CLEAROS

Asennus ja käyttöönotto

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulun opinnäytetyö

Tietotekniikan ko.

Riihimäki, 12.5.2010

Tero Nylund

HAMK
HÄMEEN AMMATTIKORKEAKOULU

OPINNÄYTETYÖ

Tietotekniikan koulutusohjelma
Riihimäki

Työn nimi	ClearOS - Asennus ja käyttöönotto
Tekijä	Tero Nylund
Ohjaava opettaja	Raimo Hälinen
Hyväksytty	_____._____.20_____
Hyväksyjä	

HAMK
HÄMEEN AMMATTIKORKEAKOULU

TIIVISTELMÄ

Riihimäki
Tietotekniikan ko.
Tietoliikenteen suuntautumisvaihtoehto

Tekijä Tero Nylund **Vuosi** 2010

Työn nimi ClearOS - Asennus ja käyttöönotto

TIIVISTELMÄ

Opinnäytetyön tarkoituksena oli tutustua ClearOS-palomuuriohjelmistoon ja eritoten tämän palomuuriominaisuuksiin.

Opinnäytetyön käsittelemiin teoria-osioihin tutustuttiin tutkimalla palomuuriin liittyvää materiaalia. ClearOS-palomuuriohjelmiston ominaisuuksiin tutustuttiin ClearFoundationin tarjoamalla käyttöohjeella. Tämän ohjekirjan avulla pystyttiin toteuttamaan ominaisuuksien testaaminen testiverkossa. Testiverkko koostui tietokoneesta, johon ClearOS-palomuuriohjelmisto asennettiin, Cisco-kytkimestä, HP-tulostimesta ja testikoneesta.

ClearOS-palomuuriohjelmisto osoittautui toimivaksi ohjelmistoksi suojaamaan sekä yrityksen, että kotikäyttäjien verkkoa. Valitettavasti ominaisuuksien puolesta ei kuitenkaan IPv6-verkolle ollut tukea, vaikka tämä on ottamassa koko aika enemmän jalansijaa nykyisissä IPv4-verkoissa.

Avainsanat Palomuuri, Linux, ClearOS

Sivut 51 s, + liitteet 1 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

Riihimäki
Degree Programme in Information Technology
Information Technology

Author Tero Nylund **Year** 2010

Subject of Bachelor's thesis ClearOS - installation and initialization

ABSTRACT

The purpose of this thesis was to explore ClearOS firewall software and in particular its firewall properties.

The theoretical part of this thesis was obtained from firewall-related material. The information on the features of the ClearOS firewall software was obtained from the user guide provided by ClearFoundation. With the help of the user guide, the features were tested in a test network. The test network consisted of a computer on which ClearOS firewall software was installed, a Cisco-switch, a HP printer, and the test machine.

ClearOS firewall software proved for be effective to protecting the company's network and user's home network. Unfortunately the properties did not support IPv6 networks which are taking a greater foothold in the current IPv4 networks.

Keywords Firewall, Linux, ClearOS

Pages 51 p + appendices 1 p.

TERMIT JA LYHENTEET

AH - Authenticating Headers - Harvemmin käyetty protokolla, jota IPsec käyttää pakettivirtojen salaamiseen.

CPU - Central Processing Unit - Prosessori on tietokoneen osa, joka suorittaa ohjelmien konekielisiä käskyjä.

CUPS - Common UNIX Printing System - Useissa UNIX-yhteensopivissa järjestelmissä toimiva avoin tulostusohjelmisto.

DCHP - Dynamic Host Configuration Protocol - Verkkoprotokolla, jonka yleisin tehtävä on jakaa IP-osoitteet lähiverkkoon liitetyille laittelle.

DNS - Domain Name System - Nimipalvelin, joka muuttaa verkkotunnukset IP-osoitteiksi.

DVB - Digital Video Broadcasting - Standardi, joka määrittelee digitaalitelevisiosignaalin jakelutavan.

ESP - Encapsulating Security Payload - Protokolla, jota IPsec käyttää pakettivirtojen salaamiseen.

FTP - File Transfer Protocol - TCP-protokollaa käyttävä tiedostonsiirtomenetelmä kahden tietokoneen välille.

GRE - Generic Routing Encapsulation - Ciscon kehittämä IP-tunnelointiprotokolla.

HTTP - Hypertext Transfer Protocol - Protokolla, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon.

HTTPS - Hypertext Transfer Protocol Secure - HTTP-protokollan salattu versio.

ICMP - Internet Control Message Protocol - TCP/IP-pinon kontrolliprotokolla, jolla lähetetään nopeasti viestejä koneesta toiseen.

IGMP - Internet Group Management Protocol - TCP/IP-pinon protokolla, joka mahdollistaa asiakkaiden liittymisen multicast-ryhmään.

IMAP - Internet Message Access Protocol - Sähköpostien lukemiseen tarkoitettu protokolla.

IP - Internet Protocol - TCP/IP-mallin Internet-kerroksen protokolla, joka huolehtii IP-tietoliikennepakettien toimittamisesta perille pakettikytkentäisessä Internet-verkossa.

IPsec - IP Security Architecture - Joukko TCP/IP-perheeseen kuuluvia tietoliikenneprotokollia Internet-yhteyksien turvaamiseen.

IPtables - Linux-kernelin sisäänrakennetun palomuurin, netfilter:in käyttöliittymä.

IPTV - Internet Protocol television - Protokolla, joka mahdollistaa DVB-signaalin siirron verkon ylitse.

LDAP - Lightweight Directory Access Protocol - Hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla.

MAC - Media Access Control - Verkkokortin ethernet-verkossa yksilöivä osoite.

NTP - Network Time Protocol - Protokolla täsmällisen aikatiedon välittämiseen tietokoneiden välillä.

POP - Post Office Protocol version - Vanhin, yksinkertainen ja tunnetuin sähköpostin hakemiseen tarkoitettu protokolla

QoS - Quality of Service - Termi, jolla tarkoitetaan tietoliikenteen luokittelua ja priorisointia.

RAM - Random access memory - Tietokoneen työmuisti, johon ladataan käyttöjärjestelmän ohjelmat, suoritettavat sovellukset ja näiden tarvitsemat muut tiedot.

SCP - Secure Copy - Suojattu tiedostojen siirto tietokoneelta palvelimelle, perustuu SSH-protokollaan.

SSDP - Simple Service Discovery Protocol - Etsintäprotokolla, jota käytetään etsimään verkossa muita vastaavia laitteita.

SSH - Secure Shell - Protokolla, joka on tarkoitettu turvalliseen tiedonsiirtoon.

SSL - Secure Sockets Layer - Salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli.

TCP/IP - Transmission Control Protocol / Internet Protocol - Usean Internet-liikennöinnissä käytettävän tietoverkkoprotokollan yhdistelmä.

TCP - Transmission Control Protocol - Tietoliikenne protokolla, jolla luodaan yhteyksiä tietokoneiden välille.

UDP - User Datagram Protocol - Yhteyskäytäntö, jolla sovellus voi lähettää viestejä toiselle tietokoneelle.

UPnP - Universal Plug and Play - Joukko verkkoprotokollia, joiden tarkoituksena on saada erilaiset laitteet (esimerkiksi mediatoistimet, mediapalvelimet ja palomuurit) toimimaan helposti yhdessä valmistajasta riippumatta.

VPN - Virtual Private Network - Termi, jolla tarkoitetaan kahden tai useamman verkon yhdistämistä julkisen verkon yli yksityiseksi verkoksi.

WAN - Wide Area Network - Tiedonsiirtoverkko, joka peittää laajoja maantieteellisiä alueita kuten Eurooppa tai kokonaisuudessa Internet.

PORTTILISTA

20/TCP - File Transfer Protocol, Tiedot - FTP

21/TCP - File Transfer Protocol, Ohjaus (komennot) - FTP

22/TCP,UDP - Secure Shell - SSH

47/TCP - Generic Routing Encapsulation - GRE

53/TCP,UDP - Domain Name System - DNS

67/UDP - Dynamic Host Configuration Protocol, Palvelin - DHCP

68/UDP - Dynamic Host Configuration Protocol, Asiakas - DHCP

80/TCP,UDP - Hypertext Transfer Protocol - HTTP

109/TCP - Post Office Protocol 2 - POP 2

110/TCP - Post Office Protocol 3 - POP 3

123/TCP - Network Time Protocol - NTP

143/TCP,UDP - Internet Message Access Protocol - IMAP

443/TCP - Hypertext Transfer Protocol Secure - HTTPS

1293/TCP,UDP - Internet Protocol Security - IPsec

1900/UDP - Simple Service Discovery Protocol - SSDP

5000/TCP - Universal Plug and Play - UPnP

SISÄLLYS

1 JOHDANTO 1

2 PALOMUURI 2

2.1. Tekniikat 2
2.2. Heikkoudet 3
2.3. ClearOS 3
2.4. Keskeisimmät ominaisuudet 3
2.5. Järjestelmävaatimukset 4
2.6. Testiympäristö 5

3 ASENNUS 7

3.1. ClearOS 7
3.2. Ensimmäinen käynnistys 15
3.3. Palomuuriohjelmiston rekisteröinti 18
3.4. Valikot ja sisältö 18
3.5. Directory (Hakemisto) 19
3.6. Network (Verkko) 19
3.7. Gateway (Yhdyskäytävä) 20
3.8. Server (Palvelin) 22
3.9. System (Järjestelmä) 22
3.10. Reports (Raportit) 23
3.11. ClearCenter 24

4 KÄYTTÖÖNOTTO 26

4.1. Palvelut 26
4.2. Yhteydet 27
4.2.1. Incoming 27
4.2.2. Outgoing 29
4.3. Advanced firewall module (Täsmentävä palomuuri moduuli) 29
4.4. Porttiohjaus 31
4.5. Universal Plug and Play (UPnP) 32
4.6. Quality of Service (QoS) 32
4.7. Intrusion Detection 35
4.8. Intrusion Prevention 37
4.9. Käyttäjän luonti 37
4.10. Elisa Viihde 40

5 PALVELUT 41

5.1. Web-palvelin 41
5.1.1. Tiedostojen siirto 42
5.1.2. Käynnistys 42
5.1.3. Yhteenveto 43
5.2. Tulostinpalvelin 43
5.3. Verkkojako 46
5.3.1. Tulostimen lisäys 48
5.3.2. Yhteenveto 48
5.4. Raportit 48

6 YHTEENVETO 50

LÄHTEET 51

Liite 1 IGMPProxyn konfiguraatio

1 JOHDANTO

Yrityksille ja kuluttajille on tärkeää nykypäivänä suojata oma verkkonsa. Tätä varten on olemassa palomuuri, jolla verkon suojaus voidaan toteuttaa. Palomuuri voi toimia, joko ohjelmisto- tai rautapohjaisena. Ohjelmistopohjainen palomuuri sopii parhaiten kun halutaan suojata yksi tietokone mutta kun määrä kasvaa, on järkevämpää ottaa käyttöön rautapohjainen versio. Tämä takaa paremman hallittavuuden suuremmissa verkoissa.

Tämän opinnäytetyön aiheena on ClearOS-palomuuriohjelmisto, eikä tässä opintonäytetyössä perehdytä ClearOS-palomuuriohjelmiston alla toimivaan Linux-käyttöjärjestelmään vaan siihen, kuinka ClearOS-palomuuriohjelmisto asetetaan käyttökuntoon. Lisäksi perehdymme työssä palomuurin toimintaan, sekä ClearOS-palomuuriohjelmiston asennukseen ja käyttöönottoon. Tämän lisäksi tutkimme, voiko ohjelmiston mukana olevia palveluita kuten Web-palvelinta hyödyntää ilman, että tämä vaarantaisi ohjelmiston tietoturvaa.

Lisäksi perehdymme eri protokollien läpivientiin palomuurissa. Tämän lisäksi tutkimme onko ClearOS-palomuuriohjelmistolla mahdollista luoda nykyaikainen IPv6-sisäverkko.

Työn laatiminen vaatii ensimmäisenä tutustumista itse ClearOS-palomuuriohjelmiston syövereihin ja sen mahdollisuuksiin.

2 PALOMUURI

Palomuurin tarkoituksena on suodattaa suojattavan verkon ja vaarallisen verkon välisiä yhteyksiä. Palomuuri voidaan toteuttaa ohjelmisto- tai rautapohjaisena. Palomuurin toimintaan ja tekniikoihin tutustuttiin Wikipedian englanninkielisellä artikkelilla, joka käsittelee palomuuria. (Firewall, Wikipedia, 2010.)

2.1. Tekniikat

Palomuuri voidaan toteuttaa monella eri tekniikalla. Ensimmäinen tapa on tehdä palomuurista pakettisuodatin. Tällöin paketit etsitään pakettien lähde- ja kohdeosoitteiden sekä porttien perusteella. Pakettisuodatinpalomuureja on olemassa kahta eri mallia, tilaton ja tilallinen. Tilaton palomuuri vertailee jokaista pakettia palomuurin sääntöihin ja jos huomataan, että paketti ei ole sallittujen joukossa, se tiputetaan. Kuitenkin tilallinen palomuuri on tässä asiassa parempi vaihtoehto, koska se tutkii liikenteen tarkemmin. Tilallinen pitää kirjaa eri TCP- sekä UDP-yhteyksistä ja näin ollen sallii vain näihin yhteyksiin kuuluvat paketit. Tämä tarkoittaa käytännössä sitä, että palomuuri pitää samoja tietoja yllä kuin TCP/IP-paketti.

Tilaton palomuuri ei kuitenkaan ole täydellinen edellä mainitun asian takia. Suurin tilattoman ongelma on, että kaikkia paluupakettien portteja ei voida tietää tarkalleen mikä johtaa siihen, että joidenkin verkkojen toimivuutta ajatellen on aukaistava kaikki yli 1024 olevat portit. Tämä taas aiheuttaa, että palveluun voidaan ottaa yhteys ilman palomuurin välissä oloa.

Kuten yllä mainittiin, niin tilallinen palomuuri tarkkailee jokaista pakettia ja tarkistaa, kuuluuko tämä olemassa olevaan yhteyteen. Jos yhteys on jo olemassa, niin palomuuri päästää nämä paketit lävitse. Ensimmäistä kertaa avattaessa yhteyttä palomuuri tutkii sääntöjään ja tarkistaa niistä onko yhteys sallittu näiden perusteella. Kun yhteys hyväksytään, lisätään tämän tiedot palomuurin yhteyslistaan ja samalla yleensä sallitaan yhteyteen liittyvät ICMP-sanomat. Yhteyden sulkeutuessa tai kun yhteys on käyttämätön tietyn aikaa, yhteys poistetaan yhteyslistalta. Tämän jälkeen tähän yhteyteen kuuluvia paketteja ei enää päästetä lävitse. Tilallisessa on myös sama ongelma tuntemattomien protokollien kanssa kuin tilattomassa, mutta tilallisen hyvänä puolena siihen voidaan lisätä sääntöjä protokollien suhteen. Pakettisuodatin toimii kuljetuskerroksella.

Viimeisenä vaihtoehtona on sovelluspalomuuri. Tässä vaihtoehdossa palomuuri tarkastelee paketin sisältämää dataa. Esimerkiksi jos paketin portti on 80 (HTTP), niin paketin sisältö tarkistetaan laittomien komentojen takia. Sovelluspalomuuri toimii sovelluskerroksella.

Suurin osa nykyisistä palomuureista on sovellus- ja tilallisen palomuurin yhdistelmiä. Näiden etuna on, että sovellus itsessään jo vaikuttaa siihen sallitaanko yhteys. Tämän etu on, että tiedetään tarkalleen mitkä palvelut ovat sallittuja ja mitkä eivät. Lisäksi tiedetään mihin liikenne kohdistuu.

2.2. Heikkoudet

Palomuurin tarkoituksena on suodattaa tämän lävitse kulkevia yhteyksiä. Joten tämä ei estä sitä, että verkkoon pääsisi kiinni toista kautta kuten langattoman lähiverkon kautta tai ennen kaikkea fyysisesti. Lisäksi palomuuri ei kykene suodattamaan esimerkiksi IPsec-salattua liikennettä, josta ei yleensä selviä kohdeporttia tai edes kohdekonetta. Tämän johdosta VPN-liikenne pyritään viemään erilliseen eteisverkkoon, josta se voidaan viedä salaamattomana palomuurin lävitse.

2.3. ClearOS

ClearOS-palomuuriohjelmiston ominaisuuksiin ja järjestelmävaatimuksiin tutustuttiin ClearFoundation-sivuston (2010) avulla.

ClearOS on ilmainen ja open source -pohjainen palomuuriohjelmisto pienille ja keskisuurille yrityksille, ja sitä on helppo käyttää Web-hallinnan kautta. Web-hallinnan takia aikaisempaa Linux kokemusta ei tarvita. ClearOS kehittäminen aloitettiin vuonna 2009 ClearFoundation toimesta. Vakaa versio 5.1 ClearOS:stä julkaistiin 23. joulukuuta 2009. ClearOS:n edeltäjänä toimi ClarkConnect-palomuuriohjelmisto, jonka kehitys päätettiin kun ClearOS julkaistiin saataville.

ClearOS-palomuuriohjelmisto perustuu CentOS-käyttöjärjestelmään, joka taas perustuu kaupalliseen Red Hat Enterprise Linuxiin. (CentOS, 2010.)

Työssäni käytän viimeisintä vakaata versiota ClearOS:stä, joka on tällä hetkellä Enterprise 5.1 Service Pack 1.

2.4. Keskeisimmät ominaisuudet

Alla olevasta listasta selviää ClearOS:n keskeisimmät ominaisuudet. ClearOS eroaa merkittävimmin muista ilmaisista palomuuriohjelmistoista tarjoamalla suoraan palvelin ominaisuuksia kuten tiedostojen jakaminen, tulostinpalvelun ja sähköpostipalvelimen.

Hakemisto-ominaisuudet

- Integroitu LDAP-hakemistopalvelu käyttäjille ja ryhmille
- Käyttäjän suojavarmennus manageri

Verkko-ominaisuudet

- Multi-WAN
- VPN - PPTP, IPsec, OpenVPN
- DMZ ja 1-to-1 NAT
- Tilallinen palomuuri
- Paikallinen DHCP- ja DNS-palvelu

Yhdyskäytävä-ominaisuudet

- Antimalware - Antivirus, Antiphishing, Antispyware
- Antispam

- Kaistanhallinta
- Tunkeilijan suojaus, tunkeilijan esto, tunkeilijan havaitseminen
- Protokollasuodatin, joka sisältää Peer-to-Peer havaitsemisjärjestelmän
- Sisällönsuodatin
- Web Proxy
- Kulunvalvonta

Serveri-ominaisuudet

- Windows-verkko PDC tuella
- Tiedosto- ja tulostin palvelut
- Flexshares
- Groupware Outlook Connector tuella
- Sähköpostipalvelin - POP, IMAP, SMTP, Webmail, Haku
- Sähköpostin suodatus - Antispam, Antimalware, Harmaalistaus, Karanteeni
- Mail Filtering - Antispam, Antimalware, Greylisting, Quarantine
- Sähköpostiarkistointi
- Tietokanta MySQL tuella
- Web-palvelin PHP tuella

2.5. Järjestelmävaatimukset

ClearOS ei vaadi juuri mitään raudanosalta. Yleensä järjestelmävaatimuksethan ovat aina suuntaa antavia. Taulukosta 1 selviää minimijärjestelmävaatimukset. Tämän lisäksi taulukosta 2 selviää mitkä ovat prosessorin ja keskusmuistin vaatimukset käyttäjämäärän mukaan.

