Heikki Rinne

AVOIMEN LÄHDEKOODIN PALOMUURI SOHO-YMPÄRISTÖSSÄ

Tieto ja viestintätekniikan koulutusohjelma

2020

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

AVOIMEN LÄHDEKOODIN PALOMUURI SOHO-YMPÄRISTÖSSÄ

Rinne, Heikki
Satakunnan ammattikorkeakoulu
Tieto ja viestintätekniikan koulutusohjelma
Lokakuu 2020
Sivumäärä: 29
Liitteitä:

Asiasanat: palomuurit, tietoturva, salaus, internet

Tässä työssä tutkittiin avoimen lähdekoodin palomuuriohjelmiston soveltuvuutta pienen yrityksen tai kotitoimiston verkkoliikenteen suojaukseen. Työssä käytiin läpi palomuurin perusperiaatteet sekä erilaiset suojausominaisuudet. Työssä keskityttiin käyttämään avoimen lähdekoodin tuotteita, sekä ilmaiseksi saatavilla olevia ohjeita ja materiaaleja.

Käytännön osuudessa verkon topologia muutettiin oikeanlaiseksi, ja palomuuri sijoitettiin reitittimen ja sisäverkon kytkimen väliin. Palomuuriohjelmisto PfSense, asennettiin palvelimelle ja tämän jälkeen konfiguroitiin palomuuriasetukset, DNS-palvelin, DHCP-palvelin, Suricata -tunkeutumisen estojärjestelmä ja DNS-osoitteisiin perustuva palomuuri.

Työssä todettiin PfSensen soveltuvan hyvin verkon suojaukseen pienessä ja isommassa ympäristössä. Tärkeää on muistaa sääntöjen riittävä testaus ja ylläpito sekä laitteiston kapasiteetin riittävyys jos käyttöympäristö kasvaa ja vaatimukset lisääntyy.

OPEN SOURCE FIREWALL IN SOHO ENVIRONMENT

Rinne, Heikki
Satakunta University of Applied Sciences
Degree Programme in Information and Communication technology
November 2020
Number of pages: 29
Appendices:

Keywords: firewalls, security, encryption, internet

In this thesis, the suitability of open source firewall software for the protection of network traffic of a small company or home office was investigated. The basic principles of the firewall and various protection features were reviewed. The thesis focused on the use of open source products, as well as freely available instructions and materials.

In the practical part, the network topology was changed to the correct type, and a firewall was placed between router and a switch. The firewall software PfSense, was installed on the server and then the firewall settings, DNS server, DHCP server, Suricata intrusion prevention system and DNS address based firewall were configured.

It was found that PfSense is well suited for network security in small and larger environments. It is important to remember that the rules are adequately tested and maintained, as well as the adequacy of hardware capacity if the operating environment grows and requirements increase.

SISÄLLYS

KÄYTETYT LYHENTEET JA SANASTO

AES-NI	Prosessorin käskykantalaajennos salauksen nopeuttamiseen (Advanced Encryption Standard New Instructions)
BIOS	Tietokoneen alustava ohjelma käynnistyksessä (Basic Input-Output System)
DHCP	Verkkoprotokolla (Dynamic Host Configuration Protocol)
DNS	Nimipalvelujärjestelmä (Domain Name System)
ETOpen	Palomuurisääntö lista, jota ylläpitää Proofpoint Inc.
HPE	Laitevalmistaja (Hewlett Packard Enterprise Company)
IPS	Tunkeutumisenestojärjestelmä (Intrusion Prevention System)
IDS	Tunkeilijan havaitsemisjärjestelmä (Intrusion Detection System)
ISO	Levykuva (ISO-Image)
LAN	Lähiverkko (Local Area Network)
MAC	Verkkolaitteen yksilöivä osoite (Media Access Control Address)
NAT	Osoitteenmuunnostekniikka (Network Address Translation)
OpenVPN	Avoimen lähdekoodin VPN ohjelmisto
SOHO	Pientoimisto/kotitoimisto (Small Office/Home Office)
SSD	Puolijohdelevy (Solid-state drive)
SSL	Salausprotokolla (Secure Sockets Layer)
Suricata	Avoimen lähdekoodin IDS ja IPS ohjelmisto
VPN	Virtuaalinen erillisverkko (Virtual Private Network)
WAN	Ulkoverkko (Wide Area Network)

1 JOHDANTO

Internetin ja siihen liitettävien palvelujen käytön määrän kasvaessa myös kyberhyökkäykset ovat lisääntyneet. Yritykset tarvitsevat Internettiä liiketoimintoihinsa enemmän kuin koskaan ja monien yritysten koko liikevaihto muodostuu Internetin avulla. Valitettavasti myös uhat sijaitsevat Internetissä ja niiden torjumiseen ratkaisuna on palomuuri. Palomuurit ovat viime aikoina kehittyneet merkittävästi ja havaitsevat uhkia ja tunkeutumisyrityksiä entistä paremmin. Palomuurien toiminnallisuus ja myös tekoälyyn perustuva analysointi on tullut käyttöön aiempaa enemmän.

Palomuurin tärkeimpiä ominaisuuksia ovat verkon suojaaminen, autentikointi, liikenteen mahdollinen salaus, luotettavuus ja tehokkuus. Palomuurin käytön tulisi olla yksinkertaista ja helposti lähestyttävää. Tämä pitää kuitenkin paikkaansa vain pienissä organisaatioissa, kun taas isoissa organisaatioissa palomuurissa voi olla tuhansia eri sääntöjä ja niiden pitää pelata yhteen.

Tässä työssä tutustutaan avoimen lähdekoodin ilmaiseen palomuuriin ja sen asennukseen sekä konfigurointiin pientä yritystä tai kotitoimistoa varten. Työssä käydään läpi perus konfiguraatio askel askeleelta ja tarpeelliset asetukset toiminnan kannalta. Lopuksi työssä testataan tehty konfiguraatio ja sen toimivuus todennetaan.

2 PALOMUURI YLEISESTI

Niin kauan, kun on ollut omaisuutta, on ollut myös tarve suojata omaisuutta. Tietoverkot ovat jonkun omaisuutta, kuten myös niissä liikkuva data, joka voi olla arvokasta. Tämän ongelman ratkaisuksi on kehitelty palomuuri. Palomuuri toimii verkon ”portinvartijana” ja kaikki liikenne, niin lähtevä kuin tuleva ohjataan sen lävitse. Verkon suojaaminen on hankala toteuttaa, koska edellytyksenä on, että käyttäjät, tietokoneet, palvelut, ja verkot tietävät milloin toiseen voi luottaa. Lisäksi isolla organisaatiolla voi olla useita liityntäpisteitä ulkopuoliseen verkkoon, jotka kaikki täytyy suojata palomuureilla. Tämä vaatii yhtenäisyyttä palomuurien asetuksissa. (Comer E. D. 2002.)

Palomuurit ovat yleensä reitittimen näköisiä laitteita kuten kuvassa 1, ja perustuvat samaan tekniikkaan kuin reitittimet, vain ohjelmisto on erilainen. Palomuureja on kuitenkin myös enemmän perinteisen palvelimen näköisiä ja tekniikaltaan samankaltaisia kuten Netgaten PfSenseä ohjelmistonaan käyttävät palomuurit kuvassa 2. (PfSense)

Kuva 1. Palo Alto Networksin tyylikäs sähkönsininen palomuuri. (Paloaltonetworks)

Kuva 2. Netgaten myymä PfSenseä ohjelmistona käyttämä palomuuri. (Netgate)

2.1 Toimintaperiaate

Palomuuri tutkii sen läpi kulkevaa liikennettä ja soveltaa siihen määriteltyjä sääntöjä. Liikennettä voidaan suodattaa IP- lähdeosoitteen, kohdeosoitteen, protokollan, ja yhteyden tilan perusteella. Liikenteen suodatus vain aiemmin mainituin keinoin on kuitenkin melko karkeaa ja sitä varten on kehitelty NGFW. (Thomas Tom. 2004.)

