Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

ONNI LEHIKOINEN

OPNsense palomuurin käyttöönotto ja konfigurointi kotiverkkoon

TIETOJENKÄSITTELYN TUTKINTO-OHJELMA
2024

TIIVISTELMÄ

Lehikoinen, Onni: OPNsense palomuurin käyttöönotto ja konfigurointi kotiverkkoon
Opinnäytetyö, AMK
Tietojenkäsittely
Maaliskuu 2024
Sivumäärä: 30

Tämän opinnäytetyön tavoitteena oli asentaa OPNsense reititys- ja palomuurijärjestelmä toimimaan kotiverkon palomuurina sekä käydä teoriassa läpi OPNsensen ominaisuuksia, joita ei otettu käyttöön tässä asennuksessa. Tarkoituksena oli myös tutkia, onko OPNsense kannattava asentaa kotiverkkoon palomuuriksi.

Opinnäytetyössä palomuuriin konfiguroitiin tärkeimmät ominaisuudet, joita kotiverkossa tarvitaan. Tarkoituksena näyttää lukijalle, miten palomuurin konfigurointi tapahtuu ja mitä siihen vaaditaan. Palomuuriksi valikoitui OPNsense, koska se oli ilmainen avoimen lähdekoodin järjestelmä, jota oli suositeltu ja kehuttu internetissä.

Lopputuloksena saatiin toimiva palomuuriratkaisu kotiverkon suojaksi. Opinnäytetyötä on mahdollista käyttää ohjeena OPNsenseä asentaessa. Opinnäytetyössä palomuuriin saatiin konfiguroitua hyvät perusominaisuudet, joista on hyvä lähteä räätälöimään palomuuria omiin tarpeisiinsa.

Avainsanat: OPNsense, palomuuri, reititin, tietoturva, VPN

Abstract

Lehikoinen, Onni: OPNsense firewall setup and configuration to home network
Bachelor's thesis
Business Information Systems
March 2024
Number of pages: 30

This thesis goal was to install OPNsense routing and firewall software to work as a home network firewall and in theory go through features that were not configured in this installation. Objective was to study, is OPNsense beneficial firewall for home network.

In this thesis firewall was configured with the most important features which are needed in home network. Objective was to show the reader, how to configure firewall and what is required for the installation. OPNsense was chosen as a firewall system because it is free and open-source system that was recommended and praised on the internet.

The result was a functional firewall for home network security. It is possible to use this thesis as a guide when installing OPNsense. In this thesis firewall was configured with important basic functions which gives ability to start customizing firewall to each one's own needs.

Keywords: OPNsense, firewall, router, information security, VPN

SISÄLLYS

SYMBOLI- JA LYHENNELUETTELO

VPN = Virtual Private Network on verkkojen teknologia, joka luo turvallisen ja salatun yhteyden kahden tai useamman laitteen välille internetin yli.

DDoS = Distributed Denial of Service ja se on tyyppi verkkohyökkäys, joka pyrkii tekemään verkko- tai verkkopalvelunsa saavuttamattomaksi tekemällä sen käyttäjille tai asiakkaille.

HTTP = HyperText Transfer Protocol on protokolla, jota käytetään tiedonsiirtoon internetissä.

OPNsense = Avoimen lähdekoodin palomuuri- ja reititysohjelmisto.

Client = Viittaa yleisesti tietokoneohjelmaan tai laitteeseen, joka pyytää palvelua tai resursseja toiselta ohjelmalta tai laitteelta, joka toimii palvelimena.

Caching = Tiedon tai resurssien väliaikaiseen tallentamiseen tarkoitettua muistia

Proxy = Välityspalvelin, joka välittää HTTP-pyyntöjä ja vastauksia.

Mbps = Megabittiä sekunnissa.

GB = Gigatavu

IP-osoite = Tunniste, joka määrittelee tietokoneen tai muun verkkoon kytketyn laitteen sijainnin ja identiteetin internetissä.

SSD = Solid state drive tarjoaa nopeampaa tallennustilaa mitä perinteisempi kiintolevy.

DNS = Domain Name System on järjestelmä, joka mahdollistaa verkkotunnusten muuntamisen IP-osoitteeksi.

DNSBL = DNS-based Blackhole List on järjestelmä, jota käytetään tunnistamaan ja estämään roskapostin lähettäjiä tai muita haitallisia toimijoita verkkoliikenteessä

NAT = Network Address Translation on tietoverkkojen tekniikka, jota käytetään muuntamaan IP-osoitteita toisiksi IP-osoitteiksi tietojen liikkuessa verkossa.

1 JOHDANTO

Tietoturvan tärkeys kotiverkoissa on noussut entistä tärkeämmäksi teknologian yleistymisen myötä. Nykyisin kodeissa on useita erilaisia laitteita tietokoneiden lisäksi kuten älypuhelimet, älytelevisiot, älyvalot ja älykaiuttimet. Kaikki laitteet, jotka ovat yhteydessä nettiin ovat alttiita erilaisille tietoturvauhkille. Tämän vuoksi on tärkeää suojata kotiverkko haitallisilta osapuolilta, esimerkiksi palomuurin avulla.

Opinnäytetyössä asennettiin OPNsense palomuuri- ja reititysohjelmisto virtualisoituun ympäristöön, jossa päästiin kokeilemaan erilaisia konfiguraatioita ja asetuksia palomuurille sekä varmistamaan niiden toimivuus. Asennus suoritettiin virtuaaliympäristöön, jotta pystyttiin tutkimaan, onko OPNsenseä kannattava asentaa kotiverkon hallintaan reitittimeksi sekä palomuuriksi. Opinnäytetyössä käydään läpi palomuurien eroavaisuuksia sekä niiden historia lyhyesti.

Työssä esitellään OPNsensen ominaisuudet, läpikäydään laitteistovaatimukset sekä konfigurointimahdollisuuksia. OPNsense asennettiin toimimaan kotiverkon palomuurina ja hallintalaitteistona. Asennuksessa keskityttiin kotiverkossa tarvittavien sekä hyödyllisten ominaisuuksien käyttöönottoon ja ominaisuuksien konfigurointiin kuten VPN, mainosten esto ja tunkeilijan havaitsemisjärjestelmä.

2 VERKKOTURVALLISUUS

Verkkoturvallisuus on kyberturvallisuuden osa-alue, joka sisältää laitteistot, ohjelmistot käytännöt ja koulutuksen, joiden tarkoituksena on estää luvaton pääsy tietokoneverkkoihin.

Verkkoturvallisuuden tyyppejä ovat fyysinen-, hallinnollinen- ja tekninen verkkoturvallisuus. Fyysiseen verkkoturvallisuuteen kuuluvat prosessit ja työkalut, joilla estetään fyysinen pääsy verkkoon, esimerkkinä kulkukortin vaatiminen työtiloihin pääsemiseksi. Hallinnollisella verkkoturvallisuudella tarkoitetaan käytäntöjä ja käyttöoikeuksia, joilla määritellään mitä käyttäjät voivat tehdä verkossa. Tekniseen verkkoturvallisuuteen lukeutuu kaikki ohjelmistot ja laitteet, joilla valvotaan verkkoprosesseja tunkeilijoiden varalta ja estetään luvaton pääsy verkkoon. Kategoriaan kuuluvat muun muassa palomuurit ja virustorjuntaohjelmat. (NordVPN, n.d.)

Palomuurit ovat ohjelmistoja ja laitteistoja, jotka ovat tehty suodattamaan ja tutkimaan tietoa, jota internet-yhteyden kautta liikkuu. Palomuurityyppejä on useita erilaisia, joissa on erilaisia suodatustapoja. Vaikka jokainen palomuurityyppi suunniteltiin korvaaman edeltäjänsä, on suuri osa ydinteknologiasta siirtynyt sukupolvelta toiselle.

2.1 Palomuurit

Palomuuriksi määritellään laite, jonka läpi verkkoliikenne tapahtuu ja sillä kyetään estämään tai sallimaan tietynlainen verkkoliikenne. Palomuurin edeltäjinä toimivat reitittimet, joita käytettiin erottamaan verkkoja toisistaan. Reitittimeen tehdyillä konfiguraatioilla pystyttiin myös esimerkiksi estämään broadcast-protokollaa hidastamasta muiden kaistanlaajuutta. (Ingham, n.d.)

Ensimmäiset varsinaiset palomuurit kehitettiin 1980-luvulla. Cisco Systems ja Digital Equipment valmistamat ensimmäiset palomuurit toimivat network layer

tasolla ja suodattivat paketteja perusinformaation perusteella kuten lähteen- ja kohteen mukaan.