Taulukko 1 Minimijärjestelmävaatimukset

Peruslaitteisto	
Prosessori/CPU	Tuki jopa 16:sta prosessorille
Keskusmuisti/RAM	512 Mt on suositeltavaa
Kiintolevy	2 Gt on suositeltavaa
CD-asema	Asennuksen ajaksi
USB	Tarvitaan vain USB-tikku asennusta varten
Näytönohjain	Mikä tahansa näytönohjain
Diskettiasema	Ei vaadita
Äänikortti	Ei vaadita
Oheislaitteet	
Hiiri	Ei vaadita
Näyttö ja näppäimistö	Asennuksen ajaksi

Taulukko 2 Prosessorin ja keskusmuistin tarve käyttäjien mukaan

RAM ja CPU	**5 käyttäjää**	**5-10 käyttäjää**	**10-50 käyttäjää**	**50-200 käyttäjää**
Prosessori/CPU	500 MHz	1 GHz	2 GHz	3 GHz
Muisti/RAM	512 Mt	1 Gt	1.5 Gt	2 Gt

2.6. Testiympäristö

Testiympäristöni rakentuu Fujistu-Siemens minipc:lle, johon ClearOS asennetaan. Tämän tietokoneen kokoonpano selviää taulukosta 3.

Taulukko 3 ClearOS -kokoonpano

Prosessori	Pentium 4 1,6 GHz
Emolevy	Fujitsu Siemens
Keskusmuisti	1 Gt DDR
Kiintolevy	20 Gt
Verkkokortti	2 kpl 10/100 Mbit
CD-asema	On
Diskettiasema	On

Tämän lisäksi muita käyttäjäkoneita simuloidaan virtuaalisesti. Virtuaalikoneen kokoonpano näkyy taulukosta 4.

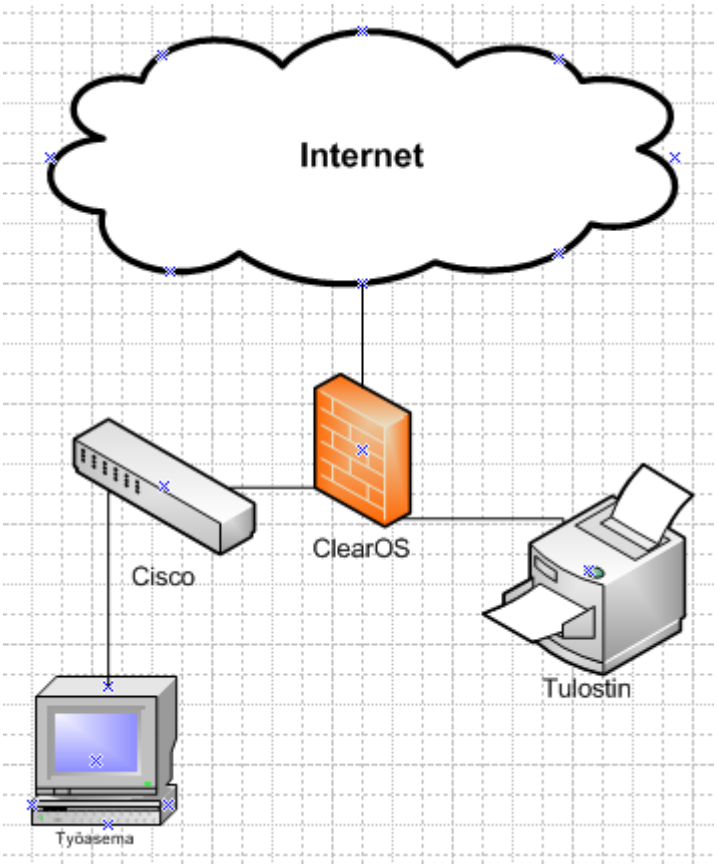
Taulukko 4 Virtuaalikoneen kokoonpano

Prosessori	Intel Core i7 920 2,6 GHz
Emolevy	Asus P6T Deluxe V2
Keskusmuisti	6 Gt DDR3
Kiintolevy	1T
Verkkokortti	2 kpl 10/100/1000 Mbit
CD-asema	Bluray

Tälle koneelle asennetaan VirtualBox-virtualisointiohjelmisto, jonka avulla voidaan asentaa virtuaalisesti mitä käyttöjärjestelmiä vain. Valitsin virtualisoitavaksi Windows 7 Ultimaten, koska suurin osa käyttäjistä käyttää Windows-käyttöjärjestelmää. Lisäksi voin tehdä tälle käyttöjärjestelmälle mitä muokkauksia vain ilman sitä pelkoa, että rikkoisin omassa käytössä olevan Windows 7:n.

Verkossa olevan kytkimen tarkoituksena on mahdollistaa myöhemmin lisättävien koneiden kytkentä testiverkkoon. Lisäämällä koneiden määrää saan tarkasteltua QoS-tekniikan toimintaa. Tulostimena testi verkossa toimii Hewlett-Packard-yhtion Photosmart 3180C -tulostin. Ulkomaailmaan toimii 24M/1M Full Rate -Internetyhteys

Testiympäristön verkkotopologia näkyy kuvasta 1.



Kuva 1 Testiympäristön verkkotopologia

3 ASENNUS

Asennus aloitettiin aluksi polttamalla ClearOS-palomuuriohjelmiston image-tiedosto CD-levylle. Kun poltto oli onnistuneesti tehty, oli aika siirtyä itse palomuuriohjelmiston asentamiseen.

3.1. ClearOS

Asennus aloitettiin laittamalla testikoneeseen äskettäin poltettu CD-levy, jolta sitten käynnistetään itse asennus käyntiin. Asennus kyseli monia perusasioita alussa, ja seuraavaksi käyn asennusvaiheet lävitse.

Kun asennus on käynnistynyt levyltä, asennus kysyy haluatko asentaa puhtaan asennuksen vai päivittää vai mennä pelastus-moodin, jolla voidaan pelastaa rikkoutunut palomuuriohjelmisto. Tästä jatketaan eteenpäin painamalla Enter-nappia, koska valitaan puhdas asennus. Tämä selviää kuvasta 2.

Kuva 2 Asennuksen aloitus

Seuraavaksi valitaan kieli, jolla ClearOS halutaan asentaa. Valitsin englannin, koska mahdollisissa eteen tulevissa ongelmatilanteissa on helpompi löytää näihin vastaus. Kielen valinta näkyy kuvassa 3. Haluttaessa voidaan myös asentaa suomenkielellä, mutta itse en nähnyt tälle tarvetta. Kielen voi kuitenkin vaihtaa asennuksen jälkeen tarvittaessa.

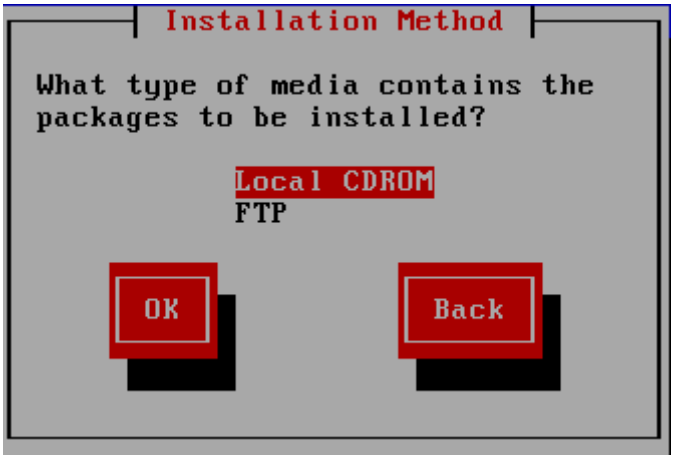
Kuva 3 Kielen valinta

Kun kieli on valittu, valitaan seuraavaksi näppäimistön tyyppi. Tähän valitsin suomenasettelun, koska muuten eivät kaikki näppäimistön merkit tule välttämättä samoista näppäinyhdistelmistä. Asennuksen aikana huomasin kuitenkin, että tällä ei juuri ole merkitystä olisiko ottanut englantilaisenasettelun koska asennuksen aikana ei ollut tarvetta käyttää mitään erikoisempia näppäinyhdistelmiä. Näppäimistönasettelu näkyy kuvasta 4.

Kuva 4 Näppäimistön tyyppi

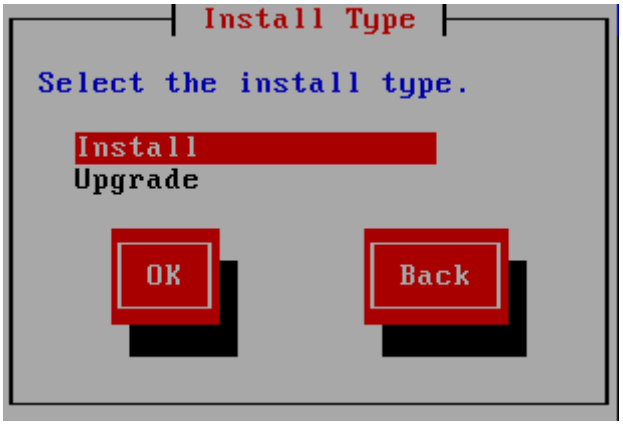
Näppäimistönasettelun jälkeen asennus kysyy mistä ClearOS halutaan asentaa. Tämä voidaan tehdä joko levyltä kuten itse tein tai vaihtoehtoisesti verkon kautta. Tämä on hyvä, jos ei ole tarpeeksi suurta

USB-tikkua saatavilla. Voidaan ClearOS asentaa verkon ylitse. Tämä näkyy kuvasta 4.



Kuva 5 Asennusmenetelmä

Asennustavan valinnan jälkeen voidaan valita halutaanko tehdä puhdas asennus vai päivittää palomuuriohjelmisto uudempaan versioon. Asennustapa näkyy kuvasta 6.



Kuva 6 Asennustapa

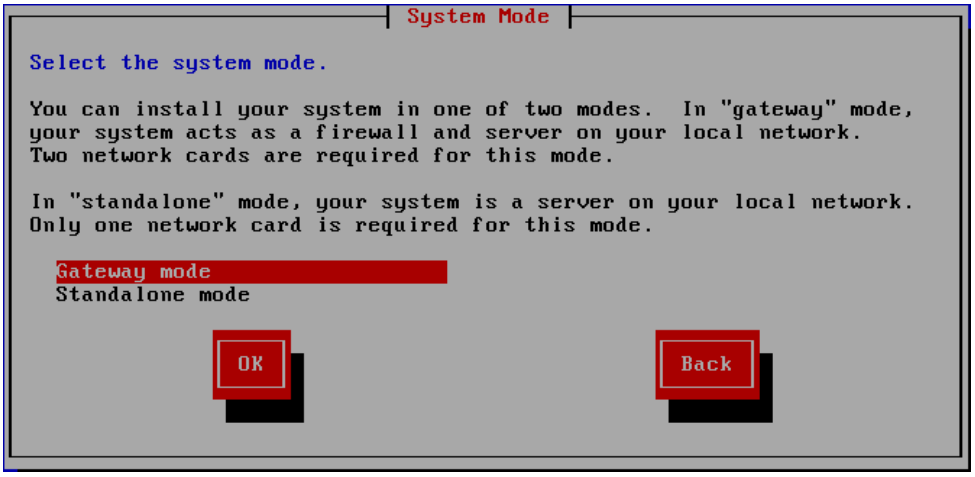
Seuraavaksi asennus kysyy haluatko varmasti jatkaa tästä eteenpäin. Tässä vaiheessa kannattaa lukea tarkkaan tiedot, koska varoitus kertoo hyvin selvästi, että kaikki kiintolevyt ja koneeseen liitetyt USB-laitteet tyhjentyvät. Tyhjennys tapahtuu kirjoittamalla ClearOS annettuun tekstikenttään. Tämä selviää kuvasta 7.

Kuva 7 Kiintolevyn tyhjennys

Tyhjennyksessä ei mennyt minulla kauaa, koska käytössä oli vain 20 Gt:n kiintolevy. Tyhjennyksen jälkeen asennus kysyy, minkätyyppiseen tilaan halutaan palomuuriohjelmisto asentaa. Vaihtoehtoina on Gateway-tila tai Standalone-tila.

Standalone-tila tarkoittaa, että järjestelmä toimii vain palvelimena olemassa olevassa verkossa. Tätä varten riittää vain yksi verkkokortti. Gateway-tilassa järjestelmä toimii palomuuria, oletusyhdyskäytävänä ja palvelimena verkossa johon se kytketään. Tätä tilaa varten tarvitaan kaksi verkkokorttia.

Palvelin asennettiin testiverkossa Gateway-tilaan, jolloin se toimii palomuurina, oletusyhdyskäytävänä ja palvelimena verkossa. Palomuuriohjelmiston tilan valinta näkyy kuvassa 8.



Kuva 8 Gateway-tila

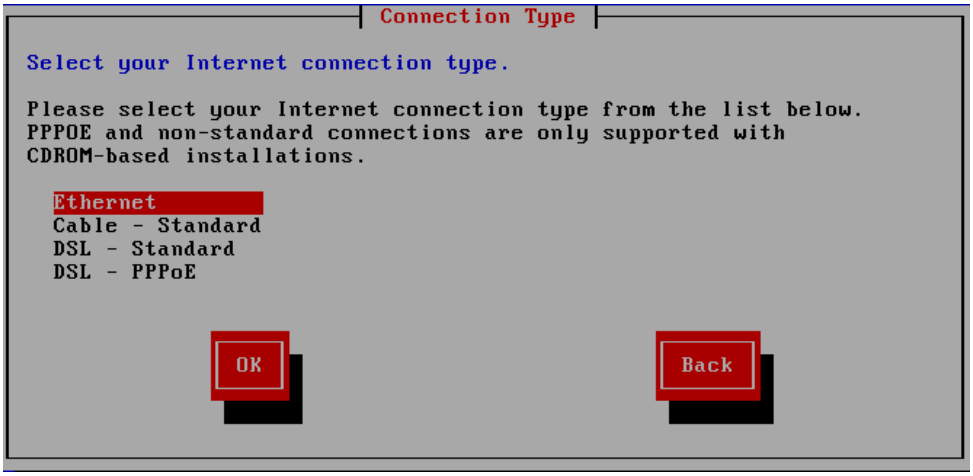
Palomuuriohjelmiston tilan jälkeen valitaan tapa, jolla Internet halutaan tuoda. Se voidaan tuoda joko suoraan verkkokortilla, kaapelilla tai DSL käyttämällä.

Verkkokortilla tuotuna Internet tarkoittaa, että on DSL-päätelaite josta tuodaan verkkokaapeli suoraan verkkokorttiin. Kaapeli ja DSL

vaihtoehdot tarkoittavat, että koneessa on erillinen PCI-väylään menevä DSL-sovitin. Nämä näkyvät kuvasta 9.

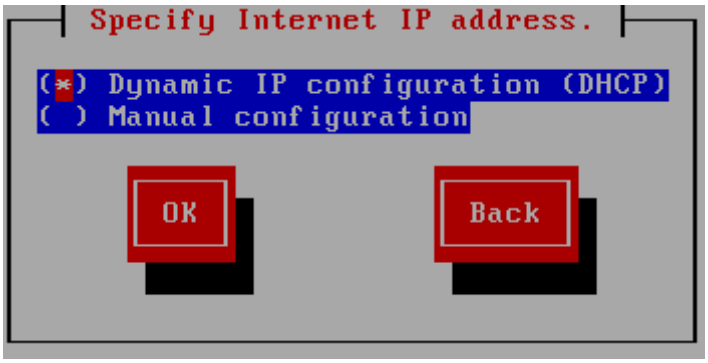
Jos asennus ei löydä verkkokortteja, voidaan näille asentaa USB-tikulta tai vastaavasta lähteestä ajurit. Kuten myös PCI-väyläisten DSL-sovittimien osalta.

Testiverkossani Internet tuodaan verkkokortille suoraan ADSL-päätelaitteelta.



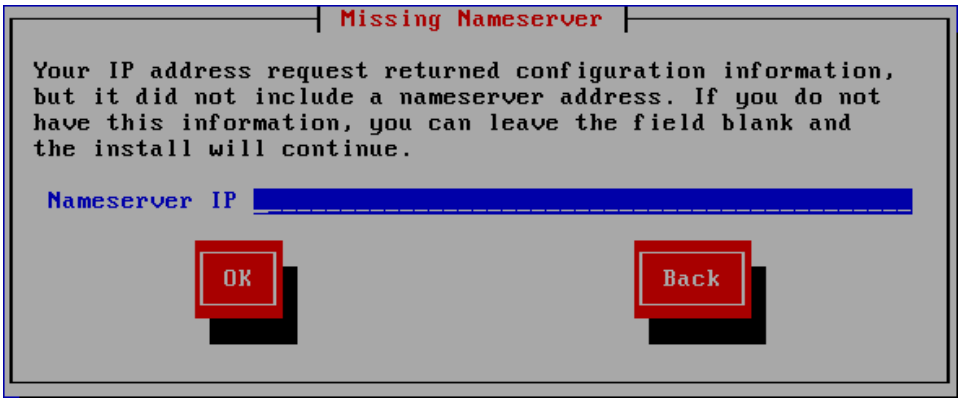
Kuva 9 Internet-liitännän valinta

Internet-liitännän jälkeen valitaan liitännälle miten tämä saa IP-osoiteen. Se voidaan ottaa suoraan DHCP:ltä kuten omassa tapauksessani tai vaihtoehtoisesti määritellä nämä asetukset manuaalisesti. Valintavaihtoehdot näkyvät kuvassa 10.



Kuva 10 Internet-liitännän IP-osoite

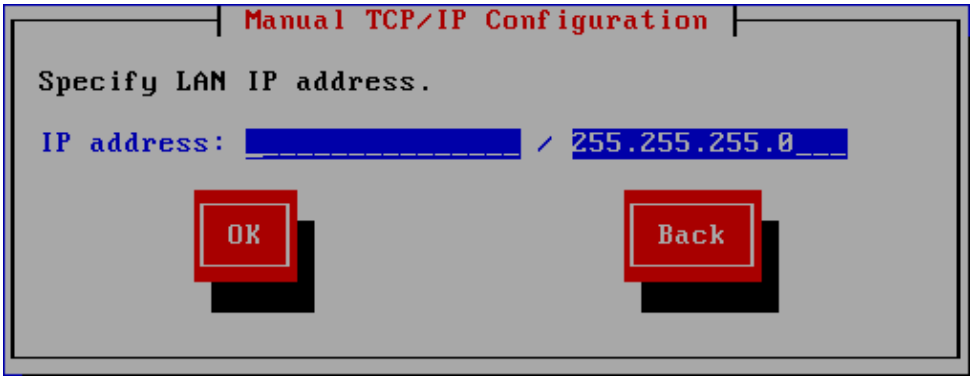
Seuraavaksi asennus ilmoittaa puuttuvasta nimipalvelimesta. Tämä johtuu siitä, että asennus ei löydä palvelinta, koska sitä ei minulla ole. Jos nimipalvelin on olemassa, voidaan sen IP-osoite määritellä sille osoitettuun kenttään, joka näkyy kuvasta 11.



Kuva 11 Puuttuva nimipalvelin

Puuttuvan nimipalvelimen jälkeen on aika määritellä sisäverkon verkkokortille tämän IP-osoiteavaruus. Tämä tehdään määrittelemällä sille varattuun kenttään IP-osoite ja tälle aliverkon maski. Tämä näkyy kuvasta 11. Harjoitusta varten määrittelin sisäverkon kortille 192.168.2.1 IP-osoitteen ja aliverkon maskiksi 255.255.255.0. Tämä antaa minulle käyttöön 254 IP-osoitetta. Lisäsyy, miksi halusin asettaa sisäverkon 192.168.2.0/24 -verkkoon, johtuu aivan siitä, että moni vakiona oleva ADSL-päätelaite jakaa automaattisesti IP-osoitteet 192.168.0.0/24 alueelta. Tällä vain halusin varmistaa, että ClearOS:n asennus ei sekoita verkkoa, jos tulee vääriä verkkokytkentöjä.

Loppupeleissä ei ole väliä minkä IP-osoiteavaruuden määrittelee sisäverkolle, koska ClearOS:ssa ei ole vakiona DHCP-palvelin päällä. Tällöin pitää muistaa se, että ensimmäistä kertaa otettaessa yhteyttä Web-hallintaan selaimen kautta pitää määritellä samasta IP-osoiteavaruudesta staattinen IP-osoite verkkokortille.

