

IT-palveluiden hallinta ja Tietoturvan toteutus (ITPH-TT)

Mikael Malste K1285 IIT14S1
Harri Jäntti H9590 IIT14S1
Joonas Lipponen H8317 IIT14S1
Juho Helander H9410 IIT14S1
Jesse Ala-Lahti H4222 IIT13S1

Huhtikuu/2017
Tekniikan ja liikenteen ala
Tietotekniikan koulutusohjelma

Sisältö

1	Johdanto	19
2	Yritys	19
2.1	Yrityksen organisaatorakenne ja laitteisto	19
2.2	Yrityksen palvelut	19
2.2.1	Henkilökunta	20
3	Teoria	20
3.1	Active Directory Domain Services	20
3.1.1	Active Directoryn rakenne	21
3.1.2	AD-metsä	22
3.1.3	AD-puut	22
3.1.4	OU	22
3.2	Groups	23
3.2.1	Domain Local Groups	23
3.2.2	Universal Groups	24
3.2.3	Global Groups	24
3.3	DHCP	24
3.4	DNS	25
3.5	Forwarders	26
3.6	Forwarders Lookup Zones	26
3.7	Reverse Lookup Zones	26
3.8	Conditional Forwarders	27
3.9	DNS Record	27
3.10	NTP	30
3.10.1	Toimintamalli	31
3.10.2	Toiminta	31

3.11 DNSSEC	32
3.11.1 Toiminta.....	32
3.12 Salasanakäytänteet	34
3.12.1 Tiivisteet.....	34
3.12.2 Suolaus.....	35
3.13 Levyjakojen teoriaa	35
3.13.1 NTFS oikeudet.....	36
3.14 Kerberos	37
3.15 Authentication, Authorization and Accounting	39
3.15.1 RADIUS.....	40
3.15.2 VyOS.....	40
3.16 Roaming profiilit	41
3.17 Public Key Infrastructure	42
3.18 NAT	44
3.19 VPN	44
3.20 SSL VPN.....	45
3.21 IPSec	46
3.22 MFA	47
3.23 Sähköposti	48
3.24 IGP	50
3.24.1 OSPF.....	50
3.25 BGP	51
3.26 Tietokantapalvelin	52
3.27 Lightweight Directory Access Protocol.....	53
3.28 Intranet.....	54
3.29 Palomuuri	56

3.30 Pilvipalvelut	57
3.31 Monitorointi	59
3.31.1 Zenoss Core.....	61
3.31.2 OpenNMS.....	62
3.31.3 Vertailu OpenNMS vs Zenoss Core	62
3.32 Tikettijärjestelmä.....	63
3.33 IDS vs. IPS.....	64
3.34 Lähiverkon koventaminen.....	65
3.34.1 BPDU Guard	65
3.34.2 DHCP Snooping	66
3.34.3 Control Plane Protection	66
3.34.4 CDP / LLDP hardening.....	67
3.35 Haavoittuskannaus	68
3.36 802.1x	68
3.37 Lokit	69
3.38 Auditointi.....	69
4 Suunnitelma	70
4.1 AD-looginen rakenne.....	70
4.2 DHCP-suunnitelma ja MAC-Binding	71
4.4 HQ Fyysinen ja looginen topologia.....	72
4.5 Pohjois-Suomen (PS) fyysinen ja looginen topologia	73
4.6 Salasanakäytänteiden toteutus.....	74
4.7 Käyttäjien profiilit, kotihakemistot ja backup	74
4.8 Levyjaot	75
4.9 Toiminnallisuustasot	76
4.10 NTP suunnitelma	76

4.11	Palveluiden Autentikointi	76
4.12	Tietokantapalvelin	77
4.13	IGP Kovennukset	77
4.14	DNS	78
4.15	Palomuuri	78
4.16	Tikettijärjestelmä.....	80
4.17	Sähköposti	80
4.18	Pilvipalvelu.....	80
4.19	Monitoroinnin suunnitelma	81
4.20	Lähiverkon kovennus.....	81
4.21	Haavoittuvuusskannaus	82
4.22	Etäyhteys	82
4.23	802.1x autentikaatio.....	83
4.24	Lokienhallinta	83
5	Toteutus	84
5.1	Pääkonttorin ohjainpalvelin DC1 ja DC2	84
5.1.1	Käyttäjien luonti	85
5.1.2	Replikointi ja DNS	86
5.1.3	RADIUS.....	89
5.1.4	Kerberos.....	91
5.1.5	Salasanakäytänteiden todennus	93
5.2	Pääkonttorin työasemat.....	93
5.3	Pääkonttorin tiedostopalvelimet FS1 ja FS2	95
5.3.1	Yleisen levyjaon tyhjennys.....	95
5.3.2	Tiedostopalvelimen FS1 backup	97
5.3.3	Roaming User.....	99

5.4 VyOS	102
5.5 VyOS NAT.....	103
5.6 Public Key Infrastructure avainten luonti ja sertifikointi	104
5.6.1 Certification Authority.....	106
5.7 Tietokantapalvelin	108
5.8 Branchien pystytys	109
5.9 Pohjois-Suomen PS ohjainpalvelimet DC1 ja DC2.....	111
5.9.1 Pohjois-Suomen IPSec tunneli	114
5.10 Keski-Suomen KS ohjainpalvelimet DC1 ja DC2	116
5.11 Ahvenanmaan palveluiden pystytys.....	118
5.12 Itä-Suomen IS ohjainpalvelinten pystytys	121
5.12.1 Itä-Suomen Tiedostopalvelimet	124
5.12.2 Itä-Suomen VyOS.....	124
5.13 Länsi-Suomen palveluiden pystytys	126
5.14 NTP toteutus.....	129
5.15 Sähköpostipalvelimen toteutus.....	136
5.15.1 Dovecot.....	136
5.15.2 Postfix	136
5.15.3 Squirrelmail.....	137
5.15.4 AD/LDAP-integraatio	140
5.16 Intra	141
5.17 Intran varmenne.....	146
5.18 IGP kovennuksen toteutus	149
5.19 DNS	150
5.20 Palomuuri	154
5.20.1 Pääkonttorin VyOS-reititin	154

5.20.2 pfSense asennus ja konfigurointi.....	155
5.20.3 Palomuurisäännöt	159
5.20.4 Palomuurisääntöjen todennus	162
5.21 Owncloud toteutus ja LDAP- integraatio.....	166
5.22 Snort	174
5.23 Monitoroinnin toteutus.....	178
5.24 Tikettijärjestelmä.....	182
5.25 Lähiverkon kovennus.....	188
5.26 Haavoittuvuuskannaus	192
5.27 Etäyhteys	198
5.28 802.1x autentikaatio.....	198
5.29 Logienhallinta	199
6 Pohdinta	206
6.1 Toimeksianto 3	206
6.2 Toimeksianto 4	207
Lähteet.....	208
Liitteet	211
Liite 1. Yrityksen laiteluettelo.....	211
Liite 2. Fyysinen topologia.....	215
Liite 3. Palomuurisäännöt	216
Liite 4. WG1-SW1	220
Liite 5. WG1-SW2	224
Liite 6. WG1-SW3	230
Liite 7. WG1-SW4	233
Liite 8. 802.1X konfiguraatio SW2	236
Liite 9. HQ VyOS konfiguraatio	237

Liite 10. Spidernettiin laajennus topologia..... 245

Kuviot

Kuvio 1. Esimerkki AD rakenteesta.....	22
Kuvio 2. Toimipisteillä sijaitsevat OU:t.....	23
Kuvio 3. DHCP toiminta Wiresharkissa.....	25
Kuvio 4. NTP viestirakenne.....	30
Kuvio 5. DNSSEC toiminta	33
Kuvio 6. Kerberoksen toiminta.....	38
Kuvio 7. PKI infrastruktuuri	43
Kuvio 8. IPSec toiminta.....	47
Kuvio 9. Sähköpostin liikenne	50
Kuvio 10. Tietokantarajapintojen toiminta	53
Kuvio 11. Etätyöntekijän yhteys intraan	55
Kuvio 12. Käyttäjän ja pilvi	58
Kuvio 13. Organisaatio rakenne	70
Kuvio 14. Pääkonttori HQn fyysisen topologia	72
Kuvio 15. Pääkonttori HQn looginen topologia	72
Kuvio 16. Pohjois-Suomen PS fyysisen topologia	73
Kuvio 17. Pohjois-Suomen PS looginen topologia	73
Kuvio 18. Levyjaot	75
Kuvio 19. Tietokannan käsitemalli	77
Kuvio 20. Palomuurin sijainti verkossa.....	79
Kuvio 21. Ohjainpalvelin nostettu domainiin ja annettu IP-osoite	84
Kuvio 22. DC1:lle luotu Reverse Lookup Zone	84
Kuvio 23. Globaalit ja lokaalit ryhmät	85
Kuvio 24. Johtaja- ryhmän käyttäjät	86
Kuvio 25. Pääkonttorin ohjainpalvelimen DC1 replikointi	86
Kuvio 26. DC1 yhteys katkaistu	87
Kuvio 27. DC2 toiminta AD:na laiterikon sattuessa	87
Kuvio 28. Käyttäjän profiili ladattu DC2:ltä	88
Kuvio 29. Työasemalta todennettu DNS:n toiminta DC2:lla	88
Kuvio 30. DNS DC2:lla.....	89

Kuvio 31. VyOS:lle määritetty RADIUS-palvelimen osoite ja salasana.....	89
Kuvio 32. Ohjainpalvelimelle luodut Policyt	90
Kuvio 33. Todennus radiuksen toiminnasta HQ-PC1:ltä	90
Kuvio 34. DC1 Event Viewer tieto väärästä käyttäjätunnuksesta kirjautuessa etänä reitittimelle.....	91
Kuvio 35. Klist komento.....	92
Kuvio 36. Kerberoksen salauksen muuttaminen	92
Kuvio 37. Salasanakäytänteiden todennus	93
Kuvio 38. Ensimmäinen pääkonttorin työasema nostettu domainiin	93
Kuvio 39. Käyttäjän kirjautuminen papankki.com domainiin	94
Kuvio 40. Todennus MAC-Binding toiminnasta pääkonttorin työasemalta	94
Kuvio 41. Ryhmäkäytänteissä ennalta määritelty taustakuva ja levyjaot.....	95
Kuvio 42. Yleinen kansion tyhjennys scripti	95
Kuvio 43. Käyttäjän sisäänkirjautumisen todennus	96
Kuvio 44. Ajastimen todennus	96
Kuvio 45. Todennus ajettavista toiminnoista.....	97
Kuvio 46. Volume Shadow Copy ajoitettu joka yö klo.01.00	97
Kuvio 47. FS1 replikointi FS2:lle	98
Kuvio 48. Todennus replikoinnista	98
Kuvio 49. Replikointi ajoitettu klo.01.00 joka päivä.....	99
Kuvio 50. Roaming profiles kansio tehty FS1-HQ:lle	100
Kuvio 51. Kansiopolun liittäminen	100
Kuvio 52. Testitiedosto säilynyt työpöydällä konetta vaihdettaessa.....	101
Kuvio 53. Roaming profiilin haun todennus.....	102
Kuvio 54. VyOs backup scripti	103
Kuvio 55. VyOs backup todennus.....	103
Kuvio 56. VyOS:lle luodut NAT-säännöt	104
Kuvio 57. Harrin RSA-avainparin luonti ja sertifikaattipyyntö	105
Kuvio 58. Jäsenten avaimet ja csr-tiedostot	105
Kuvio 59. Papankki sertifikaatin luonti.....	106
Kuvio 60. Harri.crt tarkastelu	106
Kuvio 61. Kayttajat sertifikaattipohja.....	107