Web application firewall (WAF) on palomuuri, joka suojaa verkkosovelluksia valvomalla, suodattamalla ja estämällä haitallista verkkoliikennettä kuten palvelunestohyökkäyksiä ja evästemanipulointia. WAF kehitettiin 1990-luvun lopulla ja esti aluksi kiellettyjen merkkien lähetyksen sovellukselle. Nykyisin WAF suodattaa HTTP-liikennettä ja estää haitalliset pyynnöt palvelimelle. (Paloalto, n.d.-a)

Unified Threath Management (UTM) on palomuurityyppi, joka yhdistää palomuurin, virustorjunnan, tunkeilijan havaitsemisjärjestelmä (IDS) ja tunkeilijan estojärjestelmän (IPS) yhteen kokonaisuuteen. Ensimmäiset UTM-palomuurit tulivat 2000-luvun alussa ja toivat lisää turvaominaisuuksia kuten stateful packet inspection, joka sallii sisään ja ulostulevan liikenteen. Palomuurin IDS ja IPS havaitsevat sekä estävät haitallista liikennettä palomuurin läpi. (Paloalto, n.d.-b)

Next-Generation Firewall on uuden sukupolven palomuuri, jollaisen ensimmäisenä julkaisi Palo Alto Networks vuonna 2008 (Paloalto, n.d.). NGFW sisältää ominaisuuksia kuten application awareness eli sovellustietoisuus, IPS eli tunkeilijan estojärjestelmä, deep-packet inspection eli pakettien syvätarkastus. (Clark, 2021).

2.2 Avoimen lähdekoodin palomuurit

Avoimen lähdekoodin palomuureja löytyy useita erilaisia. Avoin lähdekoodi tarkoittaa, että palomuurin päivityksistä ja kehityksestä vastaa tuotteen ympärille kehittynyt yhteisö (Tushar, 2023).

Avoimen lähdekoodin määritelmän pääkohdat ovat seuraavat:

1. Ohjelman vapaata levittämistä tai jakamista ei saa estää.
2. Johdettujen teosten luominen ja levittäminen tulee olla sallittua.

3. Lisenssin on mahdollistettava kopiointi, jakaminen ja muokkaaminen ilman lisenssimaksuja.
4. Lisenssin on sallittava muutosten tekeminen ja johdannaisten teosten luominen.

(Vilmusenaho, 2011)

Erilaisia avoimen lähdekoodin palomuuriohjelmistoja on paljon. Esimerkkeinä OPNsense, pfsense, IPFire ja NG firewall. Monista löytyy samoja ominaisuuksia kuten VPN, tunkeilijanesto järjestelmä ja web filtering. Palomuuriohjelmistoista löytyy myös eroavaisuuksia. Eroavaisuuksia löytyy esimerkiksi käyttöliittymästä ja lisäosista. (Mutune, n.d.)

2.3 Suljetun lähdekoodin palomuurit

Suurien yritysten valmistamat palomuurit ovat suljetun lähdekoodin palomuureja, koska yritykset tekevät rahansa lisensoimalla palomuurin käyttöjärjestelmää sekä sen ominaisuuksia. Esimerkkinä Paloalto, jonka liiketoiminnan tuotosta 51 % tehtiin määräaikaisilla lisensseillä vuonna 2016 (Kalogeropoulos, 2017).

Suljetun lähdekoodin ohjelmistojen tietoturva perustuu sille, että mahdollisia koodivirheitä ei näe kuin ohjelmiston tuottaja. Avoimen lähdekoodin ohjelmistoissa asia on päinvastoin ja kaikki voivat tarkistaa lähdekoodin sisällön. (Laakso, 2015). Suljetun lähdekoodin palomuureja valmistavat muun muassa Cisco, Paloalto, Fortinet, Check Point ja SonicWALL. Suljetun lähdekoodin palomuurit sisältävät esimerkiksi pilvipohjaisia haittaohjelman analysointimenetelmiä kuten Paloalton Wildfire tai Cisco Talos, joiden avulla pystytään estämään Paloalton mukaan jopa 95 % tuntemattomista haittaohjelmista. (Paloalto, n.d.-e)

2.4 Palomuurin hyöty kotiverkossa

Palomuurin auttaa kotiverkon suojaamisessa. Palomuurilla kyetään tarkkailemaan verkkoliikennettä, joka saapuu verkkoon ja lähtee verkosta. Palomuuriin on mahdollista luoda erilaisia sääntöjä, joilla voidaan estää esimerkiksi palvelunestohyökkäyksiä sekä haittaohjelmien pääsy verkkoon. Palomuureista pystytään myös estämään mainokset sekä haitallisille sivuille pääsy. Erillinen palomuuri on hyödyllinen ihmiselle, joka osaa konfiguroida sen oikein ja päivittää ajankohtaiset päivitykset. Väärin konfiguroitu tai päivittämätön palomuuri on tietoturvariski. (Freda, 2022)

3 OPNSENSE OMINAISUUDET JA LAAJENNUKSET

3.1 OPNsensen historia

OPNsensen kehitys aloitettiin haarana pfsense-palomuurista ja m0n0wall-palomuurista vuonna 2014. Ensimmäinen täysi versio OPNsensestä julkaistiin 2015. OPNsensen perustaja on Deciso B.V., joka tuottaa palomuurilaitteistoa ja myy yrityslisenssejä OPNsenseen. OPNsense tarjoaa käyttäjilleen viikoittaisia tietoturvapäivityksiä ja vuosittain kaksi suurempaa päivitystä. (OPNsense, n.d.-a)

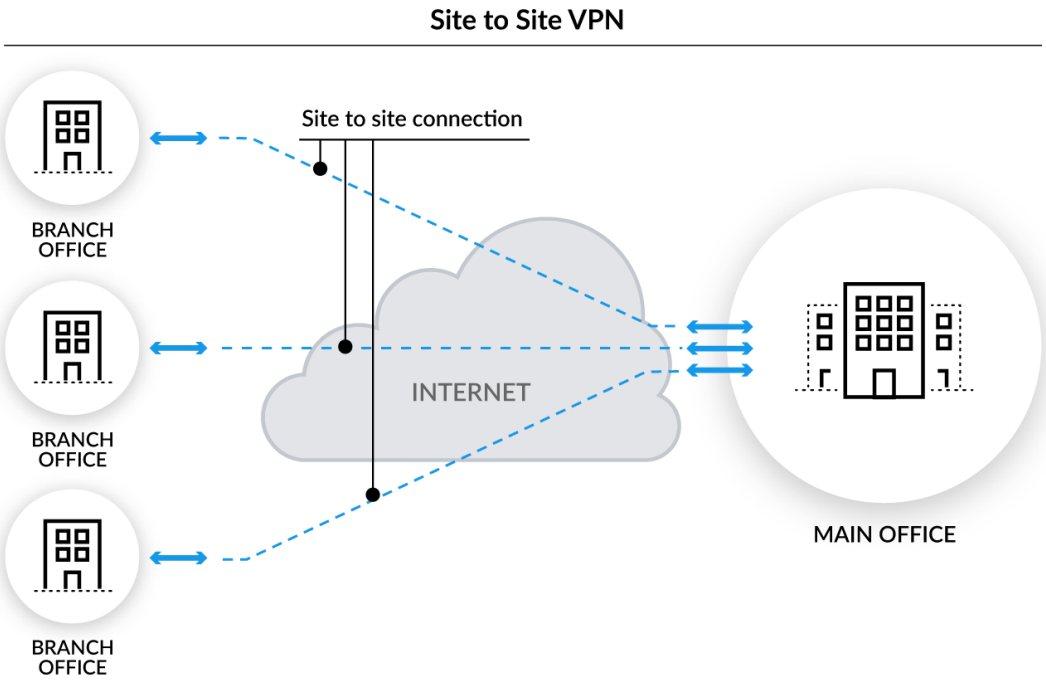
3.2 OPNsensen ominaisuudet

3.2.1 Virtual private network

VPN eli virtual private network on virtuaalinen erillisverkko, jonka avulla esimerkiksi yritysten verkkoja voidaan yhdistää julkisen verkon yli, luoden näennäisesti yksityisen verkon. (Paloalto, n.d.). VPN-toteutuksia on erilaisia, esimerkiksi site-to-site VPN, joka toimii yritysten eri toimipisteiden välillä ja mahdollistaa tiedon jakamisen turvallisesti internetin lävitse (kuva 1). Site-to-site

VPN voidaan toteuttaa kahdella tavalla. Intranet on lähiverkko, johon on yhdistetty useita toimipisteitä. Intranet-toteutuksessa eri konttorit voivat tehdä yhteistyötä ja jakaa tietoa toisilleen turvallisesti ja nopeasti. Toinen toteutustapa on extranet, joka tarkoittaa usean organisaation yhdistämistä yhdeksi lähiverkoksi. Extranetissä voidaan asettaa tietyt käyttöoikeudet jokaisen verkon väliin, jotta vain ennalta määritellyt resurssit ovat jaettuna. Extranet on usein käytössä esimerkiksi yrityksillä, jotka tekevät yhteistyötä muiden yritysten kanssa. Site-to-site yhteyden lisäksi on client-to-site yhteys, joka tarkoittaa yhteyttä esimerkiksi työntekijän- ja yrityksen verkon välillä. Client-to-site yhteydellä työntekijä pääsee käsiksi yrityksen tiedostoihin etätyöskennellessään. On olemassa myös VPN-sovelluksia, jolla voidaan yhdistää palveluntarjoajan palvelimille eripuolilla maailmaa, hyötynä on esimerkiksi verkkoliikenteen salaus ja mahdollisuus kiertää sijaintiestoja. Tämänlaisia palveluita tarjoavat muun muassa NordVPN, ProtonVPN ja ExpressVPN. (Microsoft, n.d.)