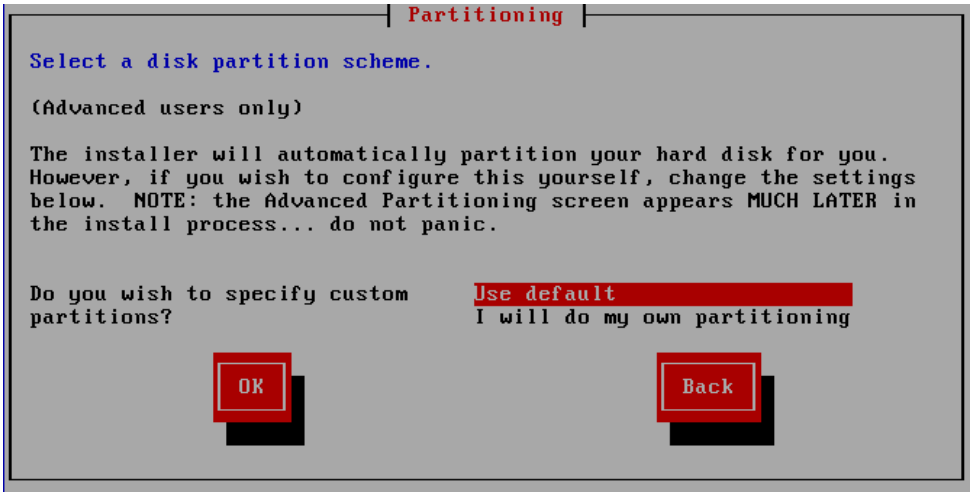


Kuva 12 Sisäverkon IP-avaruuden määrittely

IP-osoitteen määrittelyn jälkeen asennus kysyy root-käyttäjän salasanaa. On suositeltavaa, että root-käyttäjän salasanassa käytetään pieniä ja isoja kirjaimia sekä numeroita tietoturvallisuuden takia. Tämä sama ohjesääntö näkyy kuvassa 13.

Kuva 13 Salasanan määrittely root-käyttäjälle

Salasanan asettamisen jälkeen asennus kysyy miten kiintolevy halutaan osioida. Tämä voidaan toteuttaa käyttämällä asennuksen omaa automaattista osiointitapaa, jolloin koko kiintolevy varataan ClearOS varten. Vaihtoehtoinen tapa on itse määritellä omat osiot ja näiden koot. Osiointivaihtoehdot näkyvät kuvassa 14. Koska testiympäristössä ei tarvita niinkään palvelin ominaisuuksia kuten Web-palvelin tai Sambaa, niin helpointa tästä oli jatkaa valitsemalla automaattinen osiointi.

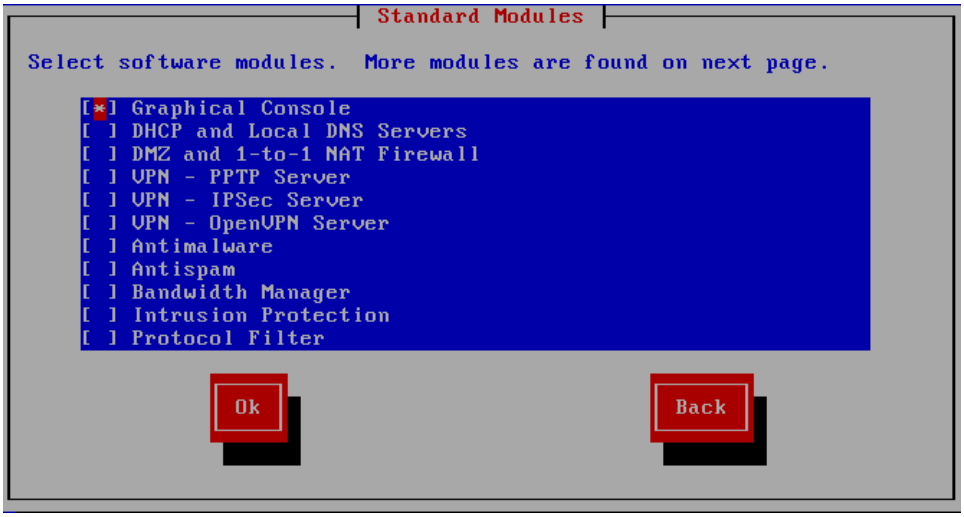


Kuva 14 Osioiden luonti

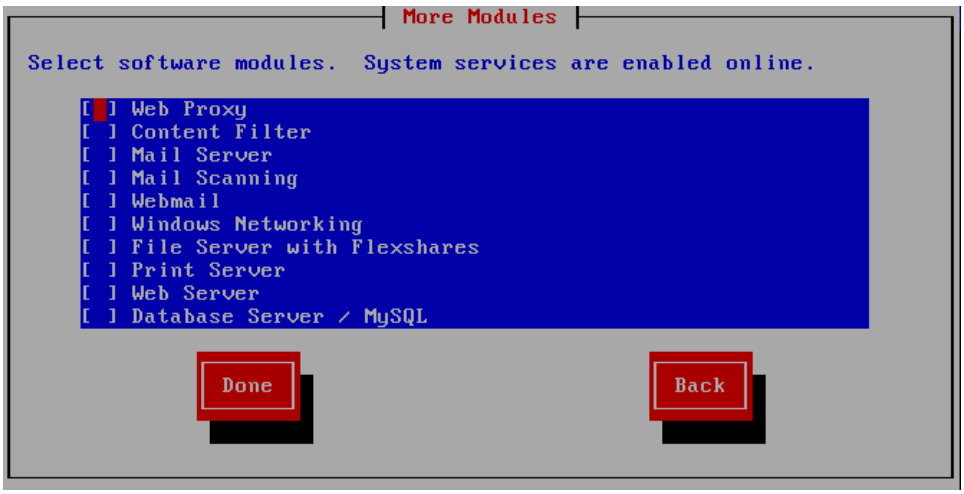
Osioiden luonnin jälkeen valitaan mitä moduuleita halutaan palomuuriohjelmistoon asentaa. Kaikkia ei ole tässä vaiheessa pakko asentaa, koska niitä voidaan asentaa tarpeen mukaan lisää kun palomuuriohjelmisto on pystyssä. Asennettavien moduulien määrä näkyy kuvista 15 ja 16.

Tässä vaiheessa valitsin testiympäristöön graafisen konsolin, joka tarkoittaa Web-hallinta, DHCP ja DNS -palvelut, kaistanhallinta, Windows-jako, tulostinpalvelu ja tunkeilijan esto moduulit. Näillä moduuleilla saadaan ilman mitään turhempia säädöksiä

palomuuriohjelmisto toimivaan kuntoon kun on ensimmäisen käynnistyksen aika.

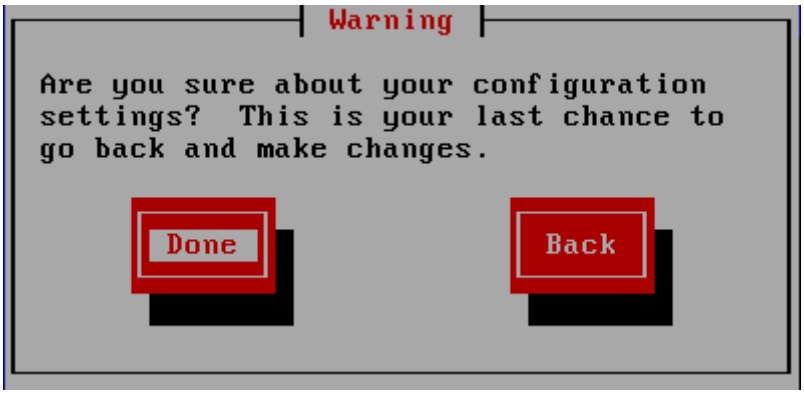


Kuva 15 Moduulien asennus



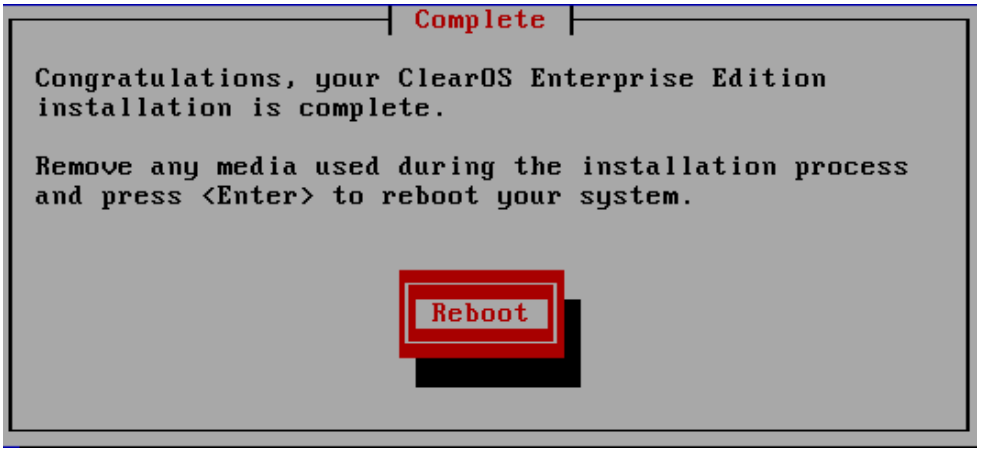
Kuva 16 Toinen listaus moduuleista

Lopuksi ennen asennuksen alkamista asennus kysyy käyttäjältä haluaako hän vielä muuttaa joitain asetuksia vai jatkaako asennukseen. Jos ei ole tarvetta tehdä muutoksia, niin varoituksesta pääsee eteen valitsemalla Done-napista, jolloin asennus alkaa. Varoitus näkyy kuvassa 17.



Kuva 17 Varoitus ennen asennusta

Tässä vaiheessa asennus alkaa asentaa kiintolevylle palomuuriohjelmiston tiedostoja ja tekemään sitä, mitä asennuksen aikana on määritelty. Kun tämä on suoritettu loppuun, antaa asennus viimeisen ilmoituksen, jossa kerrotaan, että CD-levy tulee ottaa pois asemasta ja käynnistää tietokone uudelleen Reboot-napista. Viimeinen asennusikkuna näkyy kuvassa 18.



Kuva 18 Tietokoneen uudelleenkäynnistys

3.2. Ensimmäinen käynnistys

Tietokoneen käynnistyttyä uudelleen tähän pääsee kiinni selaimella Web-hallinnan kautta, joka sijaitsee asennuksessa määritellyssä osoitteessa tai fyysisesti. Testiympäristössä Web-hallinnan osoite on https://192.168.2.1:81.

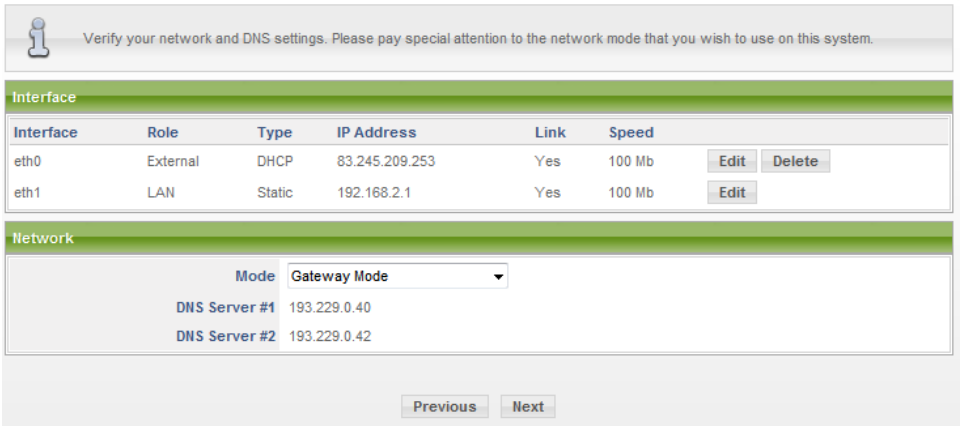
Kun selaimella on otettu yhteys, yllä mainittuun osoitteeseen avautuu ClearOS:n kirjautumissivu, joka näkyy kuvassa 19.

Kuva 19 ClearOS:n kirjautumisikkuna

Tämä sama kirjautumisikkuna näkyy myös kun konetta käytetään fyysisesti. Ainoa ero fyysisen koneen kirjautumisikkunassa on Login-napin vierestä puuttuva Exit to Console -nappi, jolla päästään koneen komentokehotetilaan.

Tästä eteenpäin kirjaudutaan root-käyttäjällä sisään, koska alussa ei ole luotuna muita käyttäjiä. Kun kirjautuminen on suoritettu, on aika valita palomuuriohjelmiston kieli. Testiympäristössä siihen valittiin englanti. Tätä kieltä voidaan myöhemmin vielä muuttaa kieliasetuksista.

Kielen määrittelyn jälkeen palomuuriohjelmisto haluaa tarkistaa verkkokorttien IP-osoitteet ja näiden tilan, joka näkyy kuvasta 20.

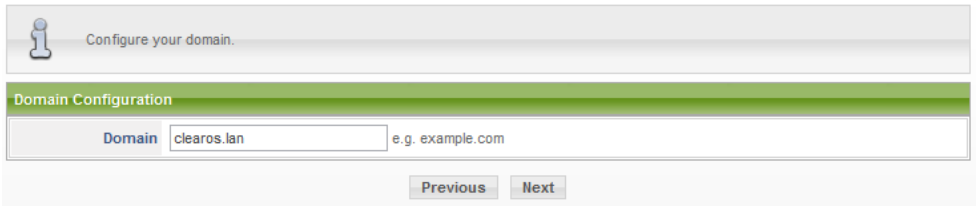


Kuva 20 Verkkokorttien asetusten tarkistus

Kuten kuvasta 20 näkyy, niin ulkoverkkoon toimii eth0-verkkokortti ja sisäverkossa eth1-verkkokortti. Lisäksi nähdään mihin tilaan ClearOS on

asennettu ja DNS-palvelimet. Tässä vaiheessa voidaan vielä muuttaa verkkokorttien asetuksia, jos on tarvetta tai määritellä jokin muu, esimerkiksi kolmas verkkokortti, myös toimimaan ulkomaailmaan.

Asetusten tarkistamisen jälkeen halutaan varmistaa aika ja päivänmäärä. Tämän jälkeen kysytään mihin domainiin halutaan kyseinen kone liittää tai luodaanko oma. Domainin luonti näkyy kuvasta 21.

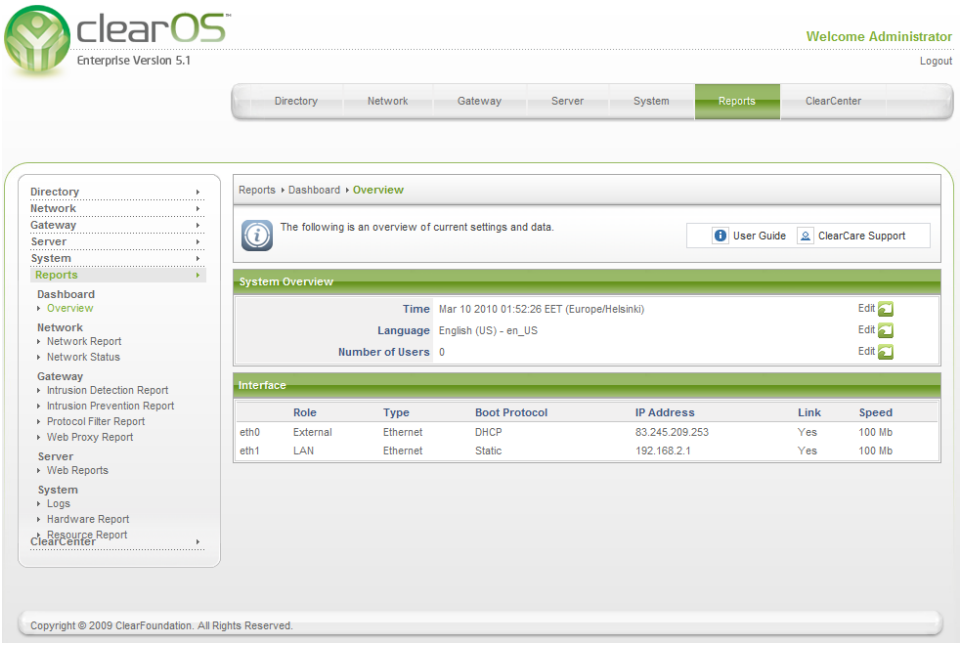


Kuva 21 Domainin luonti

Kun domain on luotu ja hyväksytty, on viimeisen kohdan vuoro. Tässä palomuuriohjelmisto kysyy organisaation tietoja ja sitä, mikä nimi koneelle asetetaan. Testiympäristössä koneen nimeksi annettiin hiiri. Tietojen antaminen näkyy kuvassa 22.

Kuva 22 Tietojen määrittely

Kun nämä vaiheet on suoritettu, on ClearOS valmis käytettäväksi ja tämän jälkeen käyttäjän eteen tulee aloitusikkuna, joka näkyy kuvassa 23.



Kuva 23 Aloitusikkuna

3.3. Palomuuriohjelmiston rekisteröinti

Ennen kuin ClearOS-palomuuriohjelmistoa voidaan käyttää kunnolla, pitää tämä rekisteröidä. Tämä tapahtuu menemällä ClearCenter-valikon alla olevaan Register-otsikon alla sijaitsevaan Register System-valikkoon.

Ensiksi täytyy luoda ClearSDN-tunnukset. Näitä varten on oma Register-linkki. Kun tunnukset on luotu, niin kirjaudutaan näillä sisään ja täytetään rekisteröintikaavake. Kun tämä on suoritettu, ClearOS on valmis ja tätä voidaan alkaa käyttää. Seuraavaksi käydään lävitse ClearOS:n valikkorakenne.

3.4. Valikot ja sisältö

Aloitusikkuna, joka näkyy kuvassa 23, on hyvin selkeä. Tästä nähdään ensimmäisenä verkkokorttien eli se, mikä on ClearOS-palomuuriohjelmiston kieli, aika ja päivänmäärä. Valikot on järjestetty ylös poikittain ja vasempaan reunaan allekkain. Molemmista löytyvät samat tiedot mutta vasemmassa reunassa oleva valikkorakenne näyttää samalla mitä kukin valikko pitää sisällä ja tästä voidaan valita suoraan se ilman, että tarvitsee valita ylävalikosta näitä osioita.

Valikkojen määrä ja sisältö riippuu siitä, mitä moduuleita palomuuriohjelmistoon on asennettu. Asennusvaiheessa testiympäristöön asennettiin Web-käyttöliittymä-, DHCP ja DNS -palvelu-, kaistanhallinta-, Windows-jako-, tulostinpalvelu- ja hyökkäyksenestomoduulit.

Lisäksi joidenkin palvelujen päälle kytkimen maksaa joitakin dollareita vuodessa, mutta näistä kerrotaan tarkemmin niiden tullessa eteen valikkoja käydessä lävitse.

Aloitamme käymällä valikot lävitse ja katsomalla mitä nämä oikein pitävät sisällään. Ensimmäisenä käydään Directory (Hakemisto) -valikko.

3.5. Directory (Hakemisto)

Tämän valikon alta löytyy Accounts (Tili), My Account (Oma tili) ja Setup (Asetukset) -otsikot.

Account pitää sisällään Users (Käyttäjät) ja Groups (Ryhmät) -valikot. Users-valikosta voidaan lisätä ClearOS-palomuuriohjelmistoon käyttäjiä tai poistaa näitä. Groups-valikosta voidaan taas lisätä käyttäjiä eri ryhmiin tai luoda oma ryhmä ja määritellä tälle myöhemmin ryhmän oikeudet.