Kuvio 62. Harrin sertifikaattipolku	107
Kuvio 63. Käyttäjien sertifikaatit	108
Kuvio 64. MySQL tietokanta palvelimella	108
Kuvio 65. Ubuntu-palvelin nostettu papankki domainiin	108
Kuvio 66. Backup.sh scripti.....	109
Kuvio 67. Varmuuskopiointi todennus.....	109
Kuvio 68. Branch:lle luodut subnetit.....	110
Kuvio 69. Pääkonttorin ja branchien välille luodut Bridgehead Serverit	110
Kuvio 70. Pääkonttorin ja branchien väliset IPSec-tunnelit	111
Kuvio 71. Pohjois-Suomen käyttäjät	112
Kuvio 72. Käyttäjän kirjautuminen ps.papankki.com domainiin.	112
Kuvio 73. Yleinen levyjako	113
Kuvio 74. Yleisen levyjaon GPO Pohjois-Suomen ohjainpalvelin DC1:ltä	113
Kuvio 75. PS toimipisteen käyttäjän taustakuva	114
Kuvio 76. Todennus PS:n IPSec tunnelin toimivuudesta.....	114
Kuvio 77. Ping pääkonttorin ohjainpalvelimelta	115
Kuvio 78. Tracert Itä-Suomen ohjainpalvelimelle	115
Kuvio 79. DC1 domain	116
Kuvio 80. Ping KS-DC1 to HQ-FS1	116
Kuvio 81. NTP KS-VyOS.....	117
Kuvio 82. Yleinen levyjako todennus	117
Kuvio 83. Ahvenanmaan palvelinten pingaus.	118
Kuvio 84. IPSec tunneli toiminnassa	118
Kuvio 85. Käyttäjät lisätty Ahvenanmaahan	119
Kuvio 86. Ahvenanmaan käyttäjien oikeudet	119
Kuvio 87. Ahvenanmaan Roaming profilet	120
Kuvio 88. Ahvenanmaan DC1 hakee HQ:Ita ajan	120
Kuvio 89. DC1 domainissa	121
Kuvio 90. IS-DC1 OU- ja ryhmärakenne.....	122
Kuvio 91. GPO-rakenne	122
Kuvio 92. Levyjako todennus.....	123
Kuvio 93. NTP- ja IP-osoite	123

Kuvio 94. Ekonomistien levyn oikeusmäärittely	124
Kuvio 95. VyOS reititystaulu	125
Kuvio 96. OSPF database	125
Kuvio 97. IPSec-tunnelin todennus	126
Kuvio 98. LS IPSec tunneli	126
Kuvio 99. LS Yhteyksien todennus	127
Kuvio 100. GPO todennus LS	127
Kuvio 101. Levyjakojen oikeudet LS	128
Kuvio 102. Levyjaot LS	128
Kuvio 103. NTP DC1-LS	129
Kuvio 104. Powershell- komennot	129
Kuvio 105. HQ NTP status	130
Kuvio 106. Event Viewer todennus	130
Kuvio 107. HQ vyOS konfiguraatio	131
Kuvio 108. NTP todennus HQ VyOS	131
Kuvio 109. HQ VyOS komennot	131
Kuvio 110. Branchien VyOS komennot	132
Kuvio 111. Länsi-Suomi branchin VyOS NTP konfiguraatio	132
Kuvio 112. Show ntp Länsi-Suomen branchilta	132
Kuvio 113. Pohjois-Suomen reitittimen NTP-aika	133
Kuvio 114. Branch DC:n NTP todennus	133
Kuvio 115. MFA todennus	134
Kuvio 116. DNS Conditional Forwarders	134
Kuvio 117. BGP asetukset	135
Kuvio 118. Show ip bgp	135
Kuvio 119. Sähköpostien sijainti	136
Kuvio 120. Postfixin konfigurointitiedosto	137
Kuvio 121. SSL:n luonti postfixille	137
Kuvio 122. Palvelimen nimen asetus	138
Kuvio 123. Squirrelmailn konfiguraatiotiedosto	138
Kuvio 124. Kissa@papankki.com saapuneet viestit	139
Kuvio 125. Testiviesti vastaanotettu	139

Kuvio 126. Domainiin liittyminen	140
Kuvio 127. Domainin käyttäjät	140
Kuvio 128. Scripti millä tehdään kotikansiot	141
Kuvio 129. ISS:n alkuvälkkö	142
Kuvio 130. Wordpress ja sille tietokanta asennettu	142
Kuvio 131. Wordpress adminsivu	143
Kuvio 132. URL:n asettaminen Wordpressiin	144
Kuvio 133. Intrasivun etusivu	145
Kuvio 134. Kuvien lataus sivulle toimii	146
Kuvio 135. AutoEnrollment GPO	146
Kuvio 136. FS1-HQ sertifikaatti	147
Kuvio 137. Intran varmenne	148
Kuvio 138. HTTPS-yhteys intraan	148
Kuvio 139. OSPF kovennukset HQ	149
Kuvio 140. LS OSPF	150
Kuvio 141. DNS- palvelimen rajapinnan osoitteet	150
Kuvio 142. Bind9 konfiguraatiotiedostot	151
Kuvio 143. Db.papankki.com tiedostoon lisättyt laitteet ja julkiset osoitteet	151
Kuvio 144. Ulkoverkon DNS- palvelinten osoitteet	152
Kuvio 145. Zone db.10	152
Kuvio 146. db.10- tiedosto	153
Kuvio 147. Nimikyselyn testaus	153
Kuvio 148. Rajapintojen osoitteet muutoksen jälkeen	154
Kuvio 149. Uudet staattiset reitit	154
Kuvio 150. pfSense rajapinnat	155
Kuvio 151. pfSense aloitussivu	155
Kuvio 152. Domain, DNS ja NTP	156
Kuvio 153. DHCP asetus pfSense:ssä	157
Kuvio 154. NAT kytketty pois päältä	157
Kuvio 155. SSH päälle	158
Kuvio 156. Floating any sääntö	158
Kuvio 157. Floating säännöt	159

Kuvio 158. Public säännöt	159
Kuvio 159. Servers säännöt	160
Kuvio 160. WS säännöt.....	160
Kuvio 161. WAN säännöt.....	161
Kuvio 162. Sivutoimipaikkojen alias	161
Kuvio 163. ICMP- liikenne sallitaan	162
Kuvio 164. ICMP- liikenne sallittu kaikkiin rajapointoihin.....	163
Kuvio 165. Ping työasemalta ohjainpalvelimelle onnistuu	163
Kuvio 166. Block ICMP	164
Kuvio 167. ICMP blokattu kaikissa rajapinnoissa	164
Kuvio 168. ICMP- todennus sääntömuutoksen jälkeen	164
Kuvio 169. PfSense tilataulu.....	165
Kuvio 170. Kohdepolku, mistä Owncloud pystyy lataamaan halutut paketit.....	166
Kuvio 171. Tietokannan luonti Owncloudille	166
Kuvio 172. Admin käyttäjän luonti asennuksen jälkeen	167
Kuvio 173. Testikäyttäjien luonti.....	167
Kuvio 174. Tiedoston lisääminen pilveen onnistui.....	168
Kuvio 175. NTP:n asettaminen	168
Kuvio 176. Konfiguraatioiden asettaminen palvelimen löytämiseksi	169
Kuvio 177. Yhteys DC1:seen testattiin	169
Kuvio 178. Samban konfiguraation testaus	169
Kuvio 179. Ubuntu palvelin yhdistetään AD:hen	170
Kuvio 180. Winbind saa oikeudet kirjautua	170
Kuvio 181. Winbind:n pääsy asetus kolmeen tiedostoon	170
Kuvio 182. LDAP lisäosan ottaminen käyttöön	171
Kuvio 183. Owncloud LDAP asetukset	171
Kuvio 184. Testikirjautuminen käyttäjällä JussiJohtaja.....	172
Kuvio 185. Kirjautumistapojen hyväksyminen	172
Kuvio 186. Jussi Johtajan kirjautumistiedot	173
Kuvio 187. Jussi Johtajan tiedostot	173
Kuvio 188. Pate Palvelimen kirjautuminen	174
Kuvio 189. Zenmap.....	175

Kuvio 190. Snort Alert	176
Kuvio 191. Snort IPS	176
Kuvio 192. Zenmap Snort IPS	177
Kuvio 193. Snort ei hälytystä.....	177
Kuvio 194. LDAP servereiden osoitteet.....	178
Kuvio 195. LDAP bind	178
Kuvio 196. Ryhmät johon täytyy kuulua	179
Kuvio 197. Liikenne toimii HQ-VyOS	180
Kuvio 198. Ongelmia havaittu FS1-HQ.....	180
Kuvio 199. SNMP R1-HQ.....	181
Kuvio 200. Kovalevy liian täynnä.....	181
Kuvio 201. SNMP konfigurointi HQ-WEB palvelimelta	181
Kuvio 202. Sähköposti harri@papankki.com	182
Kuvio 203. Tikettijärjestelmän ifconfig-tiedot	182
Kuvio 204. Osticket-palvelimen /var/www/html-tiedosto	182
Kuvio 205. Osticket-palvelimen tietokanta	183
Kuvio 206. Osticket AD/LDAP-lisäosan asetukset	184
Kuvio 207. Tikitin lähetyks Pate Palvelimella	185
Kuvio 208. Tikitin saapuminen	185
Kuvio 209. Tiketti.csr tiedosto.....	186
Kuvio 210. Tiketti.cer tiedosto	187
Kuvio 211. Apache2 default-ssl.conf tiedoston muutokset	187
Kuvio 212. OSticket:n HTTPS-varmenne	188
Kuvio 213. WG1-SW1 wlanit	189
Kuvio 214. WG1-SW2 wlanit	189
Kuvio 215. WG1-SW3 wlanit	190
Kuvio 216. WG1-SW4 wlanit	190
Kuvio 217. WG1-SW1 DHCP-snooping	191
Kuvio 218. WG1-SW2 DHCP-snooping	191
Kuvio 219. WG1-SW3 DHCP-snooping	192
Kuvio. 220 Zenmap Scan R7	193
Kuvio. 221 Zenmap topologia	194

Kuvio. 222 Zenmap VyOS	195
Kuvio. 223 VyOS SSH	195
Kuvio. 224 Kali dig	196
Kuvio. 225 Kali Sparta.....	197
Kuvio 226. Serveri Certit ja avain	198
Kuvio 227. OpenVPN toimii	198
Kuvio 228. Radius-palvelimen testaus	199
Kuvio 229. Logien hallintapalvelimen osat.....	200
Kuvio 230. Javan asennus.....	201
Kuvio 231. Elasticsearch asennus ja confi.....	201
Kuvio 232. Graylog serverin asennus	202
Kuvio 233. Salasanana luonti	202
Kuvio 234. Graylog Web- interfaces asennus	202
Kuvio 235. Graylog Web-interfaces aloitussivu	203
Kuvio 236. Graylog- palvelimen kuuntelemat portit.....	203
Kuvio 237. Lähdelista.....	204
Kuvio 238. DC1 saapuvat lokit.....	204
Kuvio 239. Lokeja Harrin kirjautumisesta	205
Kuvio 240. Sähköpostin lähetysten lokit.....	205
Kuvio 241. Harrin uloskirjautumisen loki	206

Taulukot

Taulukko 1. VyOS toimintoja	41
Taulukko 2. Zenoss Core:n ominaisuuksia	61
Taulukko 3. MAC-Binding taulukko työasemille	71
Taulukko 4. Levyjakojen oikeudet	75
Taulukko 5. Toimipaikkojen IPSec- tunnelin osoitteet, tunnelin nro ja Router ID.....	111

Lyhenteet

AAA	Authentication, Authorization and Accounting
ACE	Access Control Entries
ACL	Access Control List
AD	Active Directory
AD DS	Active Directory Domain Services
AS	Autonomous System
AXFR	Authoritative Transfer
BPDU	Bridge Protocol Data Unit
BGP	Border Gateway Protocol
CDP	Cisco Discovery Protocol
DC	Domain Controller
CNAME	Canonical Name record
DHCP	Dynamic Host Configuration Protocol
DKIM	Domain Keys Identified Mail
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DMZ	Demilitarized Zone
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol Encapsulation over LANs
FAT32	File Allocation Table 32
FC	Full Control
FQDN	Fully Qualified Domain Name
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
Intra	Internal Network
IP	Internet Protocol
IPS	Intelligent Protection System

IPSec	IP Security Architecture
ITIL	Information Technology Infrastructure Library
JAMK	Jyväskylän Ammattikorkeakoulu
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LFC	List Folder Contents
LLDP	Link Layer Discovery Protocol
MDA	Mail Delivery Agent
MFA	Multifactor authentication
MIB	Management Information Base
MTA	Mail Transfer Agent
MUA	Mail User Agency
MX	Mail Exchange Record
NAT	Network Address Translation
NS	Name Server Records
NTFS	New Technology File System
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OU	Organization Units
PAT	Port Address Translation
PHP	Hypertext Preprocessor
PTR	Pointer Record
R	Read
RADIUS	Remote Authentication Dial-In User Service
R&E	Read & Execute
RIB	Routing Information Base
RIP	Routing Information Protocol
RSA	Rivest Shamir Adleman
SHA-2	Secure Hash Algorithm 2
SNMP	Simple Network Management Protocol
SOA	Start of Authority
SPF	Sender Policy Framework
SQL	Structured Query Language
SRV	Service Record

SSL VPN	Secure Sockets Layer Virtual Private Network
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TLV	Type Length value
TXT	Text Record
UAG	Direct Access server
UDP	User Datagram Protocol
VPN	Virtual Private Network
W	Write

1 Johdanto

Tässä raportissa käsitellään IT-palveluiden hallinta ja tietoturvan toteutus-kurssilla saatua toimeksiantoa, jossa toteutamme verkkoratkaisut isolle pankkikonsernille, joka tarjoaa pankkipalveluita kansalaisille ja yrityksille. Tavoitteena on suunnitella ja toteuttaa pankin palvelut sekä infrastruktuuri, joka toimii Active Directory (AD) ympäristössä sisältäen mm. organisaatioyksiköt, ryhmät, ryhmäkäytänteet, Dynamic Host Configuration Protocol (DHCP) sekä Domain Name System (DNS) toteutus. Myös tiedostopalvelimen toteutus levyjakoinen ja kotihakemistoineen on toteutettava.