Seuraavan sukupolven palomuuri (NGFW) tarjoaa enemmän ominaisuuksia kuin vain tilallinen pakettien suodatus esimerkiksi, integroitu hyökkäysten esto (IPS), tietolähteisiin perustuvan uusien uhkien torjunnan, verkko-osoitteiden estämisen ja kehittyneiden haittaohjelmien tunnistamisen. (Cisco)

2.2 Käyttökohteet ja ominaisuudet

Palomuureja on erilaisia eri käyttökohteisiin. Usein palomuurina toimii fyysinen laite, jolla suoritetaan vain palomuuri ohjelmistoa. Mutta markkinoilla on niiden lisäksi myös virtualisoituja palomuureja, joita voidaan käyttää yksityisen tai julkisen

pilvipalveluiden suojaamiseen sekä konttipalomuureja, joita käytetään konttipalveluiden verkon suojaukseen. (Paloaltonetworks)

Palomuureissa on usein myös tietoturvaominaisuuksien lisäksi erinäisiä muita palveluita, joita tarvitaan verkon normaaliin käyttöön. Näihin kuuluvat esimerkiksi DNS palvelin ja välityspalvelin, DHCP palvelin ja välityspalvelin, NTP välityspalvelin sekä kuormantasaaja. Isoissa organisaatioissa nämä saattavat sijaita omilla palvelimillaan kun taas pienissä organisaatioissa niiden keskittäminen palomuurille on järkevää.

2.2.1 VPN

Ennen VPN-käyttöä organisaatiot joutuivat rakentamaan tai vuokraamaan fyysisen yhteyden toimipisteidensä väliin, jossa organisaatioiden sisäinen data pystyttiin siirtämään normaalin Internetin ulkopuolella. Tämä on kuitenkin melko kallista ja epäkäytännöllistä. Ongelmaan ratkaisuksi kehitettiin VPN, eli virtuaalinen yksityisverkko. Tämän tekniikka takaa sen, että ulkopuoliset eivät voi salakuunnella tätä liikennettä. VPN nojaa kahteen perustekniikkaan; tunnelointiin ja salakirjoitukseen. Tunneloinnilla luodaan reitti Internetin läpi, jonka molemmissa päissä on palomuuri ja/tai VPN ohjelmisto. Salakirjoituksella taas salataan tietosähkeet. Näin toimittaessa varmistetaan siirrettävien tietosähkeiden salaus ja eheys. (Comer E. D. 2002.)

VPN-yhteyttä voidaan hyödyntää esimerkiksi työntekijöiden etäyhteyksiä varten, jotta voidaan muodostaa turvallinen yhteys yritykseen ja käyttää sisäverkossa olevia palveluita, sekä käyttää internettiä turvattomien WLAN-verkkojen yli, esimerkiksi kahviloissa. Toinen tapa hyödyntää VPN yhteyttä on luoda kiinteä yhteys kahden toimipisteen välille. Tätä kutsutaan site-to-site-VPN-yhteydeksi. Sillä varmistetaan, että toimipisteiden välinen tietoliikenne on salattu, vaikka se kulkeekin julkisen internetin kautta. (Paloaltonetworks)

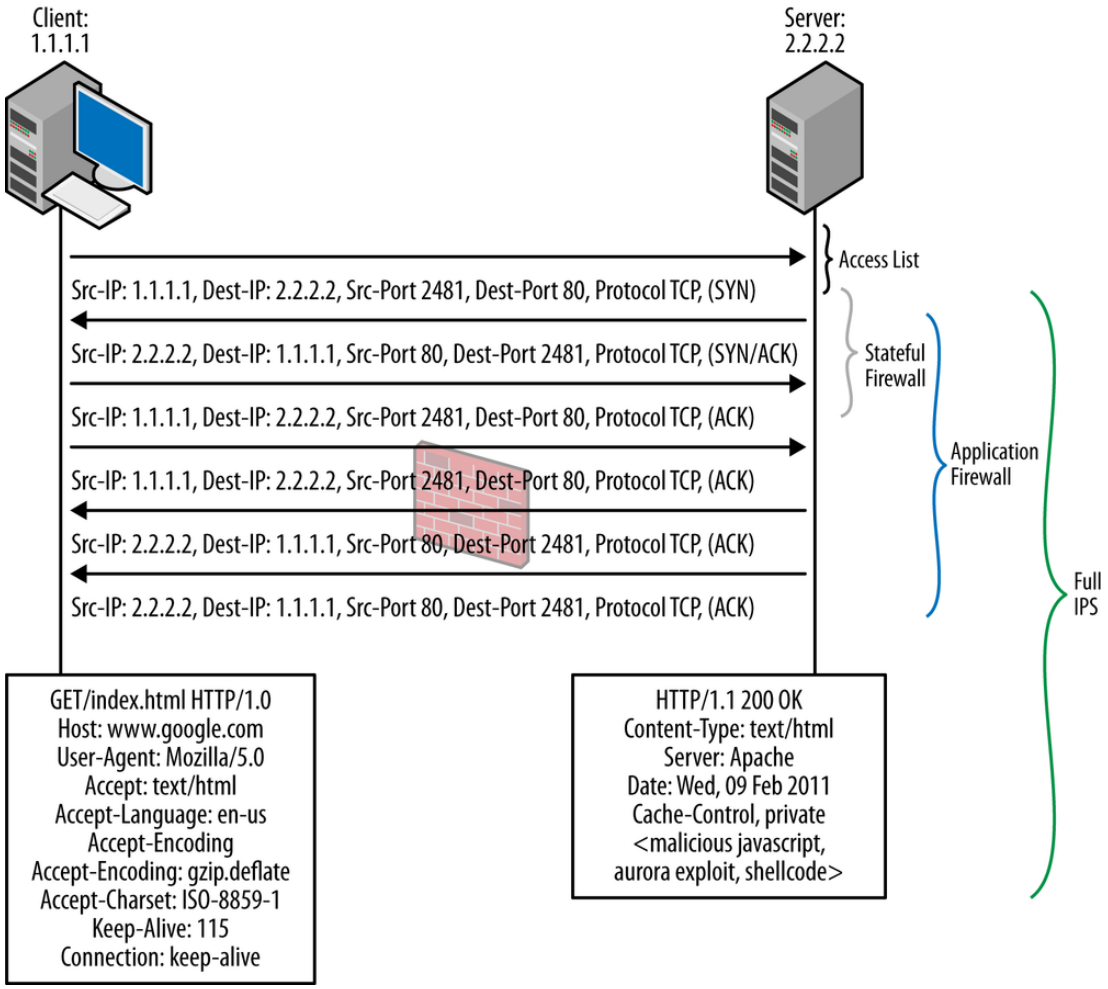
2.2.2 IDS & IPS

Tyypillisillä yrityksillä on monia eri reittejä internettiin, tämä luo haasteen pitää verkot turvallisena sekä avoimina käytölle. Pelkät palomuurisäännöt eivät tuo riittävästi turvaa nykyajan tietoturvauhkia vastaan. Ratkaisuna tähän on IDS ja IPS järjestelmä. Nämä hyödyntävät kolmea eri tapaa löytää haitallinen verkkoliikenne.

