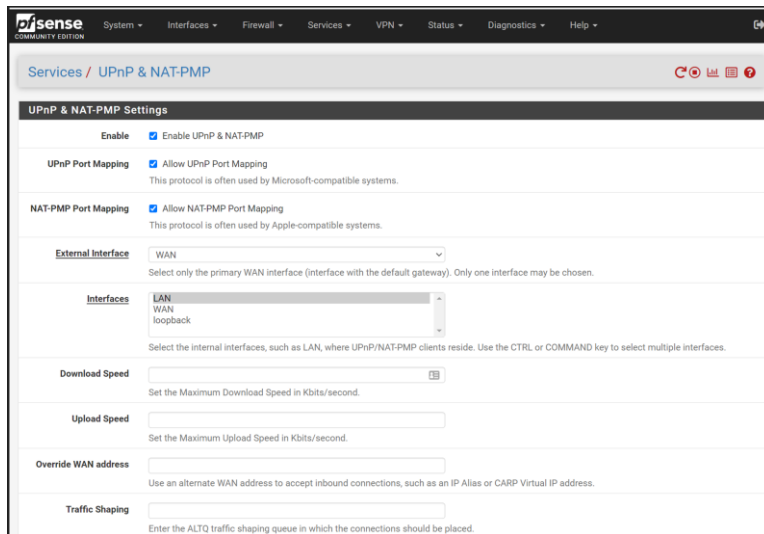
Preprocessors Basic Configuration Settings	
<b>Enable Performance Stats</b>	<input checked="" type="checkbox"/> Collect Performance Statistics for this interface. Default is Not Checked. Snort will automatically generate performance statistics for this interface. Enabling this option may have a slight negative performance impact. Statistics may be viewed on the LOGS tab for this interface. Performance Statistics are disabled by default.
<b>Protect Customized Preprocessor Rules</b>	<input type="checkbox"/> Enable this only if you maintain customized preprocessor text rules files for this interface. Default is Not Checked. Enable this only if you use customized preprocessor text rules files and you do not want them overwritten by automatic Snort Subscriber Rules updates. This option is disabled when Snort Subscriber Rules download is not enabled on the Global Settings tab. Most users should leave this option unchecked.
<b>Auto Rule Disable</b>	<input checked="" type="checkbox"/> Auto-disable text rules dependent on disabled preprocessors for this interface. Default is Not Checked. Enabling this option allows Snort to automatically disable any text rules containing rule options or content modifiers that are dependent upon the preprocessors you have not enabled. This may facilitate starting Snort without errors related to disabled preprocessors, but can substantially compromise the level of protection by automatically disabling detection rules. Enabling this feature will result in decreased protection from Snort.
<b>Enable RPC Decode and Back Orifice Detector</b>	<input checked="" type="checkbox"/> Normalize/Decode RPC traffic and detects Back Orifice traffic on the network. Default is Checked.
<b>Enable DCE/RPC2 Detection</b>	<input checked="" type="checkbox"/> The DCE/RPC preprocessor detects and decodes SMB and DCE/RPC traffic. Default is Checked.
<b>Enable SIP Detection</b>	<input checked="" type="checkbox"/> The SIP preprocessor decodes SIP traffic and detects vulnerabilities. Default is Checked.
<b>Enable GTP Detection</b>	<input type="checkbox"/> The GTP preprocessor decodes GPRS Tunneling Protocol traffic and detects intrusion attempts. Default is Not Checked.

Lopuksi otetaan Interface käyttöön kohdasta ”Services – Snort – Interfaces” painamalla Play-näppäintä (kuvassa 48).

### 4.2.4 UPnP

Aktivoidaan UPnP-protokolla siirtymällä ”Services – UpnP & NAT-PMP”. Aktivoidaan kohdat ”Enable UPnP & NAT-PMP”, ”Allow UPnP Port Mapping” ja ”Allow NAT-PMP Port Mapping” (kuvassa 52).

## Kuva 52 UPnP



### 4.2.5 pfSense ongelmia

Järjestelmän käyttöönoton jälkeen alkoi esiintyä päivittäin noin 5 minuutin katkoksia yhteyteen, mikä lamaannutti verkon täysin useamman kerran päivässä. Todettakoon, että 5G-yhteys ei ole vielä täysin aukoton, joten katkoksia yhteydessä esiintyy. Katkoksen sattuessa pfSense siirtyy hetkeksi ”lepäämään” ennen yhteyden palaamista. Tämä aiheuttaa tarpeettoman pitkän viiveen verkon toimintaan. Ratkaisuksi tähän löytyi Gateway -monitoroinnin pois kytkeminen.

Siirrytään kohtaan ”System – Routing – Gateways” ja suoritetaan sama toimenpide WAN\_DHCP- ja WAN\_DHCP6 -yhdyskäytävälle. Painetaan kynästä ”Edit” (kuvassa 53).

Valitaan kohdat ”Disable Gateway Monitoring” ja ”Disable Gateway Monitoring Action” (kuvassa 54).

Myös etätyöyhteyksissä oli pieniä haasteita riippuen käytössä olevasta VPN-yhteydestä. Pulse Secure VPN- ohjelmisto toimi moitteetta, mutta Fortinet VPN yhteys aiheutti useamman hälytyksen, jonka takia Snort puuttui peliin ja esti yhteydet täysin. Ainoana ratkaisuna yhteyksien toiminnan takaamiseksi Snortin säännöistä täytyi sammuttaa ne osat, jotka aiheuttivat vääriä hälytyksiä (kuvassa 55).



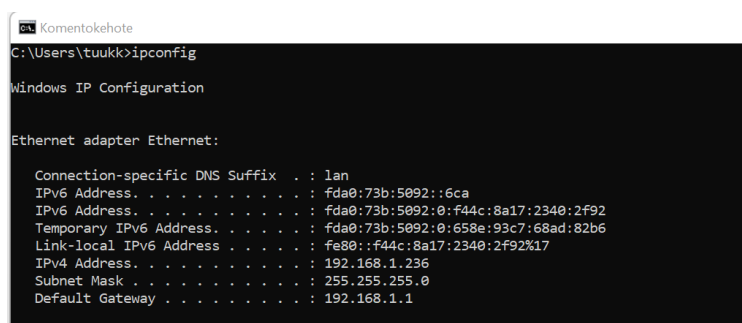


### 4.3 OpenWrt-ohjelmiston asennus

Tässä luvussa käydään lävitse OpenWrt-ohjelmiston asennus TP-link acher c6 wlan-reitittimeen.