2 Yritys

Papankki on vakavarainen kokonaan suomalaisten omistuksessa oleva pankki, jonka tavoitteena on kasvaa maailmanlaajuiseksi yritykseksi finanssialalla. Pääkonttori sijaitsee Helsingissä. Pankin sivutoimipisteet sijaitsevat Länsi-Suomessa, Itä-Suomessa, Pohjois-Suomessa, Keski-Suomessa, Etelä-Suomessa sekä Ahvenanmaalla. Yritys tarjoaa luotettavia pankkipalveluita asiakkailleen, kallonajasta ja sijainnista riippumatta. Pankin palveluksessa toimii noin 500 alan ammattilaista.

2.1 Yrityksen organisaatorakenne ja laitteisto

Yrityksen toimitusjohtajana toimii Jussi Johtaja, jonka toimipisteenä on Helsingin pääkonttori. Jokaisella toimipisteellä on oma yksikönjohtaja, viisi ATK-tukihenkilöä, 50 konttorityöntekijää ja 10 ekonomia. Yrityksen laitteisto koostuu päätelaitteista, palvelimista, reitittimistä, kytkimistä, palomuurista, sekä varavirtalähteistä. Tarkempi laiteluettelo jokaiselle toimipaikalle löytyy liitteestä (Liite 1). Myös yrityksen fyysinen topologia löytyy liitteistä (Liite 2.).

2.2 Yrityksen palvelut

Yritys tarjoaa asiakkailleen verkkopankin, jossa pystyy tarkistamaan tilin saldon, maksamaan laskuja, sekä siirtämään rahaa tililtä toiselle. Asiakkaat voivat olla yhteydessä

pankin henkilökuntaan palautelomakkeen kautta, sekä lähettämään ongelmatilanteissa tikettejä tikettijärjestelmän kautta. Modernina finanssialan edelläkävijänä, yritys tarjoaa pelkästään sähköiset palvelut asiakkailleen. Puhelinjärjestelmistä ollaan luovuttu kokonaan.

2.2.1 Henkilökunta

Henkilökunnalla on käytettävissään oma henkilökohtainen sähköposti, sekä tallennustila yrityksen tiedostopalvelimelta. Yrityksen sisäisenä tiedotuskanavana toimii yrityksen intranet. Työntekijät voivat työntekijät voivat kommunikoida keskenään VoIP-palvelun kautta.

3 Teoria

3.1 Active Directory Domain Services

AD on Microsoftin kehittämä hallintapalvelu, jolla voidaan hallinnoida verkkojen käyttäjädataa, turvallisuutta ja resurssien jakoa Windowsin verkkoympäristössä.

Active Directory Domain Services (AD DS) tarjoaa keskitetyn käyttäjien tunnistamisen Windowsin verkkoympäristössä. AD DS sisältää hierarkkisen organisaatorakenteen ja yhden kontakti kohdan, josta pääsee käsiksi verkon kaikkiin resursseihin. AD DS sisältää myösken multimaster authenticationin, jolla saadaan vikojen sietokykyä ja redundanssia. On myösken mahdollisuus tehdä luottamuksuhteita muiden verkkojen kanssa, joissa on vanhempi versioita AD:sta tai UNIX:sta. (Jäntti, H & Viilos, M. 2016)

Active Directoryn single point of authentication mahdollistaa sen, ettei enää tarvitse käydä jokaista serverikonetta erikseen muokkaamassa, vaan saadaan yhdellä kirjautumisella kaikki verkonlaitteet muokattua haluamallaan tavalla (Jäntti, H & Viilos, M. 2016)

Domain Controller (DC) on Windowsin serveritietokone, joka on konfiguroitu AD DS rooliin. Siinä on mukana AD-tietokanta ja käyttäjien varmistuspalvelu, joka varmistaa käyttäjätiedot kirjautuessa verkkoon sisään. Jokainen DC on aktiivisesti mukana varastoinissa, muokkaamisessa ja ylläpitämässä AD-tietokannan tietoja. Multimaster

tietokanta mahdollistaa jokaisen domainin käyttäjän lisäämisen mihinkä tahansa DC-koneeseen. Replikoinnin avulla pidetään tietokannat synkronisoituna. Ulospäin menevällä replikaatiolla laukaistaan replikaatio DC:ssä ja sisäänpäin menevällä replikaatiolla saadaan päivityksiä muita DC-koneilta. Multimaster replication lisää turvallisuutta, koska tietokanta voidaan aina ladata toiselta DC:ltä. (Jäntti, H & Viilos, M. 2016)

Esimerkkinä Multimaster replikaatiosta, DC2:seen tulee tietokanta muutos, jolloin se lähettilä ilmoituksen DC1 ja DC3. Seuraavalla kerralla kun tulee replikaation aika DC1 ja DC3 lähettilävät tietokantapäivitys pyynnön. DC2 replikoi muutokset DC1 ja DC3, jonka jälkeen ne päivittävät AD-tietokantansa. (Jäntti, H & Viilos, M. 2016)

DC:tä käytetään määrittelemään, ylläpitämään, jakamaan ja turvaamaan verkkojen resurssit. Resursseihin sisältyy seuraavia asioita: tiedostoja, tulostimia, käyttäjä ryhmiä, käyttäjiä ja ohjelmistoja. (Jäntti, H & Viilos, M. 2016)

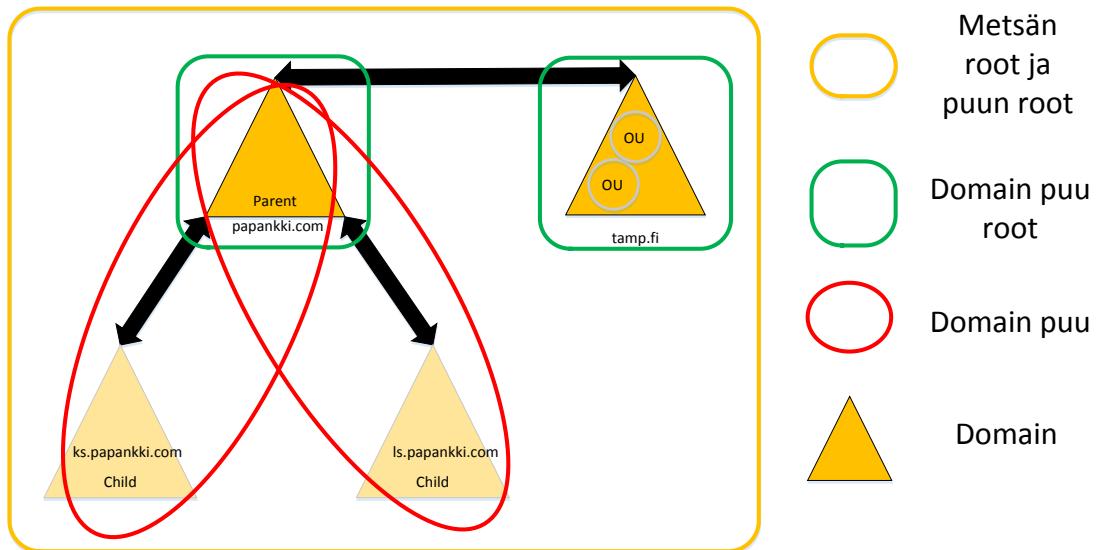
AD:ssä varastoidaan NTDS.dit tiedostoa. DC:ssä käytetään AD:tä käyttäjien varmistamiseen. DC:t varastoivat, ylläpitävät ja replikoivat. (Jäntti, H & Viilos, M. 2016)

Hyötyjä AD:n käytöstä on keskitettyhallinta, yhdestä kohdasta päästään käsiksi verkon resursseihin, vikojen sietokykyä, redundantisuuutta, voidaan käyttää montaa DC:tä, Multimaster kopointi, helpotettu resurssien sijainti ja yhteensopivuus uudempien ja vanhempien laitteiden kanssa. (Jäntti, H & Viilos, M. 2016)

Resurssien löytämisen helpottamiseksi voidaan julkaista palveluita verkossa, palveluita voidaan myöskin hakea käyttämällä sen nimeä, sijaintia tai määrittelyä. Tämä on ollut käytössä Windows 2000 lähtien. (Jäntti, H & Viilos, M. 2016)

3.1.1 Active Directoryn rakenne

AD:n loogisen rakenteen voi jakaa kahteen osaan, container tai leaf-objekteihin. Containerit voivat pitää sisällään muita objekteja, kun taas leaf-objektit eivät. Container objekteihin kuuluu seuraavat käsitteet: metsä, toimipisteet (sites), domain puut, domains ja organization units. Leaf-objekteihin kuuluvat seuraavat asiat: käyttäjät, ryhmät, kontaktit, tulostimet, jaetut kansiot, tietokoneet, Organization Units (OU) jainetOrgPersonit. Tätä on havainnollistettu kuviossa 1. (Jäntti, H & Viilos, M. 2016)



Kuvio 1. Esimerkki AD rakenteesta

3.1.2 AD-metsä

Isoon container objekti on metsä ja sillä määritellään verkon turvallisuuden rajat.

Käyttäjä pystyy pääsemään käsiksi yhdellä sisäänsinkirjautumisella kaikkiin metsän resursseihin, jos halutaan päästää toisen metsän resursseihin käsiksi, joudutaan kirjautumaan erikseen siihen metsään mihin halutaan. (Jäntti, H & Viilos, M. 2016)

3.1.3 AD-puut

Domain puu on looginen verkon ryhmittely resurssien ja laitteiden suhteen, joka käyttää vanhempi-lapsi periaatetta. Monta domainia voi olla yhdellä organisaatiolla käytössä. Domainien replikointi on itsenäinen global catalogista ja schema replikoinnista. (Jäntti, H & Viilos, M. 2016)

3.1.4 OU

Organization Units, OU tarkoittaa, kuinka käyttäjät liitetään omiin ryhmiinsä, jotta niitä on helppo hallita. Tätä suunniteltaessa kannattaa miettiä tulevaisuuteen. Mikä malli on helpoin sekä selkein hallita. Erilaisia malleja on useita ja mallin muuttaminen jälkkikäteen voi olla työlästä.

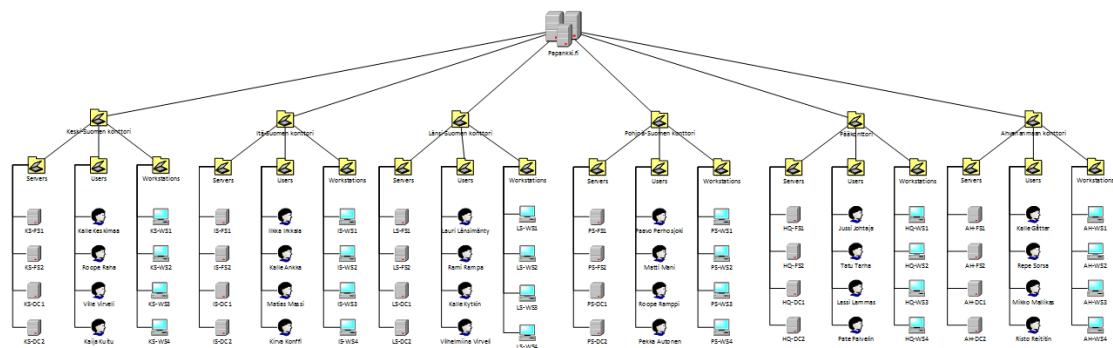
Esimerkiksi, tämä voidaan tehdä niin että se heijastaa organisaation eri työryhmiä.

Tällaisessa järjestelmässä olisi esimerkiksi johto, kirjanpito, myynti ja adminit. Toinen mahdollinen on järjestää nämä sijainnin perusteella, esimerkiksi Jyväskylä ja Helsinki.

Edellä mainittuja malleja voi myös yhdistellä ja luoda juuri omalle organisaatiolle sopiva ratkaisu. Tätä tehdessä kannattaa pitää mielessä, että kerroksien määrä kannattaa pitää pienenä, jotta järjestelmästä ei tulisi liian sekavaa.