- Tunnistepohjainen tunnistus (signature based detection) on yksinkertaisin menetelmä, jolla paketin sisältöä verrataan tunnettuihin haitallisen liikenteen pakettien tunnisteisiin. Menetelmä on hyvä tunnettujen haitallisten pakettien estoon, mutta huono jos hyökkäys on uusi eikä tunnistetta sille vielä ole olemassa.
- Poikkeavuuspohjainen tunnistus (anomaly based detection) on monimutkaisempi ja työläämpi menetelmä. Sillä luodaan malli normaalista liikenteestä ja jos liikenne merkittävästi poikkeaa tästä mallista, tehdään hälytys.
- Protokollan tila analyysi (stateful protocol analysis) analysoi liikennettä protokolla tasolla ja etsii siitä esimääriteltyjä poikkeavuuksia, esimerkiksi jos joku koittaa lähettää väärällä tavalla muotoiltuja pyyntöjä. (Juniper)

Kuvassa kolme on eri palomuurin tekniikoiden ero. Yksinkertaisilla pääsylistoilla voi estää tai sallia tietyistä ip-ositteista liikennettä. Tilallisella palomuurilla taas voi estää tai sallia tiettyjä portteja tai ip-osoitteita, ja seurata yhteyden tilaa. Sovelluspalomuurilla voi seurata mitä esimääritetty sovellus voi kommunikoida, mutta se ei estä hyökkäyksiä.

Hyökkäyksen estojärjestelmä pystyy seuraamaan viestintää kaikilla aiemmin mainituilla tavoilla ja lisäksi tutkimaan pakettien sisällön ja päättelemään niistä mahdolliset uhkatekijät kuten kuvassa kolme huomataan. (Cameron R, Woodberg B. 2013.)



Kuva 3. Eri palomuuri tekniikoiden ero, ainoastaan IPS näkee paketin sisällön eli haitallisen javascript koodin. (Cameron R, Woodberg B. 2013.)

3 PFSENSE

PfSense on avoimen lähdekoodin ilmainen palomuuriohjelmisto, joka perustuu FreeBSD käyttöjärjestelmään. Se tarjoaa saman tai jopa paremman toiminnallisuuden kuin kaupalliset vastaavat järjestelmät.

PfSense sisältää graafisen käyttöliittymän, jonka kautta voi konfiguroida kaikki ominaisuudet. UNIX osaamista ei tarvita, eikä komentoriviin tarvitse koskea, jos ei halua. Netgate tarjoaa ohjelmistoon myös kaupallista tukea, jos sitä haluaa hyödyntää, mutta lähtökohtaisesti kaikki ominaisuudet ovat vapaasti käytettävissä eikä niistä tarvitse maksaa. PfSense on seuraavan sukupolven palomuuri eli NGFW. (PfSense. 2020)
PfSensellä ei varsinaisesti ole julkaisuaikataulua uusista versioista, mutta korjauspäivityksiä tarjotaan yleensä muutaman kerran vuodessa, tarvittaessa useamminkin.
(PfSense 2020)

Ohjelmiston lähin kilpailija, OPNsense on alankomaalaisen Decison alun perin PfSensen tehty kopio, jota on lähdetty kehittämään itsenäisenä projektina. Se on myös avointa lähdekoodia sekä ilmainen. (OPNsense)

PfSenseä voidaan käyttää esimerkiksi seuraavia sovelluksia varten.

- VPN palvelin
- Korkea saatavuus (High Availability)
- Kuorman tasaus (Load Balancing)
- Kaistan hallinta (Traffic Shaping)
- Vierailijoiden tunnistautuminen verkkoon (Captive Portal)
- Keskitetty uhkien torjunta (UTM Device)
- Palomuuri / reititin (Firewall / Router)
- DNS / DHCP palvelin
- IDS / IPS järjestelmä
- Välityspalvelimena (Transparent Caching Proxy)
- Verkon sisällön suodatus (Web Content Filter)

(PfSense 2020.)

4 PALOMUURIN ASENNUS

4.1 Suunnittelu

Ennen laitteiston hankkimista pitää pohtia, kuinka suureen ympäristöön palomuuria ollaan hankkimassa, mitä suodatusominaisuuksia halutaan käyttää ja kuinka paljon kaistanleveyttä tarvitaan. Prosessorissa on hyvä olla aes-ni käskykantalaajennos, jolloin salaaminen sujuu paljon nopeammin ja pienemmällä prosessorin rasituksella.

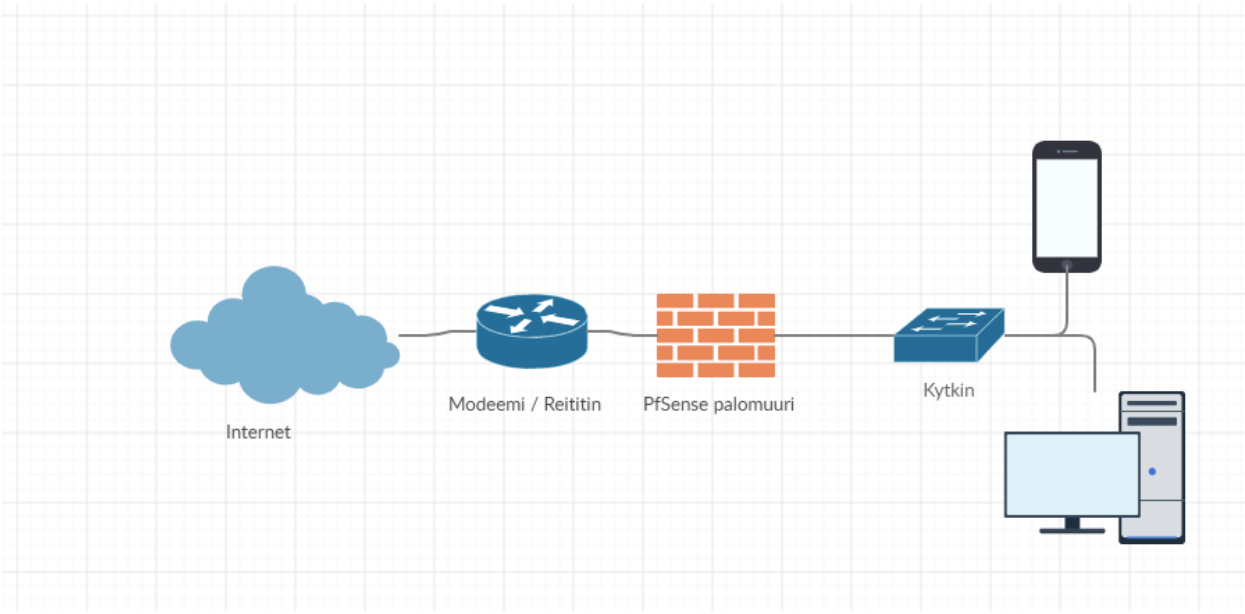
Mitä enemmän palveluita palomuurista valitsee, sitä enemmän tarvitaan muistia ja tehoa prosessorilta. Samoin myös sääntöjen iso määrä tai monimutkaisuus voi helposti viedä paljon resursseja.

Taulukossa 1 on arviot työmuistin määrästä mitä tietty määrä avoimia yhteyksiä kuluttaa.

States	Connections	RAM Required
100,000	50,000	~97 MB
500,000	250,000	~488 MB
1,000,000	500,000	~976 MB
3,000,000	1,500,000	~2900 MB
8,000,000	4,000,000	~7800 MB

Taulukko 1. (PfSense 2020.)

Lisäksi on hyvä miettiä verkon topologiaa ja miten se muuttuu kun käyttöön otetaan palomuuri. Kuvassa neljä on tässä työssä hyödynnettävän verkon topologia.