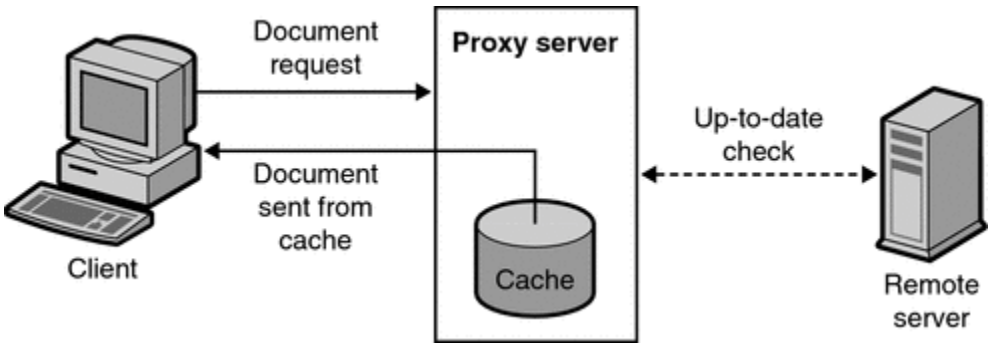
OPNsense tarjoaa paljon erilaisia VPN-teknologioita käytettäväksi lisäosiensa kautta kuten OpenVPN, IPSec, WireGuard ja Zerotier, jotka ovat erilaisia VPN-protokollia ja määrittävät miten yhteys salataan (OPNsense, n.d.-b). Jokainen VPN-protokolla keskittyy tiettyihin ominaisuuksiin, esimerkiksi viiveen minimointiin, tiedonsiirtonopeuteen, yhteyden vakauteen, tai vahvaan salaukseen. (Nakutavičiūtė, 2023)



Kuva 1. Esimerkki yrityksen käyttämästä site-to-site VPN-toteutuksesta (Palo-alto n.d.-c)

3.2.2 Forward Caching proxy

Forward caching proxy-palvelin sieppaa datapyynnöt asiakkaalta ja hakee tarvittavan tiedon web-palvelimelta. Forward Caching proxy-palvelin tallentaa sisältöä välimuistiin, ennen kuin toimittaa sen pyynnön tekijälle, jotta sisältö saadaan seuraavalla hakukerralla nopeammin toimitettua asiakkaalle (kuva 2). (IBM, 2023)



Kuva 2. Caching proxyn toiminta (Oracle Corporation, 2010)

3.2.3 Traffic shaping

Traffic shaping tai toiselta nimeltä packet shaping on ruuhkan hallinnassa käytetty metodi, jolla voidaan hidastaa epäolennaisten pakettien kulkua. Verkkoliikennettä voidaan hallita säätämällä verkkoon pääsevää liikennettä tai hallitsemalla verkosta ulos pääsevää liikennettä. (Froehlich, 2022)

OPNsense tukee verkkoliikenteen rajoittamista. OPNsensen avulla pystytään määrittämään kullekin liitännälle henkilökohtainen verkon nopeus. Verkkoliikenteen rajoittamisen hoitaa Dummynet, joka on verkkoemulointityökalu, joka luotiin alun perin verkkoprotokollien testaamiseen. (Rizzo, n.d.)

3.2.4 Vikasietoryhmä

OPNsense voidaan konfiguroida käyttämään vikasietoryhmään, jonka avulla voidaan yhdistää kaksi tai useampi palomuuria toisiinsa. Palomuurien ollessa samassa vikasietoryhmässä, toinen palomuuri ottaa hallinnan ensisijaisen palomuurin mennessä vikatilaan. (OPNsense, n.d.-c)

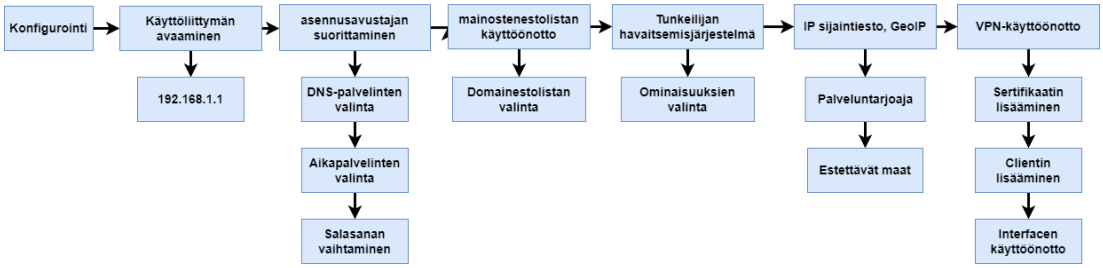
3.3 OPNsensen laajennukset

OPNsense tukee yhteisön luomia lisäosia sekä kolmannen osapuolen lisäosia, jotka ovat lisenssiltään maksullisia. Yhteisön luomiin lisäosiin kuuluvat muun muassa erilaiset VPN-lisäosat kuten Wireguard ja OpenConnect sekä erilaisia virustorjunta-lisäosia kuten ClamAV sähköposteille tai ICAP Anti Virus Engine Web selaukselle. (OPNsense, n.d.-c)

4 OPNSENSE PALOMUURIN ASENNUS

4.1 Työn tavoite

Tavoitteena suorittaa OPNsensen asennus ja käyttöönotto virtualisointiympäristössä, jossa voidaan varmentaa konfiguroinnin toimivuus ennen mahdollista tuotantoympäristöön asentamista. Tarkoituksena sekä antaa lukijalle kuva OPNsensen ominaisuuksista ja niiden käyttöönotosta (kuva 3). Lisäksi tarkoituksena on käydä läpi asennukseen liittyviä vaatimuksia ja termejä. Tavoitteena on myös tutkia, onko OPNsense järkevä ratkaisu kotiverkon palomuuriksi.



Kuva 3. OPNsense palomuurin konfigurointi

4.2 Laitteistovaatimukset

OPNsensen vähimmäisvaatimukset standardiominaisuuksilla, jotka eivät vaadi levylle kirjoittamista (kuva 4). Laitteistovaatimuksiin vaikuttaa pienin haluttu internetin nopeus ja halutut ominaisuudet. Suositellut laitteistovaatimukset, joilla kyetään suorittamaan kaikki OPNsensen perusominaisuuksista 350-750 mbps nopeudella, vaativat vähintään 8GB keskusmuistia, moniydinprosessorin sekä vähintään 120GB SSD tallennustilaa.

Processor	1 GHz dual core cpu
RAM	2 GB
Install method	Serial console or video (vga)
Install target	SD or CF card with a minimum of 4 GB, use nano images for installation.

Kuva 4. Laitteiston vähimmäisvaatimukset OPNsense asennukselle (OPNsense, n.d.-d).