Tässä esimerkissä on kuvattu yrityksen maantieteellinen topologia ja se on keitetyt töissä milläkin toimipisteellä. Myös tiedossa olevat palvelimet on sijoitettu toimipisteille.

(Kts. Kuvio 2). (Ala-Lahti, J & Malste, M & Nieminen, M. 2016)



Kuvio 2. Toimipisteillä sijaitsevat OU:t

3.2 Groups

3.2.1 Domain Local Groups

Domain Local Groups voi sisältää käyttäjiä, tietokonetilejä ja saman domainin muita ryhmiä, mutta myös globaaleja ja universaaleja ryhmiä muista domaineista. Tarkoituksena on jakaa oikeuksia ja resursseja paikallisesta domainista. Tämä ryhmä on kuitenkin lähimpänä itse resursseja, koska se on lokaali. Tämä on myös ensimmäinen ryhmä mikä luodaan, koska palvelimelle ei pääse muuten, jos ei käyttäjiä ole tehty.

(Jesse, A & Mikael, M & Mikko, N 2016)

3.2.2 Universal Groups

Universal Groups voi sisältää erilaisia käyttäjiä. Se voi sisältää käyttäjiä, tietokoneitä, globaaleja ja universaaleja ryhmiä. Pääkäyttötarkoitus on mahdollistaa käyttäjien ja ryhmien organisointi globaaleissa ryhmissä. Isot yritykset voivat käyttää Universal Groups:a ryhmien ryhmittämiseen eri toimipisteiden välillä. (Jesse, A & Mikael, M & Mikko, N 2016)

3.2.3 Global Groups

Global Groups voi sisältää käyttäjätilejä, tietokonekäyttäjiä ja globaaleja ryhmiä. Globaalilla ryhmällä voi estää tai sallia pääsyn resursseihin, jotka sijaitsevat metsän domainissa. Global Groupsia käytetään käyttäjien organisoimiseen toimipaikan sisällä. Organisoiminen toteutetaan yleensä työn nimikkeen tai roolin mukaan. (Jesse, A & Mikael, M & Mikko, N 2016)

3.3 DHCP

DHCP on protokolla jonka avulla tietokone (host) saa automaattisesti Internet Protocol (IP)-osoitteen ja muuta oleellista tietoa, kuten oletusyhdyskäytävän osoitteen ja aliverkon maskin. DHCP protokolla perustuu Bootstrap Protocol (BOOTP) nimiseen protokollaan ja jakaa monia yhteisiä ominaisuuksia kyseisen protokollan kanssa. DHCP ja BOOTP on Internet Engineering Task Force:n (IETF) kehittämiä protokollia. (Lipponen, J & Tanninen, T. 2016)

DHCP toimii siten, että ensiksi asiakaskone lähettää DHCP-pyyynnön yleislähetyksen (Discovery). Jos verkossa on DHCP-palvelu, DHCP-palvelin lähettää IP-osoiteen (Offer) asiakaskoneelle. Tämän jälkeen asiakaskone lähettää DHCP-pyyynnön (Request) yleislähetyssosoitteesseen, minkä palvelin hyväksyy lähettämällä hyväksymispaketin (DHCP ACK) missä on sopimuksen kestoaika ja muita konfiguraatiotietoja. Alla alevasta kuviosta 3, voidaan nähdä miten DHCP-paketit näkyvät Wireshark ohjelmassa (lukusuunta alhaalta ylöspäin). (Lipponen, J & Tanninen, T. 2016)

192.168.0.1 0.0.0.0	192.168.0.15 255.255.255.255	DHCP	363 DHCP ACK
192.168.0.1 0.0.0.0	192.168.0.15 255.255.255.255	DHCP	342 DHCP Request
		DHCP	363 DHCP Offer
		DHCP	342 DHCP Discover

Kuvio 3. DHCP toiminta Wiresharkissa

3.4 DNS

DNS on IETF:n kehittämä järjestelmä, jolla pystytään käänämään TCP/IP-liikenne nimimuotoiseen liikenteeseen. Kyseisen järjestelmän avulla ilman että käyttäjän tarvitssee muistaa tietyn Web-sivun IP-osoite, vaan hän pystyy saavuttamaan palvelun tiettyllä yksinkertaisella nimellä. (Lipponen, J & Tanninen, T. 2016)

DNS-nimiavaruus toteuttaa hyvin paljon puumaista rakennetta, jossa eri domainit sekä hostit erotellaan pisteellä. Täydellinen osoite yksittäiselle host koneelle on Fully Qualified Domain Name (FQDN) esimerkiksi riku.labranet.jamk.fi. Toisinkuin IP-osoitteistuksessa DNS:ssä osoite luetaan käännetyssä järjestysessä, jossa aloitetaan host osalla ja jatketaan domain osioilla. (Lipponen, J & Tanninen, T. 2016)

DNS-kyselyt jaetaan kahteen osaan rekursiivisiin ja iteratiivisiin kyselyihin. Rekursiiviset kyselyt vastaanottava nimipalvelin vastaa kyselyyn, jos sillä on omassa muistisaaan oikea informaatio. Jos informaatiota ei ole lähtee nimipalvelin kyselemään itse ensin root tason domainilta jatkaen top tason domain palvelimeen ja niin edelleen tason kaksi domainiin. Yleensä kuitenkin pelkästään host koneelta tulevat kyselyt ovat rekursiivia, mutta on mahdollista, että nimipalvelin käännetää lähetämään rekursiivia kyselyitä toiselle palvelimelle, jolloin vastaanottava palvelin toimii forwarderina. (Lipponen, J & Tanninen, T. 2016)

DNS-palvelimena voi toimia mikä tahansa tietokone, joka on määritetty toimimaan nimipalvelimena. Tätä varten palvelimen täytyy olla yhteydessä hierarkisesti ylempanä oleviin nimipalvelimiin. Maailmanlaajuisilla 13:sta DNS-juuripalvelimilla on tiedossaan koko internetin tietokanta nimistä ja osoitteista, joihin voidaan liikkennöidä. Kaikki muut DNS-palvelimet ovat asetettu toimimaan hierarkisesti alempalla tasolla ja ne ylläpitävät vain tiettyä osaa nimistä ja osoitteista.

Paikallinen internet palveluntarjoaja ylläpitää omaa DNS-palvelintaan omille asiakkailleen. DNS perustuu client/server arkkitehtuuriin, jossa käyttäjän selain toimii DNS-client:na ja välittää DNS-kyselyt palveluntarjoajan DNS-palvelimelle.

DNS-palvelimen saadessa kyselyn client:ltä, jota ei löydy omasta tietokannasta, se väitetään eteenpäin muille DNS-palvelimille, tai hierarkisesti ylempänä oleville DNS-palvelimille. DNS-palvelin voi siis hetkellisesti toimia myös client-roolissa. Prosessia jatketaan niin pitkään, kunnes kysely saavuttaa DNS-palvelimen jonka tietokannasta löytyy oikea nimi ja IP-osoite. Kyselyt voivat siis välittyä jopa DNS-juuripalvelimille asti. (Mitchell, B. 2017)

3.5 Forwarders

Käytännössä ollaan konfiguroitu tietyt nimipalvelimet lähetämään nimikyselyt johonkin tiettyyn nimipalvelimeen, joka selvittää ulko-tai sisäverkkoon kohdistuvat nimikyselyt. Hyvä puoli forwarders- tekniikassa on, että voidaan vähentää ulkoisten nimipalvelimien taakkaa, kun vain yksi DNS-serveri lähetää nimikyselyitä monien palvelimien sijasta. (Lipponen, J & Tanninen, T. 2016)

3.6 Forwarders Lookup Zones

Puhutaan alueesta, joka vastaa DNS-nimikyselyihin ja välittää niitä eteenpäin palveluntarjoajalle tai toiselle DNS-palvelimelle, jos se ei itse tiedä vastausta. Toimeenpanee DNS:n perustoimintoa ja mitä suurin osa kyselyistä sisältää eli käantää nimet IP-osoitteiksi. Alueet ovat yleensä suunniteltu pieniksi, koska yhden ison forwarder zonen ylläpitoa voi olla monimutkaisempaa kuin pienempien alueiden ylläpito. (Lipponen, J & Tanninen, T. 2016)

3.7 Reverse Lookup Zones

Alue jonka nimipalvelimet suorittavat päinvastaista toimintoa mitä forward lookup alue toimittaa. Eli käantää IP-osoite kyselyt nimiksi, mikä on päinvastainen toiminto mihiin DNS alun perin suunniteltiin (Understanding Reverse Lookup). Koska IP-

osoitteita luetaan verkko-osasta host osaan ja DNS-nimiä alidomainista ylmpään tar-koittaisi tämä sitä, että kun kyselyihin vastattaessa jouduttaisiin käymään kaikki do- mainit läpi nimiavaruudessa, tällaisissa kyselyissä nimipalvelimien kuormitus kasvaisi ja aikaa kuluisi enemmän. Tätä varten on kehitetty in-addr.arpa domain, joka käänää IP-osoitteet domain nimiksi käyttäen tietueita. Nimikyselyn lähettävä resolveri kään- tää osoitteen ympäri ja Pointer tietuetta (PTR) käyttäen lisää.in-addr.arpa nimen osoitteen perään. (Lipponen, J & Tanninen, T. 2016)

3.8 Conditional Forwarders

Conditional Forwardersit ovat forward- kyselyitä, jonkin tietyyn DNS-nimen mukaan (Using Forwarders). Eli kuten nimi kertoo, niin kyselyt edelleen lähetetään tiettyyn osoitteeseen vain, kun haluttu ehdollisuus tulee voimaan. Conditional Forwarding tulee silloin vitaaliksi ominaisuudeksi, kun halutaan olla suorassa yhteydessä kahden nimipalvelimen välillä laajemmissa AD-puissa. Ilman Conditional Forwarding:a esi- merkiksi yrityksen sisäisessä AD-ympäristössä olevan käyttäjän DNS-kyselyt, jotka ovat osoitettu toiseen containeriin AD-puussa osoittavat suoraan kantadomainiin, joka aloittaa rekursiivisen DNS-nimen selvittämisen mikä ei ole tehokas tapa DNS- kyselyihin, kun voitaisiin yhtä hyvin olla suorassa yhteydessä haluttuun nimipalveli- meen. (Lipponen, J & Tanninen, T. 2016)

3.9 DNS Record

Seuraava näkökulma DNS:n hallintaan ovat DNS-recordit, jotka todellisuudessa vas- taavat verkkotunnuksesta aina IP-osoitteisiin. DNS-tietueet ovat siten automaattisesti nipputettuna vyöhykkeen tiedostoon, joka mahdollistaa verkkotunnuksen IP- osoitteen löytämisen. Alla on muutama yleinen DNS-recordi. A-record vastaa siitä, miten verkkotunnus saadaan matchaamaan IP-osoitetta. AAAA on sama mutta toimii IPv6:lla. (Krout 2015.)

AXFR:ää (Authoritative Transfer) käytetään DNS replikoinnissa, vaikka on myös nyky- aikaisempiakin tapoja. AXFR:ää ei käytetä tavallisissa vyöhyketiedostoissa, vaan niitä

käytetään orja DNS-palvelimella kun yritetään jäljitellä vyöhyketiedostojen isäntää DNS-palvelinta. (Krout 2015.)

CNAME (Canonical Name Record)-tietueet ovat olemassa, sen takia jotta verkkotunnuksilla voi olla aliaksia. CNAME-tietueita ei pitäisi käyttää verkkotunnuksissa jotka voivat vastaanottaa sähköpostia, koska jotkut sähköpostipalvelimet käsittelevät postia kummallisesti verkkotunnuksissa joissa on CNAME. MX-tietueet eivät voi viittata CNAMEN määritämiin isäntäniimiin. (Krout 2015.)

DKIM (Domain Keys Identified Mail) näyttää julkisella avaimella autentikoitua viestejä, jotka ovat allekirjoitettu DKIM protokollalla. Tämä lisää kykyä tarkistaa sähköpostin aitous. (Krout 2015.)

MX (Mail Exchange) -tietue asettaa sähköpostin jakelun koteen verkkotunnusella tai aliverkkotunnusella. MX-tietueen ei välttämättä tarvitse osoittaa sinun serverillesi, jos käytät kolmannen osapuolen sähköpostipalveluita niin sinun tulisi käyttää niitä MX-tietueita mitä he tarjoavat. (Krout 2015.)