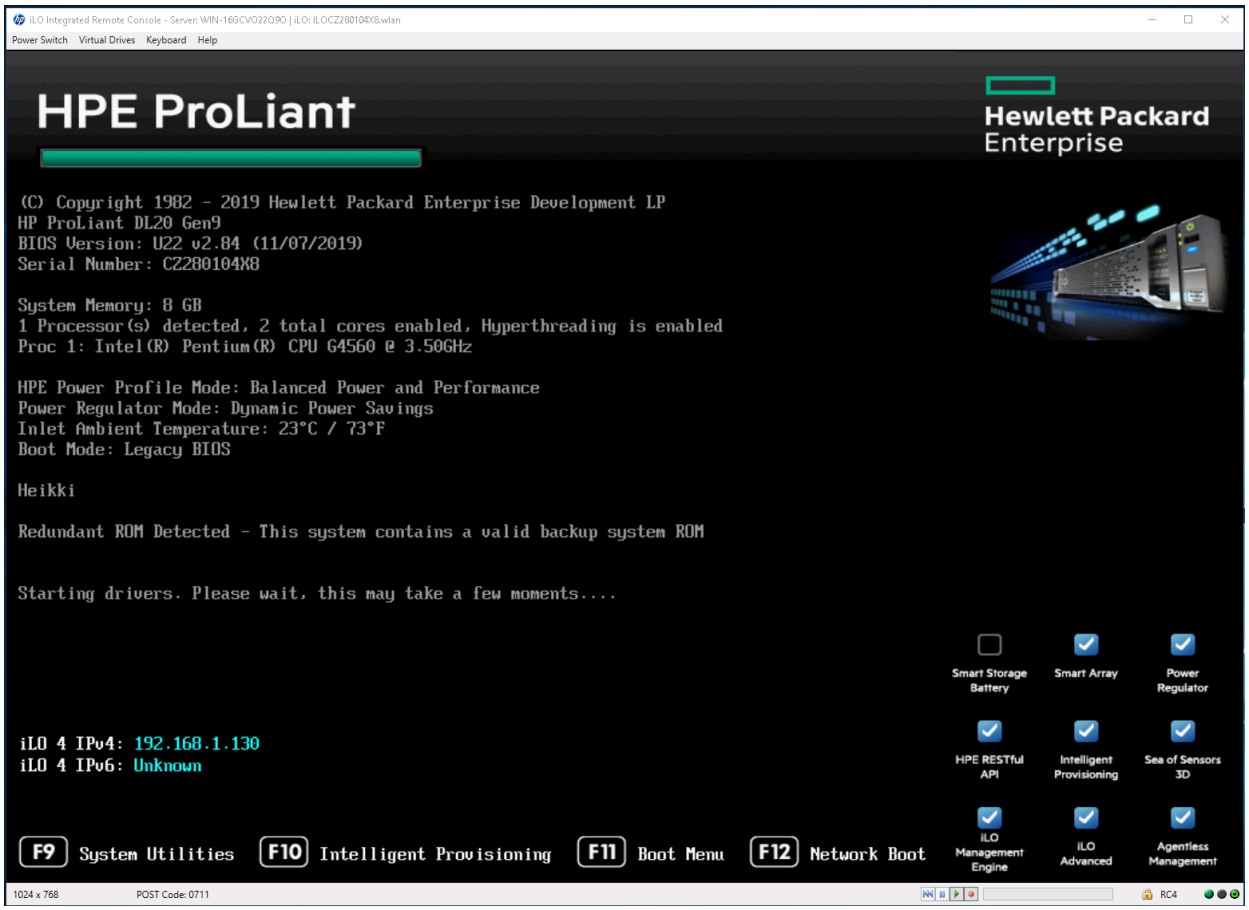


Kuva 4. Työssä käytettävän verkon topologia.

4.2 Laitteiston esittely

Laitteistona toimii yhdeksännen sukupolven HPE:n DL20 palvelin. Siinä on 8 gigatavua virheenkorjaavaa DDR4 muistia, Intelin G4560 kaksi ydin prosessori sekä kaksi gigabitin verkkokorttia. Tallennustilana on yksi 120 gigatavun SSD asema.

Asennuksessa hyödynnetään HPE:n palvelimissa olevaa etäkäyttö mahdollisuutta, jolloin asennuksen aikana päästään konsoli-istuntoon käsiksi. Palvelimessa on Intelligent Provisioning, jolla voidaan tarkkailla laitteiston tilaa ja lämpötiloja. Sillä voidaan myös päivittää laitteiston firmwaret sekä muuttaa laitteiston asetuksia. Tässä tapauksessa laitteiston BIOS asetukset ovat vakiona oikein eikä niihin tarvitse puuttua.

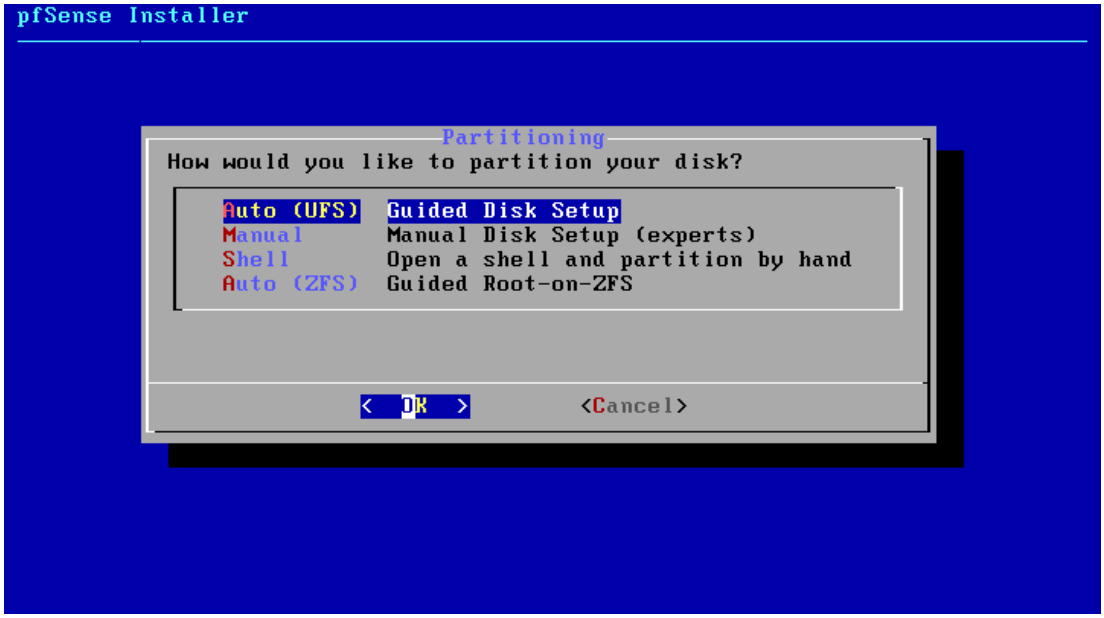


Kuva 5. Palvelin käynnistymässä.

4.3 Palomuuriohjelmiston asennus

Kun uusin versio PfSensestä on ladattu voidaan ISO tiedosto kirjoittaa muistitikulle. Koska käytössä on HP:n ILO etätyökalu, voidaan ottaa käyttöön (mount) ISO tiedoston verkon yli, josta se näkyy palvelimelle suoraan. Seuraavaksi painetaan F11 ja valitaan virtuaali cd/dvd levy käynnistyslevyksi. Asennus käynnistyy ja näkyviin tulee tekijänoikeustiedot. Painetaan hyväksy ja päästään eteenpäin. Asennusohjelma toivottaa tervetulleeksi pfSenseen ja valitaan asenna (Install).

Seuraavaksi vuorossa on levyn osiointi. Tarjolla on automaattinen osiointi UFS tiedostojärjestelmällä, manuaalinen sekä automaattinen ZFS tiedostojärjestelmällä. ZFS on uudempi ja enemmän ominaisuuksia sisältävä tiedostojärjestelmä, sitä on suositeltavaa käyttää, jos esimerkiksi tarvitsee enemmän vikasietoisuutta ja haluaa käyttää kahta levyasemaa. Koska käytössä on vain yksi levy, valitaan UFS tiedostojärjestelmä.