My Account pitää sisällään User Profile (Käyttäjäprofiili) -valikon. Täältä voidaan muuttaa käyttäjän tietoja, kuten vaihtaa salasana ja vaihtaa käyttäjän tietoja.

Setup pitää sisällään Domain and LDAP (Verkkotunnus ja LDAP), Organization (Organisaatio) ja Import/Export (Tuonti7Vienti) -valikot.

Domain and LDAP -valikosta voidaan vaihtaa palomuuriohjelmiston domain ja tarkistaa mihin tällä hetkellä se kuuluu. Lisäksi nähdään toimiiko LDAP-palvelin.

Organization-valikon alta nähdään ClearOS-palomuuriohjelmiston tietokoneen nimi ja ensimmäisessä käynnistyksessä annetut organisaation tiedot.

Viimeisenä Directory-valikossa on Import/Export-valikko, josta voidaan käyttäjiä tuoda CSV-tiedostolla tai viedä nämä CSV-tiedostoksi. Lisäksi voidaan ladata valmispohja käyttäjien tekoa varten, joko .CSV, .XLS tai .ODS -tiedostona.

3.6. Network (Verkko)

Network-valikko pitää sisällään Settings (Asetukset) ja Firewall (Palomuuri) -otsikot.

Settings alta löytyy seuraavat valikot IP Settings (IP-asetukset), Multi-WAN, DHCP Server (DHCP-palvelin) ja Local DNS Server (Paikallinen DNS -palvelin).

IP Settings -valikosta voidaan määrittää verkkokorttien IP-osoitteet tai vaihtaa näiden tilaa staattisesta IP-osoitteesta DHCP:ltä saatavaan tai määrittää DSL/PPPoe -yhteys. Lisäksi täältä nähdään missä tilassa palomuuriohjelmisto toimii Gateway, Standalone tai Standalone no Firewall. Nähtävinä ovat myös DNS-palvelimien IP-osoitteet. Tätä kautta voidaan myös lisätä virtuaalinen IP-osoite verkkokorteille, jos tälle on tarvetta.

Multi-WAN-valikosta voidaan muuttaa kuormaa eri verkkokorteille joilla on ulkomaailmaan yhteys. Lisäksi voidaan määrittää, että tietty protokolla tai tietty IP-osoitteen omaava laite käyttää määritettyä verkkokorttia ulkomaailmaan. Testiympäristössä on käytössä vain yksi ulkomaailmaan menevä verkkokortti.

DHCP Server -valikosta voidaan käynnistää tai pysäyttää DHCP-palvelin. Määrittää tälle IP-osoiteavaruus, josta IP-osoitteet jaetaan verkkoon liittyville laitteille. Lisäksi voidaan määrittää staattinen IP-osoite ja nähdään kelle DHCP-palvelin on luovuttanut mitkäkin IP-osoitteet ja näiden laitteiden MAC-osoitteet.

Local DNS Server -valikko pitää sisällään paikallisen verkon laitteiden IP-osoitteet ja näiden isäntänimet aliaksineen. Tänne voidaan tarvittaessa manuaalisesti lisätä omia osoitteita ja näille isäntänimet aliaksineen.

Firewall alta löytyvät seuraavat valikot Groups (Ryhmät), Incoming (Sisääntuleva), Outgoing (Ulosmenevä) ja Port Forwarding (Porttienohjaus) -valikot.

Groups-valikosta voidaan kytkeä päälle tai pois palomuurille tehtyjä sääntöjä.

Incoming-valikosta voidaan tehdä muutoksia sisään tulevan liikenteen osalta. Sisään tulevalle liikenteelle voidaan tehdä erilaisia sääntöjä kuten sallia tietty palvelu, osoittaa tämä tiettyyn porttiin tai porttialueeseen. Lisäksi voidaan torjua tietystä IP-osoitteesta tuleva liikenne kokonaan.

Outgoing-valikosta voidaan tehdä muutoksia ulosmenevän liikenteen osalta. Tässä on samat vaihtoehdot kuten sisään tulevalla liikenteellä mutta lisäksi voidaan valita joko niin, että palomuuri estää kaiken ulosmenevän liikenteen, paitsi sallitut ,tai sitten päästää kaiken ulos mutta estää estetyksi merkityn liikenteen.

Viimeisenä valikkona on Port Forwarding -valikko. Täällä voidaan tehdä erilaisia porttiohjauksia, joko palvelujen mukaan, määrittelemällä tietty portti toiseen porttiin tai porttialue tiettyyn IP-osoitteeseen.

3.7. Gateway (Yhdyskäytävä)

Gateway-valikko pitää sisällään seuraavat otsikot Antimalware, Bandwidth and QoS (Kaistanhallinta ja QoS), Intrusion Protection (Tunkeutumisen havaitsemisen suojaus), Protocol Filter (Protokolla fillteri) ja Proxy and Filtering (Proxy ja filtteröinti).

Antimalware alla on Antivirus Configuration (Virustorjunnan konfigurointi) ja Antiphishing Configuration (Tietojen kalastelun suojauksen konfigurointi)-valikot. Vakiona tämä ominaisuus ei ole päällä koska, jos tämä halutaan aktivoida, se maksaa 50 dollaria vuodeksi tai

vaihtoehtoisesti 135 dollaria kolmeksi vuodeksi. (ClearSDN Services, 2010.)

Antivirus Configuration -valikosta voidaan määrittää seuraavat asiat, estetäänkö kryptatut tiedostot, paljonko sallitaan Zip-tiedostoja ja mikä yksittäisen Zip-tiedoston koko saa olla ja kuinka useasti tietokanta päivitetään. Valitettavasti tästä ominaisuudesta pitää maksaa, koska tämä kuuluu Antimalwaren ominaisuuksiin.

Antiphishing Configuration -valikosta voidaan määrittää seuraavat asiat päälle tai pois, allekirjoitusmoottori, heuristinen moottori, estää SSL eroavaisuudet ja estää peitetyt url-osoitteet. Valitettavasti tästä ominaisuudesta pitää maksaa, koska tämäkin kuuluu Antimalwaren ominaisuuksiin.

Bandwidth and QoS alla sijaitsevasta Bandwidth (Kaistanhalinta) -valikosta voidaan määritellä miten eri protokollat tai portit saavat kaistaa käyttää. Kun valikko aukaistaan ensimmäistä kertaa, niin tähän pitää asentaa ulosmenevän liikenteen lähetys ja latausnopeudet kilobitteinä sekunnissa. Lisäksi voidaan käynnistää tai pysäyttää tämä palvelu.

Intrusion Protection alta löytyy Intrusion Detection (Tunkeutumisen havaitseminen) ja Intrusion Prevention (Tunkeutumisen esto) -valikot. Nämä ominaisuudet eivät ole automaattisesti ja näiden listojen päivittäminen maksaa viikossa 60 dollaria ja kuukausittain 35 dollaria. (ClearSDN Services, 2010.)

Intrusion Detection -valikko pitää sisällään jo valmiiksi kattavan listauksen yleisimmistä havaituista tavoista. Tämä lista voidaan käynnistää tai pysäyttää ja tarvittaessa käynnistymään uudelleen käynnistyksen yhteydessä.

Intrusion Prevention -valikosta voidaan suoraan estää tietty IP-osoite ja samalla nähdään mitkä IP-osoitteet on estetty tämän ominaisuuden toimesta. Näitä voidaan joko poistaa tai jättää listalle.

Protocol Filter -otsakkeen alla sijaitsee Protocol Filter Configuration (Protokolla filtterin konfigurointi) -valikko, joka pitää vakiona kattavan listan eri protokollista ja tiedoston päätteistä. Protokollia voidaan estää yksitellen tai estää kokonaisia ryhmiä. Tämä ominaisuus voidaan käynnistää tästä valikosta tai sammuttaa. Lisäksi voidaan tehdä omia ohituksia protokollille.

Proxy and Filtering alla on seuraavat valikot Content Filter (Sisällönsuodatus) ja Web Proxy.

Content Filter -ominaisuus on maksullinen ja listojen päivitys maksaa viikoittain 80 dollaria ja kuukausittain 40 dollaria. Onneksi kuitenkin tässäkin on kattava lista jo valmiina ja se sisältää yleisimmät tiedostonpäätteet. Tämä ominaisuus voidaan joko pysäyttää tai käynnistää. Vakiona tämä on poissa käytöstä. (ClearSDN Services, 2010.)

Web Proxy -valikosta voidaan määrittää proxyn toimintaa, ominaisuuksia ja paljonko tämä saa syödä kiintolevy tilaa. Vakiona tämä ei ole päällä. Lisäksi voidaan tehdä ohituksia eri domaineille tai IP-osoitteille.

3.8. Server (Palvelin)

Tämän valikon alta löytyy seuraavat otsikot Windows Networking (Windows-verkko), File and Print (Tiedosto ja Tulostus) ja Web.

Windows Networking pitää sisällän Windows Settings (Windows asetukset) -valikon, josta voidaan määritellä palvelimen nimi, mihin domainiin tämä kuuluu ja Windows järjestelmävalvojan salasana. Ennen kuin jakoa voidaan käyttää, pitää määritellä järjestelmänvalvojan salasana. Tämän jälkeen päästää valitsemaan mitä halutaan jakaa. Jakaminen toteutetaan Samba-ohjelmistolla.

File and Print sisältää Advanced Print Server (Kehittynyt tulostin palvelin) -valikon, josta voidaan tämä palvelu kytkeä päälle tai pois ja lisätä tulostin jaettavaksi. Tulostimen jakamisessa käytetään CUPS (Common UNIX Printing System) -ohjelmistoa. Tämä ohjelmisto toimii ClearOS:n kanssa omassa portissaan, joka on 631 ja versionumeroltaan ohjelmisto on 1.3.7, vaikka uusin vakaa versio on 1.3.9.

Viimeisenä valikkoa on Web Server (Web palvelin), joka sijaitsee Web-otsikon alla. Täältä voidaan käynnistää tai sammuttaa Web-palvelin ja nähdä tämän dokumentin päähakemisto. Vakiona tämä sijaitsee /var/www/html -polun takana. Tiedostojen siirto voidaan toteuttaa SCP:llä tai sitten FTP:n ylitse, joka voidaan asentaa valikon takaa.

3.9. System (Järjestelmä)

Tämän valikon alta löytyy seuraavat otsikot Settings (Asetukset), Backup (Varmuuskopiointi), Hardware (Kokoonpano), Resources (Resurssit) ja Security (Suojaus).

Settings pitää allaan Administrators (Järjestelmänvalvojat), Date (Päivänmäärä), Language (Kieli), Mail Notification (Sähköposti ilmoitus) ja Shutdown - Restart (Sammutus - Uudellenkäynnistys) -valikot.

Administrators-valikosta voidaan määritellä palomuuriohjelmiston käyttäjille eri oikeuksia. Näillä voidaan rajata eri käyttäjiä tiettyjä tehtäviä varten ja näin ollen parantaa samalla tietoturvaa. Vaikka joku ulkopuolinen saisi käyttöönsä yhden näistä käyttäjistä, hän ei voisi kuin vaikuttaa yhteen osaan, ja näin ollen muut osat säästyisivät ilkivallalta.

Date-valikosta voidaan määritellä käyttääkö ClearOS koneen omaa kelloa vai synkronoidaanko tämä NTP-palvelimen kanssa.

Language-valikosta voidaan valita palomuuriohjelmiston kieli. Englannin lisäksi löytyy lista muita kieliä, joista suomenkieli on yksi. Valitettavasti suomen kieli ei vielä kata kokonaan kaikkia valikoita ja osa valikoista onkin englanniksi.

Mail Notification -valikosta voidaan asettaa palomuuriohjelmisto lähettämään hätätilanteissa sähköpostia järjestelmänvalvojan sähköpostiin. Tämän avulla nopeutetaan vikatilanteiden korjaamista. Ennen kuin tämä lähetys toimii, pitää sinne määritellä ISP:n lähtevän postin palvelin.

Shutdown - Restart -valikosta voidaan tarvittaessa uudelleen käynnistää tai sammuttaa ClearOS. Tämä tulee tarpeeseen siinä vaiheessa kun palomuuriohjelmistoon on ajettu päivityksiä, jotka vaativat uudelleen käynnistyksen.

Backup pitää sisällään Backup Settings (Varmuuskopioiden asetukset) -valikon. Tällä järjestelmänvalvoja voi lataa omalle koneelleen suoraan varmuuskopiot palomuuriohjelmistosta ja tarvittaessa palauttaa nämä. Lisäksi sivulta näkyy, milloin viimeisin varmuuskopio on otettu.

Hardware pitää sisällään RAID-valikon. Täältä voidaan hallita RAID-pakkoja, jos näitä on tehty.

Resources pitää sisällään Processes (Prosessit) ja Services (Palvelut) -valikot.

Processes-valikon takaa paljastuva sivu näyttää ClearOS:ssa toimivat prosessit ja levossa olevat. Lisäksi voidaan tarvittaessa tappaa tai pysäyttää jokin prosessi.

Services-valikon takaa paljastuva sivu listaa palomuuriohjelmistossa toimivat palvelut. Näitä voidaan täältä sammuttaa, käynnistää ja muokata tarpeen mukaan.

Security pitää sisällään Certificate Manager (Sertifikaattien hallinta) -valikon. Täältä voidaan luoda SSL-sertifikaatteja ja hallita näitä. Tarvittaessa luoda oma, poistaa tai tarkastella näiden sisältöä.

3.10. Reports (Raportit)

Tämän valikon alta löytyy seuraavat otsikot Dashboard (Yleisnäkymä), Network (Verkko), Gateway (Yhdyskäytävä), Server (Palvelin) ja System (Järjestelmä).

Dashboars pitää sisällään vain yhden valikon Overview (yleiskatsaus). Täältä nähdään verkkokorttien tila, aika, päivänmäärä ja käyttäjien määrä. Tämä sama sivu näkyy ensimmäisenä kun kirjaudutaan käyttäjällä sisään.

Network pitää sisällään Network Report (Verkon raportointi) ja Network Status (Verkon tilanne) -valikot.

Network Report -valikon takaa löytyy graafisessa muodossa verkkokorttien käytön tilanne eri aikoina. Graafiset kuvaajat ovat päivän, viikon, kuukauden ja vuoden mukaan.

Network Status -valikon takaa voidaan monitoroida ja diagnosoida verkon yhteyksiä.

Gateway pitää sisällään Intrusion Detection Report (Tunkeutumisen havaitsemisen raportit), Intrusion Prevention Report (Tunkeutumisen esto raportit), Protocol Filter Report (Protokolla fillterin raportit) ja Web Proxy Report (Web proxyn raportit) -valikot. Näistä valikoista voidaan generoida näiden moduuloiden raportteja koko koneen käytön ajanjaksolta tai tietyltä ajanjaksolta.

Server pitää sisällään vain yhden valikon Web Reports (Web raportit). Täällä nähdään miten Web-palvelin on toiminut ClearOS:ssa.

System pitää sisällään Logs (Logit), Hardware Report (Kokoonpanon raportti) ja Resource Report (Resurssien raportti) -valikot.

Logs-valikko näyttää kaikki koneen logit ja näitä voidaan suodattaa eri hakusanoilla tai valita alasvetovalikosta mitä raporttia halutaan tarkastella.

Hardware Report -valikon takaa nähdään tietokoneen kokoonpano, muistin tilanne ja tyhjänä olevan kiintolevyn tilan. Käytössä ollut 20 Gt -kiintolevy on jaettu /boot ja / -liitoksiin. /boot-liitoksen koko on 76 Mt ja /-liitoksen loput eli 17,44 Gt.

Resource Report -valikon takaa paljastuva sivu näyttää graafisessa muodossa ClearOS prosessien määrän, käytön, swapin määrän ja uptimen.

3.11. ClearCenter

Tämän valikon alla on seuraavat otsikot Register (Rekisteröinti), Software (Ohjelmat) ja ClearSDN.

Register, sisältää Register System (Rekisteröi järjestelmä) -valikon. Täällä tehtiin ensimmäisen käynnistyksen yhteydessä ollut palomuuriohjelmiston rekisteröinti. Lisäksi täältä nähdään mitä maksettuja ominaisuuksia on ostettu.

Software sisältää Software Modules (Ohjelmistomoduulit), Software Updates (Ohjelmistopäivitykset) ja Third Party Applications (Kolmannen osapuolen ohjelmat) -valikot.

Software Modules -valikon kautta voidaan asentaa asennusvaiheessa pois jääneet moduulit, jos näille tulee myöhemmin käyttöä. Näitä ovat esimerkiksi VPN-moduulit, joita käytetään VPN-tunnelin tekoon. Software Updates -valikon kautta voidaan päivittää palomuuriohjelmistoon asennettuja moduuleita.

Third Party Applications -valikon kautta nähdään palomuuriohjelmistoon asennetut kolmannen osapuolen moduulit. Näiden asennus tapahtuu yleensä ottamalla SSH-yhteys ja asentamalla nämä yum-paketinhallinnan katta.

ClearSDN sisältää Remote Server Backup (Etäpalvelimelle varmuuskopiointi) -valikon. Täältä voidaan määritellä toiselle palvelimelle suojattu yhteys, jonne varmuuskopiointi suoritetaan.

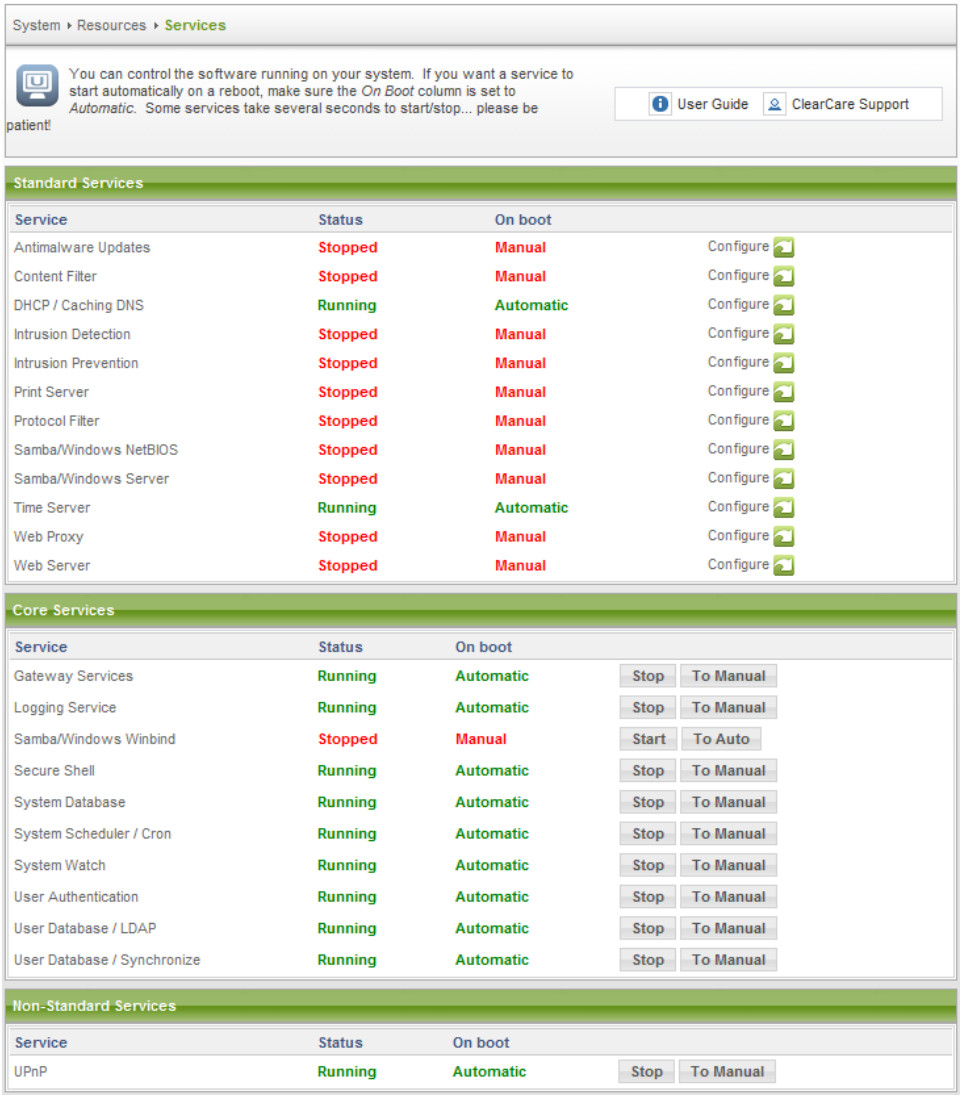
4 KÄYTTÖÖNOTTO

Käyttöönoton pohjana käytettiin ClearFoundationin tarjoamaa ohjekirjaa (2010), joka löytyy heidän sivuiltaan.