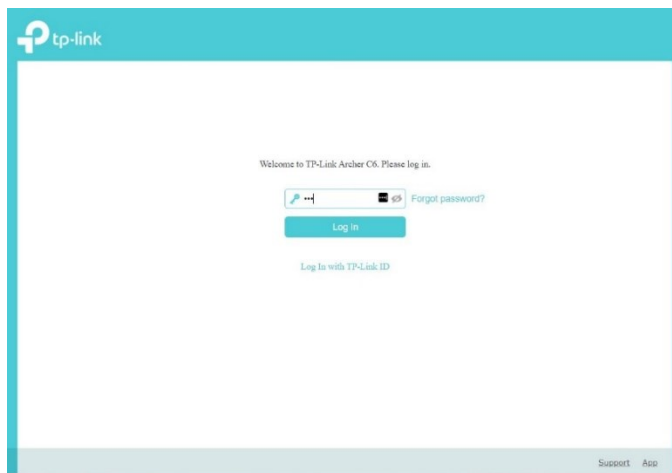
Aluksi kytketään reitittimeen virta ja liitetään Ethernet-kaapeli kiinni. Windows-laitteissa painetaan "ctrl + r" ja kirjoitetaan avautuvaan, suorita ikkunaan "cmd". Avautuvaan komentokehotteeseen kirjoitetaan "ipconfig". Kohdasta "Default Gateway" saadaan selville reitittimen yhdyskäytävän osoite. Tällä osoitteella päästään kirjautumaan reitittimen asetuksiin (kuvassa 56).

Kuva 56 Ipconfig

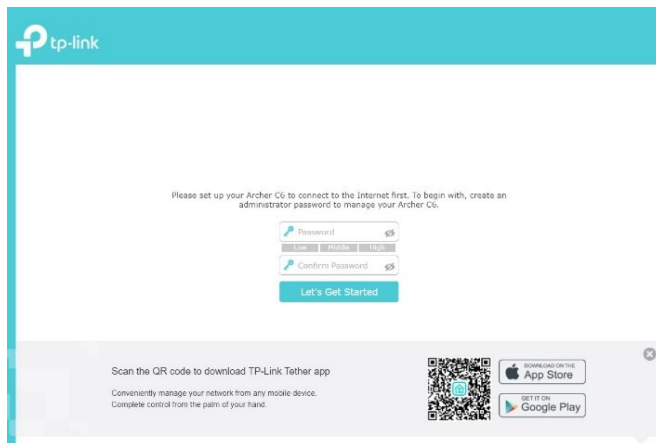


Seuraavaksi avataan internetselain ja kirjoitetaan osoiteriville 192.168.0.1 ja siirrytään TP-link-hallintasivustolle. Syötetään oletussalasana, joka on Admin (kuvassa 57). Tämän jälkeen tulee syöttää uusi salasana tietoturvasyistä (kuvassa 58), jonka jälkeen avautuu näkymä Quick Setup (kuvassa 59). Valitaan sivun ylälaidasta Advanced (kuvassa 59). Siirrytään Advanced- sivulla valikoita alaspäin ja valitaan kohtaan "Firmware Upgrade" (kuvassa 61). Valitaan kohdasta "Manual Upgrade" asennettava Image browse -painikkeella ja painetaan "Upgrade". Hyväksytään päivitys painamalla "Yes" (kuvassa 61). Päivityksen asentuminen kestää noin viisi minuuttia. Asennuksen edistymisen voi todentaa, kun Ethernet-yhteys katkeaa ja palautuu.