Kuva 6. PfSensen asentaja, levyn osiointi.

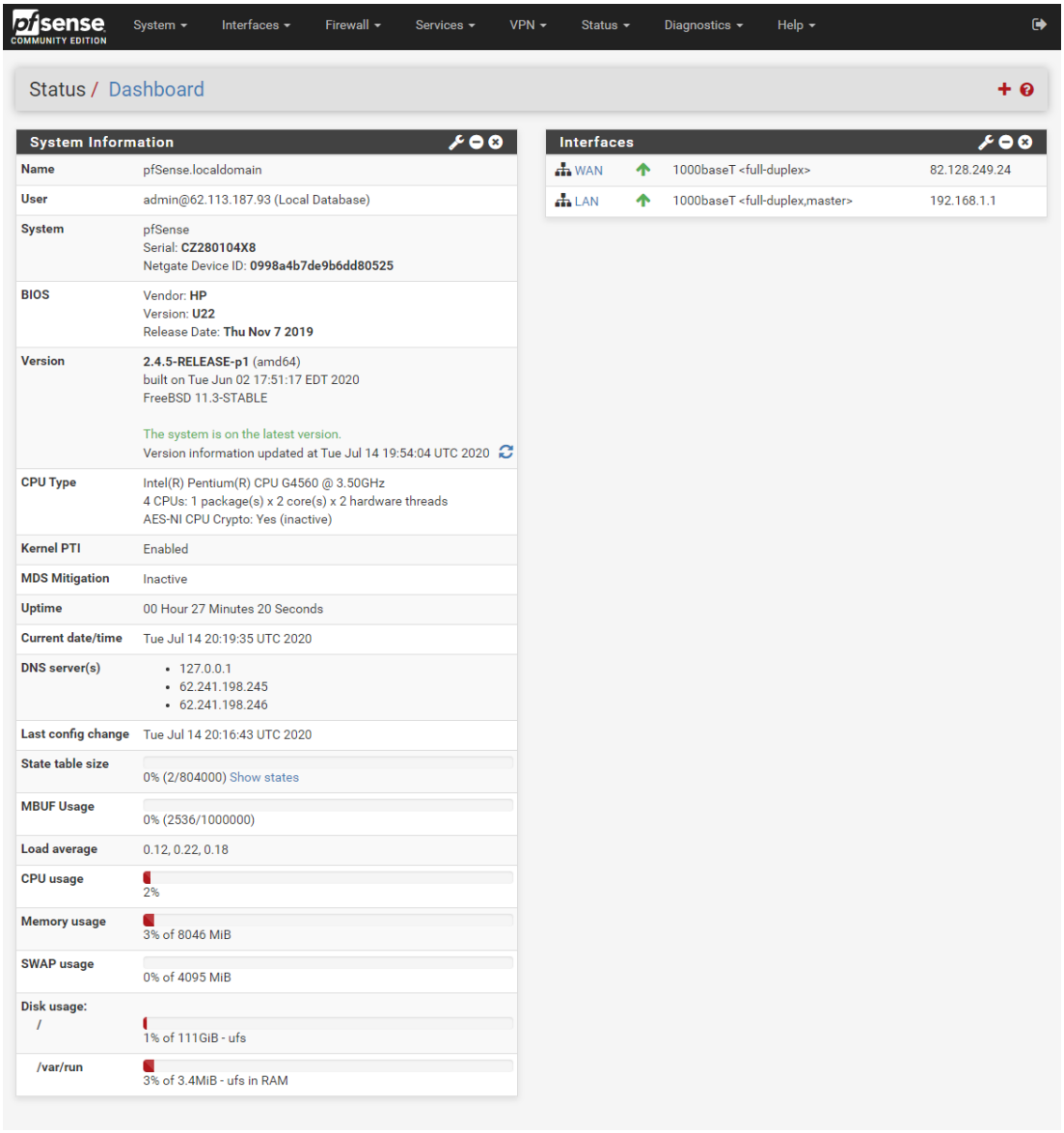
Asentaja varoittaa, että kaikki tiedot levyltä ylikirjoitetaan, valitaan OK ja jatketaan. Seuraavaksi valitaan näppäimistöasettelu, valitaan suomi ja jatketaan. Kun asennus on valmis, asentaja kysyy, halutaanko avata komentorivi ja tehdä käsin muutoksia. Valitaan ei ja käynnistetään palvelin uudestaan.

Asennuksen jälkeen järjestelmä käynnistyy ensimmäisen kerran ja palomuuri kysyy kumpi verkkokorteista, on ulko- ja kumpi sisäverkon puoli. Valitaan WAN puoleksi bge0 ja LAN puoleksi jäljelle jäänyt bge1. Ulkoverkon puolella valitaan DHCP käyttöön, sillä ip-osoite tulee internet palveluntarjoajalta. Sisäverkon puolella taas valitaan ip-osoitteeksi 192.168.1.1 ja aliverkon peitteeksi 255.255.255.0, jolloin käyttöön jää 253 ip-osoitetta.

4.4 Ohjelmiston konfigurointi

Asennus on nyt saatu tehtyä ja voidaan kirjautua web hallintaan sisäverkon ip-osoitteella https://192.168.1.1/. Ensimmäisenä tervehtii ohjattu asennus, jonka avulla voi suorittaa perusasetukset. Ohitetaan tämä vaihe ja määritellään asetukset itse.

Ensimmäiseksi vaihdetaan admin käyttäjän salasana. Tämän jälkeen vaihdetaan laitteen nimi sekä aikavyöhyke. PfSensessä on oletusarvoisesti NAT sekä kaiken ulkoa sisäänpäin suuntautuvan liikenteen esto käytössä.



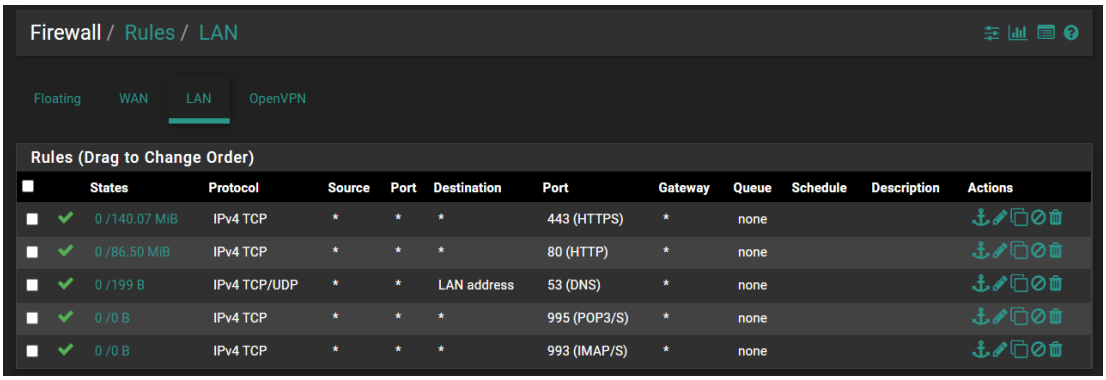
Kuva 7. Palomuurin oletusnäkymä.

4.4.1 Yleiset asetukset

Perusasetuksien jälkeen voidaan ryhtyä syvällisemmin konfiguroimaan palomuuria. PfSensessä on oma pakettienhallinta ja sieltä löytyy palomuurin toiminnallisuuksia laajentavia ohjelmia. Ladataan sieltä Suricata, pfBlocker sekä OpenVpn export. Asetuksista löytyy myös palomuurin hallintaa koskevia valintoja.