Ensimmäisenä kannattaa tarkistaa mitä palveluita ClearOS-palomuuriohjelmistossa on päällä ja onko yhteyksiä olemassa sisään tai ulospäin. Näiden avulla voidaan päätellä kuinka hyvin palomuuriohjelmisto on suojattu vakioasetuksilla.

4.1. Palvelut

Palveluiden toimintaa on helppo tarkastella System-otsikon alta löytyvästä Resources-otsikon alla olevasta Services-valikosta. Tämä valikko listaa ClearOS:ssa olevat palvelut ja niiden tilat. Palveluiden tilat ja toiminta näkyvät kuvassa 24.



Kuva 24 Palveluiden tilat ja toiminta

Kuvassa 24 näkyvät palvelut ovat listattuna kolmeen eri kategoriaan. Ensimmäisenä on Standard Services (Vakiopalvelut), toisena Core Services (Ydinpalvelut) ja viimeisenä Non-Standard Services (Epämääräiset vakiopalvelut), näillä tarkoitetaan kolmannen osapuolen palveluita, joita palomuuriohjelmsistoon on asennettu.

Standard Services -otsikon alta selviää, että vakiona ClearOS:ssa on päällä DHCP- ja DNS-palvelimet. Tarvittaessa palveluita päästään tästä suoraan konfiguroimaan Configure-linkin kautta ilman, että kyseistä palvelua pitää etsiä muiden valikoiden takaa.

Core Services -otsakkeen alta selviää, että suurin osa tämän palveluista on päällä. Koska jos nämä eivät olisi päällä, ei koko palomuuriohjelmisto toimisi kunnolla. Tärkeimpänä näistä palveluista voidaan pitää tietokantoja. Näihin tallentuu suurin osa siitä mitä palomuuriohjelmistolla tehdään, jolloin nämä myös vaikuttavat palomuurin toimintaan suuriltaosin.

Kuten kuvasta 24 selviää, niin kaikki muut palvelut ovat päällä paitsi Samba. Tämä on ihan vakioasetus, koska Samban toimimista varten pitää se konfiguroida oikeaan Windows-verkkoon, jotta se toimisi oikein.

Kuten edellisiäkin niin näitä palveluita voidaan tältä välilehdeltä suoraan pysäyttää tai muuttaa niiden toimintaa.

Viimeisestä otsakkeesta, joka on, Non-Standard Services nähdään, että ClearOS:n on asennettu UPnP-palvelu. UPnP-palvelu ei tule järjestelmän mukana vakiona vaan tämä pitää asentaa erikseen komentokehotteen kautta. Näilläkin palveluilla on samat mahdollisuudet pysäyttää tai käynnistää palvelut tämän välilehden kautta.

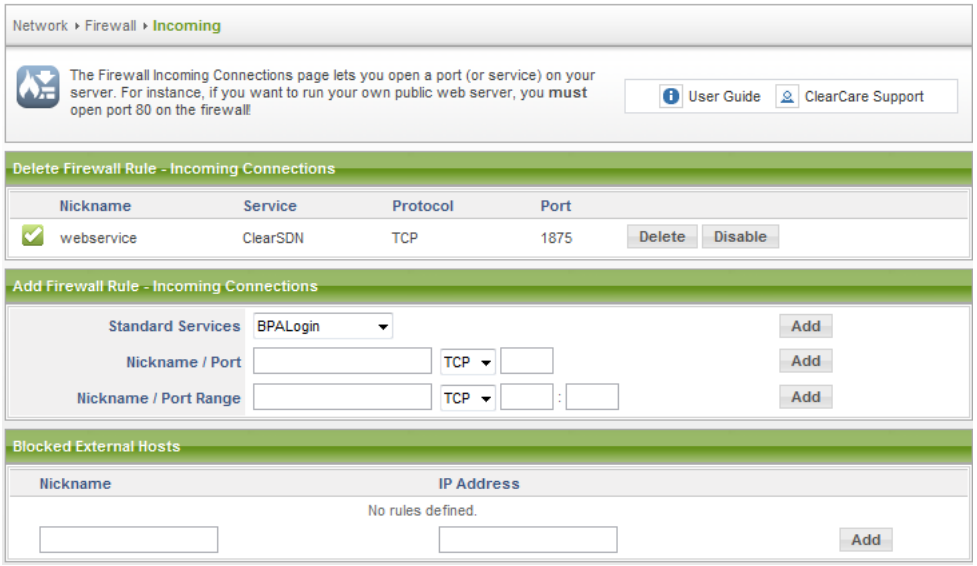
Palveluiden määrä on alussa sopivan pieni. Lisäksi ClearOS:ssa ei pyöri vakiona mitään ylimääräistä, joka voisi vaarantaa palomuurin toiminnan.

4.2. Yhteydet

Sisään ja ulosmenevää liikennettä voidaan tarkastella Network-otsikon alta löytyvän Firewall-otsikon alla olevasta Incoming ja Outgoing -valikoista.

4.2.1. Incoming

Incoming-valikko kertoo käyttäjälle verkkoon pääsevien yhteyksien nimen, palvelun, protokollan ja portin. Tällä tapaa käyttäjän on helppo seurata mitä portteja on avattu sisäänpäin. Valikko näkyy kuvassa 25.



Kuva 25 Palomuurisäännöt, Sisääntuleva liikenne

Ensimmäisenä otsakkeena on Delete Firewall Rule - Incoming Connections (Poista palomuurisääntö - Sisääntuleva liikenne). Tämän otsikon alle niputetaan kaikki palomuuriohjelmistoon lisätyt säännöt, jolloin ne näkyvät käyttäjälle listana. Käyttäjä voi tästä suoraan nähdä säännöt ja poistaa tai disabloida tarpeen mukaan.

Tämän otsikon alle on lisätty palomuuriohjelmsiton vakiona avaama portti 1875, joka on varattu ClearSDN-palvelun käyttöön. Tämä palvelu huolehtii näistä maksullisien ominaisuuksien toiminnasta, jos niitä on otettu toimintaan.

Toisena otsikkona on Add Firewall Rule - Incoming Connections (Lisää palomuurisääntö - Sisääntuleva liikenne). Tämän alla on kolme eri tapaa, joilla palomuuriin voidaan avata portteja sisäänpäin. Ensimmäisenä tapana on valita suoraan valmiista alasvetovalikosta palvelun nimi ja lisätä tämä painamalla Add-nappia. Alasvetovalikko pitää sisällään yleisimmät palvelut, joita ovat esimerkiksi SSH (22), HTTP/S (80/443), IMAP (143/993) jne.

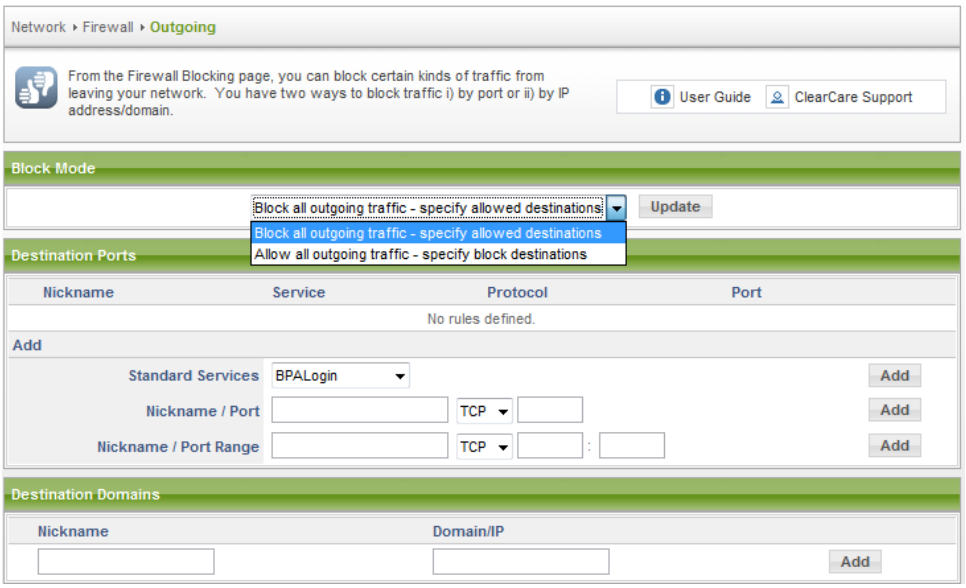
Toisena tapana voidaan määrittää oma nimi avattavalle portille, valita sille protokolla, jota se käyttää, TCP vai UDP sekä antaa portti. Tämä on hyvä tapa avata esimerkiksi jollekin palvelulle portti, jos tämä ei vaadi kuin yhden toimiakseen. Suurempien porttimäärien avaamiseksi on suositeltavaa käyttää viimeistä tapaa.

Viimeinen tapa ei eroa toisesta kuin sillä tapaa, että voidaan määritellä porttialue eikä vain tiettyä porttia. Tätä on hyvä käyttää esimerkiksi Steam-palvelun porttien aukaisemiseen, koska tämä palvelu käyttää yli 20 porttia ja portit menevät järjestyksessä 27000 – 27030 välille. Turhia portteja ei ole kuitenkaan suositeltavaa avata tietoturvan takia. Avataan vain ne joille on tarvetta, on hyvä muistisääntö. (Steam Support 2010.)

Viimeisenä otsikkona on Blocked External Hosts (Estetty ulkoinen isäntä). Tällä asetuksella voidaan estää tietyn IP-osoitteen omaavan koneen pääseminen sisäverkkoon.

4.2.2. Outgoing

Outgoing-valikko kertoo käyttäjälle ulospäin sallitun liikenteen samalla kaavalla kuin sisääntulevassa. Kuvasta 26 näkyy Outgoing-valikko.



Kuva 26 Ulosmenevä liikenne

Kuten kuvasta 26 selviää, vakioasetuksena palomuurissa on estetty kaikki ulosmenevä liikenne. Tämä voidaan myös muuttaa siihen muotoon, että päästetään kaikki ulos mutta kielletään listassa olevat, joka on Destination Ports (Kohdeportit) -otsikon alla. Asetuksen muuttaminen tapahtuu ottamalla toinen vaihtoehto Block Mode -otsikon alla olevasta alasvetovalikosta. Itse suosin vakioasetusta koska se on tietoturvallisempi kuin tämä toinen vaihtoehto.

Seuraavan otsikkona on Destination Ports. Tässä on samat säädöt kuten sisääntulevassa. Voidaan lisätä valmiista listasta tietty portti tai porttialue.

Viimeisenä otsikkona on Destination Domains (Kohde domainit). Tällä asetuksella voidaan kieltää tai sallia kokonaisia domaineja.

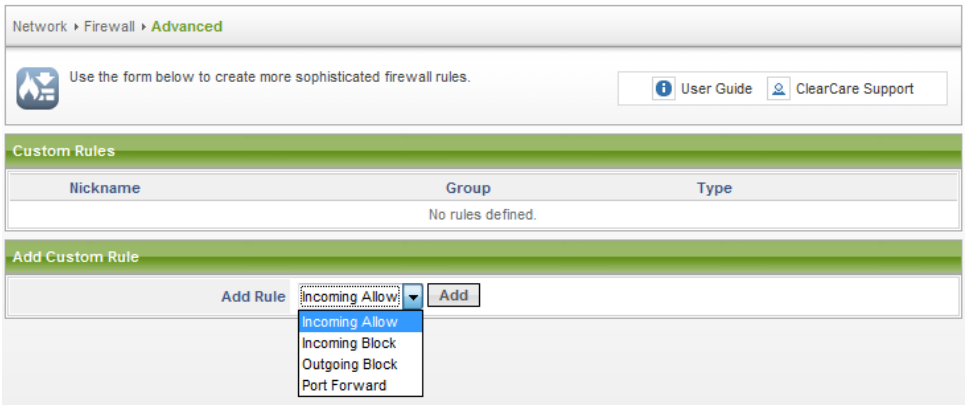
Jotta sisäverkon koneet pääsisivät ulospäin, on syytä avata yleisimmät portit. Näitä ovat HTTP/S, FTP (21), SSH, POP, IMAP jne. Lisäksi pitää avata DNS-palvelinta (53) varten portit, jos ei käytetä ClearOS-palomuuriohjelmistoa DNS-palvelimena.

4.3. Advanced firewall module (Täsmentävä palomuuri moduuli)

Jos palomuurin asetuksiin halutaan, monipuolisempia vaihtoehtoja on, syytä asentaa Advanced firewall module. Moduulin asennus suoritetaan

Software Modules-valikon alta, joka sijaitsee Software-otsikon alla, joka on ClearCenter-otsikon alla. Täältä valikosta vain yksinkertaisesti valitaan tämä moduuli ja asennetaan painamalla Go-nappia.

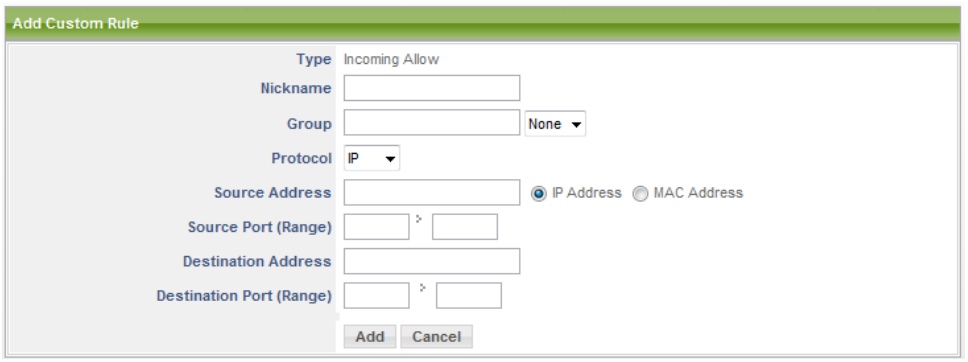
Tämä moduuli ilmestyy saman otsikon alle missä Ingoming ja Outgoing -valikot sijaitsevat nimellä Advanced (Täsmentävä). Moduuli mahdollistaa muiden protokollien käytön kuten AH, ESP, GRE ja IP. Moduulin valikko näkyy kuvassa 27.



Kuva 27 Advanced firewall module

Kuvasta 27 näkyy neljä vaihtoehtoa joita tällä moduulilla voidaan suoraan tehdä: Incoming Allow (Sisääntulevan salliminen), Incoming Block (Sisääntulevan kielto), Outgoing Block (Ulomenevän kielto) ja Port Forward (Porttiohjaus).

Nämä vaihtoehdot eivät eroa juurikaan vakioasetuksissa kuin paitsi, että voidaan käyttää muitakin protokollia kuin TCP ja UDP. Lisäksi voidaan ohjata tietystä IP-osoitteesta tuleva liikenne tarvittaessa johonkin muuhun IP-osoitteeseen. Tai voidaan myös käyttää MAC-osoitetta liikenteen ohjaamiseen. Tämä valikko näkyy kuvasta 28.



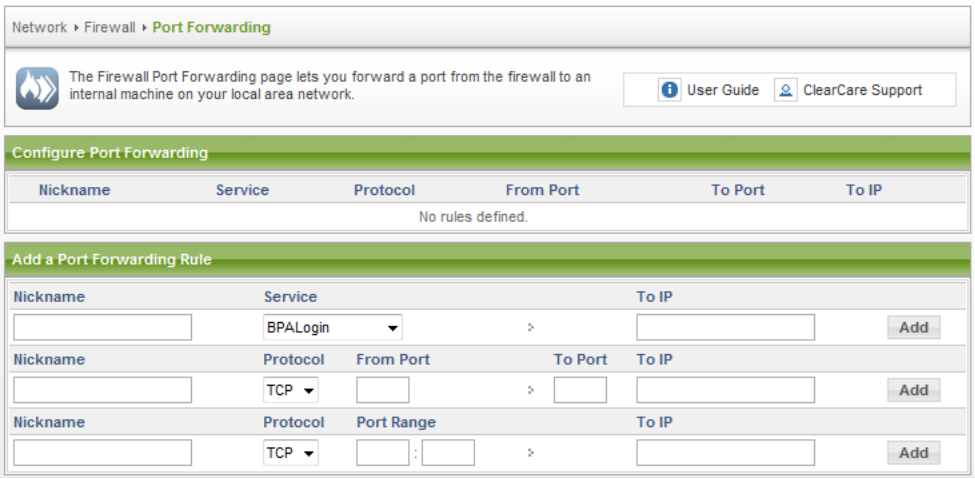
Kuva 28 Kehittynyt liikenteen salliminen

Lisäksi tällä moduulilla tehdyt säännöt menevän omaan Custom Rules -otsikon alle, joka näkyy kuvassa 27. Tämä tarkoittaa sitä, että jos Advanced firewall -moduulilla päästetään sisäänpäin liikennettä tai vastaavaa, niin tämä ei näy ollenkaan Incoming-valikon alla. Onneksi tähän on olemassa ratkaisu. Firewall-otsikon alta löytyy Groups-valikko,

joka listaa kaikki säännöt, joita palomuuriin on tehty, jolloin kannattaa sieltä tarkistaa miten säännöt on laitettu kokonaisuudessa.

4.4. Porttiohjaus

Porttiohjaus on tarpeellinen joitakin ohjelmia varten. Porttiohjauksia voidaan tehdä Port Forwarding -valikon takaa, joka sijaitsee Firewall-otsikon alla. Port Forwarding -valikko ikkuna näkyy kuvassa 28.

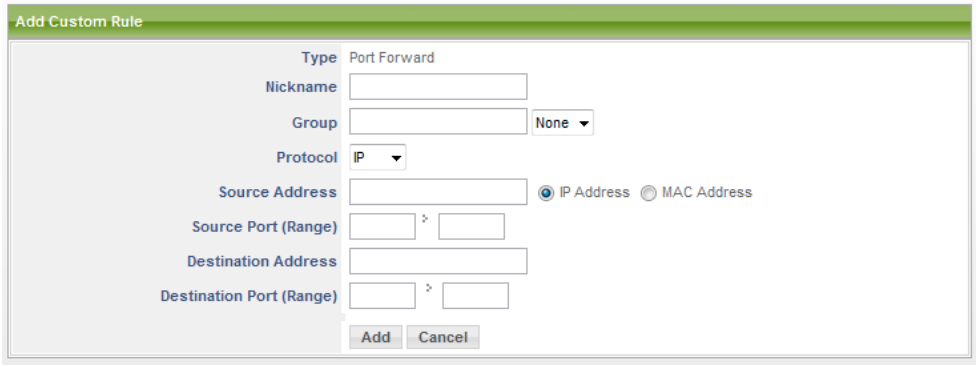


Kuva 29 Port Forwarding

Kuten kuvasta 29 näkyy, niin vakiona ei ole yhtään porttiohjausta tehtynä koska näille ei ole tarvetta ennen kuin käyttäjän tarvitsee tehdä omansa. Valikosta porttiohjauksia voidaan tehdä kolmella eri tavalla. Ensimmäinen tapa on helpoin mutta myös vähiten säädettävissä. Tällä tapaa voidaan valita suoraan alasvetovalikosta valmiiden palveluiden portteja ja ohjata nämä tiettyyn IP-osoitteeseen.