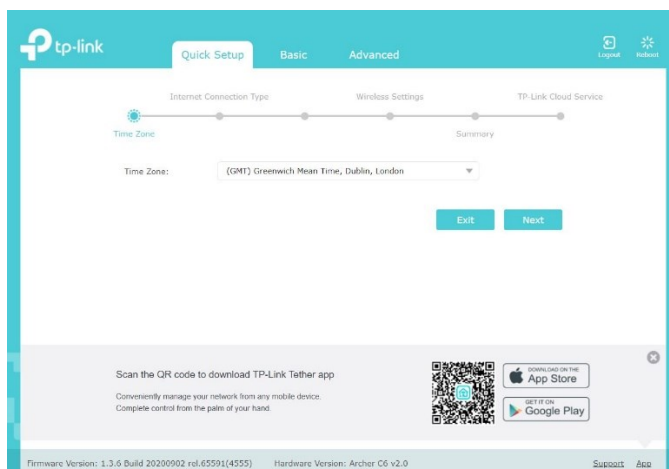
Kuva 57 TP-Link kirjautuminen



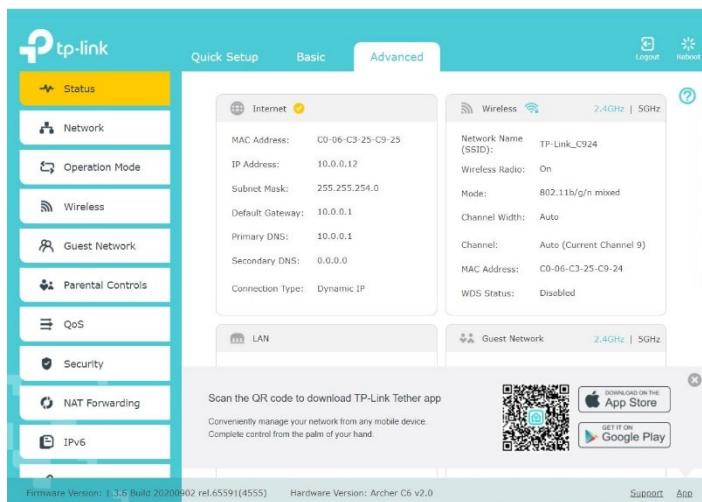
Kuva 58 TP-Link salasanan vaihto



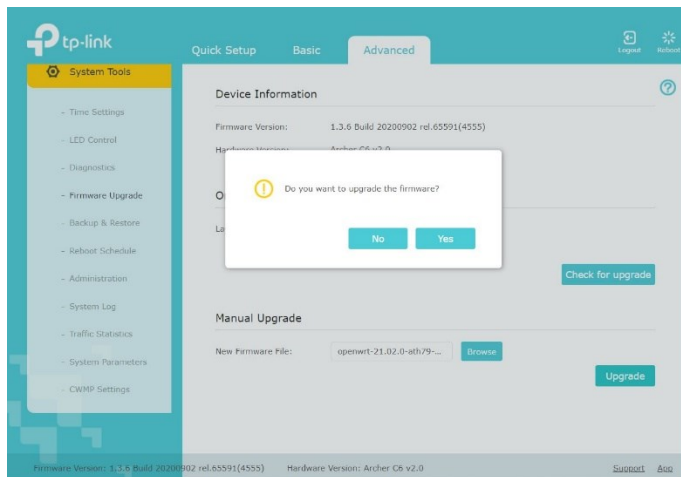
Kuva 59 TP-Link Quick Setup



## Kuva 60 TP-Link Advanced

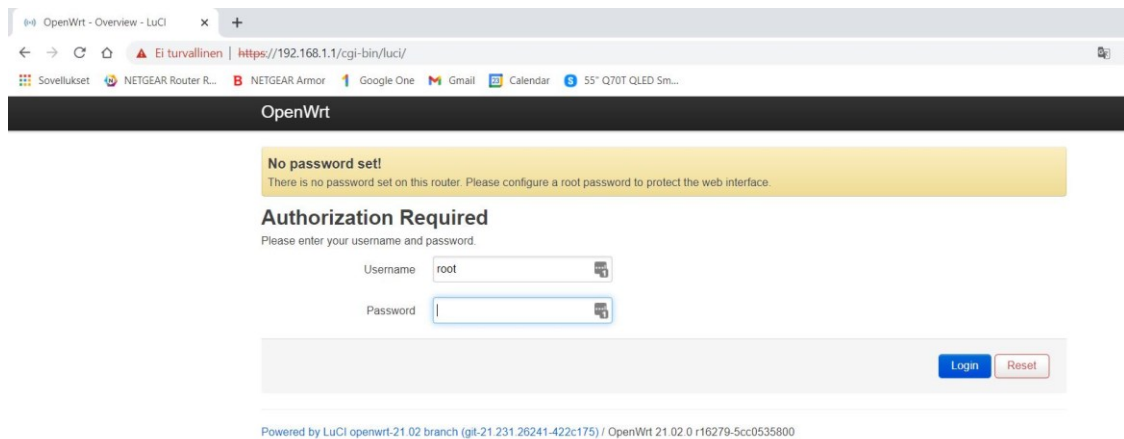


## Kuva 61 Firmware Upgrade



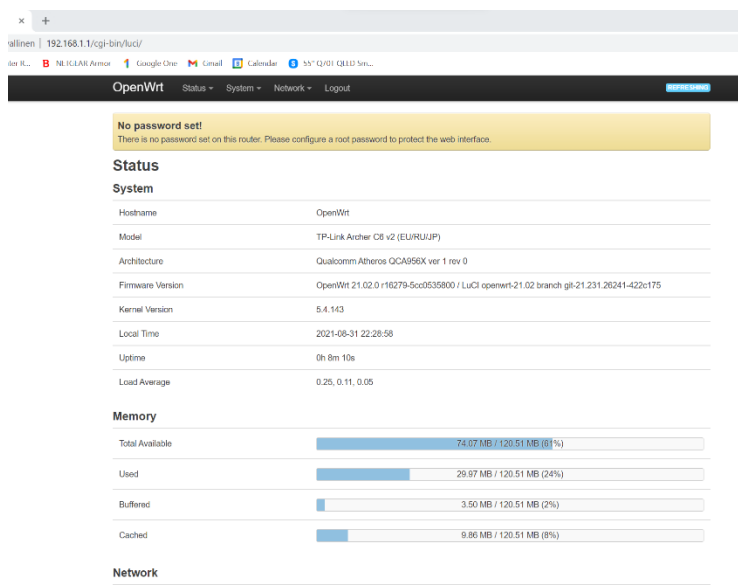
Onnistuneen asennuksen ja yhteyden palautumisen jälkeen selvitetään uusi hallinta osoite `ipconfig` -komennolla (kuvassa 56).

## Kuva 62 OpenWrt kirjautuminen



Siirrytään osoitteeseen 192.168.1.1 ja painetaan Login-painiketta. Oletuksena salasanaa ei ole asetettu ja se on syytä asettaa heti kirjautumisen jälkeen (kuvassa 62).

## Kuva 63 OpenWrt etusivu



Siirrytään System -välilehdelle ja sieltä "General settings" (kuvassa 63). Valitaan oikea aikavyöhyke ja päivitetään laitteen kellonaika. Hostname-kohtaan laitetaan kuvaava nimi esimerkiksi AP1 (Accesspoint 1). Kuvaukseen voi laittaa esimerkiksi laitteen sijainnin (kuvassa 64).

## Kuva 64 OpenWrt ajan asettaminen

**OpenWrt** Status System Network Logout [Help & Support](#)

### System

Here you can configure the basic aspects of your device like its hostname or the timezone.

#### System Properties

[General Settings](#) [Logging](#) [Time Synchronization](#) [Language and Style](#)

Local Time: 1.9.2021 klo 15:04:11  
[Sync with browser](#) [Sync with NTP-Server](#)

Hostname: OpenWrt

Description:   
 An optional, short description for this device

Notes:   
 Optional, free-form notes about this device

Timezone: Europe/Helsinki

[Save & Apply](#) [Save](#) [Reset](#)

Powered by LuCI openwrt-21.02 branch (git-21.231.26241-422c175) / OpenWrt 21.02.0 r16279-5cc0535800

Asetetaan reititin pelkäksi kytkimeksi. Aluksi poistetaan WAN ja WAN6 Interfacet painamalla Delete-näppäintä (kuvassa 65). Tämän jälkeen siirrytään muokkaamaan LAN-interfacea painamalla "Edit" (kuvassa 65).