4.4.2 Palomuurisäännöt

Oletuksena kaikki ulkoa sisälle päin suunnattu liikenne on estetty, kun taas sisältä ulos päin suuntautuva liikenne on sallittu. Hyvänä käytäntönä on kuitenkin estää kaikki portit ja avata vain ne, joita tarvitaan. Avaataan portit 80, 443, 53, 995 ja 993. Näiden ansiosta sisäverkon puolelta voidaan selata nettiä, tehdä DNS pyyntöjä palomuurille, ja lähettää sekä vastaanottaa sähköpostia. Ulkoapäin sisälle suuntautuviin avataan vain portti 1194 VPN yhteyksiä varten.



Kuva 8. Palomuurin LAN puolen säännöt.

4.4.3 Pfblockerng

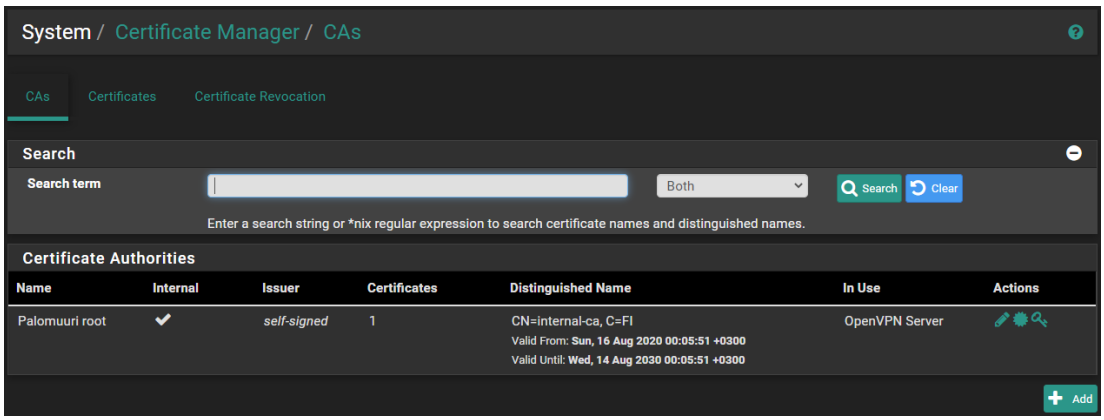
Pfblockerng on pakettienhallinnasta ladattava laajennos palomuuriohjelmistoa varten. Sen avulla voidaan helposti estää verkkotunnuksia, ip-osoiteavaruuksia ja fyysiseen

sijantiin perustuen kokonaisia maita. Verkkotunnuksien estäminen on hyödyllistä, jos halutaan rajoittaa mitä sivuja käyttäjä pääsee katsomaan. Tämä vaatii kuitenkin Unboundin käyttöä, jota ei välttämättä ole mielekästä käyttää kaikissa ympäristöissä.

Asennuksen jälkeen voidaan lisätä verkkotunnuslista. Käytetään yhteisön luomia ja ylläpitämiä listoja, jotka ovat ilmaisia. Näillä listoilla voidaan estää esimerkiksi mainosten latautumisen sivuilla ja rajoittaa seurantaa. Koska listoilla tapahtuu jatkuvasti muutoksia, päivitetään lista kerran viikossa uusien haitallisten verkko-osoitteiden ilmaantuessa.
Valitaan myös asetus, jotta VPN käyttäjien liikenne kierrätetään myös pfblockerin lävitse, eivätkä käyttäjät näin ollen pääse haitallisille sivuille.

4.4.4 Varmenteet

Myöhemmin työssä tarvitaan varmenne, jolla VPN yhteys voidaan salata sekä käyttäjät todentaa. Luodaan palomuurille juurivarmenne, jolla voidaan luoda uusia varmenteita muuhun käyttöön. Käytännössä juurivarmenne ostetaan varmenteita myöntävältä taholta ja on sidottu yrityksen omistamaan domain nimeen. Ensiksi tehdään palomuurista kuvitteellisen varmenteen myöntäjä ja luodaan juurivarmenne. Mennään kohtaan System -> Certificate Manager -> CAs -> Add+. Palomuuri kysyy juurivarmenteelle nimeä sekä toimitaanko itse varmentajana vai käytetäänkö varsinaisen varmenteen myöntäjän myöntämää varmennetta. Valitaan toimivamme itse varmentajana (Create an internal Certificate Authority). Loput asetukset jätetään oletusasetuksiksi.



Kuva 9. Luotu juurivarmenne.

Seuraavaksi luodaan palomuurille VPN käyttöön varmenne. Valitaan System -> Certificate Manager -> Certificates -> Add+. Annetaan varmenteelle nimeksi “Vpn cert” ja varmenteen tyypiksi valitaan palvelimen sertifikaatti (server certificate). Varmenteen yleiseksi nimeksi (Common name) laitetaan palomuurin ip-osoite, 82.128.249.24.

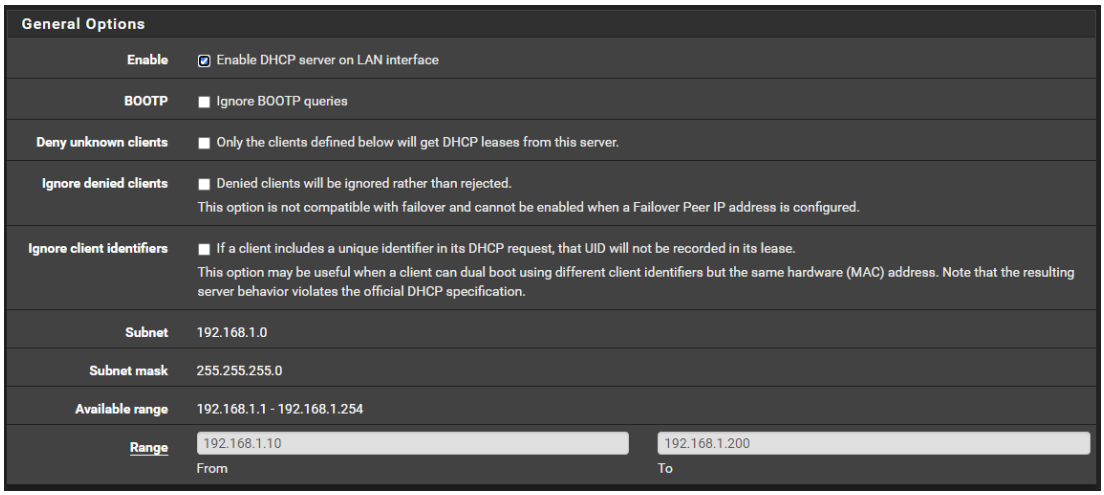
4.4.5 DNS

Palomuurissa käytetään Unbound nimistä nimipalvelin ohjelmistoa (DNS resolver), joka tekee nimipalvelukyselyt suoraan juuripalvelimilta. Tällöin voidaan käyttää DNSSEC suojausta, joka takaa sen, että nimipalvelu kyselyitä ei ole muokattu. Lisäksi myöhemmin on helppo asentaa pfblockerng, joka hyödyntää Unbound ohjelmistoa.

Unboundin asetuksista valitaan, että kuunnellaan vain sisäverkkoa sekä itse palomuuria nimipalvelu kyselyissä. Lisäksi laitetaan päälle asetus, jolla sisäverkon laitteiden nimet rekisteröityvät ja tällöin voidaan lähettää ping kutsu laitteen nimellä.