Toisella tapaa voidaan ohjata joko TCP tai UDP -protokollan omaava palvelua tietystä portista tiettyyn porttiin tietylle IP-osoitteelle. Viimeisellä tavalla voidaan ohjata tietty porttialue tiettyyn IP-osoitteeseen.

Edellä mainittu Advanced firewall -moduuli lisää myös porttiohjauksiin samat protokollat, jotka tulivat sisääntulevaan ja ulosmenevään liikenteeseen. Lisäksi tämä antaa mahdollisuuden ohjata portteja IP-osoitteesta toiseen tai voidaan käyttää MAC-osoitetta. Tämä näkyy kuvassa 30.



Kuva 30 Kehittynyt porttiohjaus

4.5. Universal Plug and Play (UPnP)

UPnP-protokolla on nykypäivänä hyvin yleisessä käytössä koska tämän avulla käyttäjä voi välttyä tekemästä porttiohjauksia. UPnP-protokolla käyttää hyväkseen SSDP-protokollaa, joka mahdollistaa UPnP-protokollan löytämään UPnP-laitteita verkosta.

Moni ohjelma hyödyntää UPnP-protokollaa siten, että etsii UPnP-laitteen kuten modeemin ja avaa sitten ohjelmalle tämän vaatiman portin.

ClearOS-palomuuriohjelmisto ei vakiona sisällä UPnP-protokollaan tukea vaan se pitää asentaa käsin palomuuriohjelmistoon. Asennus tapahtuu ottamalla SSH-yhteys ClearOS koneeseen ja kirjautumalla root-käyttäjällä sisään. Tämän jälkeen syötetään seuraava komento *yum --enablerepo=base-extras install linuxigd*. Tämä komento asentaa yum-paketinhallinnan kautta UPnP-protokollalle tuen. UPnP-palvelu tulee näkyviin Services-valikkoon, josta se voidaan pysäyttää tai käynnistää.

Kun tuki on asennettua, niin palomuuri osaa ohjelmasta saadulla tiedolla avata tälle portin ilman, että käyttäjän itse tarvitsee tehdä mitään.

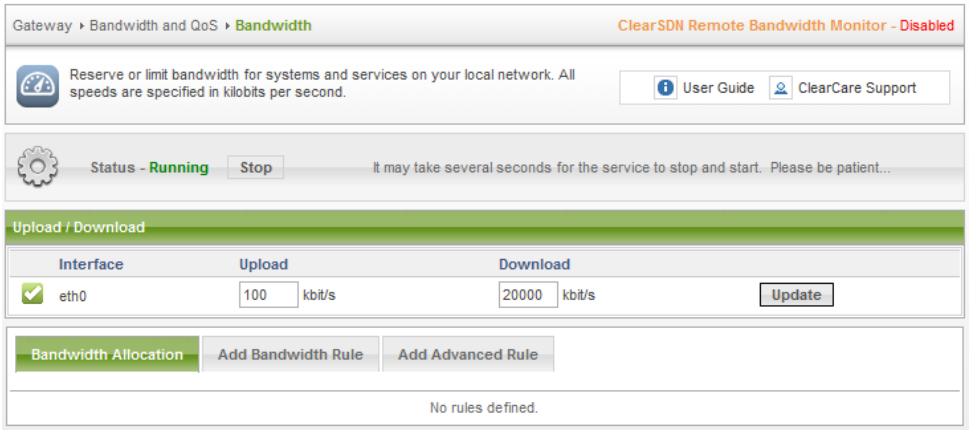
4.6. Quality of Service (QoS)

Kaistanhallinta eli QoS tai Bandwidth -nimitys riippuu ihan valmistajasta ja tekijästä mitä tämä haluaa käyttää. Molemmat ovat kuitenkin käytännössä sama asia. Se mikä tästä tekee nykypäivänä hyödyllisen, on se, että tällä voidaan tarkastella liikennettä suuntaan ja toiseen ja määrittää tietylle liikenteelle tietyt rajat. Testiverkon nopeus on 24/1 fullrate mikä tarkoittaa 24 megatavua sisäänpäin ja 1 megatavun ulospäin.

ClearOS-palomuuriohjelmisto pitää sisällään oman kaistanhallinnan nimellä Bandwidth. Tämä löytyy Gateway-otsikon alla olevan Bandwidth and QoS -otsikon alta.

Ensimmäisenä kun tämä valikko avataan, määritellään yhteyden nopeus kilobittiä sekunnissa. Testiverkon tapauksessa tämä tarkoittaa teoriassa sisäänpäin 24 000 kbit/s ja ulospäin 100 kbit/s. Tarkemmat tiedot nopeudesta saa kokeilemalla siirtää ja ladata tiedostoja Funetin tarjoamista

FTP-palvelimista. Nykypäivänä ostettu laajakaistan nopeus ei välttämättä tarkoita suoraan sitä mitä paperissa lukee. Testiverkon todellinen nopeus selvisi minulle, kun testasin ladata ja lähettää tiedostoja seuraavanlaiseksi: sisäänpäin saan maksimissa 20000 kbit/s ja ulospäin 110 kbit/s. Kuvasta 31 näkyy kaistanhallinnan valikko.



Kuva 31 Kaistanhallinta

Alussa kun kaistanhallinta on päällä, niin ClearOS on rajoittanut kaiken liikenteen 1000 kbit/s sisäänpäin, mikä on huomattavasti vähemmän kuin mitä olisi tarjolla.

Tämä voidaan korjata sillä, että luodaan sääntö, joka antaa HTTP/S-liikenteelle koko kaistan käyttöön. Sääntöjä voidaan luoda kahdella eri tavalla, jotka näkyvät kuvasta 31. Ensimmäinen tapa on luoda Add Bandwidth Rule eli normaali sääntö valmiina olevista palveluista. Kuten kuvasta 32 näkyy, niin normaalin säännön luominen ei ole vaikeaa.

Kuva 32 Kaistanhallinnan normaali sääntö

Seuraavassa esimerkissä luodaan sääntö, joka antaa koko kaistan HTTP/S-liikenteelle. Kun sääntöä luodaan, valitaan ensimmäisenä tämän moodi, joka voi olla Reserve (Varattu) tai Limit (Raja). HTTP/S-liikenteen tapauksessa tähän asetetaan rajaksi koko kaistan liikenne. Koska HTTP/S-liikennettä käytetään hyvin paljon selaimella mentäessä eri sivuille.

Seuraavaksi valitaan itse palvelu, joka on tässä tapauksessa HTTP/S, joka näkyy kuvassa 32. Lisäksi voidaan valita kyseisestä alasvetovalikosta muitakin valmiita palveluita.

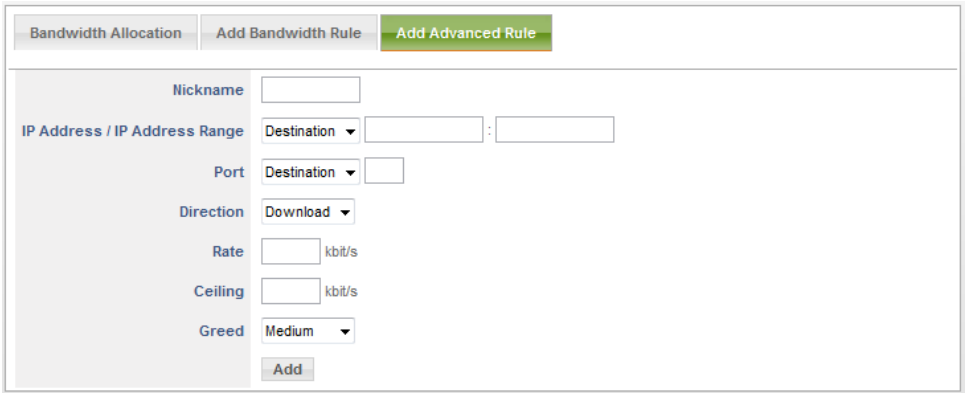
Seuraavaksi valitaan Direction (Suunta) johon halutaan tätä liikennettä ohjata. Vaihtoehtoina on Flowing from my network, Flowing to my network, Flowing from my system ja Flowing to my system. Näistä ensimmäinen tarkoittaa liikenteen suuntaan sisäverkosta ulospäin, toinen sisäverkkoon, kolmas tietystä koneesta ulospäin ja neljäs tietystä koneesta sisäänpäin. HTTP/S-liikenteen tapauksessa tähän valitaan Flowing to my network, koska halutaan ottaa koko kaista sisäverkon koneille käyttöön.

Seuraavaksi määritellään Rate (Nopeus), joka testiverkon tapauksessa on 20000 kbit/s. Lopuksi voidaan määritellä Greed eli taso kuinka tärkeänä tätä HTTP/S-liikennettä pidetään muihin sääntöihin verrattuna. Vaihtoehdot ovat Very High, High, Medium, Low ja Very Low. Tässä tapauksessa kannattaa asettaa HTTP/S-liikenne Medium-tasolle, koska sitten voidaan luoda tarvittaessa sääntöjä jollekin muulle liikenteelle, joka voi tarvita enemmänkin kuin HTTP/S-liikenne tai vähemmän.

Kun sisäänpäin sääntö on luotu HTTP/S-liikenteelle, pitää tälle myös luoda ulospäin menevä sääntö. Asetukset ovat muuten samat mutta Flowing to my network valinnan sijaan valitaan Flowing from my system -valinta ja nopeudeksi määritellään 100 kbit/s.

Kun molemmat säännöt on tehty näkyvät nämä Bandwidth Allocation -otsikon alla, josta näitä voidaan tuhota tai poistaa käytöstä.

Lisäksi kaistanhallinnan sääntöjä voidaan luoda kehittyneemmällä vaihtoehdolla Add Advanced Rule -valikosta, jonka sisältö näkyy kuvassa 33.



Kuva 33 Kaistanhallinnan kehittyneempi sääntö

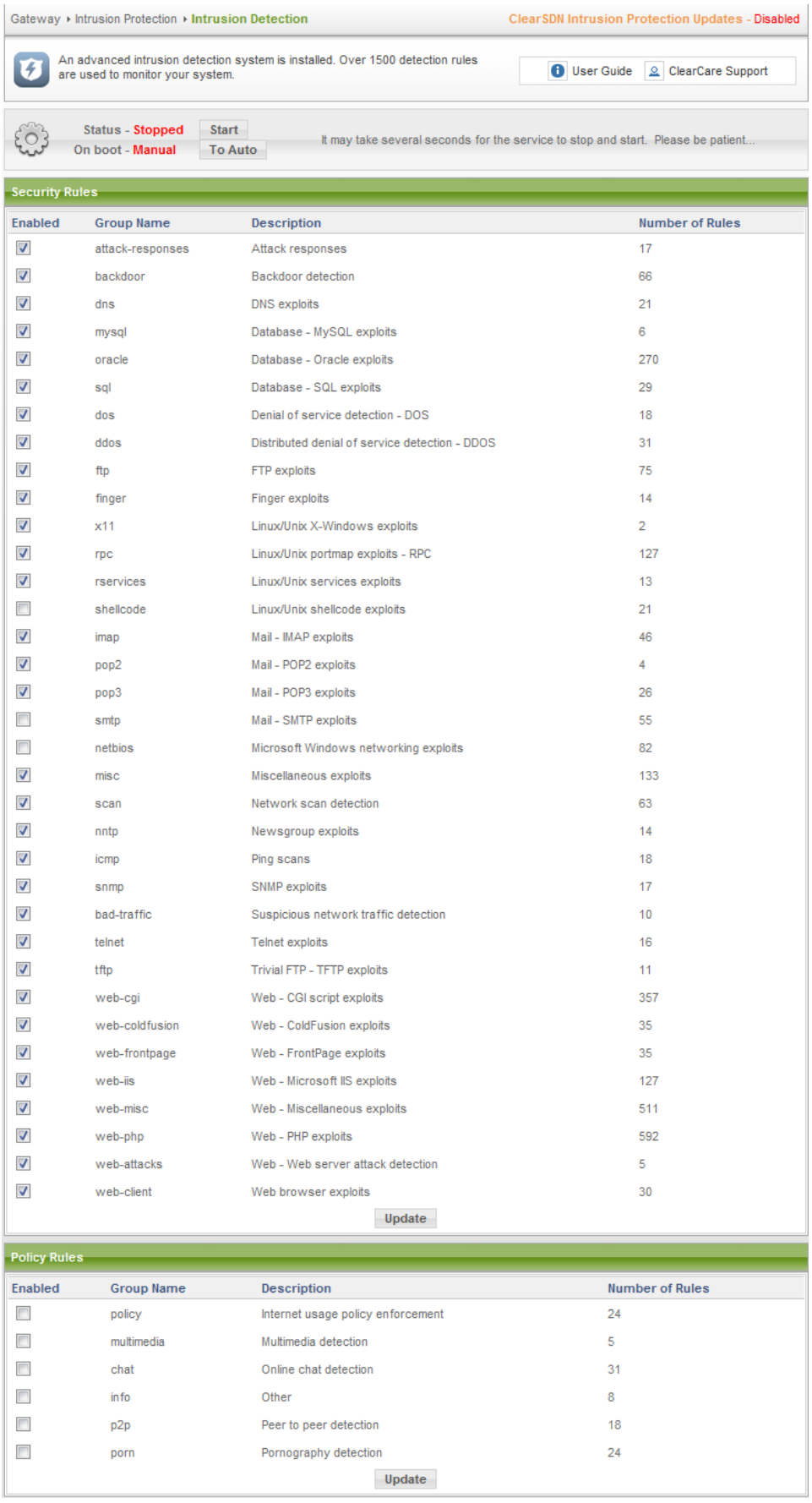
Kehittyneemmän säännön tekeminen ei eroa juurikaan sisällöltä normaalista. Ainoat erot tulevat siinä, että käyttäjän pitää tietää itse määrittää portti protokollaa varten ja kirjoittaa verkko tai koneiden IP-osoitteet käsin, koska ei voida valita suoraan koko verkkoa.

Sääntöjen määrää ei ole rajattu millään lailla, joten käyttäjä voi itse lisätä sääntöjä kuinka paljon tykkää.

4.7. Intrusion Detection

Palomuuriin voi kohdistua monenmoisia hyökkäyksiä ulkoverkosta. Tähän ClearOS-palomuuriohjelmisto on varautunut sisällyttämällä itseensä tunkeilijan havaitsemisjärjestelmän. Tämä ominaisuus löytyy Gateway-otsikon alla olevasta Intrusion Protection -otsikon alla olevasta valikosta Intrusion Detection. Vaikka valikko listaakin, kattavat määrät eri sääntöjä ei tänne valitettavasti voi omia sääntöjä luoda. Sääntöjen päivitys tapahtuu suoraan ClearSDN:n palvelun kautta, joka on maksullinen.

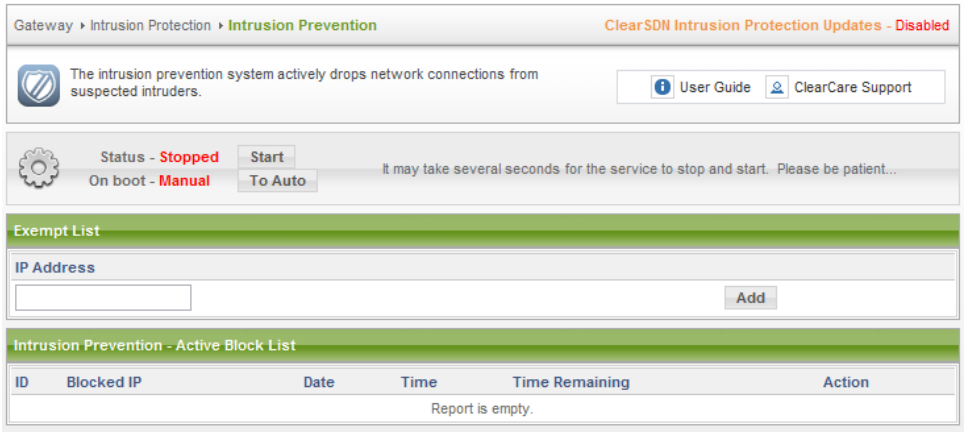
Havaitsemisen päälle kytkeminen tapahtuu vain yksinkertaisesti käynnistämällä tämä moduuli omasta Start-napista, jolloin voidaan tuloksia seurata ClearOS:n logeista. Kuvasta 34 selviää valikon sisällä olevat säännöt.



Kuva 34 Tunkeilijanhavaitsemis-moduulin säännöt

4.8. Intrusion Prevention

Tunkeilijanesto-moduuli, joka löytyy samasta paikasta kuin havaitsemis-moduuli, listaa käyttäjän tekemät IP-osoite-estot. Tämän valikon kautta käyttäjä voi itsekin lisätä IP-osoitteen perusteella estoja palomuuriin. Ennen kuin tämän moduulin toimivuutta voidaan kokeilla, testiverkossa pitää tämä käynnistää. Käynnistäminen tapahtuu samaan tapaan kuin aikaisemmissa. Klikkaamalla Start-nappia. Valikko näkyy kuvasta 35.



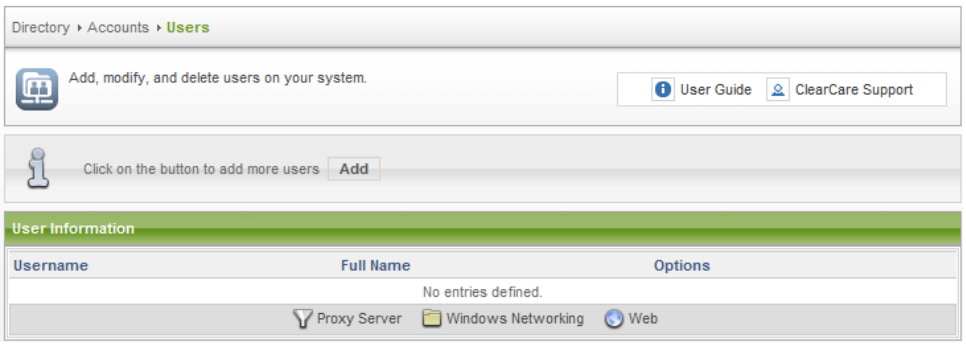
Kuva 35 Tunkeilijanesto-moduuli

Kun tähän lisättiin jokin verkossa oleva IP-osoite, niin ei tällä ollut enää mitään asiaa palomuurin suojelemaan verkkoon, jolloin totesin, että moduuli toimii niin kuin pitääkin.

4.9. Käyttäjän luonti

Tietoturvallisuuden parantamiseksi on järkevää luoda omat käyttäjät tietyille palveluille. Tällä vähennetään sitä varaa, että jos ulkopuolinen saa tietoonsa jonkun käyttäjän ja tämän salasanan, ei tämä voi tuhota koko palomuuria.

Käyttäjän luominen aloitetaan menemällä Users-valikkoon, joka löytyy Accounts-otsikon alta, joka sijaitsee Directory-otsikon alla. Josta löytyy Add-nappi, jolla voidaan lisätä käyttäjä, kuten kuvassa 36 näkyy.

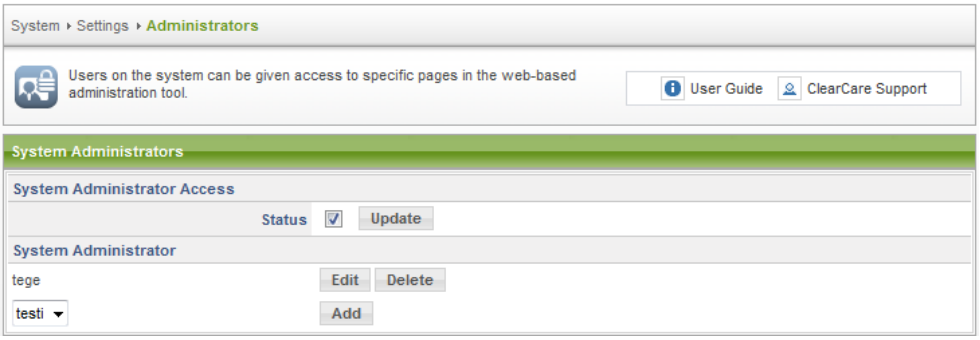


Kuva 36 Käyttäjän luonti

Kun nappia on painettu, ClearOS kysyy perustiedot käyttäjästä kuten käyttäjänimen, salasanan, oikean nimen jne.