## Kuva 65 OpenWrt interfaces

**OpenWrt** Status System Network Logout [Help & Support](#)

[Interfaces](#) [Devices](#) [Global network options](#)

### Interfaces

Interface	Protocol	MAC	RX	TX	IPv4	IPv6	Actions
LAN eth0.1	Static address	C0:06:C3:25:C9:24	740.54 KB (4707 Pkts.)	1.24 MB (3452 Pkts.)	192.168.1.1/24	fd00::1/64	<a href="#">Restart</a> <a href="#">Stop</a> <a href="#">Edit</a> <a href="#">Delete</a>
WAN eth0.2	DHCP client	C0:06:C3:25:C9:24	86.05 KB (600 Pkts.)	69.49 KB (217 Pkts.)			<a href="#">Restart</a> <a href="#">Stop</a> <a href="#">Edit</a> <a href="#">Delete</a>
WAN6 eth0.2	DHCPv6 client	C0:06:C3:25:C9:24	86.05 KB (600 Pkts.)	69.49 KB (217 Pkts.)			<a href="#">Restart</a> <a href="#">Stop</a> <a href="#">Edit</a> <a href="#">Delete</a>

[Add new interface...](#)

[Save & Apply](#) [Save](#) [Reset](#)

Powered by LuCI openwrt-21.02 branch (git-21.231.26241-422c175) / OpenWrt 21.02.0 r16279-5cc0535800

Asetetaan Protocol tyyiksi "Static adress" ja kannetaan kiinteän verkon puolelta ensimmäinen looginen osoite 10.0.1.2. Jatkossa tämä toimii myös laitteen hallintaosoitteena (kuvassa 66)

## Kuva 66 Staattinen osoite

Interfaces » LAN

General Settings | Advanced Settings | Firewall Settings | DHCP Server

Status Device: br-lan  
Uptime: 0h 13m 56s  
MAC: 00:06:C3:25:C9:24  
RX: 888.50 KB (6218 Pkts.)  
TX: 1.77 MB (4948 Pkts.)  
IPv4: 192.168.1.1/24  
IPv6: fda0:73b:5092::1/60

Protocol: Static address

Device: br-lan

Bring up on boot: ☒

IPv4 address: 10.0.1.2

IPv4 netmask: 255.255.254.0

IPv4 gateway: 10.0.0.1

IPv4 broadcast: 10.0.1.255

Dismiss Save

Siirrytään Advanced Settings -välilehdelle ja syötetään DNS-osoite, joka on 10.0.0.1 (kuvassa 67). Siirrytään Firewall Settings -välilehdelle ja jätetään palomuuuri määrittelemättä (kuvassa 68). DHCP Server -välilehdeltä valitaan Ignore Interface -kohdasta "General setup". Sama tehdään myös IPv6 -verkolle. (kuvassa 69) Tallennetaan muutokset painamalla Save-paniketta.

## Kuva 67 OpenWrt custom dns

Interfaces » LAN

General Settings | Advanced Settings | Firewall Settings | DHCP Server

Force link: ☒ Set interface properties regardless of the link carrier (If set, carrier sense events do not invoke hotplug handlers).

Use default gateway: ☒ If unchecked, no default route is configured

Use custom DNS servers: ☒ 10.0.0.1

DNS search domains:

DNS weight: 0 The DNS server entries in the local resolv.conf are primarily sorted by the weight specified here

Use gateway metric: 0

Override IPv4 routing table: unspecified

Override IPv6 routing table: unspecified

Delegate IPv6 prefixes: ☒ Enable downstream delegation of IPv6 prefixes available on this interface

IPv6 assignment length: 60 Assign a part of given length of every public IPv6-prefix to this interface

IPv6 assignment hint: 0 Assign prefix parts using this hexadecimal subprefix ID for this interface.

IPv6 prefix filter: -- Please choose --

## Kuva 68 OpenWrt Firewall Settings

Interfaces » LAN

General Settings Advanced Settings **Firewall Settings** DHCP Server

Create / Assign firewall-zone unspecified

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *custom* field to define a new zone and attach the interface to it.

Dismiss Save

## Kuva 69 OpenWrt DHCP

Interfaces » LAN

General Settings Advanced Settings Firewall Settings **DHCP Server**

General Setup Advanced Settings IPv6 Settings IPv6 RA Settings

Ignore interface ☒ Disable DHCP for this interface.

Start  Lowest leased address as offset from the network address.

Limit  Maximum number of leased addresses.

Lease time  Expiry time of leased addresses, minimum is 2 minutes (2m).

Dismiss Save

## Kuva 70 Interfaces-määrittäminen valmis

Interfaces Devices Global network options

**Interfaces**

<b>LAN</b>  br-lan	Protocol: Static address Interface has 7 pending changes	Restart Stop <b>Edit</b> Delete
<b>WAN</b>  Not present	Interface is marked for deletion	Restart Stop <b>Edit</b> Delete
<b>WAN6</b>  Not present	Interface is marked for deletion	Restart Stop <b>Edit</b> Delete

[Add new interface...](#)

Apply unchecked Save Reset

Powered by LuCI openwrt-21.02 branch (git-21.231.26241-422c175) / OpenWrt 21.02.0 r16279-5cc0535800

Määrittysten jälkeen on vaihtoehtona painaa Save & Apply -painiketta. Tällöin OpenWrt-ohjelmisto käy läpi asetusten oikeellisuuden. Valitettavasti Rollback-ominaisuus palauttaa alkuperäiset asetukset ristiriitojen vuoksi takaisin. Asetukset tallennetaan valitsemalla (kuvassa 65) näkyvän Apply & Save -painikkeen oikealta puolelta olevasta nuolesta "Apply

unchecked ”ja näpäyttämällä lopuksi painiketta (kuvassa 70). Asetusten määrittämisen jälkeen laite liitetään osaksi lähiverkkoa ja hallintaliittymä löytyy osoitteesta 10.0.1.2.

Seuraavaksi lähdetään luomaan wlan-verkkoa. Valitaan ”Wireless Overview”- näkymästä ”5Ghz radio (radio)” ja painetaan Edit-painiketta (kuvassa 71). Koska työssä määritellään kaksi tukiasemaa, tulee seuraavien asetusten olla identtiset molemmissa laitteissa käytettävää kanavaa lukuun ottamatta. Työssä käytetään kahta ”Non over Flap Channelia”, jotka ovat 52 ja 64. Tiedonsiirtotaajuus on 80mhz. Trasmit Power rajataan 20dBm, jotta saadaan paremmin tukiaseman vaihto suoritettua ja pidetään verkon suorituskyky hyvänä. Kohdassa ESSID annetaan verkolle haluttu nimi (kuvassa 72).