4.4.6 DHCP

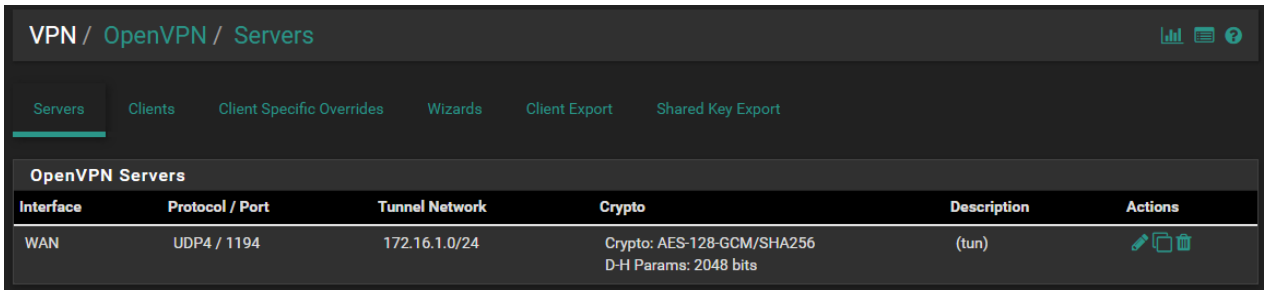
Jotta sisäverkon laitteet saisivat ip-osoitteen, otetaan käyttöön DHCP palvelin. Aikaisemmassa vaiheessa valittu sisäverkon ip-osoite 192.168.1.1 ja aliverkon peite 255.255.255.0, joten käyttöön jäi 253 osoitteen alue. Valitaan DHCP alueeksi (range) 192.168.1.10-192.168.1.200. Koska verkko on pieni ja sisältää vain vähän laitteita ja laitteiden vaihtuvuus on pientä, laitetaan osoitteen voimassaoloajaksi 86400 sekuntia eli 24 tuntia.



Kuva 10. DHCP palvelimen konfiguraatio.

4.4.7 VPN

Palomuuri sisältää myös VPN toiminnon, joka on monelle yritykselle tärkeä ominaisuus. Valitaan tähän tehtävään OpenVPN joka on myös avointa lähdekoodia. VPN palvelin tarvitsee toimiakseen varmenteen, joka on luotu aiemmin. Autentikoinniksi valitaan käyttöön käyttäjä autentikointi (User Authentication). Tällöin jokainen etäkäyttäjä joutuu tunnistautumaan käyttäjätunnuksella ja salasanalla, sekä palvelimen myöntämällä sertifikaatilla. Pakotetaan VPN asiakkaat käyttämään palvelimen tarjoamaa DNS osoitetta, jolloin liikenne varmasti kiertää nimipalvelusuodattimen kautta.



Kuva 11. VPN palvelin ja sen käyttämä protokolla, tunnelin ip-osoite sekä salaustekniikka.

Aikaisemmin valitulla OpenVPN Client Export paketilla pystytään helposti luomaan VPN käyttöä varten profiileita tai exe tiedostoja jossa profiili on integroituna. Tämä helpottaa VPN käyttöönottoa yrityksissä ja yksinkertaistaa ylläpitoa.

4.4.8 IDS & IPS

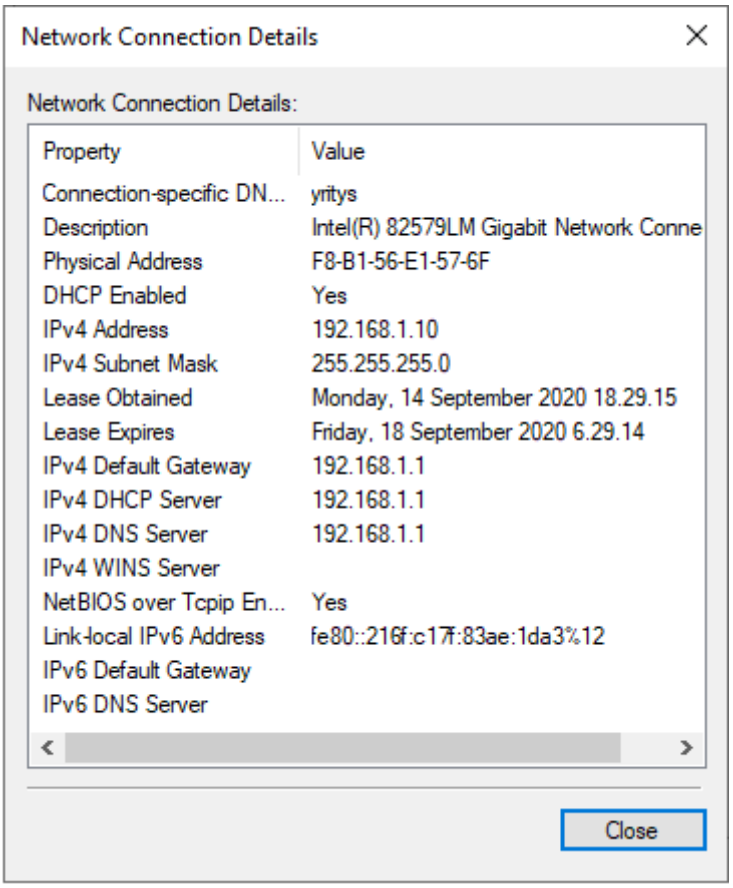
Tunkeilijan estojärjestelmänä palomuurissa toimii Suricata, joka on myös avointa lähdekoodia ja ilmainen. Suricatan lähin vastine on myös avoimen lähdekoodin tuote Snort. Laitetaan Suricata LAN porttiin, jolloin kuluu vähemmän resursseja kuin käyttämällä järjestelmää WAN portissa.

Paketin asennettua valitaan säännöt, joita halutaan käyttää. Otetaan käyttöön ETOpen säännöt, jotka ovat ilmaisia. Kun säännöt on ladattu, päästään valitsemaan kategoriat, mitä liikennettä halutaan oikeasti valvoa ja estää ja mistä ei olla kiinnostuneita. Tarjolla on esimerkiksi telnet liikennettä valvova lista, mikä ei ole mielekäs, koska verkossa on telnet portti kiinni eikä siten telnet liikennettä voi syntyä. Näin toimimalla säästetään palomuurin työmuistia sekä prosessori syklejä.

Kun kategoriat ovat valittu käynnistetään Suricata hälytystilassa, jolloin liikennettä ei estetä, mutta saadaan ilmoitus, jos sääntöjä rikkovaa liikennettä esiintyy. Samalla voidaan tutkia, tuleeko paljon vääriä hälytyksiä ja muokata sääntöjä niiden mukaan.
Lopuksi laitetaan järjestelmä estotilaan, jolloin kaikki liikenne kulkee Suricatan kautta ja analysoidaan sekä estetään jos tarpeen. Suricata ei kuitenkaan ole järjestelmä, joka asetetaan kerran ja unohdetaan, vaan säännöt on hyvä tarkistaa tietyin väliajoin tai kun verkkoa muutetaan.

5 VERKON TESTAUS

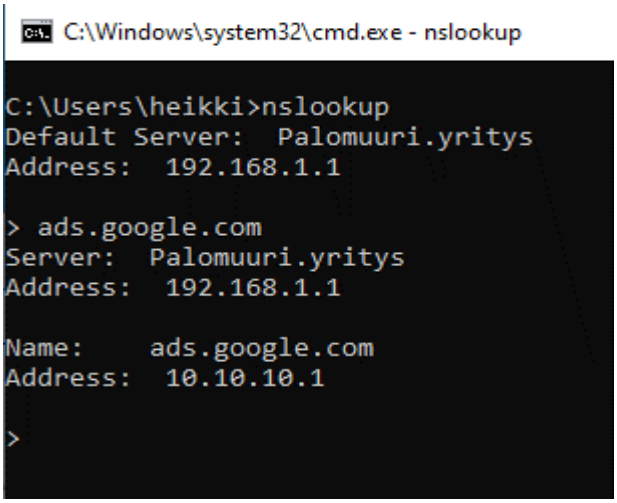
Konfiguraatioiden jälkeen on aika testata verkon toimivuus. Sisäverkossa oleva tietokone on saanut ip-osoitteet oikein, kuten kuvasta 12. voidaan päätellä.



Kuva 12. Sisäverkon tietokoneen verkkoyhteyden tiedot.