Priority on toinen osa MX-tietueissa. Tämä numero kirjoitetaan tietuetyypin ja kohdepalvelimen välille. Priority antaa sinun varapalvelimen sähköpostin varalle tälle kyseiselle verkkotunnuselle. Matalammat numerot ovat etusijalla. (Krout 2015.)

NS (Name Server) asettaa nimipalvelimen verkkotunnuselle tai aliverkkotunnuselle. Ensisijainen nimipalvelimen verkkotunnus rekisteröidään vyöhyketiedostoosi. Nimipalvelimet jotka ovat rekisteröity kuljettavat vyöhyketiedoston verkkotunnusellesi. (Krout 2015.)

Ensisijaiset nimipalvelimet konfiguroivat rekisterisi, joten toissijaiset nimipalvelimet konfiguroidaan ensisijaisen palvelimen vyöhyketiedostossa. (Krout 2015.)

PTR (Pointer Record) vastaa siitä, että IP-osoite ja verkko-osoite ovat samoja, jotta käänneiset DNS-kyselet toimivat. (Krout 2015.)

Se suorittaa päinvastaisen palvelun A-tietueessa, jotta sen avulla voidaan etsiä verkkotunnus, joka liittyy IP-osoitteeseen eikä päinvastoin. (Krout 2015.)

PTR-tietueet ovat yleensä asetettu palveluntarjoajaan. Ne eivät ole verkkotunnuksen vyöhyketiedostossa. Tämä tarkoittaa, että voit aina määrittää käänteisen DNS:än vaikka nimipalvelimesi olisivat muualla. (Krout 2015.)

SOA (Start of Authority) kirjaan vyöhyketiedostoihin host-nimen, jossa se alun perin luotiin. Seuraavaksi listassa on henkilön sähköpostiosoite, joka vastaa verkosivuston toiminnasta. Sielä on myös erilaisia numeroita. (Krout 2015.)

- Serial number: Versionumero tämän verkkotunnuksen vyöhyketiedostossa. Se muuttuu, kun tiedosta päivitetään.
- Refresh time: Ajanmäärä (sekunteina) ennen kuin toissijainen DNS-palvelin alkaa tarkistamaa muutoksia.
- Retry time: Aika, kuinka paljon toissijainen DNS-palvelin odottaa ennen uutta yritystä siirtää vyöhyketiedostoa, jos aikaisempi on epäonnistunut
- Expiry time: Aika, kuinka paljon toissijainen DNS-palvelin odottaa ennen kuin kopioi vyöhyketiedoston, jos se ei pysty päivittämään itseänsä.
- Minimum TTL: Pienin aika, mitä muiden palvelimen täytyisi pitää vyöhyketiedostoa välimuistissansa. (Krout 2015.)

SPF (Sender Policy Framework) -tietue kirjaan luetteloihin sähköpostipalvelimia varten verkkotunnuksia tai aliverkkotunnuksia. Se auttaa luomaan oikeellisuuden sähköpostipalvelimelle ja vähentää mahdollisuuksia tietojen väärrentämiseen, joka tapahtuu, kun joku feikki otsikoi sähköpostin, jotta se näyttää kuin olisi lähtöisin omalta verkkotunnukselta. Roskapostittajat yrittävät kiertää roskapostisuodattimet. SPF-tietue verkkotunnuksellasi kertoo muiden vastaanottajien sähköpostipalvelimet, jotta he voivat hylätä väärennetyn sähköpostin, jotka ovat peräisin luvattomilta palvelimilta. (Krout 2015.)

SRV (Service Record) vastaa siitä, että verkkotunnuksesi on oikealla kohdealueella. Nämä voit ohjata liikennettä tiettyihin palveluihin, kuten viestintä toiselle palvelimelle. (Krout 2015.)

TXT (Text Record) tuottaa tietoja verkkotunnuksestasi internetissä. Se on DNS-recordien joustava tyyppi, joka voi palvella useita eri tarkoitukset riippuen sisällöstä. Yksi käyttötapa on käyttää DNS-recordia. TXT voi luoda tiedostoistaan nimipalvelimia, jotka eivät suoraan tuo SPF:ää. Toinen käyttötapa on luoda DKIM-record postin allekirjoittamista varten. (Krout 2015.)

3.10 NTP

Tietokoneen kello ei usein pysty vaadittaviin tarkkuuksiin. NTP (Network Time Protocol) avulla kellot pysyvät aina ajassa, jos se nähdään tarpeelliseksi. Internetin kautta NTP tarjoaa suuren tarkkuuden aina millisekunteihin asti, mutta tavallinen tietokoneen käyttäjä ei tarvitse näin suuria tarkkuuksia (Katso kuvio 4.). (Lehtinen, M. 2007)

NTP-palvelimet ylläpitävät kellonaikaa, ja jakavat sitä muille tietokoneille. Työasemassa on ohjelma, joka kysyy kellonajan tällaiselta palvelimelta. Yleensä kellonaika tarkastetaan useammalta luotettavalta palvelimelta, joiden ajoista lasketaan keskiarvo, jolloin päästään melko suuriin tarkkuuksiin. (Katso kuvio 4.) (Lehtinen, M. 2007)

0	7	15	23	31	
LI (2)	VN (3)	Mode (3)	Stratum (8)	Poll (8)	Precision (8)
Root Delay (32)					
Root Dispersion (32)					
Reference Identifier (32)					
Reference Timestamp (64)					
Original Timestamp (64)					
Receive Timestamp (64)					
Transmit Timestamp (64)					
Optional Authenticator (96 or more)					

Kuvio 4. NTP viestirakenne

Kriittisiä alueita joissa tarvitaan tarkkaa aikaa ovat:

- Pankkipalvelut
- Pörssi
- Radio ja tv
- Verkkojen ylläpito
- Verkonvalvonta
- Kulunvalvonta

(Lehtinen, M. 2007)

3.10.1 Toimintamalli

Arvojärjestys protokolla. Palvelimet on jaettu tasonumeron perusteella. Palvelimet on jaettu loogisesti puumaiseen järjestykseen. Primääriset palvelimet ovat tasolla yksi ja seuraavat palvelimet arvojärjestyksessä tasolla kaksi jne. Mitä isompi arvojärjestysnumero on, sitä kauempana palvelin on aikalähteestä. Mitä pienempi palvelimen numero on sitä tarkempi sen ajan pitäisi olla. (Lehtinen, M. 2007)

Alempien tasojen palvelimet tarkistavat aikansa ja synkronoivat kellonsa pienemmän arvojärjestysnumeron palvelimilta. Saman tason tarkistusta voidaan käyttää vain hätätapauksissa ja tarkastus tapauksissa. (Lehtinen, M. 2007)

3.10.2 Toiminta

- Palvelimet kuuntelevat UDP-porttia 123
- Ajan tarkistus tapahtuu paketinvaihdolla, pyyntö-vastaus.
- Client lähettää ajan tarkastus kyselyn ja lisää kyseiseen pakettiin oman leimansa.
- Palvelin, johon paketti laitetaan lisää siihen leiman, jolloin se vastaanotti kyseisen paketin ja toisen ajan, jolloin kyseinen paketti lähti takaisin alkuperäiselle clientille.
- Client laittaa vielä muistiinsa kyseisen paketin saapumisajan.
- Client laskee vielä edellä mainitun kierros ajan ja lisää tämänkin muistiinsa.
- Client säätää kelloansa näiden tietojen perusteella.
- Uusi palvelin ei heti kelpaa viralliseksi aikapalvelimeksi.

- NTP virittää palvelimen kelloa hiljalleen.
- Muutaman synkronoinnin jälkeen päästään jo parempiin tuloksiin. (Lehtinen, M. 2007)

3.11 DNSSEC

Domain Name System Security Extensions (DNSSEC) ei ole monimutkaisesta nimessään huolimatta kovinkaan vaikea tekniikka. Syvemmällä tekniikkassa tutuksi tulevat mm. salausalgoritmit, luottamusketjut sekä avainten päivittäminen. Suurelle osalle DNSSECin kanssa työskenteleville riittää tieto, että se on julkisen ja yksityisen parin allekirjoitustekniikka. (Viestintävirasto 2014 B.)

DNSSEC määritettiin jo 1990-luvulla, mutta tekniikka otettiin käyttöön pääosin Internetin nimipalveluissa vasta vuosina 2010-11. Samaan aikaan DNSSEC-tuki otettiin käyttöön myös fi-tunnuksilla. (Viestintävirasto 2014 B.)

DNSSEC on yleistynyt Euroopassa hiljalleen ja suuntaa antavia ovat Tsekki ja Hollanti. Hollannin .NL suojaatua tunnuksia on absoluuttisesti eniten. (Viestintävirasto. 2014)

Suomessa käyttö on suhteellisen vähäistä. 2015 on 0,06 prosentilla on ollut DNSSEC käytössä. Vaikka tekniikan kiistattomista hyödyistä on selkeää näyttöä niin 2015 vain kaksi pankkia ja yksi verkkokauppa ovat suojaaneet asiakkaidensa asioinnin DNSSECillä. (Viestintävirasto 2014 B.)

DNSSECin vähäiseen käyttöön Suomessa ei varmasti ole mitään yhtä syytä. Tsekeissä ja Hollanissa julkisen hallinnon on velvoitettu käyttämään DNSSECin tuomaa lisäturvaa omissa palveluissaan, mutta myös julkinen sektori on lähtenyt joukolla mukaan. (Viestintävirasto 2014 B.)

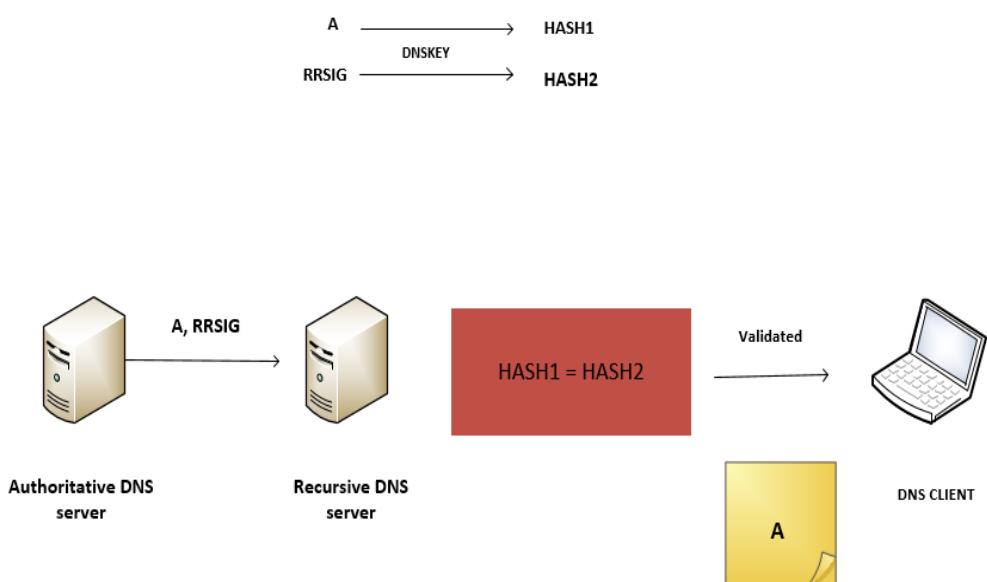
3.11.1 Toiminta

DNSSEC:n perustuu digitaalisien allekirjoituksien käyttöön ja niiden avulla luotuun luottamusketjuun. Protokolla mahdollistaa viestien alkuperän selvittämisen. Tämä vaatii sitä, että DNSSEC on käytössä juuripalvelimelta aina toimialueen nimipalveli-

melle asti. Nimikysely toimii samalla tavalla kuin DNS:iä käytettäessä, mutta nimipalvelin varmistaa vastauksen oikeellisuuden. Vastauksena saadaan resurssitietue, joka pitää sisällään mm. haetun IP-osoitteen tai nimipalvelimen osoitteen. DNSSEC lisää tuohon kaksi kenttää: RRSIG ja DNSKEY. (Orpana, P. 2014)

Allekirjoituksessa käytetään julkista avainta. RRSIG on digitaalinen allekirjoitus, jonka lähettilä on laskenut resurssitietueesta yksityisellä avaimellaan. (Orpana, P. 2014)

Lähettilä lisää julkisen avaimen mukaan viestiin ja laittaa sen DNSKEY-kenttään. Vastaanottaja pystyy tarkistamaan, että viesti on peräisen alkuperäiseltä lähettiläältä käyttämällä julkista avainta ja allekirjoitusta. Julkisen avaimen on oltava luotettava. Tarvitaan siis vähintään yksi julkinen avain, jonka luotettavuus on pystytty tarkistamaan eli puhutaan luottamusankkurista (trust anchor). Tämä on yleensä asetettu manuaalisesti nimipalvelimeen adminin toimesta ja juuripalvelimet toimivat luottamusankureina. Näin kun tiedämme varmasti hierarkian ylimmän nimipalvelimen julkisen avaimen, voimme luottamusketjun ansiosta olla varmoja siitä jokaisen nimikyselyn eri vaiheet ovat oikeita (kts. Kuvio 5). (Orpana, P. 2014)



Kuvio 5. DNSSEC toiminta

3.12 Salasanakäytänteet

Salasana ja käyttäjätunnusia käytetään nykyään opiskellessa, vapaa-ajalla ja työelämässä. Näiden tietoturvallinen käyttö on entistä tärkeämpää. Prosessointi tehon noustessa on myöskin tietoturvariskit nousseet ja salasanoja on entistä helpompi murtaa. Salasanojen tekemiseenkin on suosituksia ja eri laatuja. Pelkkä käyttäjätunnus ja salasana tunnistautuminen luokitellaan heikoksi. Saadaksemme vahvemman tunnistautumis metodin, tarvitaan vähintään kaksi tunnistamistapaa. Tunnistamista poja ovat esimerkiksi oma tieto (salasana käyttäjä tunnus), hallussa oleva tieto (sirukortit, PIN-koodit tai omalle laitteelle lähetetyt varmenteet) tai biometrinen tunnistaminen. (Viestintävirasto 2014 A.)