Kuva 71 Wireless Overview

The screenshot displays the 'Wireless Overview' section of the LuCI web interface. It lists two wireless interfaces: 'radio0' and 'radio1'. 'radio0' is active and shows details for Qualcomm Atheros QCA9886 802.11nac, including channel (auto 5.000 GHz) and bitrate (? Mbit/s). 'radio1' is inactive, showing 'Device is not active' for Qualcomm Atheros QCA9560 802.11bgn. Below the interface list is an 'Associated Stations' table, which is currently empty with the message 'No information available'. At the bottom right, there are three buttons: 'Save & Apply', 'Save', and 'Reset'.



## Kuva 72 General Setup

Wireless Network: Master "Vasama\_5G" (wlan0)

### Device Configuration

General Setup Advanced Settings

Status

-63/-106 dBm

Mode: Master | SSID: Vasama\_5G  
BSSID: C0:06:C3:25:C9:23  
Encryption: mixed WPA/WPA2 PSK (CCMP)  
Channel: 48 (5.240 GHz)  
Tx-Power: 21 dBm  
Signal: -63 dBm | Noise: -106 dBm  
Bitrate: 607.5 Mbit/s | Country: FI

Wireless network is enabled Disable

Operating frequency

Mode	Channel	Width
AC	48 (5240 Mhz)	80 MHz

Maximum transmit power 21 dBm (125 mW) - Current power: 21 dBm

Specifies the maximum transmit power the wireless radio may use. Depending on regulatory requirements and wireless usage, the actual transmit power may be reduced by the driver.

### Interface Configuration

General Setup Wireless Security MAC-Filter Advanced Settings

Mode Access Point

ESSID Vasama\_5G

Network lan: 8

Choose the network(s) you want to attach to this wireless interface or fill out the custom field to define a new network.

Hide ESSID ☐

Where the ESSID is hidden, clients may fail to roam and airtime efficiency may be significantly reduced.

WMM Mode ☒

Where Wi-Fi Multimedia (WMM) Mode QoS is disabled, clients may be limited to 802.11a/802.11g rates.

Dismiss Save

Kohdasta "Interface Configuration" syötetään salaustyyppi. Suositeltavaa on käyttää WPA3, mikäli talouden kaikki laitteet tukevat tätä. Muussa tapauksessa valitaan WPA-PSK/WAP-PSK mixed Mode. Lisäksi valitaan Cipher – Force CCMP (AES), jolloin käytetään parempaa salausta, jos mahdollista. Syötetään haluttu verkon salausavain kohtaan "Key". Otetaan käyttöön 802.11r Fast Transition -protokolla. Syötetään Mobility Domain- kohtaan 4-merkinen heksadesimaaliluku. Luvun tulee olla sama molemmissa tukiasemissa, jotta roaming-ominaisuus saadaan käyttöön (kuvassa 73).

## Kuva 73 Interface Configuration

Interface Configuration

General Setup

Wireless Security

MAC-Filter

Advanced Settings

Encryption

WPA-PSK/WPA2-PSK Mixed Mode

Cipher

Force CCMP (AES)

Key

802.11r Fast Transition

☒

Enables fast roaming among access points that belong to the same Mobility Domain

NAS ID

Mobility Domain

AB11

4-character hexadecimal ID

Reassociation Deadline

1000

time units (TUs / 1.024 ms) [1000-65535]

FT protocol

FT over DS

Generate PMK locally

☒

When using a PSK, the PMK can be automatically generated. When enabled, the R0/R1 key options below are not applied. Disable this to use the R0 and R1 key options.

R0 Key Lifetime

10000

minutes

R1 Key Holder

00004f577274

6-octet identifier as a hex string - no colons

PMK R1 Push

☐

Interface Advanced Settings -välilehdeeltä syötetään vielä maakoodi, jolla tukiasema osaa rajata Suomessa kielletyt radiotaajuuudet pois. Lopuksi painetaan "Save" ja käynnistetään radio (kuvassa 71) valitsemalla "Enable" ja tallennetaan kaikki asetukset valitsemalla "Save & Apply" (kuvassa 74).

## Kuva 74 Interface Advanced Settings

Wireless Network: Master "OpenWrt" (radio0.network1)

Device Configuration

General Setup

Advanced Settings

Country Code

FI - Finland

Coverage cell density

Disabled

Configures data rates based on the coverage cell density. Normal configures basic rates to 6, 12, 24 Mbps if legacy 802.11b rates are not used else to 5.5, 11 Mbps. High configures basic rates to 12, 24 Mbps if legacy 802.11b rates are not used else to the 11 Mbps rate. Very High configures 24 Mbps as the basic rate. Supported rates lower than the minimum basic rate are not offered.

Distance Optimization

auto

Distance to farthest network member in meters.

Fragmentation Threshold

off

RTS/CTS Threshold

off

Force 40MHz mode

☐

Always use 40MHz channels even if the secondary channel overlaps. Using this option does not comply with IEEE 802.11n-2009!

Beacon Interval

100



## 5.2 Mittaustulokset

Tarkasteltaessa mittaustuloksia (kuvassa 76), voidaan havaita päivitettyillä laitteilla saavutettavan 88 % nopeampi yhteys koko talossa kuin vanhalla laitteella. Langaton lähiverkkoyhteys jäi kuitenkin keskiarvollisesti 40 % langallista verkkoa hitaammaksi. Nopeudet ovat laskettu käyttämällä Speedtest-palvelua. Signaalinarvot saatiin Windowsin omasta verkon statistiikasta. Kehityskohdetta tarkasteltaessa numeroiden valossa keittiön tiedonsiirtonopeudessa ei tapahtunut merkittävää nousua. Tämän voisi korjata sijoittaa vielä kolmannen tukiaseman keittiöön.