4.3 OPNsensen asennus

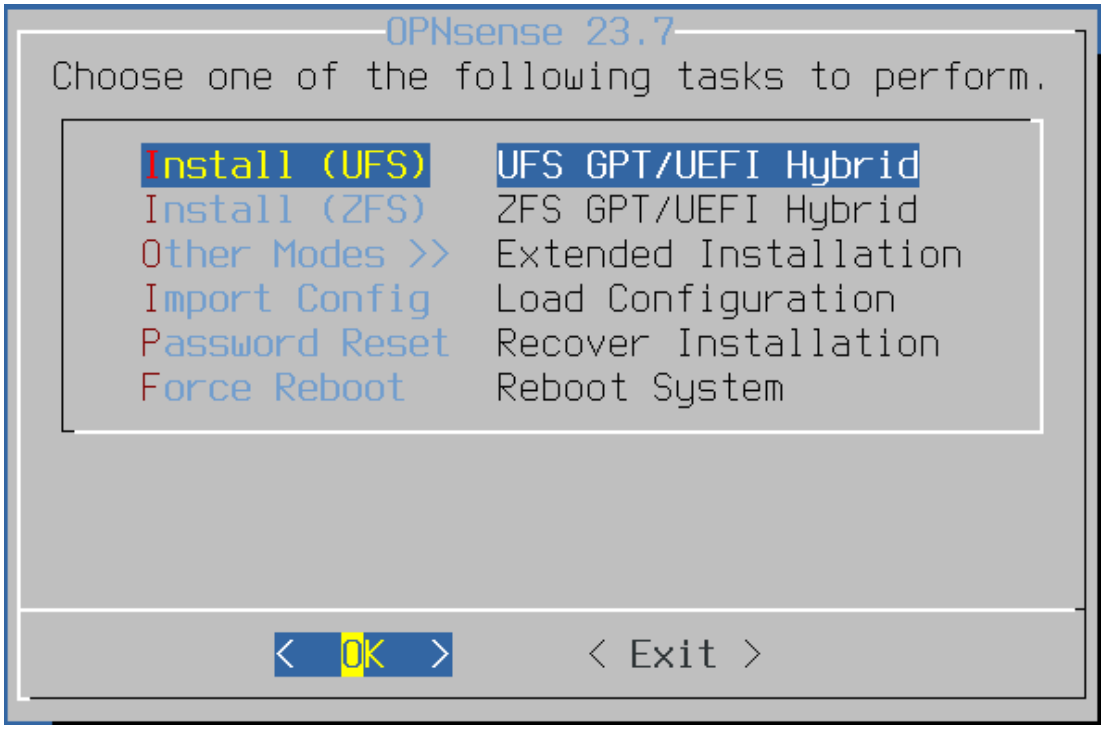
Työssä käytetään OPNsensen 23.7 amd64 versiota, joka asennetaan halutulle laitteistolle. Ladatulle asennusmedialle on syytä suorittaa checksum verification, jonka avulla varmistetaan tiedoston eheys. OPNsensen kotisivuilla kerrotaan checksum verification numerosarja, eli hash, joka tulisi saada suorittaessa komennot (kuva 5). Todettua komennosta saadun arvon olevan sama, kuin OPNsensen verkkosivuilla kerrotaan, voidaan todeta tiedoston olevan eheä.

```
PS C:\Users\onnil> cd desktop
PS C:\Users\onnil\desktop> certutil -hashfile OPNsense-23.7-dvd-amd64.iso sha256
SHA256 hash of OPNsense-23.7-dvd-amd64.iso:
bf67374d04fb00a29d80f9870ac86491b0a87d5dd386c2bd97def0691547e263
CertUtil: -hashfile command completed successfully.
```

Kuva 5. Checksum verification

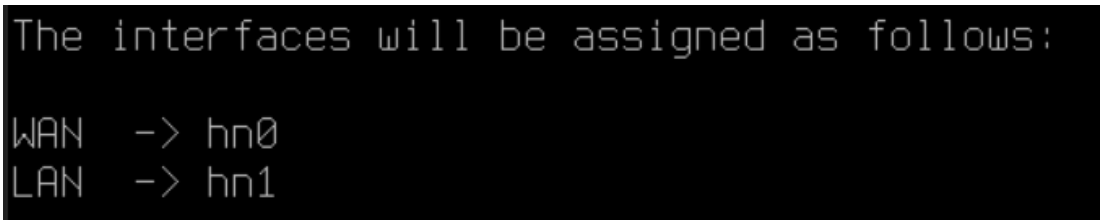
OPNsensen käynnistyttyä, voidaan jatkaa asennusta kirjautumalla sisään käyttäjätunnuksella installer, salasanalla OPNsense tai jatkaa ilman kovalevylle asentamista, eli live modessa, kirjautumalla käyttäjälle root. Tässä asennuksessa suoritetaan OPNsense installer, ensimmäisenä asennusavustaja pyytää valitsemaan näppäimistökielen, etsitään valikosta suomi. Toisessa vaiheessa valitaan tiedostojärjestelmä (kuva 6). Valitaan joko UFS tai ZFS, UFS eli unix file system on tiedostojärjestelmä, jossa ei ole tiedostojen eheys tarkistuksia ja on vanhempi tiedostojärjestelmä. ZFS on moderni

tiedostojärjestelmä, joka tukee datan eheyden tarkistuksia, ominaisuuksissa on myös muita eroja, mutta asennuksessa käytetään ZFS tiedostojärjestelmää. Kolmannessa vaiheessa valitaan mahdollinen redundanssi levylle, redundanssilla pyritään estämään tiedostojen korruptoitumista. Käytetään stripe-ominaisuutta, jotta saadaan kaikki tallennustila käyttöön. Neljännessä kohdassa valitaan levy, jolle asennus suoritetaan, tässä tapauksessa da0. Viidennessä kohdassa voidaan vielä vaihtaa root käyttäjän salasana, valitaan exit and reboot.



Kuva 6. Tiedostojärjestelmän valinta.

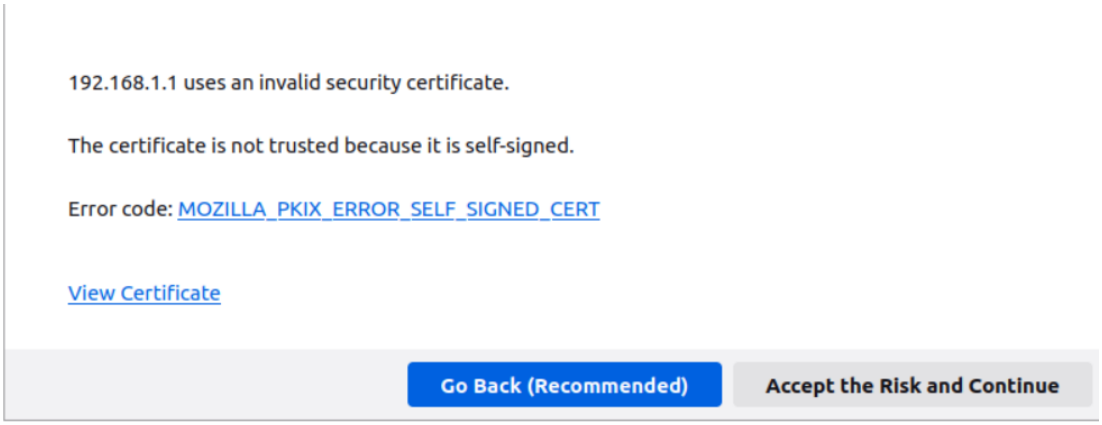
Sammutetaan OPNsense ja poistetaan asennusmedia, jonka jälkeen voidaan käynnistää OPNsense uudelleen. Kirjaudutaan sisään käyttäjänä root ja salananana opnsense ja vaihdetaan verkkosovitin portit oikeiksi LAN- sekä WAN-verkoille (kuva 7). Valitaan Assign interfaces ja ei konfiguroida LAGG ominaisuutta tai VLAN-verkkoja, vain WAN- ja LAN-interfaces.



Kuva 7. Verkkosovittimien konfigurointi

4.4 OPNsensen konfigurointi

OPNsensen ominaisuuksia konfiguroidaan nettiselaimella käytettävästä graafisesta käyttöliittymästä, jonne yhdistetään LAN-IP-osoitteen avulla (192.168.1.1 tai itsevalitun IP-osoitteen avulla) sisäverkossa olevalta koneelta. Ensimmäistä kertaa yhdistäessä nettiselain varoittaa sertifikaattivirheestä (kuva 8). Hyväksytään ja jatketaan.

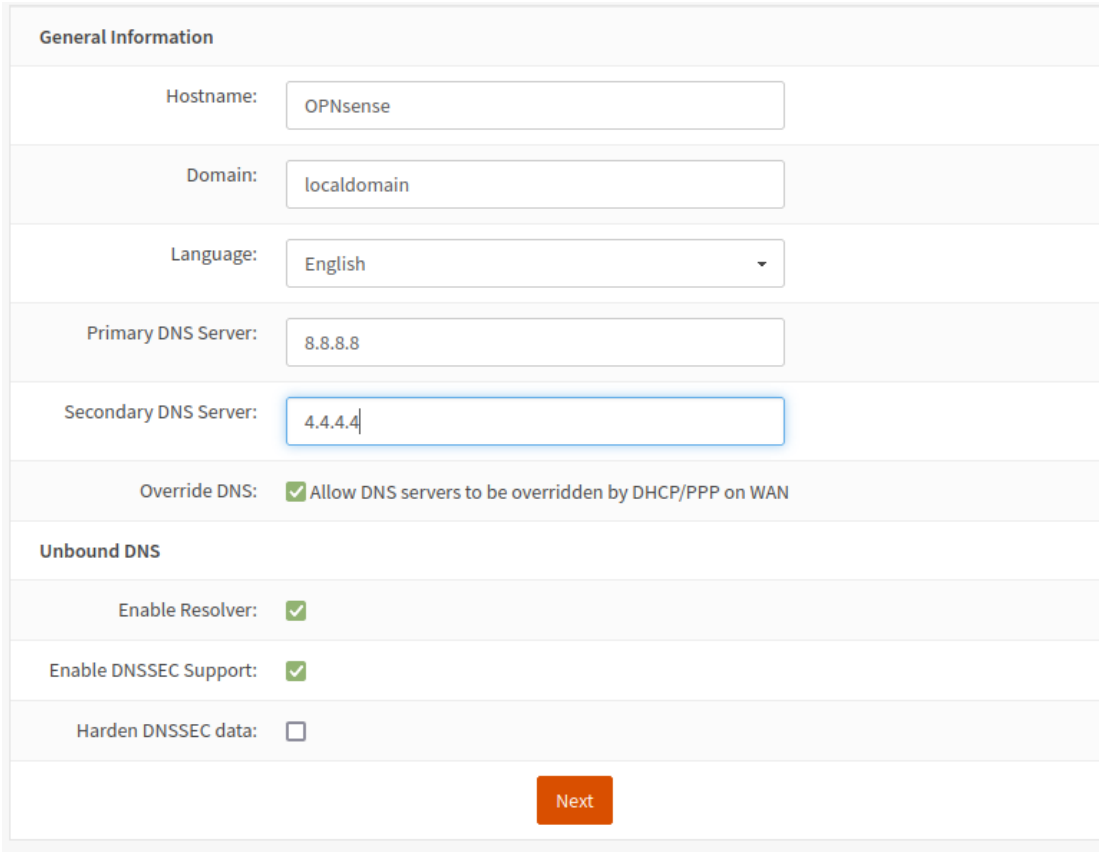


Kuva 8. Sertifikaattivirheilmoitus.