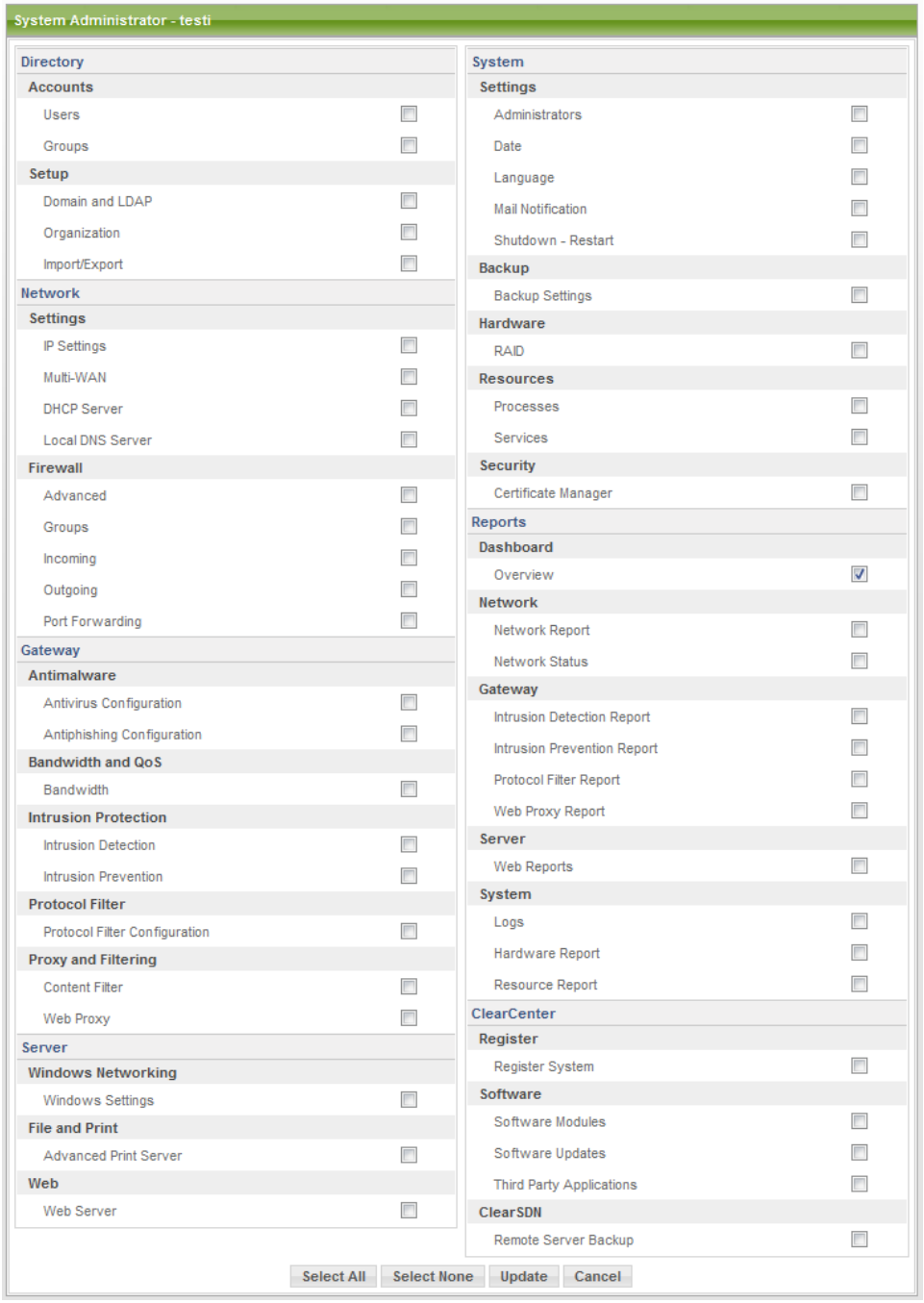
Kun nämä on, annettu voidaan lopussa painaa Add-nappia, joka lisää käyttäjän ClearOS-palomuuriohjelmistoon. Seuraavaksi pitää käyttäjälle antaa jotain oikeuksia ja tämä tapahtuu Administrators-valikon takaa, joka löytyy Settings-otsikon alta, joka sijaitsee System-otsikon alla.

Klikkaamalla tähän valikkoon tämä avaa kuvan 37 näkymän.



Kuva 37 Oikeuksien antaminen

Kuten kuvasta 37 selviää, niin testi-käyttäjälle ei ole vielä annettu mitään oikeuksia. Tästä eteenpäin jatketaan valitsemalla testi-käyttäjä alasvetovalikosta ja painamalla Add-nappia, joka avaa käyttäjän näytölle listan mitä oikeuksia voidaan testi-käyttäjälle antaa. Tämä lista näkyy kuvasta 38.



Kuva 38 Lista oikeuksista

Kuten kuvasta selviää, käyttäjällä on jo oikeudet Dashboardiin. Tämä on palomuuriohjelmiston etusivu. Tästä itse käyttäjälle voidaan helposti valita oikeudet vain rastittamalla kohdat. Kuitenkin kannattaa pitää mielessä se, että ei anneta liikaa oikeuksia tietyille henkilöille. Lisäksi jos ClearOS:n asennetaan uusia moduuleita, niin näitä varten pitää antaa sitten myöhemmin oikeudet, koska niitä ei vakiona anneta.

Oikeuksien annon jälkeen painetaan Update-nappia, joka lisää käyttäjälle tämän oikeudet. Kun tällä käyttäjällä kirjaudutaan sisään, ei kaikkia valikoita näy vaan näkyvät juurikin ne mihin tällä käyttäjällä on oikeudet. Tämä parantaa huomattavasti tietoturvaa.

4.10. Elisa Viihde

Halusin ottaa tämän Elisa Viihde -palvelun testauksen mukaan tähän opinnäytetyöhön koska monille Linux-pohjaisille muureille on ongelmana siirtää IGMP-protokollaa lävitse, jota käytetään IPTV:ssä. Tämä johtaa Elisa Viihde -palvelussa siihen, että palomuurin lävitse ei pääse IPTV-signaali. Tallenteet kuitenkin näkyvät koska nämä ladataan suoraan Elisan palvelimelta ja nämä käyttävät HTTP-protokollaa.

Jotta, saataisiin IPTV-signaali tulemaan palomuurin lävitse pitää ClearOS-palomuuriohjelmistoon asentaa IGMPProxy-ohjelma. Tämän saa seuraavasta osoitteesta http://sourceforge.net/projects/igmpproxy/.

IGMPProxy-ohjelman asennus aloitetaan ottamalla SSH-yhteys järjestelmään ja kirjautumalla root-käyttäjällä sisään.

Aluksi IGMPProxy-ohjelmiston asennuspaketti ladataan yllä olevasta osoitteesta, tämän jälkeen se puretaan komennolla *tar -zxvf igmpproxy-0.1.tar.gz*. Tämän jälkeen mennään igmpproxy-0.1-kansioon ja käännetään ohjelma seuraavilla komennoilla *./configure*, *make* ja lopuksi *make install*.

Kun ohjelma on käännetty ja asennettu, niin voidaan tarkastella tätä. Ohjelman käynnistäminen tapahtuu komennolla */usr/local/sbin/igmpproxy /usr/local/etc/igmpproxy.conf -d,* jossa viimeisenä oleva d-vipu tarkoittaa debuggaus-tilaa. Konfiguraation löytää liitteestä1.

Ohjelman lisäksi pitää palomuuriin tehdä portille 1234 reikä, jotta IPTV-signaali kulkee sisäänpäin.

Monista yrityksistäni huolimatta en saanut kuitenkaan IPTV-signaalia kulkemaan palomuurin lävitse Elisan digiboksille asti. En tarkalleen tiedä mistä tämä on voinut johtua koska debuggaus tilassa IGMPProxy ei anna mitään erikoista virheilmoitusta, joka voisi vaikuttaa tähän toimintaan.

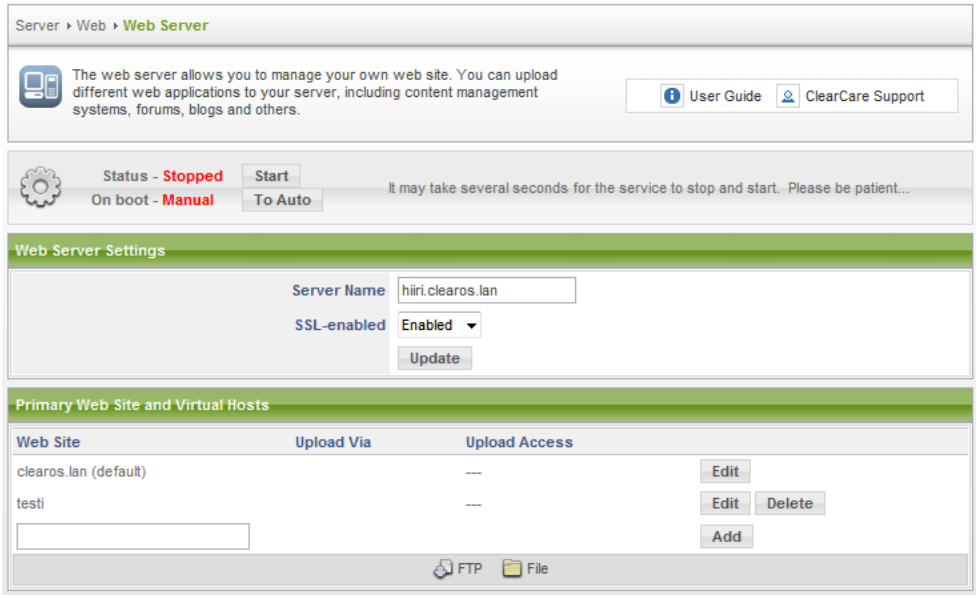
Olen kuitenkin viaksi epäillyt sitä, että IPtablesiin olisi pitänyt tehdä liikenteen ohjauksia käsin mutta en löytänyt näihin mistään mitään ohjeita siihen, kuinka nämä olisi pitänyt tehdä. Uskaliaasti kokeilemalla olisi voinut löytää oikean ratkaisun mutta tämä on kuin etsisi neulaa heinäsuovasta.

5 PALVELUT

ClearOS-palomuuriohjelmisto pitää sisällään erinäisiä palveluita kuten Web-palvelin, tulostinpalvelin ja verkkojako. Nämä toimivat muiden moduulien rinnalla. Seuraavaksi tutustumme näihin kolmeen palveluun.

5.1. Web-palvelin

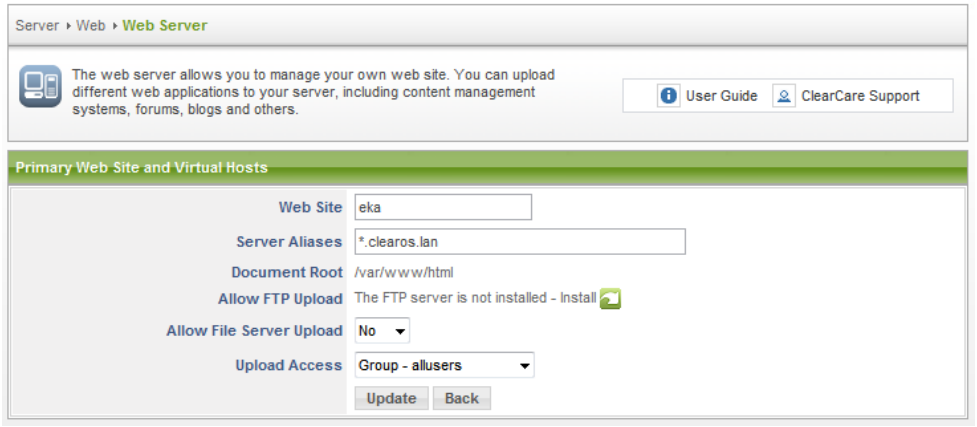
Web-palvelin sijaitsee Server-otsikon alla olevassa Web-otsikossa nimellä Web Server. Täältä voidaan hallita Web-palvelimen tiedostoja ja käynnistää tai sammuttaa tämä. Kuten kuvasta 39 näkyy.



Kuva 39 Web-palvelin

Vakiona tämä ominaisuus on pois päältä ja se on hyvä koska tietoturvallisesti ei ole turvallista pitää Web-palvelinta päällä ilman, että tietää mitä tämä näyttää ulospäin.

Omien verkkosivujen tiedostojen siirtäminen on helppoa. Aluksi pitää katsoa clearos.lan-verkkosivun tiedot, koska tämä toimii oletusverkkosivuna. Kun tämän perässä olevasta Edit-napista painaa, saadaan tämän tiedot näkyviin, jotka näkyvät kuvassa 40.



Kuva 40 clearos.lan-asetukset

Kuten kuvasta 40 näkyy, niin oletus verkkosivujen tiedot voidaan muuttaa omanlaisekseen. Lisäksi selviää tiedostojen sijoitus kansio, joka sijaitsee /var/www/html -hakemistossa. Tänne käyttäjä voi lisätä omia verkkosivun tiedostoja.

Tiedonsiirto voidaan tehdä FTP-yhteydellä, joka vaatii FTP-moduulin asennuksen tai vaihtoehtoisesti käyttämällä SCP-yhteyttä. Verkkosivujen siirtoon käytän SCP-yhteyttä. Koska tämä on suojattu yhteys ja jos joku yrittää kurkkia tiedostojen siirron aikana, niin tämä ei saa datasta selkoa.

Lopuksi kun tiedot on muutettu tai tarkastettu painetaan Update-nappia, joka tallentaa tiedot.

5.1.1. Tiedostojen siirto

Tiedot voidaan siirtää esimerkiksi käyttämällä WinSCP-ohjelmistoa, joka tukee SCP-yhteyttä. Tällä otamme yhteyden ClearOS:n IP-osoitteeseen, joka voi olla sisäverkon IP-osoite tai ulkoinen, riippuen siitä missä itse käyttäjä sijaitsee. Kun yhteys on luotu, on käyttäjän mentävä /var/www/html -hakemistoon ja lisättävä tänne omat tiedostonsa, minkä jälkeen on aika testata sivujen toimivuutta.

5.1.2. Käynnistys

Testausta varten pitää Web-palvelin käynnistää. Käynnistys tapahtuu kuvan 39 näkyvästä Start-napista, minkä jälkeen palvelin käynnistyy. Verkkosivuun voidaan ottaa yhteys käyttämällä sisäistä tai ulkoista osoitetta. Ulkoista osoitetta varten palomuuriin on avattava portit 80 ja 443 suojaamatonta ja suojattua HTTP-yhteyttä varten. Sisäverkossa palvelin toimii normaalisti ilman porttien avaamista.

Kun tarvittavat portit ovat auki, niin käyttäjälle avautuu tämän oma verkkosivu, joka omassa tapauksessani oli kuvan 41 näköinen.

Kuva 41 Verkkosivun etusivu

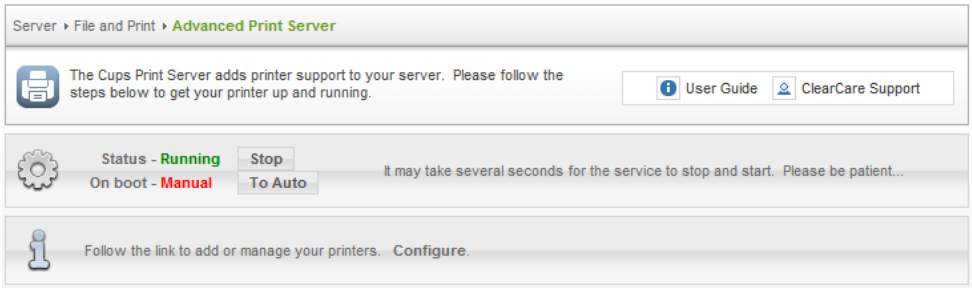
5.1.3. Yhteenveto

Web-palvelimen käyttäminen samalla koneella missä on itse palomuuri, ei ole suositeltavaa. Yleisempänä syynä voidaan pitää sitä, että jos ulkopuolinen käyttäjä pääsee hakkeroimaan Web-palvelimeen sisään, niin tämä voi myös päästä muualla tässä koneessa, joka voi mahdollistaa pahimmassa tapauksessa ulkopuolisen käyttäjän pääsemisen suoraan verkossa oleviin palvelimiin käsiksi.

Lisäksi ei ole muutenkaan järkevää ajaa Web-palvelinta samalla koneella palomuurin kanssa koska jotkut sivuilla olevat kokonaisuudet voivat vaatia koneelta ylimääräisiä tehoja.

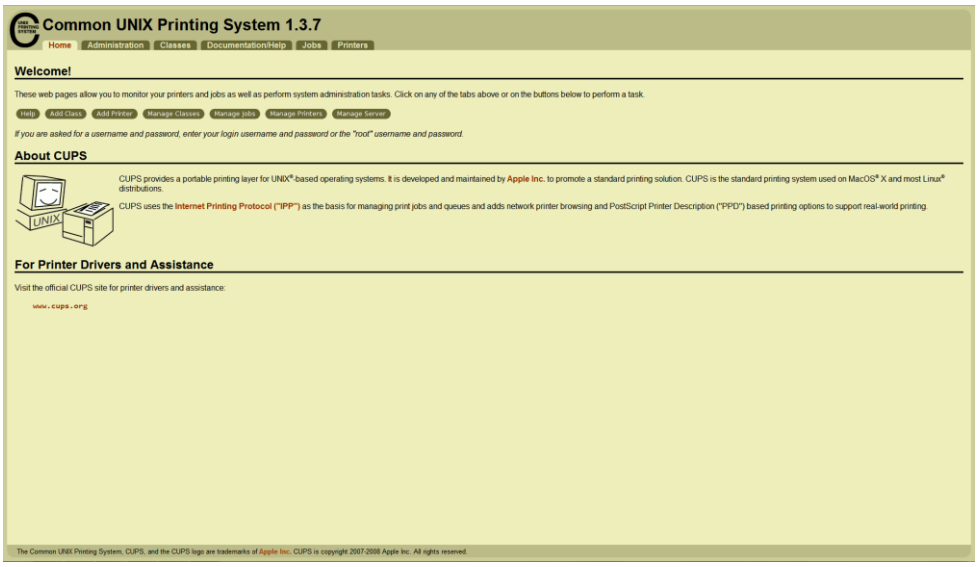
5.2. Tulostinpalvelin

Tulostinpalvelin sijaitsee samassa paikassa missä Web-palvelin mutta nimellä Advanced Print Server. Tämän valikon takaa aukeaa perussivu, josta voidaan palvelin käynnistää. Ilman käynnistämistä ei voida palvelinta konfiguroida toimintaan, joten käynnistäminen on välttämätöntä, kuten kuvasta 42 selviää.