Hyvä salasana on nykyään minimissään 15 merkkiä ja ei ole löydettävissä sanakirjasta. Tämän ohi ei kuitenkaan pääse tekemällä simppeleitä numero lisäyksiä, kuten Kissa salasanan voi arvata helposti, vaikka se olisikin tehty K1ssa123 formaattiin. Salasanan keksimisen voi tehdä, vaikka nappaamalla lauseen kaikista sanoista etukirjaimet. Numeroiden ja erikoismerkkien lisääminen salasanaan on myöskin suotavaa. Geometriset kuviot näppäimistöltä ovat myöskin riskialttiita. (Viestintävirasto 2014 A.)

Hyvä salasanaan kannattaa muistaa seuraavat viisi asiaa.

- Tarpeeksi pitkä
- Ei ole sana
- Numerot, kirjainten koko ja erikoismerkit käyttöön
- Apuohjelmia löytyy
- Yleiset sanat, henkilökohtaiset tiedot ja näppäimistön geometriset kuvioita ei suositella (Viestintävirasto 2014 A.)

3.12.1 Tiivisteet

Palveluntarjoajalle on suositeltavaa säilöä salasanat tiivistefunktion avulla. Huolella säilönnällä vähennetään tietoturva riskejä, mikäli salasanat joutuisivat väriin käsiin. Käyttäjän syöttäessä salasanansa järjestelmä saa saman tiivisteen, kuin järjestelmässä on, joten järjestelmän ei tarvitse edes tietää käyttäjien salasanoja ainoastaan tiivisteet. Viestintävirasto suosittelee, että näiden tiivisteiden luontiin ei käytetä

standardoitua kryptografista tiivistefunktiota, kuten Secure Hash Algorithm 2 (SHA-2), vaan käytetään salasanatiivistealgoritmia, kuten PBKDF2, bcrypt ja scrypt. (Viestintävirasto 2014 A.)

3.12.2 Suolaus

Suolauksella parannetaan salasanatiivistealgoritmien turvallisuutta entisestään. Suolauksella tehdään satunnaisesti muodostettu uniikki merkkijono, joka on käyttäjäkohtainen. Tätä käytetään yhtenä algoritmin parametrina salasanan lisäksi. Mikäli suola muuttuu, niin muuttuu myösken salasanatiiviste, vaikka salasana ei muuttuisikaan. Tällä saadaan tiivisteisiin lisää turvallisuutta ja vaikka muutama salasana saataisiinkin murrettua, niin se ei auta muiden salasanatiivisteiden murtamiseen. (Viestintävirasto 2014 A.)

3.13 Levyjakojen teoriaa

Levyjaoilla määritellään minne käyttäjät varastoivat tiedostonsa, kuka pääsee niihin käsiksi ja miten niihin pääsee käsiksi. Tämän tarkoituksena on tuoda verkkoon omaisuuksia, kuten tiedostojen jakoa, helpompaa varmuuskopointia, pääsyn hallintaan tiedostoihin, jakojen määärän vähennyksiä verkossa, eikä tarvitse jakaa pääsyä työase-malle, myösken voidaan silmällä pitää käyttäjien tilan käyttöä tai rajoittaa sitä ja rajoittaa käyttäjien oikeuksia. (Jäntti, H & Viilos, M. 2016)

Shared permissionin oikeuksia voidaan ainoastaan antaa kansiolle, kun taas toisaalta New Technology File System (NTFS) oikeuksia voi antaa myösken tiedostolle. Share permissions käytetään yleensä hallinnoimaan vanhempia tietojärjestelmiä kuten File Allocation Table 32 (FAT32) tai muita tietokoneita mitkä eivät käytä NTFS tiedosto-järjestelmää. Muutokset Share permissionissa eivät vaikuta NTFS oikeuksiin ja päinvastoin. Jaetun kansion lopulliset oikeudet muodostuvat molempien Shared permissionista ja NTFS määrittelyistä. Tiukemmat säännöt tulevat aina voimaan olivat ne kummasta tahansa. (Share and NTFS Permissions on a File Server 2016.)

Access Control List (ACL) on lista missä säilytetään oikeuksia. ACL kerätään yksilöllisiä oikeuksia, joita kutsutaan Access Control Entries (ACEs). Jokainen ACE kostuu turvallisuus oikeuksista, joita on annettu käyttäjille, ryhmille tai tietokoneille ja kaikista täsmennetyistä oikeuksista mitä on turvallisuus ryhmälle annettu. (Jäntti, H & Viilos, M. 2016)

Kun puhutaan periytymisestä, sillä tarkoitetaan sitä että, kansiot tai tiedostot saavat samat oikeudet mitä ylemmällä kansiossa annettiin. Tämä voidaan ylajaa antamalla Explicit permissionit oikeus tai estämällä periytyvyys inheritance blockin avulla. (Jäntti, H & Viilos, M. 2016)

NTFS on windowsin päätöimininen tiedosto järjestelmä, joka sai alkunsa Windows NT:stä. NTFS tarvitaan toteuttamaan monia turvallisuus ja hallinta ominaisuuksia. NTFS tukee Active Directory domain nimiä ja tiedostojen encryptausta. NTFS myöskin mahdollistaa kuinka paljon levytilaa käyttäjällä on. FAT32 verrattuna se pystyy myöskin parempaan palautumaan levy vioista. (Jäntti, H & Viilos, M. 2016)

3.13.1 NTFS oikeudet

NTFS voidaan antaa määritellä 6 erillistä oikeutta kansioille ja tiedostoiille. Full Control (FC) annettaan kaikki oikeudet tiedostoon tai kansioon. Modify on käytännössä Full Control, josta on poistettu mahdollisuus poistaa alikansioita ja tiedostoja, muuttaa oikeuksia tai ottaa tiedostojen omistusta itsellesi. Read & Execute (R&E) ja List Folder Contents (LFC) jakavat käytännössä samat oikeudet, eli ne pystyvät ajamaan tiedostoja/kansioita, lukemaan tietoja, lukemaan tiedostojen/kansioiden normaleja/ylimääriä ominaisuuksia ja synkronisoida. Eroavaisuudet edellä mainittujen oikeuksien kanssa tulevat periytyvyydessä. LFC periytyvyys tulee ainoastaan kansiolle ja R&E periytyys tulee tiedostoiille ja kansiolle. Read (R) antaa oikeudet lukea tiedostoja/kansioita, niiden ominaisuuksia ja synkronisoida. Write (W) antaa oikeudet luoda tiedostoja/kirjoittaa tietoa, tehdä kansioita/lisätä tietoa, kirjoittaa ominaisuuksia, luku oikeuden ja synkronisoinnin. (Jäntti, H & Viilos, M. 2016)

3.14 Kerberos

Kyseessä on todennusprotokolla, joka perustuu luotettuun kolmanteen osapuoleen. Tämä tarkoittaa, että todennus toimii Kerberos-palvelimen välityksellä. Tietokoneet ja palvelimet luottavat Kerberos-palvelimeen heidän keskinäisessä kanssakäymisesään, joten kaikki todennuspyynnöt kulkevat sen välityksellä. (Garman 2003,6.)

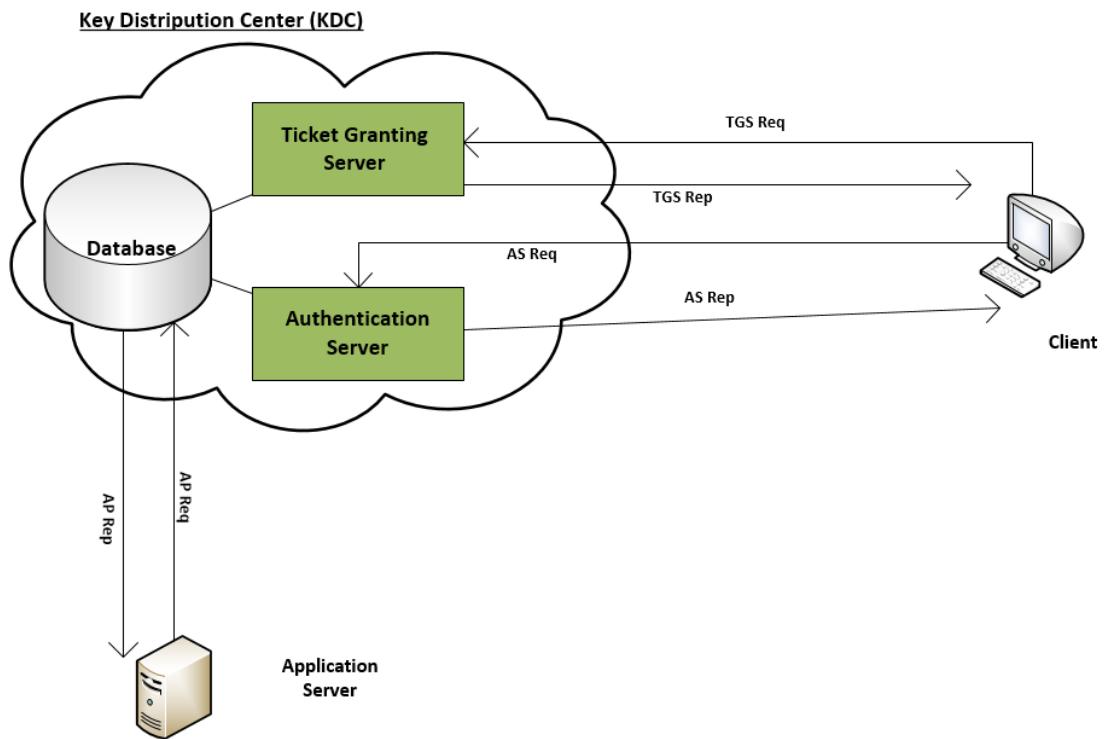
Kerberos toimii TCP/IP-verkon vartijana päästään vain ressusseihin, joita se itse valvoo. Toiminnan periaatteisiin sisältyy kertakirjautuminen (single sign-on). Tämä tarkoittaa sitä, että tarvitsee vain kirjautua kertaalleen sisään niin voi käyttää Kerberoksen valvonnassa olevia resursseja.

Käynnistyksessä tapahtuneen käyttäjän varmistamisen jälkeen Kerberos todentaa sen vielä muille käyttäjille lippu (flag) viesteillä kirjautumisen aikana. Viestinsä salaumisessa Kerberos käyttää symmetristä salausta. Aluksi käytetty salausalgoritmi oli 56-bittinen DES, mutta nyt luotettavammat algoritmit ovat käytössä. Käyttäjän todennus perustuu käyttäjä- ja palvelukohtaisiin salaisiin avaimiin. Kerberoksella on tiedossa kaikkien eri osapuolien avaimet, joiden kautta nämä voivat varmistaa toistensa henkilöllisyyden. (Schneier 1996, 566; Garman 2003, 6.)

Kerberos rakentaa todennusvaiheessa sanomia jotka ovat salattua todennusta pyytävän osapuolen avaimella tehtyjä eikä niitä voi avata kuin se henkilö joille tämä sanoma on tarkoitettu. Tämä taas tarkoittaa, että salasanaa ei tarvitse lähettää verkon ylitse. Todennus tapahtuu vastaanottajan koneella purkamalla Kerberoksen salaus ja vastaamalla kyseiseen sanomaan. Jos halutaan enemmän varsinaista kommunikointia niin Kerberos muodostaa sitä varten molemmille osapuolille istuntokohtaisen avaimen, joilla kyseinen liikenne salataan. Istuntoavain (session key) on ainoastaan kyseistä istuntoa varten ja se tuhotaan, kun istunto päättyy. (Schneier 1996, 566.)