4.4.1 Asennusavustajan suorittaminen

Kirjaudutaan sisään verkkoselaimen kautta, jonka jälkeen OPNsense ohjaa käyttäjän asennusavustajaan. Ensimmäisessä kohdassa muutetaan vain DNS-palvelimet seuraavanlaisiksi, Primary DNS Server 8.8.8.8 ja Secondary DNS server 4.4.4.4. Molemmat näistä ovat Googlen nimipalvelimia, DNS-palvelimet voi halutessaan vaihtaa myös muihin, vaihtoehtoja on valtavasti.

Otetaan käyttöön myös DNSSEC support, jolla varmistetaan nimipalvelimilta saatavat tiedot. Muut asetukset jätetään oletuksiksi (kuva 9).



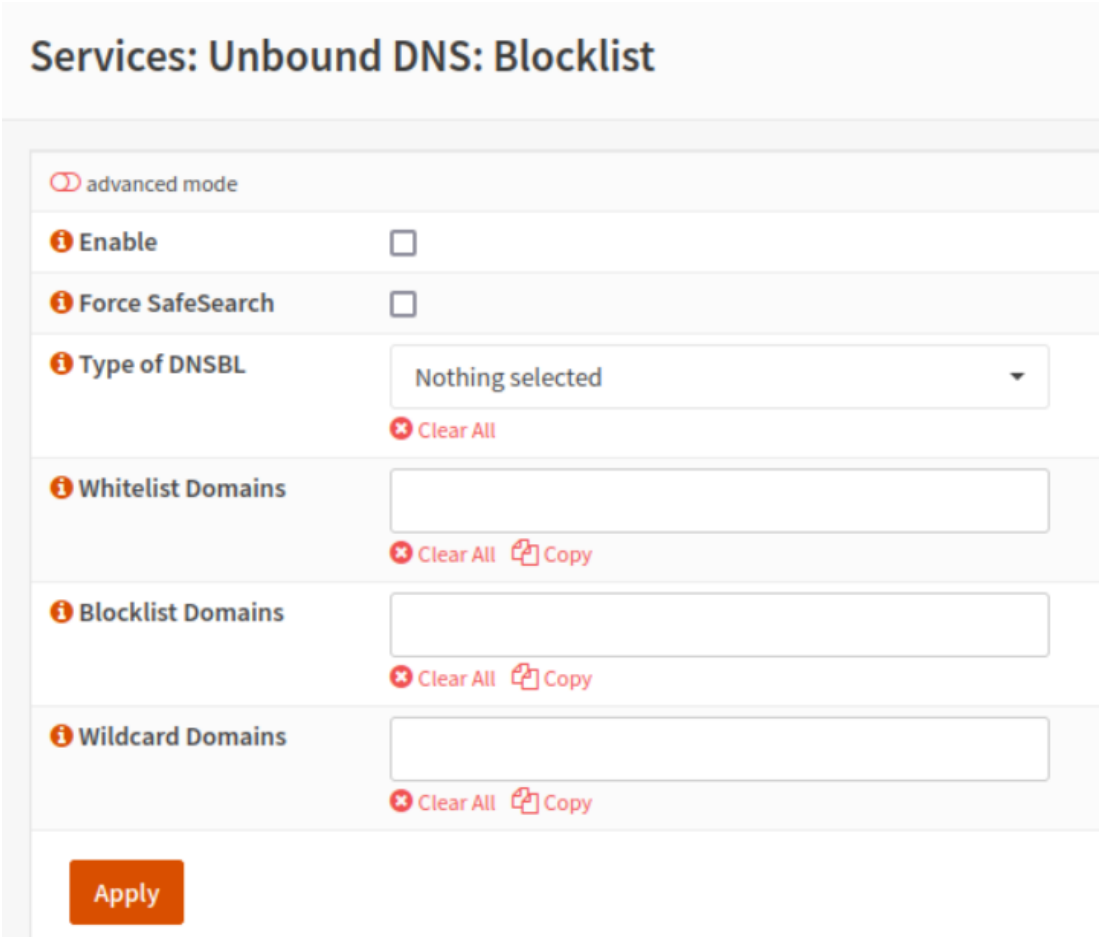
Kuva 9. Asennusavustajan ensimmäinen vaihe.

Toisessa kohdassa valitaan aikavyöhyke sekä aikapalvelimet. Muutetaan aikavyöhykkeeksi Europe/Helsinki ja jätetään aikapalvelimet oletusasetuksiin. kolmannessa vaiheessa ei tarvitse muuttaa mitään, jatketaan oletusasetuksilla. Neljännessä vaiheessa jatketaan myös oletusasetuksilla. Viidennessä vaiheessa vaihdetaan käyttäjän salasana, jonka jälkeen alustava konfigurointi on suoritettu. Tämän jälkeen valitaan dashboard-valikosta check for updates ja päivitetään palomuuri uusimpaan versioon.

4.4.2 Mainosten estolistan käyttöönotto

Otetaan käyttöön domainestolista valitsemalla service, unbound DNS ja blocklist. Valitaan enable ja force safe search (kuva 10). Valitaan myös DNSBL

valikosta halutut estolistat käyttöön, asennukseen valitaan mainosten estolistat. Estolistaan voidaan lisätä itse mahdollisia domaineja, jotka halutaan estää.



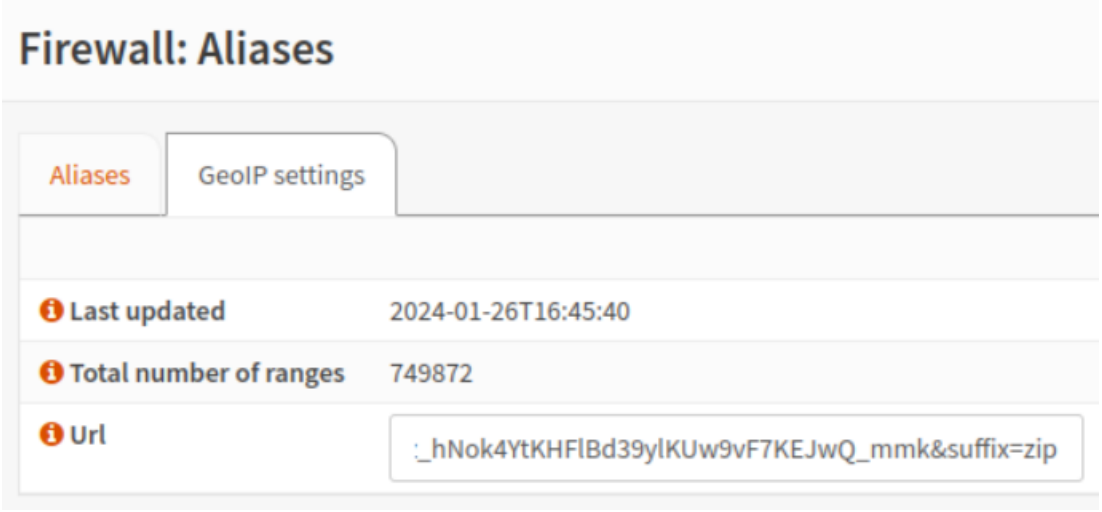
Kuva 10. DNS estolistan käyttöönotto

4.4.3 Tunkeilijan havaitsemisjärjestelmän käyttöönotto

Otetaan käyttöön myös tunkeilijan havaitsemisjärjestelmä palomuurista, joka tutkii verkkoliikenteestä tunnettuja haittaohjelmien piirteitä sekä käyttäytymistapoja. Käyttöönotto tapahtuu seuraavasti, valitaan services, intrusion detection, download ja valitaan valikosta halutut ominaisuudet, jonka jälkeen valitaan download and update rules. Odotetaan, että lataus ja käyttöönotto on suoritettu, jonka jälkeen valitaan settings ja enable.