Kuva 76 Mittaustulokset

dBm	Keittiö	Työhuone (MH1)	MH2	Olohuone	MH3	Työhuone	Kodinhuone	Sauna
Peking_5G (Huawei)	-70	-60	-50	-49	-52	-60	-96	-101
Vasama_5G (AP1)	-60	-33	-57	-50	-37	-54	-72	-76
Vasama_5G (AP2)	-59	-78	-71	-45	-52	-31	-59	-49

Mbps	Keittiö	Työhuone (MH1)	MH2	Olohuone	MH3	Työhuone	Kodinhuone	Sauna
Peking_5G (Huawei)	120	110	130	220	160	150	13	14
Vasama_5G (AP1)	120	240	230	240	110	60	40	56
Vasama_5G (AP2)	110	86	67	240	240	250	160	240

Mbps	Kytin
Langallinen	300

Keskiarvo	dBm
Huawei	-67
Vasama_5G (AP1)	-55
Vasama_5G (AP2)	-56

Keskiarvo	Mbps
Huawei	115
Vasama_5G (AP1)	137
Vasama_5G (AP2)	174
Vasama_5G (merkitsevät)	215

Nopeusero Vasama_5G vert Huawei (%)	88
Nopeusero langallinen yhteys vert Vasama_5G (%)	40

## 5.3 Hinnat

Opinnäytetyössä käytettävien laitteistojen hinnat jakautuvat alla olevan taulukon mukaisesti (taulukossa 1). Merkillepantavaa on 5G-reitittimen melko korkea hankintahinta.

Kokonaiskustannukseksi opinnäytetyölle kertyi 772,30 €.

Taulukko 1 laitteiston hinnat

Selite	Malli	Hinta
5G-reititin	Huawei 5G CPE Pro2	420 €
pfSense-reittimen emolevy	PC Engines APU2E5	200 €

pfSense-reitittimen virtälähde	AC Power Adapter for APU Boards	6,20 €
pfSense-reitittimen kotelo	APU Chase	12,90 €
pfSense-reitittimen tallennusmedia	16GB mSATA SSD	19,50 €
2x wlan-reititin	TP-LINK Acher C6 Dual-band	85,80 €
Kytkin, 8-porttia	TP-LINK TL-SG108	27,90 €

## 5.4 NMAP-porttiskannaus

Tietoturvan varmistamiseksi työssä käytettiin NMAP-porttiskannaustyökalun online-versiota. Porttiskannauksen avulla saadaan selvitettyä, onko pfSensen palomuuuri asennettu oikein ja avonaisia portteja ei ole jäänyt ulkopuolisten käyttöön. Kaikki löydettyt portit ovat filtered-tilassa eli NMAP ei pysty määrittelemään, ovatko ne auki vai kiinni. Tämä johtuu siitä, että ohjelma ei saa palomuurilta paluusanomaa, eli yhteyttä ei estetä, eikä sallita (kuvassa 77). Tämä esiintyy yleensä silloin, kun palomuuuri rajoittaa liikennettä. (Nmap.org, n.d.)

Kuva 77 NMAP

```
Host is up.
PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
80/tcp    filtered  http
110/tcp   filtered  pop3
143/tcp   filtered  imap
443/tcp   filtered  https
3389/tcp  filtered  ms-wbt-server
```

## 5.5 Snort testaus ja pohdinta

pfSense tarjoaa oletuksena todella hyvät palomuuriominaisuudet, sillä oletuksena kaikki ulkoapäin tuleva verkkoliikenne on lähtökohtaisesti estetty. Snort-järjestelmän testausta pohdittaessa testijaksolla järjestelmän lokeihin ei tallentunut merkillepantavia hälytyksiä. Lähdin purkamaan asiaa sallimalla pfSensen vastata ping-kyselyyn, joka altistaa reitittimen hyökkäyksille.

Testausta varten palomuuriin on luotava uusi sääntö, joka sallii IPv4 ICMP-yhteyden (kuvassa 78). Muutaman tunnin odottelun jälkeen Snortin hälytyslistaan alkoi tulla tuloksia, kun tunkeutumisenestojärjestelmä havaitsee ICMP-protokollassa epävallista ping-liikennettä (kuvassa 79).

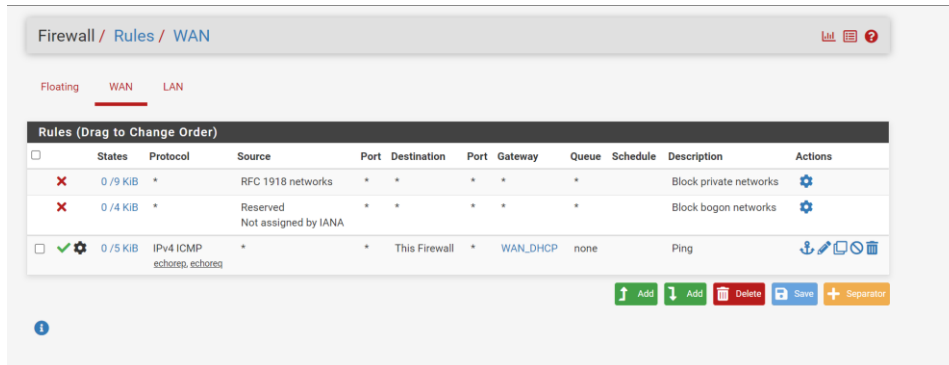
Tapahtuman Security Identifier (SID) tunnisteella 1-29456 löytyy Snortin dokumentaatiosta Cisco Talos Intelligence Groupin laatima sääntödokumentti. Dokumentissa kerrotaan hälytyksen aiheutuneen epätavallisesta ping-liikenteestä, joka ei noudata normaalia kaavaa.(Snort.org, n.d.)

Sääntöluokassa kerrotaan Snortin varoittavan Internet Control Message Protocol (ICMP) - liikenteestä, jonka avulla palvelun isännät (host) voivat lähettää virheilmoituksia liikenteen katkoksista. Järjestelmänvalvojat voivat käyttää ICMP:tä diagnostiikkaan ja vianmääritykseen, mutta myös hyökkääjät voivat käyttää protokollaa tiedon hankkimiseen verkossa. Tämä protokolla on alttiina useille hyökkäyksille ja monet järjestelmänvalvojat estävät sen kokonaan tai estävät valikoidut viestit. (Snort.org, n.d.).