Yleisesti todentamisprosessi menee näin: käyttäjä (principal) kertoo itsestään ja toteaa todennuspalvelulle, että haluaa asioida lippupalvelussa ja vastaanottaa siltä myös lipun (Ticket Granting Ticket). Käyttäjä näyttää lippunsa lippupalvelulle ja vaatii pääsyä ressusseihin. Jos käyttäjällä on oikeus toimia pyytämässään resurssissa, niin kaikki on niin kuin pitää ja lippupalvelu myöntää käyttäjälle palvelulipun (Server

Ticket). Käyttäjä tunnistaa itsensä palvelulipulla sisään palvelimelle ja pystyy näin käyttämään haluamaansa resurssia. Kts. Kuvio 6. (Schneier 1996, 567.)



Kuvio 6. Kerberoksen toiminta

Kerberos on teoriassa erittäin varma tapa todentaa käyttäjiä, mutta koska teoria ja käytäntö ovat eri asioita niin on hyvä tietää muutamista asioista. Vaikka Kerberosta on kehitetty kauan niin se ei silti ole täydellinen, mutta koska ohjelmakoodi on avoin niin ongelmat ovat olleet helposti paikannettavissa. Kerberos on pelkästään todennuspalvelu, eikä se siten voi estää esim. heikkoja salasanoja, virheellisiä palvelinohjelmistoja tai ihmillisillä virheitä. (Garman 2003, 100.)

Alun perin Kerberoksen neljäs versio antoi lippuja kaikille, jotka niitää kysyivät. Todennus siis tapahtuu purkamalla salausta tästä lipusta oikealla avaimeilla, tämä taas tarkoittaa sitä, että koko järjestelmän toiminta on riippuvainen tästä. Mahdollinen hyökkääjä voi pyytää KDC-palvelimelta lippua toisen käyttäjänimellä. Vaikka ilman salasanaa ei ole mahdollista purkaa salausta, mutta siihen voi käyttää sanakirjahökkääystä.

Siinä syötetään yleisesti käytettyjä salasanoja murto-ohjelmaan, joka alkaa arvailemaan. Yksi mahdollisuus on käyttää bruteforce attackia salasanoille, joka alkaa arvalla kaikkia merkkiyhdistelmiä hyväksi käyttäen. (Garman 2003, 104.)

3.15 Authentication, Authorization and Accounting

Authentication, Authorization and Accounting (AAA) on termi, jota käytetään, kun halutaan viisaasti hallinnoida pääsyä tietokoneiden resursseihin, käytäntöjen toimenpanoa, käytön auditointiin ja tarpeellisen informaation saamiseksi, jotta voidaan laskuttaa palveluista. Näitä prosesseja pidetään tärkeinä tehokkaan verkon hallinnoinnin ja turvallisuuden kannalta. (Rouse, M. 2010)

Authenticationilla tunnistetaan käyttäjä, tyyppillisesti käyttäjän syöttämällä käyttäjä-nimi ja salasana, ennen kuin käyttäjälle annetaan päästyjärjestelmään. Tämä prosessi nojaa siihen, että jokaisella käyttäjällä on uniikit tunnukset. AAA serveri vertaa käyttäjän tunnuksia muiden käyttäjien tunnuksiin tietokannassa. Tunnusten vastatessa toisiaan käyttäjä pääsee verkkoon. Mikäli tunnukset eivät täsmää, tunnistautuminen epäonnistuu ja pääsy evätään. (Rouse, M. 2010)

Authorizationilla käyttäjälle annetaan oikeudet tehdä ennalta määritellyjä toimia. Siäärkirjautumisen jälkeen käyttäjä voi yrittää tehdä erilaisia toimintoja ja authorization prosessilla määritellään, pystykö käyttäjä näin tekemään. Tällä prosessilla laiteitaan käytännöt voimaan ja määritellään minkä tyypissä tai minkä laadun toimintoja, resursseja tai palveluita käyttäjän annetaan tehdä. Yleensä tämä tapahtuu, kun käyttäjä kirjautuu järjestelmään sisään eli authenticationin yhteydessä. Authenticated käyttäjien oikeudet voivat vaihdella pääsyn tai toimintojen suhteenv. (Rouse, M. 2010)

Accountingilla seurataan mitä resursseja käyttäjät kuluttavat, kun ovat yhteydessä järjestelmään. Tämä voi sisältää paljonko aikaa käyttäjä kuluttaa järjestelmässä tai kuinka paljon dataa käyttäjä lähettää ja/tai vastaan ottaa istunnon aikana. Accountingin kerää tietoa istunnon statistiikan kautta ja käyttö informaation kautta. Näitä tietoauthorize oja käytetään oikeuksien kontrollointiin, laskutukseen, trendien analysointiin, resurssien hyötykäyttöön ja kapasiteettien suunnittelun toimintoihin. (Rouse, M. 2010)

AAA palvelut yleensä tuodaan dedikoidulle AAA serverillä, jossa ajetaan ohjelmaa, joka suorittaa nämä palvelut. Nykyinen standardi millä verkkoyhteydenottopalvelimen (network access servers) rajapinnat saavat yhteyden AAA serverille on Remote Authentication Dial-In User Service (RADIUS). (Rouse, M. 2010)

3.15.1 RADIUS

RADIUS on client/server protokolla ja ohjelmisto, joka mahdollistaa etäkäyttöpalvelinten (remote access servers) kommunikoinnin keskeisten servereiden (central servers) kanssa. Tällä saadaan todennettua sisään pääsy käyttäjille ja valtuudet haluttuun järjestelmään tai palveluun. RADIUS antaa yrityksen ylläpitää käyttäjä profiileja keskitetyssä tietokannassa, jota kaikki etäserverit voivat jakaa. Tällä saadaan parempaa turvallisuutta ja myöskin mahdollistaa yrityksen oikeuksien laiton yhden hallinnointi verkkopisteen kautta. Yhden keskitetyn serverin ansiosta on myöskin helpompaa seurata käytöä laskutukselle ja verkon tilastotietojen keräämiseen. RADIUS on de facto standardi, jota käyttää moni verkko palvelu yritys ja jota on suositeltu IETF standardiksi. (Rouse, M. 2007)

3.15.2 VyOS

VyOS on avoimen lähdekoodin verkonhallinnointi ohjelmisto, joka voidaan asentaa fyysisille laitteille tai virtuaalikoneille omaan serveriin tai pilvipalveluun. VyOS perustuu GNU/Linux järjestelmiin ja tuo samanlaisia palveluita, kuten Quagga, ISC DHCPD, OpenVPN ja StrongS/WAN. Tämä kaikki myöskin toteutetaan yhden hallinnointi raja-pinnan kautta. (VyOS)

Toiminnallisesti VyOS:ssa on enemmän perinteisen reitittimen mukainen verrattaessa esimerkiksi OpenWRT tai pfSenseen. Järjestelmässä ollaan keskitetty kattavaan tukeen kehittyneempien reititys toimintojen suhteen, kuten dynaamisen reititys protokollien ja komentorivin suhteen. Järjestelmästä löytyy myösken VPN ja palomuuri toiminnallisuudet. VyOS toimintoja on havainnollistettu taulukossa 1. (VyOS)

Taulukko 1. VyOS toimintoja

VLAN	802.1q ja QinQ
Static ja dynamic reititys	BGP IPv4 ja IPv6, OSPFv2, RIP, RIPng, Politikka pohjaista reittiystä, equal cost multi-path
Palomuuri	IPv6 ja IPv6 palomuuri säännöt. Liikenteen määrittämisen rajapintoihin. Aluekohtaiset palomuurit. Osoite/verkko/portti ryhmät IPv4 palomuureille.
Tunneli rajapinnat	PPPoE, GRE, IPIP, SIT, static L2TPv3, VXLAN
VPN	Site-to-site IPSec palvelut IPv4 ja IPv6 osoitteille. L2TP/IPSec serveri, PPTP serveri, OpenVPN site-to-site ja remote access palvelut
NAT	Source NAT, porttien forwardaus, yksi yhteen, yksi moneen ja moni moneen käänökset.
DHCP	DHCP ja DHCPv6 serverit ja välitys palvelut
Redundanttisuutta	VRRP ja yhteystaulukoiden synkronisointi
Flow accounting	NetFlow ja sFlow
Proxy	Web proxy ja URL filtteröinti
Shaping	QoS politiikat, joihin sisältyy ddrop tail, fair queue ja muut. Liikenteen uudelleenohjaus

3.16 Roaming profiilit

AD ympäristössä käytettävä ominaisuus, jossa käyttäjän profiilitiedot esimerkiksi työpöydän asetukset, tehtäväpalkki, tulostimet, kansioasetukset jne. tallennetaan erilliselle tiedostopalvelimelle, josta profiili ladataan aina käyttäjän kirjautuessa uudestaan verkon tietokoneelle (Roaming User Profiles).

Tämä mahdollistaa työntekijöiden yksilöllisten profiiliiden saatavuuden riippumatta, millä verkon tietokoneella työskennellään. Roaming profiili on tavallaan myös varmuuskopio käyttäjäprofiilista, jolloin ei olla vain yhden paikallisen profiilin varassa, vaan vikatilanteen sattuessa voidaan käyttäjän profiili palauttaa aikaisempaan tilaan.

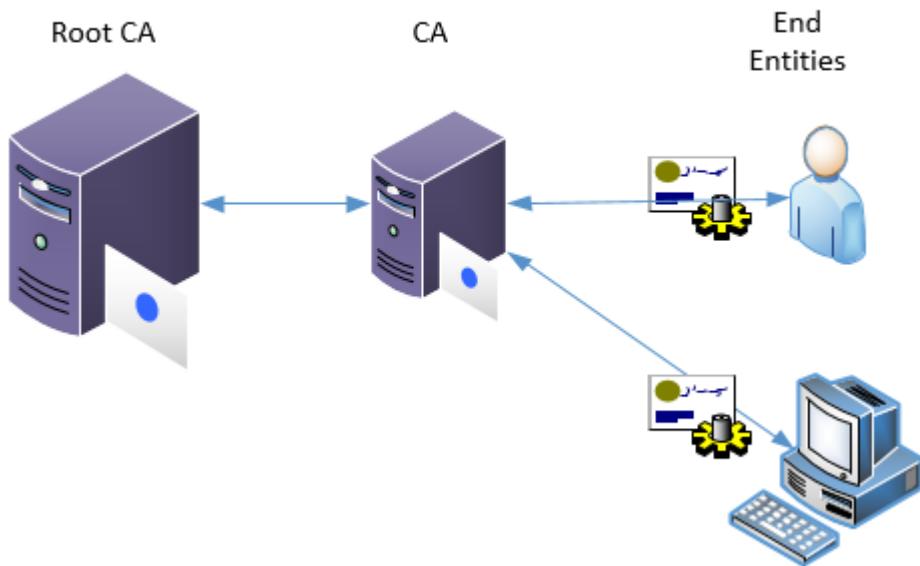
Roaming profiili tuo myös haasteita, jos profiilin koko kasvaa suureksi, jolloin käyttäjien kirjautumisajat kasvavat, kun profiilia haetaan tiedostopalvelimelta.

Tähän ongelmaan on olemassa helpottavana ratkaisuna Folder Redirection, joka uudelleenohjaa käyttäjän data-hakemistoja erilliselle verkkolevylle pois profiilista (Folder Redirection Overview). Näin ollen, vaikka data on uudelleenohjattua, sitä voidaan käyttää kuitenkin paikallisesti millä verkon työasemalla tahansa. Esimerkiksi Roaming profiilin pienennykseen voidaan käyttäjäprofiilista uudelleenohjata Desktop, Appdata tai Documents hakemistot, jotka yleisimmin ovat raskaimmat kansiot.