4.4.4 Sijainnin estolistan käyttöönotto

GeoIP on tietokanta, jossa on tallennettuna IP-osoitteiden sijaintitietoja ja niiden avulla voidaan valita esimerkiksi minkä maan IP-osoitteiden yhteyksiä ei sallita palomuurissa. OPNsensessä käytetään Maxmind-yrityksen geoip-tietokantaa. Käyttöönottoa varten joudutaan luomaan käyttäjätili Maxmind-yrityksen verkkosivuilla, jonka jälkeen voidaan luoda ilmaisversiolle lisenssiavain (Maxmind, 2023). Käyttöönotto tapahtuu OPNsensen firewall: aliases, geoip kohdasta. Lisätään Geoip kohtaan linkki, joka on saatu maxmind-verkkosivulta, varmistetaan että kohta Total number of ranges on päivittynyt, jotta tiedetään linkin toimivan (kuva 11).

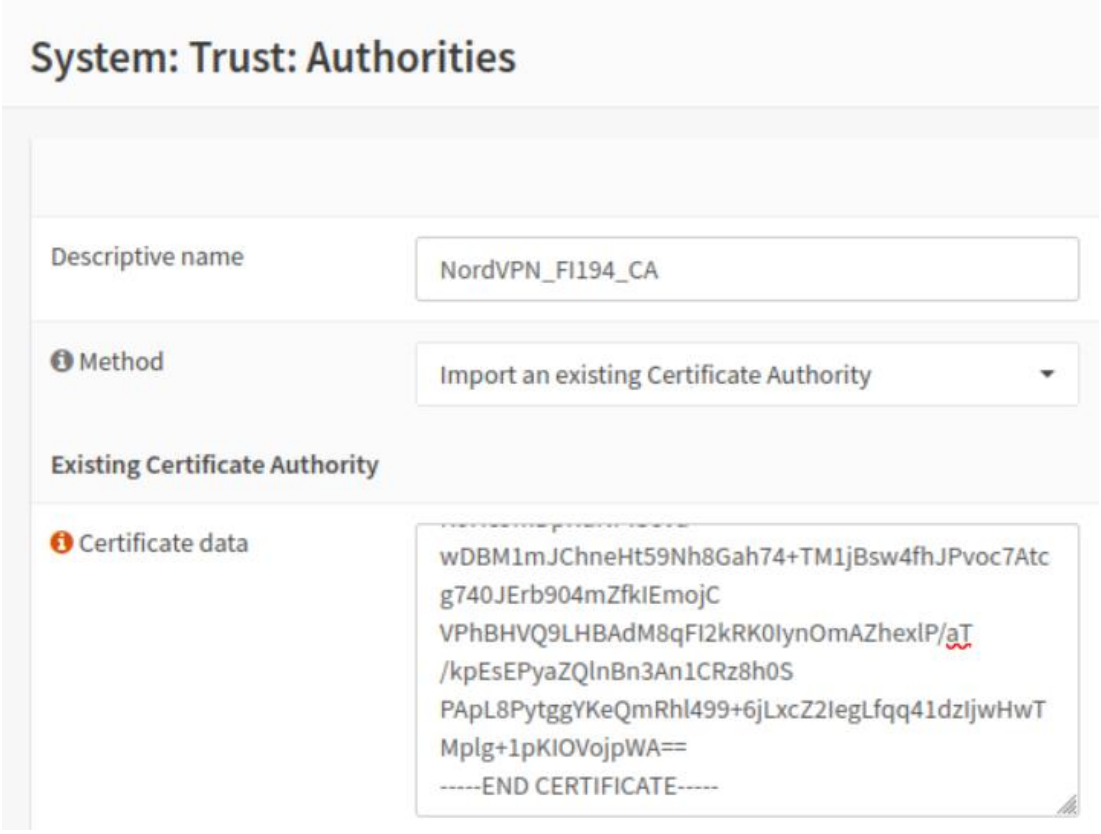


Kuva 11. GeoIP lista.

Seuraavaksi palataan kohtaan firewall: alias ja lisätään sääntö, jossa määritellään maat, jotka halutaan estää. Sääntöä lisätessä Type kohtaan valitaan GeoIP ja nimeksi estetyt_maat, valitaan Content osiosta halutut maat ja tallennetaan asetukset ja hyväksytään muutokset. Seuraavaksi konfiguroidaan sääntö kohtaan firewall: rules ja WAN. Lisätään sääntö, jolla estetään liikenne GeoIPn määrittelemiin maihin. Action kohtaan valitaan block, ja source kohtaan valitaan Estetyt_maat. Loput asetuksista jätetään oletuksiksi. Hyväksytään tehdyt muutokset.

4.4.5 VPN-käyttöönotto

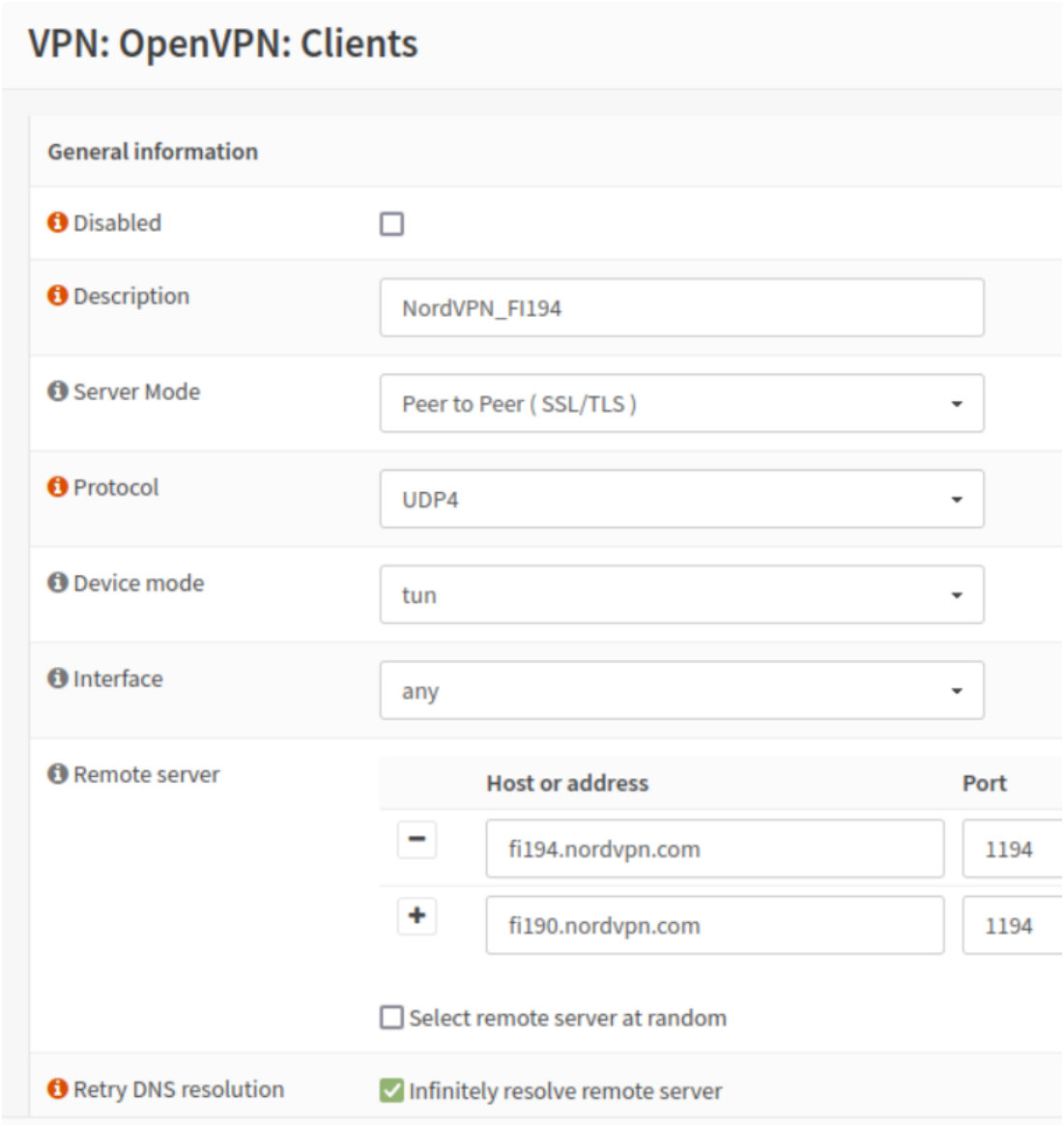
Asennuksessa yhdistetään NordVPN palvelimille. Asennus muiden palveluntarjoajan VPN-palvelimille tapahtuu lähes samalla tavalla. Muutokset asetuksiin kerrotaan VPN-palveluntarjoajan sivuilla. VPN-otetaan käyttöön, jotta saadaan salattua verkosta lähtevä liikenne. VPN-käyttöönotto aloitetaan valitsemalla System, Trust ja Authorities. Lisätään uusi sertifikaatti authority. Method: Import an existing cerificate, nimeksi voidaan lisätä mitä halutaan, mutta nimen suositellaan olevan kuvaileva ja helposti tunnistettava. Certificate data löydetään NordVPN nettisivuilta kopioidaan ja lisätään ceritifcate data kohtaan (kuva 12). Tallennetaan muutokset.