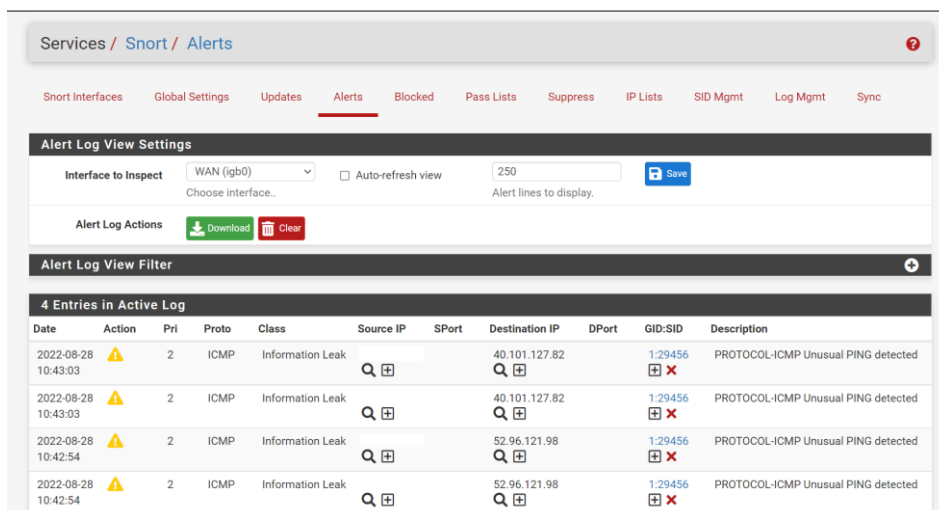
Johtopäätöksenä voidaan todeta Snortin toimivan ja suojaavan käyttäjiä verkon uhilta. Tämä tuo myös turvaa, mikäli palomuuriin täytyy avata portteja verkkoliikenteelle tietyille palveluille. Oletuksena Snort toimii tunkeutumisen estojärjestelmänä (IDS), mikäli käyttäjä ottaa käyttöön asetuksen ”Block Offenders” (kuvassa 50) astuu järjestelmän IPS-määritykset voimaan, jolloin havaittu tunkeutuminen myös estetään. Aloitteleva käyttäjä voi mahdollisesti alkuun lamauttaa verkon palveluita, mikäli Snort tulkitsee nämä haitalliseksi. Otettaessa käyttöön IPS-suojausta tulisi aina alkuun monitoroida verkon liikennettä esimerkiksi viikon ajan ja katsoa mitä havaintoja IDS-lokeihin tulee. Analysoimalla nämä

ilmoitukset käyttäjä voi sallia tietyt virheelliset havainnot ja ottaa varsinaiset IPS-toiminnon käyttöön, ilman että verkon käytettävyys kärsii.

Kuva 78 ICMP-sääntö



Kuva 79 Snort Alerts



## 6 Yhteenveto

Opinnäytetyössä saatiin toteutettua tietoturvallinen lähiverkko kotiin huomioiden nykyajan vaatimukset. Käytettäessä avoimen lähdekoodin järjestelmiä on huomioitava myös se, että tietoturvallinen kotiverkko vaatii aktiivista havainnointia laitteiston päivitysten osalta.

Operaattoreiden laitteet päivittyvät automaattisesti. Käytettäessä opinnäytetyössä mainittuja sovelluksia tulee päivittää manuaalisesti hallintaliittymän kautta, mikäli palveluntarjoajan tuottama päivitys on saatavilla. Tietoturvallinen kotiverkko saadaan toteutettua opinnäytetyön ohjeilla, sekä sillä, että käyttäjä on valveutunut ja huolehtii laitteiden päivittämisestä säännöllisesti.

5G-yhteys saatiin asennettua sille optisimpaan sijaintiin peilaten operaattorin 5G-tukiasemaa. Liittymän konfiguraatio ja lisäpalveluiden käyttöönotto, kuten julkinen IP-osoite onnistui hyvin.

Langaton lähiverkko koostui kahdesta wlan-reitittimestä, joihin asennettiin avoimen lähdekoodin OpenWrt-ohjelmisto. Tukiasemat muodostavat koko asunnon kattavan kokonaisuuden hyödyntäen nopeaa siirtymää, Fast Transit, jolla saadaan viiveetön tukiaseman vaihto liikkeessä asunnossa. Mittaustuloksissa verkon nopeus kasvoi 88 % verrattuna vanhaan verkkoratkaisuun. Lisäksi OpenWrt tarjoaa järjestelmäpäivitysten osalta tukea kauaksi tulevaisuuteen, jolloin laitteen elinkaari pitenee.

Lähiverkon sydämeksi asennettiin pfSense-palomuurijärjestelmä, joka koottiin käsin komponenteista. pfSense-järjestelmä huolehtii koko kodin tietoliikenteen reitittämisestä ja monitoroinnista. pfSensen laaja lisäosavalikoima mahdollisti tietoturvaan panostamisen. Snort Intrusion Prevention System (IPS)-järjestelmä mahdollistaa vielä yhden kerroksen turvallisuutta palomuurin lisäksi pyrkien estämään hyökkäyksiä ja haitallisia sivustoja.

Opinnäytetyö vastasi hyvin sille annettuihin tutkimuskysymyksiin. Opinnäytetyön kautta todettiin, että avoimenlähdekoodin ohjelmistoja voidaan hyödyntää käyttämällä niitä kotiloissa kaupallisten laitteiden kanssa. Tämän kaltaisten ohjelmistojen käyttö parantaa laitteiden tietoturvaa ja elinkaarta, jos niitä käytetään, kuten opinnäytetyössä on aihetta käsitelty. Opinnäytetyön toteutustavalla koko asunnon kattava langaton lähiverkko on



mahdollista toteuttaa kotioloihin tietoturvalisesti. Myös verkon suorituskyky paranee merkittävästi operaattorin yleisesti käyttämineen laitteisiin verrattuna.

Kehitysehdotuksena voisi jatkossa tutkia mitä uusia ominaisuuksia Wi-Fi-6-verkko tuo nopeampien 5G yhteyksien rinnalle. Toinen mahdollinen kehityskohta olisi tuoda säännöllisesti automaattisesti päivittyvät suojauspäivitykset laitteille, jolloin verkon haavoittuvuuksia voidaan pienentää entistä enemmän.

## Lähteet

Batard, P. (2021). *Rufus - Create bootable USB drives*. Batard Pete .

<https://rufus.ie/en/#>

Brunoli, J. (2022, January 20). *European Commission wants EU to build its own DNS infrastructure*. Dolphin Publications B.V.