Seuraavaksi kokeillaan, toimiiko mainosten esto. Avataan komentokehoite ja kirjoitetaan nslookup. Kehotteeseen tulostuu käytössä oleva DNS-palvelimen osoite, eli palomuurin osoite. Tehdään DNS kyselyn osoitteelle ads.google.com, joka on Googlen mainospalvelun osoite. Täältä mainokset tulevat monelle verkkosivustolle.

DNS-palvelin vastaa että ads.google.com ip osite on 10.10.10.1. Tämä ei tietenkään ole oikea ip-osoite vaan keksitty kuvitteellinen sisäverkon osoite. Voidaan todeta, että mainostenesto toimii.



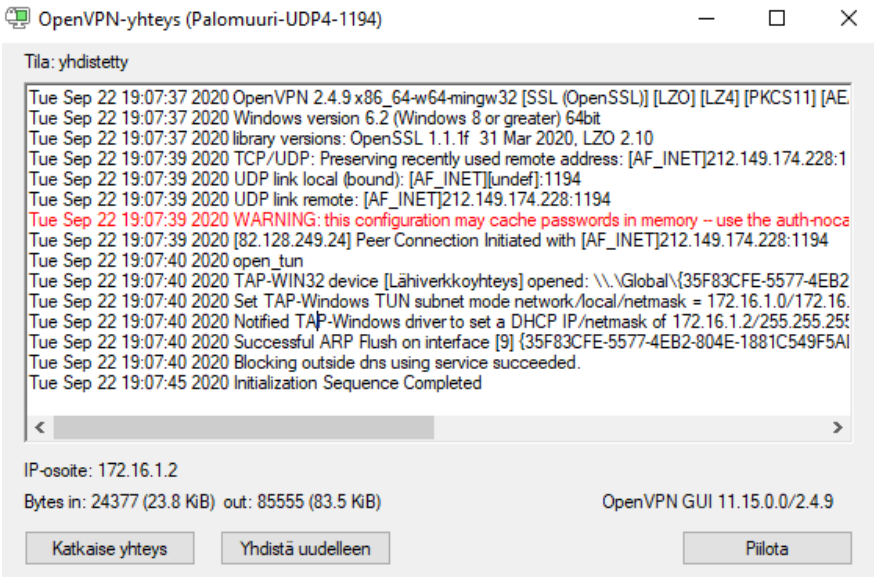
Kuva 13. Nslookup komennon tuloste.

Jotta voidaan kokeilla Suricatan toimintaa, kokeillaan ladata tiedostoa HTTP yhteyden yli. Tästä syntyy hälytys, sillä exe tai dll päätteellisten tiedostojen lataaminen suojaamattoman yhteyden kanssa on säännöissä estetty. Lisäksi voidaan huomata, että sisäverkossa olevaa tietokonetta on koitettu käyttää luvattomasti yhdistämällä etätyöpöytäyhteyden käyttämään porttiin. Ip-osoitteet, joista hyökkäykset ovat tulleet kuuluu kuitenkin huonon maineen omaaviin osoitteisiin, joten pääsy on estetty. Kuvassa 14. on Suricatan lokitusta näistä yrityksistä.

Date	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
09/19/2020 20:13:56	2	TCP	Misc Attack	170.130.187.50	50822	192.168.1.10	3389	1:2525007	ET 3CORESec Poor Reputation IP group 8
09/19/2020 18:44:42	2	TCP	Misc Attack	52.175.248.102	49707	192.168.1.10	3389	1:2403333	ET CINS Active Threat Intelligence Poor Reputation IP group 34
09/19/2020 18:39:25	1	TCP	Potential Corporate Privacy Violation	62.165.155.122	80	192.168.1.10	51461	1:2018959	ET POLICY PE EXE or DLL Windows file download HTTP

Kuva 14. Suricatan loki.

VPN yhteyden testaamista varten asennetaan OpenVPN asiakasohjelma ja ladataan luotu profiili. Kuvassa 15. huomataan, että VPN yhteyden luominen onnistuu ja saadaan ip-osoite 172.16.1.2 kuten pitääkin.



Kuva 15. OpenVPN asiakasohjelma.

6 YHTEENVETO

PfSense on kustannustehokas ratkaisu, ohjelmistoon ei tarvitse ostaa lisenssejä. Sen tarjoamat ominaisuudet ovat laajat ja vastaavat tai jopa ylittävät kaupallisten palomuurien tarjonnan. Konfiguraatio on tehty helposti lähestyttäväksi, sekä tehokkaaksi. Ohjelmisto on hyvin dokumentoitu ja vinkkejä löytyy Netgaten ylläpitämältä keskustelupalstalta.

Tässä työssä törmäsin vain yhteen ongelmaan, IPv6 ei saatu toimimaan. Syy ei kuitenkaan ollut palomuurissa itsessään vaan valokuitumodeemissa, jolla verkkoyhteys muodostetaan. Huonona puolena palomuurissa on vaikeus analysoida salattua liikennettä, jota iso osa verkkoliikenteestä nykyään on.

Työssäni havaitsin PfSensen toimivaksi ratkaisuksi SOHO-ympäristön suojaukseen. Suosittelen sen käyttöön ottamista kaikissa yli yhden henkilön yrityksissä. Etätyön lisääntyessä ja ihmisten työskennellessä kotoa käsin on ajankohtaista miettiä myös verkon suojaamista. Tässä on hyvä tilaisuus it alan yrityksille tarjota palveluna palomuurin asennusta ja konfiguroimista.

LÄHTEET

Dr. Comer, E. Douglas. Internetworking with TCP/IP Principles, Protocols and Architectures, Fourth Edition 2002.

Tom Thomas. Network Security first-step 2004.

PfSense. pfSense Documentation 2020. Viitattu 16.7.2020. https://docs.netgate.com/pfsense/en/latest/

PfSense. pfSense Firewall Appliance Features 2020. Viitattu 12.7.2020. https://www.netgate.com/solutions/pfsense/features.html

PfSense. Getting Started 2020. Viitattu 12.7.2020. https://www.pfsense.org/getting-started/

PfSense. Software Release Schedule 2020. Viitattu 1.9.2020. https://docs.netgate.com/pfsense/en/latest/development/software-release-schedule.html

Cisco. What Is a Next-Generation Firewall? Viitattu 17.7.2020. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html

Cisco. What Is a Firewall? Viitattu 22.7.2020. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Juniper. What is IDS and IPS? Viitattu 2.8.2020. https://www.juniper.net/uk/en/products-services/what-is/ids-ips/

Juniper. Intrusion Detection and Prevention 2016. Viitattu 2.8.2020. https://www.juniper.net/documentation/en_US/learn-about/LA_IntrusionDetectionandPrevention.pdf

Paloaltonetworks. The World's First ML-Powered NGFW. Viitattu 5.8.2020. https://www.paloaltonetworks.com/network-security/next-generation-firewall

Paloaltonetworks. What Is a Site-to-Site VPN? Viitattu 29.9.2020. https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn

Paloaltonetworks. PA-220 firewall. Viitattu 2.10.2020. https://www.paloaltonetworks.com/network-security/next-generation-firewall/pa-220

Opnsense. About OPNsense. Viitattu 6.8.2020. https://opnsense.org/about/about-opnsense

Rob Cameron, Brad Woodberg. Juniper SRX Series 2013. Viitattu 1.10.2020. https://www.oreilly.com/library/view/juniper-srx-series/9781449339029/ch13.html#acl_versus_fw_versus_appfw_versus_ips

Netgate. XG-1537 1U palomuuri. Viitattu 2.10.2020. https://www.netgate.com/solutions/pfsense/xg-1537-1u.html

Pfsense. Hardware. Viitattu 2.10.2020. https://docs.netgate.com/pfsense/en/latest/hardware/index