Kuva 12. Sertifikaatin lisääminen

Seuraavaksi valitaan valikosta VPN, OpenVPN ja Clients. Lisätään uusi client. Client on ohjelmisto, joka yhdistää käyttäjän ja VPN-palveluntarjoajan toisiinsa. Server mode: Peer to Peer, protokollaksi UDP4, Device mode: tun, interface: WAN. Remote server kohtaan lisätään kahden tai useamman

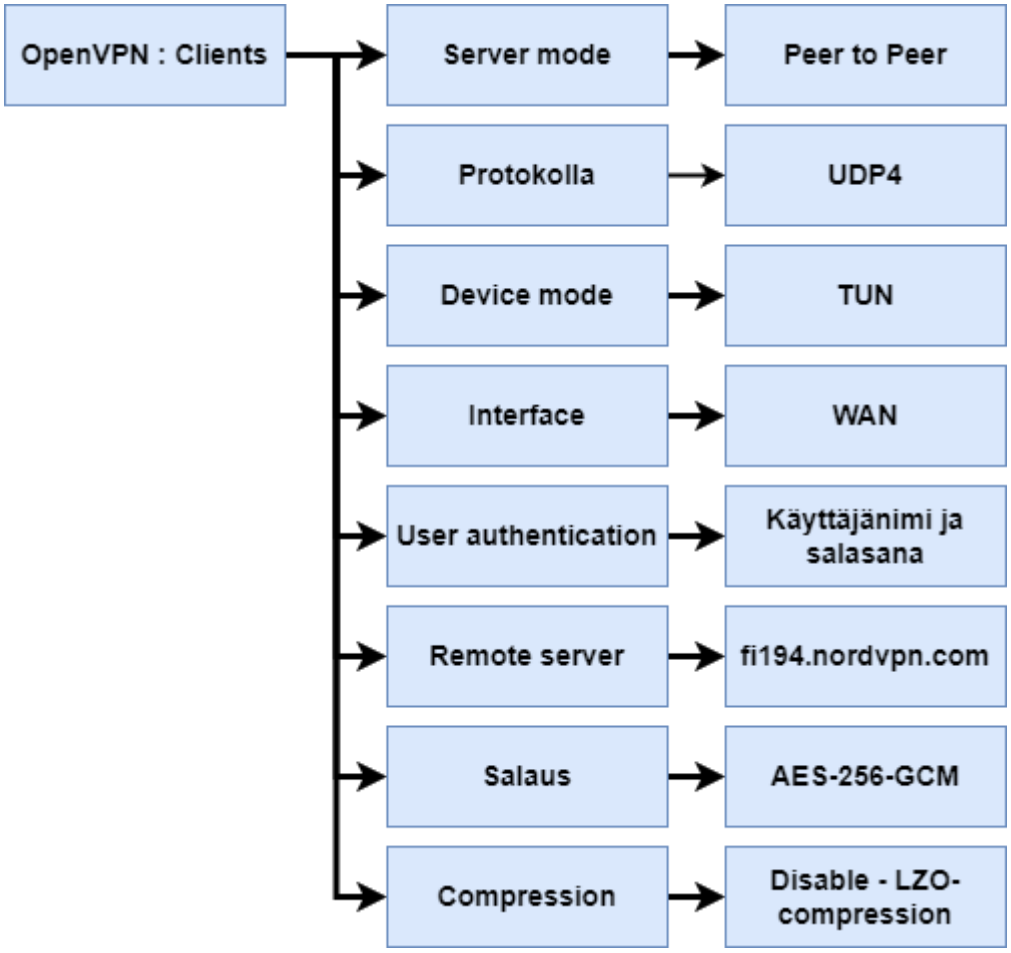
palvelimen osoite, jotta yhden palvelimen kaatuessa on mahdollista yhdistää toiseen palvelimeen (kuva 13). Valitaan aktiiviseksi Retry DNS Resolution kohta.



Kuva 13. OpenVPN Clients konfiguraatio.

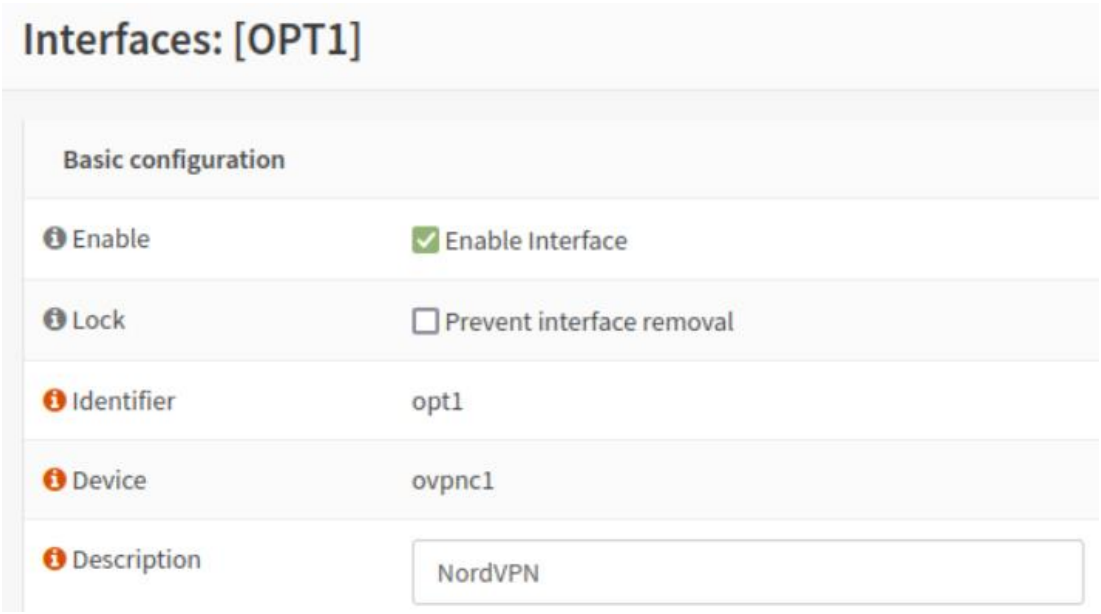
User authentication settings kohtaan kirjoitetaan käyttäjätunnus ja salasana, joka saadaan VPN-palveluntarjoajan sivuilta. Cyrptographic Settings kohdasta valitaan TLS Authentication: enabled ja liitetään NordVPN sivuston tarjoama TLS shared key. Peer certificate Authorityksi valitaan viimeksi luotu Certificate Authority. Vaihdetaan salausalgoritmiksi AES-256-GCM sekä Auth Digest Algorithm SHA512. Nämä asetukset hoitavat liikenteen salaamisen ja asetukset

vaihtuvat palveluntarjoajan mukaan. Tunnel Settings osiosta vaihdetaan vain compression kodasta – Disabled LZO algorithm (kuva 14).



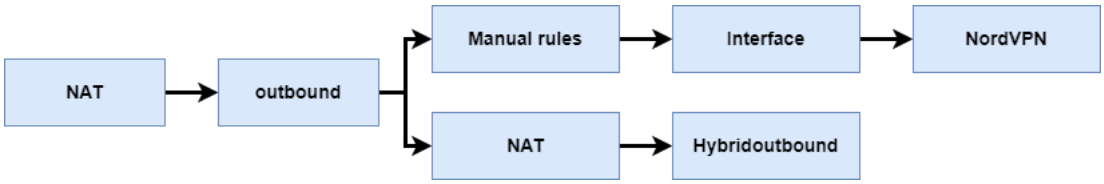
Kuva 14. VPN-yhteyden Clients kohdan asetukset.

Konfigurointia jatketaan valitsemalla valikosta Interfaces, Assignments. Lisätään ovpnc1 käyttöön valitsemalla add. Interface otetaan käyttöön, jotta palomuuri pystyy suodattamaan VPN-liikennettä ja toteuttamaan palomuurin säännöt VPN-yhteydelle. Nimeksi voidaan valita mitä tahansa (kuva 15). Ei vaihdeta muita asetuksia ikkunasta.