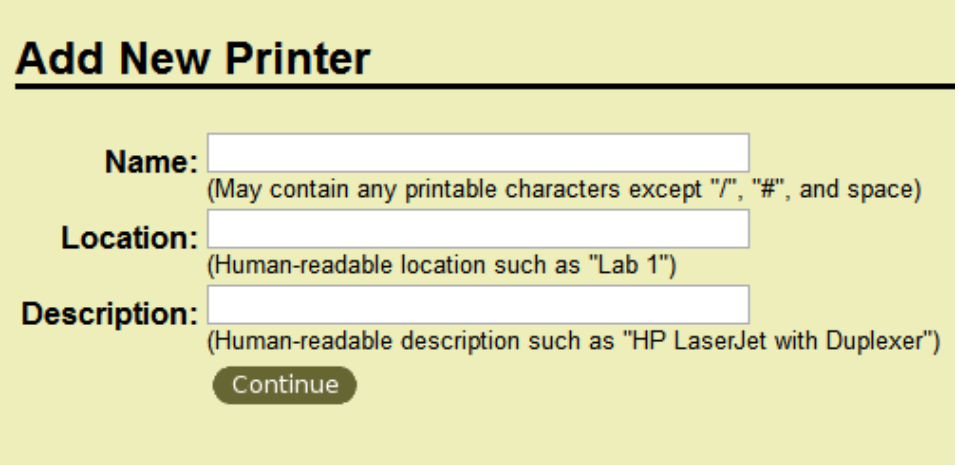
Kuva 42 Tulostinpalvelin

Tästä eteenpäin jatketaan painamalla Configure-linkkiä, joka siirtää käyttäjän Common UNIX Printing System -sivustolle, joka tunnetaan paremmin nimellä CUPS. Sivun etusivu näkyy kuvassa 43.



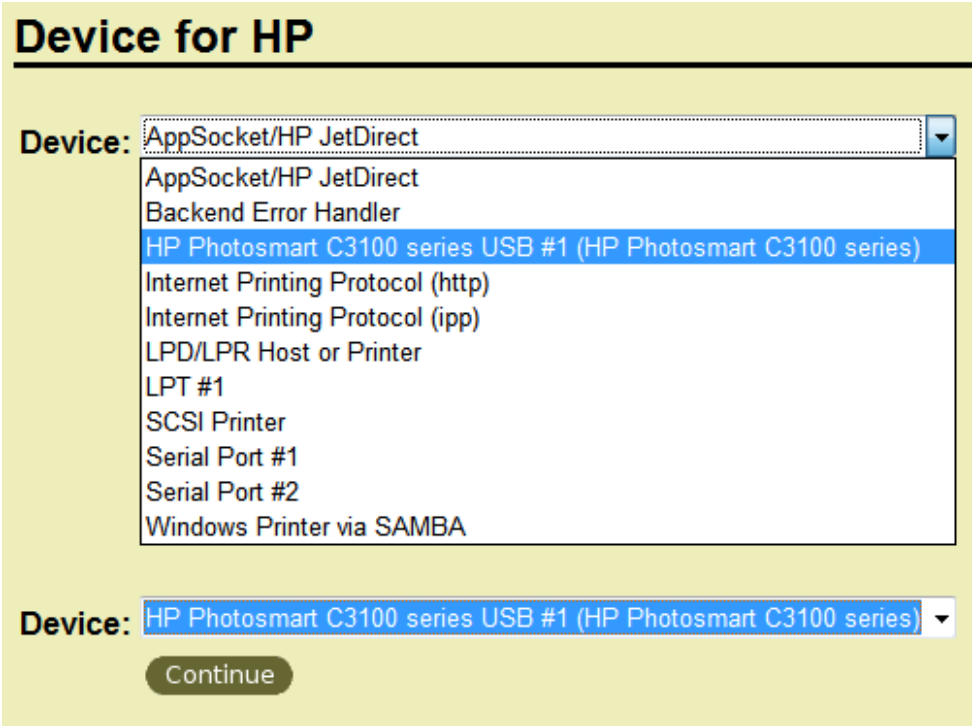
Kuva 43 CUPS:n etusivu

Tämän ohjelman etusivu on hyvin selkeä ja käyttäjälle heti selviää mitä tällä voidaan tehdä. Tulostimen lisääminen tapahtuu klikkaamalla Add Printer -nappia, joka avaa käyttäjälle kuvan 44 valikon.



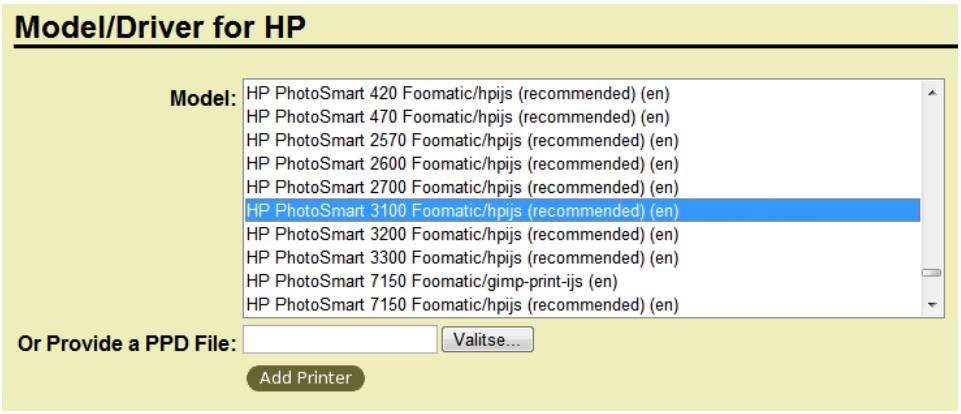
Kuva 44 Tulostimen lisäys

Tähän annetaan tulostimen perustiedot, nimi, sijainti ja nimitys. Lopuksi klikataan Continue-nappia, joka avaa käyttäjälle kuvan 45 näköisen sivun.



Kuva 45 Tulostimen liitännän valinta

Tässä valikossa valitaan alasvetovalikosta tulostimen liitäntä, johon tulostin on kytketty. Eteenpäin päästään painamalla Continue-nappia, joka avaa käyttäjälle kuvan 46 näköisen sivun.



Kuva 46 Tulostimen valinta

Tällä sivulla valitaan tarkemmin tulostimen malli ja lopuksi painetaan Add Printer -nappia, joka lisää tulostimen palomuuriohjelmistoon ja avaa käyttäjälle lopuksi tulostimen asetussivun, joka näkyy kuvasta 47.

Kuva 47 Tulostimen asetukset

Annoin näiden asetusten olla vakiomäärityksillä, koska en huomannut näissä mitään erikoisempaa tulostuksen kannalta.

Tulostinta voi tarkastella etusivun yläpalkissa olevan Printers-valikon takaa lopuksi ja tämän toimivuutta voidaan testata tulostamalla testisivu Print Test Page -napista.

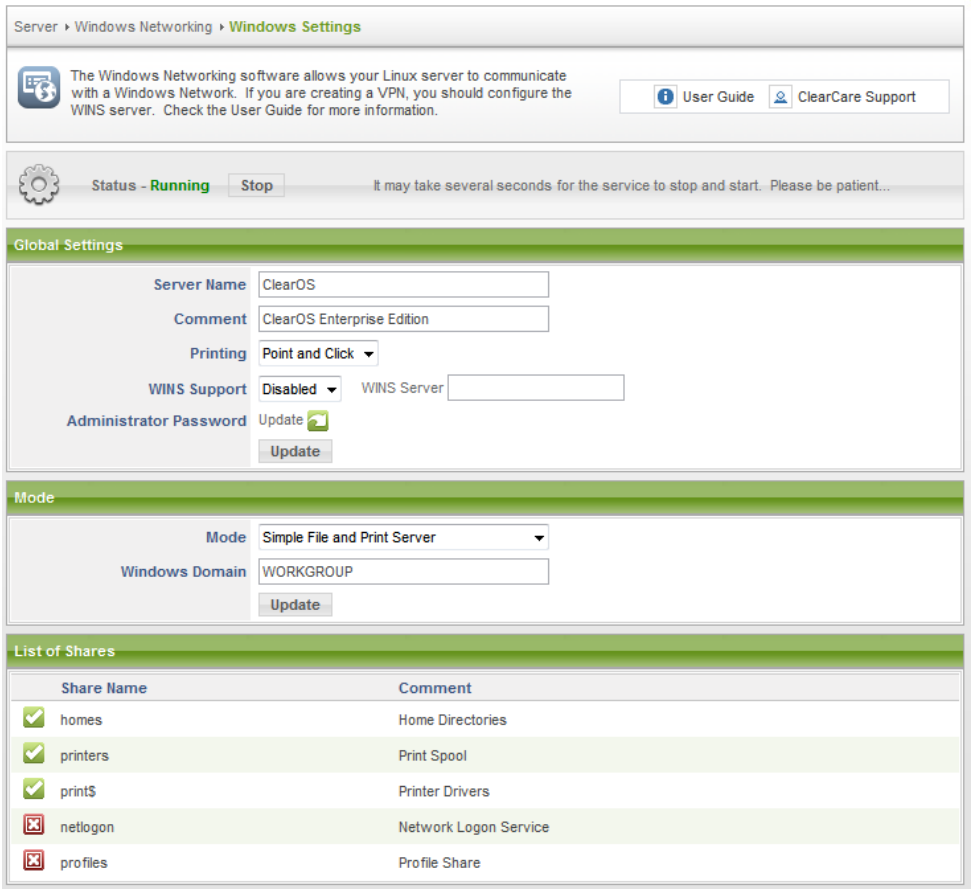
Tulostimen lisääminen Windows-käyttöjärjestelmään käsitellään seuraavassa osiossa, jossa käsitellään verkkojako, koska tämän kautta tulostimen lisääminen on helpompaa.

5.3. Verkkojako

Tiedostojen jakoon sisäverkossa ClearOS-palomuuriohjelmisto käyttää Linux-käyttöjärjestelmien tapaan Samba-palvelinta.

Samba-palvelin sijaitsee saman otsikon alla kuin edelliset Web-palvelin ja tulostinpalvelin nimellä Windows Settings.

Samba-palvelimen kongifurointi on helppoa graafisen käyttöliittymän kautta. Samban valikko näkyy kuvassa 48.



Kuva 48 Samba-palvelin

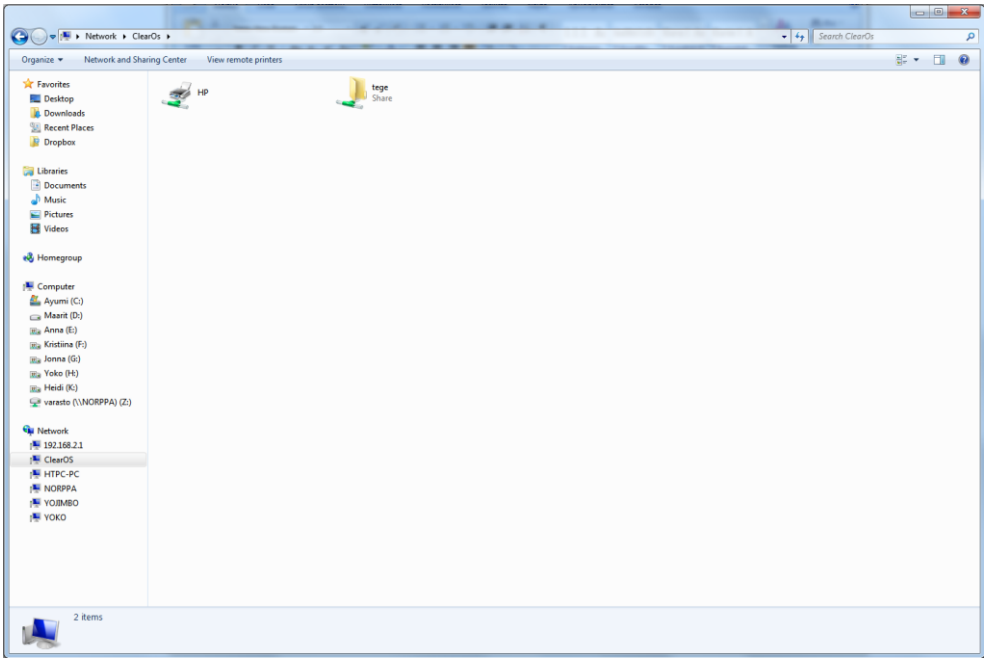
Aluksi pitää tämä käynnistää painamalla Start-nappia, joka on kuvassa 46 Stop-napin tilalla. Valikon alussa on Server Name (Palvelimen nimi) tähän voidaan vaihtaa se minkä käyttäjä itse haluaa. Testauksen vuoksi tähän vaihdettiin Clear-nimi. Seuraavaksi Printing (Tulostus) -kohtaan valitaan Point and Click, jolloin saamme tulostimen näkymään myös verkkojakojen yhteydessä. Lopuksi painetaan Global Settings (Yleisasetukset)-otsikon alla olevaan Update-nappia. Tämä päivittää edellä tehdyt asetukset.

Seuraavaksi muokataan Mode (tila)-otsikon alla olevaan Mode-kohtaan Simple file and Print Server (Yksinkertainen tiedoston- ja tulostimen palvelin) ja muutetaan Windows Domain -kohtaan oikea ryhmä, joka testiverkossa on WORKGROUP. Lopuksi painetaan Update-nappia, joka päivittää edellä tehdyt muutokset.

Nyt voidaan Windows-tietokoneelta ottaa normaaliin tapaan yhteys avaamalla esimerkiksi Oma Tietokone ja kirjoittamalla osoiteriville \\Clear tai vaihtoehtoisesti \\palvelimen IP-osoite. Sen jälkeen kysytään käyttäjältä tämän käyttäjätunnus ja salasana. Kun nämä on annettu, avautuu käyttäjälle oma home-kansio ja tulostin, joka oli aiemmin luotu.

Nyt käyttäjällä on mahdollista siirtää omaan verkkokansioonsa tiedostoja, joita käyttäjä haluaa tallentaa, palvelimme tai poistaa tiedostoja palvelimelta.

Kuvassa 49 näkyy onnistunut verkkojakoon otettu yhteys ja tulostin.



Kuva 49 Onnistunut verkkojako

5.3.1. Tulostimen lisäys

Tulostimen lisäys aloitetaan kaksoisklikkaamalla tulostimen kuvaketta, joka näkyy kuvassa 49. Jonka jälkeen Windows ilmoittaa käyttäjälle, että tulostimen ajureita ei löydetty ja sen, haluaako tämä asentaa ne. Tähän vastataan myöntävästi ja asennettaan tulostimelle tarkoitetut Windows-ajurit, jotka löytyvät tulostimen valmistajan sivuilta.

Kun ajurit on asennettu, tulostin asentuu kiltisti Windowsin tulostimeksi ja tämän jälkeen tulostimella voidaan tulostaa normaaliin tapaan.

5.3.2. Yhteenveto

Tulostimen lisäys ClearOS:n on helppoa ja tämä ei vaadi käyttäjältä juurikaan suurempia ponnistuksia. Tietoturvan kannalta tällä ei ole väliä onko palvelimeen kytketty tulostin vai ei. Koska tässä ei ole tietoturvallisuuden takia mitään riskiä.

Verkkojaossa itsessään ei ole tietoturvariskiä vaan riskit tulevat silloin esiin, jos käyttäjä tallentaa palvelimella jotain arkaluontoisia tiedostoja joista on mahdollisesti hyötyä tunkeutujalle.

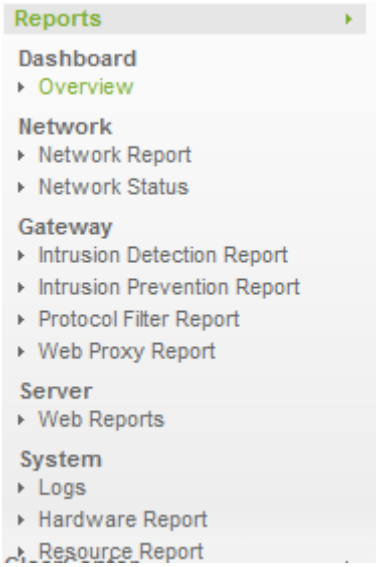
5.4. Raportit

Reports-otsikko pitää allaan koko järjestelmän yhteenvedon ja tämän raportit eri moduulien toiminnasta. Näiden avulla käyttäjän on helppo

selvittää vikatilanteissa missä vika on ja täten korjata tämä. Lisäksi raportteja voidaan lukea SSH-yhteyden ylitse ClearOS:n /var/log -hakemiston takaa.

Huomasin kuitenkin itse, että Web-käyttöliittymä pitää sisällään haun, joka helpottaa tietyissä raporteissa oikean kohdan löytämistä.

Kuvasta 50 selviää Web-käyttöliittymän sisältämät raportit ClearOS-palomuuriohjelmistosta.



Kuva 50 ClearOS-palomuuriohjelmiston raportit

6 YHTEENVETO

ClearOS-palomuuriohjelmisto suoriutuu mallikkaasti palomuurin tehtävistä ja samalla pystyy myös tarjoamaan toimivia palveluita kuten Web-palvelimen. Näillä ominaisuuksilla on tämä ohjelmisto saatu erottumaan paljon enemmän muista vastaavista Linux-pohjaisista ohjelmistoista.

Valikot ovat selkeät mutta näiden sisällyttäminen opinnäytetyöhön oli vaikeaa koska valikon alta paljastuu lista otsikoita, joiden alle itse moduulin valikot on sijoitettu. Se miksi on näin, johtuu aivan siitä, että palomuuriohjelmistoon voidaan asentaa moduuleja käyttäjän tarpeen mukaan ja näin saadaan sijoitettua uudet moduulit oikeille kohdille.

Raportteja selatessani itselläni tuli tunne, että ClearOS-palomuuriohjelmiston oma raportointijärjestelmä on peruskäyttäjälle aivan tarpeeksi hyvä. Aktiivisempi käyttäjä saa paremmin kuitenkin tiedon irti logs-kansioon tulevista tiedostoista ja näitä tiedostoja tutkimalla. Tämä johtuu suurimmaksi osin siitä, että koska itse olen käyttänyt aika paljon Linux-käyttöjärjestelmiä, niin tulee automaattisesti katsottua tuota kansiota vikatilanteissa.

IPv6-verkolle ClearOS-palomuuriohjelmisto ei valitettavasti tarjoa tukea laisinkaan. Ohjelmistoon on kyllä mahdollista manuaalisesti lisätä IPv6-osoite mutta tämän kautta ei ole mahdollista ohjata IPv6-liikennettä. IPv4-liikenteen ohjaamisesta ohjelmisto suoriutuu mallikkaasti.

LÄHTEET

CentOS, The Community Enterprise Operating System, 2010, Viitattu 10.3.2010,
http://www.centos.org/

Firewall, Wikipedia the free encyclopedia, 2010, Viitattu 10.3.2010,
http://en.wikipedia.org/wiki/Firewall_(computing)

Steam Support, 2010, Viitattu 15.3.2010,
https://support.steampowered.com/kb_article.php?ref=8571-GLVN-8711

ClearSDN Services, 2010, Viitattu 30.3.2010,
https://secure.clearcenter.com/portal/build3.jsp

ClearFoundation, 2010, Viitattu 12.4.2010,
http://www.clearfoundation.com/

ClearOS Enterprise 5.1, ClearFoundation, 2010, User Guide, Viitattu 12.4.2010,
http://www.clearcenter.com/support/documentation/clearos_enterprise_5.1/user_guide/start

Liite 1

IGMPProxyn konfiguraatio

```
#############################################################
#
#  Example configuration file for the IgmpProxy
#  ----------------------------------------
#
#  The configuration file must define one upstream
#  interface, and one or more downstream interfaces.
#
#  If multicast traffic originates outside the
#  upstream subnet, the "altnet" option can be
#  used in order to define legal multicast sources.
#  (Se example...)
#
#  The "quickleave" should be used to avoid saturation
#  of the upstream link. The option should only
#  be used if it's absolutely nessecary to
#  accurately imitate just one Client.
#
#############################################################

##------------------------------------------------
## Enable Quickleave mode (Sends Leave instantly)
##------------------------------------------------
quickleave


##------------------------------------------------
## Configuration for eth0 (Upstream Interface)
##------------------------------------------------
phyint eth0 upstream  ratelimit 0  threshold 1

##------------------------------------------------
## Configuration for eth1 (Downstream Interface)
##------------------------------------------------
phyint eth1 downstream  ratelimit 0  threshold 1
altnet 192.168.2.0/24

##------------------------------------------------
## Configuration for eth2 (Disabled Interface)
##------------------------------------------------
#phyint eth2 disabled
```