<https://www.techzine.eu/news/infrastructure/71552/european-commission-wants-eu-to-build-its-own-dns-infrastructure/>

CellMapper. (2022). *Elisa (Finland) - Cellular Coverage and Tower Map*. CellMapper.

<https://www.cellmapper.net/map?MCC=244&MNC=5&type=LTE&latitude=61.55721537547089&longitude=23.675101830895684&zoom=14.69631377550249&showTowers=true&showTowerLabels=true&clusterEnabled=true&tilesEnabled=true&showOrphans=false&showNoFrequencyOnly=false&showFrequencyOnly=false&showBandwidthOnly=false&DateFilterType=Last&showHex=false&showVerifiedOnly=false&showUnverifiedOnly=false&showLTECAOnly=false&showENDCOnly=false&showBand=0&showSectorColours=true&mapType=roadmap>

Chiark.greenend.org.uk. (2022). *PuTTY FAQ*. PuTTY FAQ.

<https://www.chiark.greenend.org.uk/~sgtatham/putty/faq.html#faq-what>

Delgado, C. (2017, March 8). *How to hack a Wi-Fi Network (WPA/WPA2) through a Dictionary attack with Kali Linux*. Our Code World.

<https://ourcodeworld.com/articles/read/407/how-to-hack-a-wi-fi-network-wpa-wpa2-through-a-dictionary-attack-with-kali-linux>

Electric Sheep Fencing. (2022). *Learn About the pfSense Project*. Electric Sheep Fencing, LLC. <https://www.pfsense.org/about-pfsense/>

Electric Sheep Fencing LLC and Rubicon Communications LLC. (2022). *Hardware — Connect to the Console*. Electric Sheep Fencing LLC and Rubicon Communications LLC. <https://docs.netgate.com/pfsense/en/latest/hardware/connect-to-console.html>

Elisa. (2022a). *Huawei 5G CPE Pro 2*. Elisa.

<https://elisa.fi/asiakaspalvelu/aihe/mobiililaajakaista/ohje/huawei-5g-cpe-pro-2/>

Elisa. (2022b). *Mobiililaajakaistan julkinen IP-osoite*. Elisa.

<https://elisa.fi/asiakaspalvelu/aihe/mobiililaajakaista/ohje/ip-osoitteet/>

Elisa. (2022c). *Saunalahti Mobiililaajakaista 5G 300M*. Elisa.

<https://elisa.fi/kauppa/nettiliittymat/mobiililaajakaista?5G=true>

HomeTechHacker. (2018, August 23). *6 Reasons to Use a pfSense Home Router*.

HomeTechHacker. <https://hometechhacker.com/pfsense-home-router/>

Huotari, A. (2015, April 27). *What is 802.11r? Why is this Important?* Cisco Blogs.

<https://blogs.cisco.com/networking/what-is-802-11r-why-is-this-important>

Kaspersky Lab. (n.d.). *Kuinka turvallinen kotiverkko määritetään*. Kaspersky.Fi. Retrieved

August 26, 2022, from <https://www.kaspersky.fi/resource-center/preemptive-safety/how-to-set-up-a-secure-home-network>

Malmelin, S. (2021, September 23). *Helpot niksit – näin teet kotinetistäsi*

*tietoturvallisemman*. Dna.Fi/Blogi. <https://www.dna.fi/blogi/-/blogs/helpot-niksit-nain-teet-kotinetistasi-tietoturvallisemman>

Myip.fi. (n.d.). *myip.fi*. Myip.Fi. Retrieved February 17, 2022, from <https://myip.fi/>

Nmap.org. (n.d.). *Port Scanning Basics*. Port Scanning Basics. Retrieved August 12, 2022,

from <https://nmap.org/book/man-port-scanning-basics.html>

Openwrt.org. (2021, September 4). *Welcome to the OpenWrt Project*. OpenWrt.

<https://openwrt.org/>

Palo Alto Networks. (2022). *What is an Intrusion Prevention System?* Palo Alto

Networks. <https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips>

PC Engines GmbH. (2022). *PC Engines apu4d4 product file*. PC Engines GmbH.

<https://pcengines.ch/apu4d4.htm>

Qualcomm Technologies. (2022). *What is 5G*. Qualcomm Technologies, Inc.

<https://www.qualcomm.com/5g/what-is-5g>

Rami, S. (2021, May 6). *Top 10 Apache License Questions Answered*. WhiteSource

Software. <https://www.whitesourcesoftware.com/resources/blog/top-10-apache-license-questions-answered/>

SignalBoosters. (2020, October 29). *What are IEEE 802.11 Standards?*

Signalboosters.Com/Blog. <https://www.signalboosters.com/blog/ieee-802.11-standards-explained-802.11abgnacax/>

Snort.org. (n.d.). *Snort Rule Docs*. Snort Rule Docs. Retrieved September 4, 2022, from

[https://www.snort.org/rule\\_docs/1-29456](https://www.snort.org/rule_docs/1-29456)

Telia. (2022a). *Huawei CPE Pro 5G-modeemin käyttöohje*. Telia.

<https://www.telia.fi/asiakastuki/laitteet/huawei-cpe-pro-5g-modeemi#huawei-cpe-pro-5g-kayttoonotto>

Telia. (2022b). *Nokia Fastmile 5G-reititin*. Telia.

<https://www.telia.fi/asiakastuki/laitteet/nokia-fastmile-5g-reititin#nokia-fastmile-5g-hallintasivu>

TP-Link Corporation Limited. (2022). *Archer C6 / AC1200 Wireless MU-MIMO Gigabit Router*. TP-Link Corporation Limited. <https://www.tp-link.com/fi/home-networking/wifi-router/archer-c6/#specifications>

## **Liite 1: Aineistohallintasuunnitelma**

### Aineistohallintasuunnitelma

Opinnäytetyö kirjoitetaan henkilökohtaisella työasemalla, joka on varmuuskopioitu Google Drive-pilvipalveluun. Työssä kerätyt tutkimustulokset on myös tallennettu Googlen pilvipalveluun.

Opinnäytetyö on tehty yksityishenkilölle, eikä se pidä sisällään salassa pidettävää aineistoa.

Omistan itseni opinnäytetyöni aineiston ja tulokset.