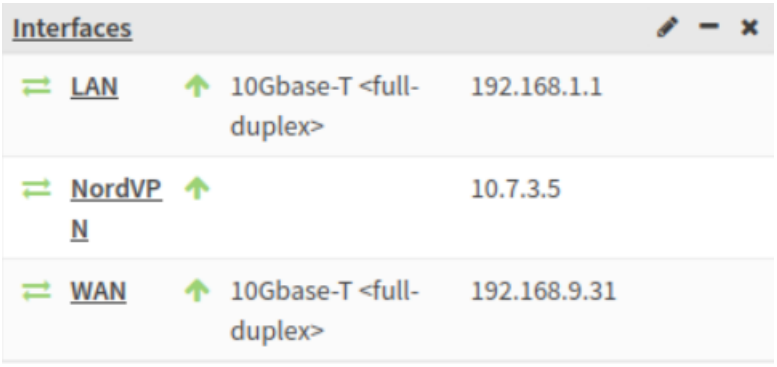
Kuva 15. OPT1 interface käyttöönotto

Seuraavaksi palomuuriin täytyy asettaa NAT-sääntö, NAT-säännöt määrittävät liikenteen, joka päästetään läpi tai estetään (kuva 16). Sääntö asennetaan valitsemalla: Firewall, NAT ja outbound, josta valitaan Hybridoutbound. Hybridoutbound on NAT sääntö, joka sallii sääntöjen lisäämisen manuaalisesti. Otetaan tehdyt muutokset käyttöön. Lisätään manual rules kohtaan uusi sääntö, jossa interface kohtaan muutetaan valinnaksi NordVPN ja jätetään loput asetuksista oletuksiksi.



Kuva 16. Palomuurin NAT-säännöt

Viimeisenä VPN-käyttöönotossa valitaan valikosta: firewall, rules ja LAN. Poistetaan IPv6 sääntö, koska NordVPN ei tue IPv6 liikennettä. Tämän jälkeen muokataan IPv4-säännöistä Gateway kohtaan NORDVPN_4 ja tallennetaan muutokset, yhdyskäytävän eli gatewayn muutos ohjaa verkkoliikenteen VPN-yhteyden kautta. Dashboard kohdasta nähdään interface ja VPN IP-osoite, jolla todetaan VPN-yhteyden olevan toiminnassa (kuva 17).



Kuva 17. VPN-yhteyden tila

5 POHDINTA JA YHTEENVETO

Opinnäytetyön tavoitteena oli asentaa OPNsense toimimaan kotiverkon palomuurina ja ottaa käyttöön tärkeät ominaisuudet kotiverkkoon kuten VPN ja mainosten esto ja IP-sijaintiestolista. Lisäksi työssä käytiin läpi OPNsensen ominaisuudet läpi teoriassa ja tutustuttiin sen laitteistovaatimuksiin. OPNsensen dokumentaatio oli laadukasta ja se helpotti asennusta huomattavasti.

Työ ja aihe olivat itselle mielenkiintoisia. Työstä sain hyvää kokemusta palomuurien konfiguroinnista, josta uskon olevan hyötyä tulevissa työtehtävissä. Ongelmitta ei työtä saatu tehtyä, mutta ongelmat olivat helposti ratkaistavia ja antoivat työhön haastetta. Mielestäni opinnäytetyöstä tuli tiivis kokonaisuus, jonka avulla palomuureista vähän tietävä kykenee asentamaan itselleen samanlaisen kokonaisuuden ongelmitta.

OPNsense vaikuttaa olevan monipuolinen ja hyvä ratkaisu kotiverkon palomuuriksi. OPNsensen käyttöönotto ja konfigurointi onnistuu helposti ohjeiden avulla, jotka löytyvät internetistä. Laitteiston hankintakustannukset ovat korkeat, jos haluaa hankkia valmiiksi rakennetun palomuurin OPNsensen sivuilta. Hyvänä puolena on, että OPNsense on mahdollista asentaa itse lähes mihin laitteistoon tahansa, kunhan verkkoportteja on riittävästi. OPNsense on hyvä vaihtoehto, jos tarvitsee enemmän hallintaa kotiverkkoonsa ja haluaa

tarkemmin seurata verkon tapahtumia. Kuluttajareitittimeen verrattuna OPNsenseen on mahdollista ottaa käyttöön eri palveluntarjoajien VPN-yhteyksiä, joita esimerkiksi Huawein kuluttajareititin ei tue.

Ominaisuuksista asennettiin vain keskeisimmät ja tärkeimmät ominaisuudet kotiverkkoon, mutta OPNsense tarjoaa valtavasti lisää konfigurointimahdollisuuksia ja sopisi hyvin myös yrityksen palomuuriksi.

LÄHTEET

Clark, C. (2021) next-generation firewall (NGFW) https://www.techtarget.com/searchsecurity/definition/next-generation-firewall-NGFW

Freda, A. (25.11.2022) What Is a Firewall and Why Do You Need One? https://www.avast.com/c-what-is-a-firewall

Froehlich, A (2022) traffic shaping https://www.techtarget.com/searchnetworking/definition/traffic-shaping

Gavrilenko, A (20.8.2023) The Network System Design Cheat Sheet: Load Balancer, Reverse Proxy, Forward Proxy, API Gateway https://hackernoon.com/the-network-system-design-cheat-sheet-load-balancer-reverse-proxy-forward-proxy-api-gateway

Gregersen, E. (12.9.2023). firewall https://www.britannica.com/technology/firewall

IBM (4.4.2023a) Caching Proxy Overview https://www.ibm.com/docs/en/wasnd/9.0.5?topic=proxy-caching-overview

Ingham, K. & Forrest, S. (n.d.). A History and Survey of Network Firewalls Haettu 20.9.2023 osoitteesta https://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf

Kalogeropoulos, D. (20.6.2017) How Palo Alto Networks, Inc. Makes Most of Its Money https://www.fool.com/investing/2017/06/20/how-palo-alto-networks-inc-makes-most-of-its-money.aspx

Laakso, M (4.1.2015) Avoin vs suljettu lähdekoodi – kumpi on turvallisempaa? https://tietojesiturvaksi.fi/blogi/avoin-vs-suljettu-lahdekoodi-kumpi-on-turvallisempaa

Maxmind (21.04.2023) Geolocation Accuracy https://support.maxmind.com/hc/en-us/articles/4407630607131-Geolocation-Accuracy

Microsoft (n.d.) What is vpn service? Haettu 10.12.2023 osoitteesta https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn#vpndefenition

Mutune, G. (n.d.) Best Open Source Firewall (Top 8). Haettu 22.10.2023 osoitteesta https://cyberexperts.com/best-open-source-firewall/

Nakutavičiūtė, J. (29.6.2023a) What is deep packet inspection? https://nordvpn.com/fi/blog/deep-packet-inspection/

Nakutavičiūtė, J. (25.9.2023b) The best VPN protocols and differences between VPN types https://nordvpn.com/fi/blog/protocols/

NordVPN (n.d.). Mitä on verkkoturvallisuus Haettu 04.09.2023 osoitteesta https://nordvpn.com/fi/cybersecurity/network-security/

OPNsense (n.d.-a) About OPNsense. Haettu 26.09.2023 osoitteesta https://opnsense.org/about/about-opnsense/

OPNsense (n.d.-b) Virtual Private Networking. Haettu 10.10.2023 osoitteesta https://docs.opnsense.org/manual/vpnet.html#

OPNsense (n.d.-c) Welcome to OPNsense's documentation! Haettu 04.03.2024 https://docs.opnsense.org/index.html

OPNsense (n.d.-d) Kuva 4. Hardware sizing & setup Haettu 04.03.2024 osoitteesta https://docs.opnsense.org/manual/hardware.html

Oracle Corporation (2010) Kuva 2 How Caching Works https://docs.oracle.com/cd/E19575-01/821-0053/adyml/index.html

Paloalto Networks (n.d.-a) What is WAF | Web Application Firewall Explained. Haettu 16.10.2023 osoitteesta https://www.paloaltonetworks.com/cyberpedia/what-is-a-web-application-firewall

Paloalto Networks (n.d.-b) The Evolution of Firewalls: From Packet Filtering to Machine Learning-Powered NGFWs Haettu 4.11.2023 osoitteesta https://www.paloaltonetworks.com/cyberpedia/the-evolution-of-firewalls-from-packet-filtering-to-machine-learning-powered-ngfws

Paloalto (n.d.-c) What Is a Business VPN? Understand Its Uses and Limitations. Haettu 25.11.2023 osoitteesta https://www.paloaltonetworks.com/cyberpedia/what-is-a-business-vpn-understand-its-uses-and-limitations

Paloalto (2023d) PAN-OS Web Interface Reference https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/web-interface-basics/features-and-benefits

Paloalto (n.d.-e) Stop malvare in its tracks. Haettu 25.01.2024 osoitteesta https://www.paloaltonetworks.com/network-security/wildfire

Rizzo, L (n.d.) The dummynet project. Haettu 2.11.2023 osoitteesta http://info.iet.unipi.it/~luigi/dummynet/

Sajid (2.5.2023) Difference between ZFS and UFS https://www.tutorialspoint.com/difference-between-zfs-and-ufs

Tushar, K. (3.1.2023) Top 10 Best Open-Source Firewall to Protect Your Enterprise Network 2023 https://cybersecuritynews.com/best-open-source-firewall/

Vilmusenaho, S. (14.4.2011) Avoimen lähdekoodin lisenssit https://wiki.aalto.fi/pages/viewpage.action?pageId=56199997

Yasar, K. (n.d.) Web application firewall (WAF). Haettu 7.10.2023 osoitteesta https://www.techtarget.com/searchsecurity/definition/Web-application-firewall-WAF