3.17 Public Key Infrastructure

Public Key Infrastructure eli julkisen avaimen infrastruktuuri on jakelumenetelmä, jossa luotetut tahot todentavat kunkin tiedonsiirtoon osallistuvan entiteetin oikeellisuuden. PKI vastaa käytännössä julkisten avaimien sekä varmenteiden hallinnoinnista toteuttaen puumaista rakennetta. (Karamanian, A. Tenneti, S. Dessart, F. 2010)

PKI rakenne muodostuu puun ylimmästä palvelimesta eli Root Certification Authority:tä (CA) eli palvelimista, jotka käsittelevät vain CA:en sertifikaatteja sekä yksittäisistä CA:sta, jotka käsittelevät ja säilövät digitaalisia sertifikaatteja omassa tietopankisaan, lisäksi CA:n tehtäväնä on varmentaa loppukäyttäjien identiteetti. Alla kuviossa 7 on kuvattu yksinkertainen PKI infrastruktuuri. (Karamanian, A. Tenneti, S. Dessart, F. 2010)



Kuvio 7. PKI infrastruktuuri

Isommissa organisaatioissa puuhun kuuluu myös Subordinate CA:t, joiden rooli PKI puussa on CA:en kanssa sama, mutta ne nähdään ennenminkin lapsi CA:na luoden hierarkkisen rakenteen suuremmissa PKI kokonaisuuksissa. Viimeisenä loppukäyttäjät eli End Entity:t (EE), jotka voivat olla palvelimia, tietokoneita tai vaikkapa ihmisiä, jolle CA on allekirjoittanut sertifikaatin. (Karamanian, A. Tenneti, S. Dessart, F. 2010)

Sertifikaatit, joita CA:t käsittelevät ovat digitaalisia dokumentteja, jotka yleisimmin turvautuvat julkisen avaimen standardiin X.509. Standardi X.509 määrittelee mitä tietoa sertifikaatit sisältävät esimerkiksi kuka on myöntänyt sertifikaatin, julkisen avaimen, digitalisen allekirjoituksen sekä sertifikaatin myötäjän ja voimassaolo ajan. (Karamanian, A. Tenneti, S. Dessart, F. 2010)

Sertifointi prosessi alkaa, kun EE luo oman julkisen ja yksityisen avaimensa. EE lähetää oma julkisen avaimensa sertifointipyyntönä Certificate Signing Request (CSR) CA:lle. CA allekirjoittaa EE:n CSR:n sen omalla salatulla avaimella luoden näin sertifikaatin, lopuksi sertifikaatti lähetetään takaisin EE:lle. (Karamanian, A. Tenneti, S. Dessart, F. 2010)

3.18 NAT

Network Address Translation (NAT) on TCP/IP-verkoissa käytettävissä oleva osoiteenmuunnostekniikka, jonka avulla yhtä julkista IP-osoitetta voi käyttää useampi verkkoa käyttävä laite. Tällöin kaikilla koneilla näkyy sama osoite ulospäin, joka on samalla NAT:sta huolehtivan laitteen IP-osoite. NAT:sta vastaa yleensä reititin, joka huolehtii siitä, että eri verkkolaitteiden välinen verkkoliikenne ohjataan oikeaan osoitteeseen.

Suurin osa NAT-toteutuksista on Port Address Translation (PAT) -mallisia, eli NAT-laitte muuttaa datapaketin käyttämän portin ja IP-osoitteen toiseksi. Tämän vuoksi NAT:sta huolehtivan laitteen on pidettävä kirjaan käytetyistä porteista, jotta yksi portti on käytössä vain yhdellä verkon koneella kerrallaan.

NAT:in avulla saavutetaan tavallista parempi tietoturva julkisessa verkossa, sillä sen avulla NAT:in takana oleviin laitteisiin ei saada suoraan yhteyttä, ellei sitä ole erikseen sallittu tai pyydetty. Tästä tulee myös NAT:in suuri ongelma, eli palvelimien pitäminen ei onnistu suoraa NAT:in kanssa, koska ulkopuoliset tahot eivät voi ottaa oletuksena yhteyksiä NAT:in takana oleviin laitteisiin. Tämän vaikuttaa mm. monien P2P-ohjelmien käyttöön, jolloin se yleensä vaikuttaa tiedonsiirtonopeuksiin hidastaen niitä. Tämän ongelman voi kuitenkin kiertää laittamalla NAT:in asetuksiin porttiohjauksen (Port forwarding), jolloin NAT sallii yhteydet ulkoa päin tiettyyn porttiin ja palvelimen pitäminen onnistuu jälleen normaalisti. NAT siis varaa tietyn portin tiettylle verkkolaitteelle.

NAT:a käytetään tietoturvan lisäksi myös sen takia, että nykyään käytössä oleva IPv4-protokolla tarjoaa vain noin 4 miljardia IP-osoitetta, jotka eivät riitä kaikille verkkolaitteille. Koska NAT:n avulla saa yhden IP-osoitteen taakse useamman verkkolaitteen, voidaan verkkoon liittää useampi laite ilman ylimääräisiä IP-osoitteita. (Afterdawn.com. 2017)

3.19 VPN

VPN:ää (Virtual Private Network) käytäen organisaatiot voivat turvata yksityisen verkkoliikenteen, joka kulkee turvattomien verkkojen kautta, kuten internetin kautta.

VPN auttaa tuomaan turvallisuus mekanismin salaukselle ja kapseloinnille yksityiselle verkkoliikenteelle ja sen siirtämiselle välittäjäverkoissa. Tiedot salataan luottamuksellisuuden takia ja paketit jotka voitaisiin kaapata jaetuissa tai julkisissa verkoissa ovat lukukelvottomia ilman oikeata salausavaimia. Tiedot myösken kapseloidaan tai pake-toidaan IP headerin kanssa, joka sisältää reititystiedot. (Technet. 2003)

VPN avulla käyttäjät voivat työskennellä kotona, tien päällä tai sivukontoreissa turvallisesti saaden etäyhteyden internetin välityksellä yrityksen serveriin. Käyttäjän perspektiivistä VPN on pisteestä pisteeseen yhteys käyttäjän tietokoneen ja yrityksen serverin välillä. Välittäjäverkkojen luonteella ei ole väliä käyttäjälle, koska tiedon kulku näyttäisi siltä, että tietoja lähetetään oman yksityisen linkin kautta. (Technet. 2003)

Yleisin tapa käyttää VPN yhteyttä on se, kun käyttäjä ottaa etäyhteyden yksityiseen verkoon internetin välityksellä käyttäen etäyhteys (remote access) VPN:ää. Toisessa tapauksessa sivukonttorin yhteys pääkonttoriin tehdään käyttäen jatkuva tai tarpeen vaatiessa site-to-site VPN yhteyttä. (Technet. 2003)

Käyttäjän ottaessa yhteyden käyttäen etäyhteys VPN:ää yhteys luodaan etäyhteys ohjelmalla käyttäjän päästä. Etäyhteys asiakas on käytännössä yksi tietokonene käyttäjä, joka yhdistää yksityiseen verkoon etäisestä paikasta. VPN-serveri tuo yhteydelisyyden verkon resursseihin, johon VPN-serveri on yhdistetty. Asiakkaan VPN ohjelma tunnistaa itsensä VPN-serverille ja, jotta saadaan molemminpuolinen tunnitus, VPN-serveri tunnistaa itsensä asiakasohjelmistolle. (Technet. 2003)

3.20 SSL VPN

SSL VPN:ää (Secure Sockets Layer Virtual Private Network) voidaan käyttää tavallisella Web-selaimella. Sitä käytetään antamaan etäkäyttäjälle pääsyn Web-sovellukseen, client/server-sovelluksiin ja sisäisen verkon yhteyksiin. VPN tarjoaa turvallisen viestinnän mekanismin tietojen lähettämiseen kahden päätepisteen välillä. SSL VPN koostuu yhdestä tai useammasta VPN-laitteesta, joihin käyttäjä yhdistää web-selaimella. Liikenne Web-selaimen ja SSL VPN laitteen välillä salataan. (Rousse, M. 2009)

SSL VPN tarjoaa monipuolisuitta ja helppokäyttöisyyttä. On olemassa kaksi erilaista SSL VPN-verkkoa:

- SSL Portal VPN: Tämän tyypin SSL VPN mahdollistaa yksittäisen SSL-yhteyden Web-sivustoon, joten loppukäyttäjä voi turvallisesti käyttää useita verkkopalveluita. Sivusto on nimeltään portaali, koska se on yksi ovi, joka johtaa moniin muihin resursseihin. Etäkäyttäjä käyttää Web-selainta, jotta pääsee SSL VPN-yhdyskäytävään, että voi tunnistautua ja tämän jälkeen pääsee käyttämään eri palveluita. (Rousse, M. 2009)
- SSL Tunnel VPN: Tämän tyypin SSL VPN mahdollistaa Web-selaimen turvallisen pääsyn eri palveluihin mukaan lukien sovellukset ja protokollat, jotka eivät ole Web-pohjaisia. SSL Tunnel VPN edellyttää että Web-selain pystyy käsittelemään aktiivista sisältöä, jonka avulla voidaan tarjota toimintoja, joilla ei ole sisäänkäyntiä SSL Portal VPN:ään. Esimerkkejä aktiivisista sisällöistä ovat Java, JavaScript, ActiveX, Flash-sovellukset tai erilaiset laajennukset. (Rousse, M. 2009)

3.21 IPSec

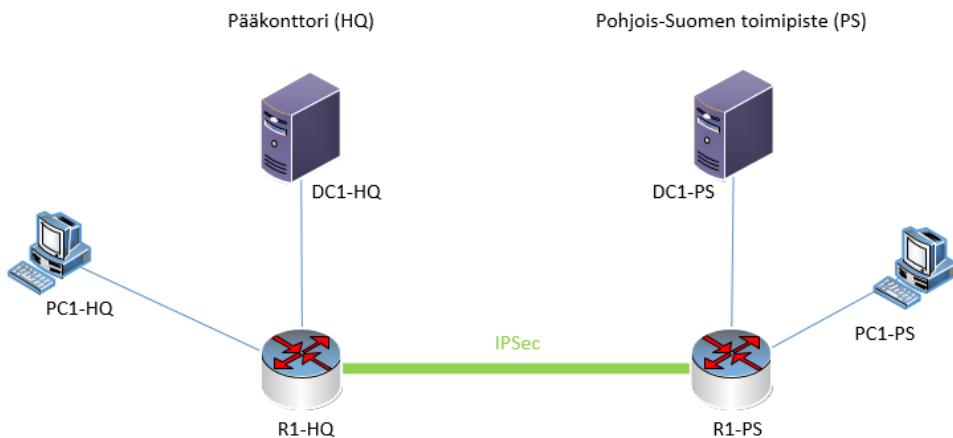
IP Security Architecture (IPSec) on protokolla, jonka avulla kaksi verkkolaitetta pystyvät luomaan salatun yhteyden internetin yli. IPSec todentaa yhteyden molemmat osapuolet ja salaa kaikki IP-paketit istunnon aikana. Istunto alkaa molempien osapuolten todentamisella ja salausavaimen neuvottelusta. IPSec yhteys voidaan luoda kahden loppukäyttäjän, kahden reitittimen tai tietyn verkon ja loppukäyttäjän välille.

IPSec sisältää verkkotason todennuksen, tiedon alkuperän todennuksen, tiedon eheyden, tiedon luottamuksellisuuden (salausen) ja uudelleenlähetyksen suojaus.

IPSec toimii OSI-mallin verkkokerroksella. Muut laajasti käytössä olevat salausjärjestelmät mm. Transport Layer Security (TLS) ja Secure Shell (SSH) toimivat yleensä OSI-

mallin ylemmillä kuljetus- ja sovelluskerroksilla. IPsec suojaa siis kaiken liikenteen jota kuljetetaan IP-verkon yli. (Mason, A. 2002)

IPSec toiminta voidaan pilkkoa viiteen eri vaiheeseen, jotka ovat esitetty kuviossa 8.



1. PC1-PS kysyy DC1-HQ:lla sijaitsevaa käyttäjäprofillia. Osapuolet aloittavat IKE-prosessin
2. Internet Key Exchange (IKE) ensimmäinen vaihe:
- IKE todentaa molemmat osapuolet ja neuvottelee IKE Secure Association:in (SA)
3. Internet Key Exchange (IKE) toinen vaihe:
- IKE neuvottelee SA parametrit ja asettaa ne yhteyden molemmille osapuolille
4. Tiedonsiirto. Tiedot siirretään IPSec osapuolten välillä
5. IPSec yhteyden katkaisu. Yhteys osapuolten välillä katkaistaan manuaalisesti tai aikakatkaisaan

Kuva 8. IPSec toiminta

3.22 MFA

Yksi suurimmista ongelmista perinteisen käyttäjätunnuksen ja salasanan kirjautumisessa on tarve säilyttää salasana tietokantoja. Olipa tietokanta salattu tai ei, jos se on kaapattu, se tarjoaa hyökkääjälle lähteen tarkistaa arvauksiaan vain hänen tietokoneensa nopeudella. Riittävästi aikaa niin salasana tietokanta pystytää murtamaan. Koska prosessorien nopeudet ovat kasvaneet niin brute force- hyökkäyksistä on tullut todellinen uhka. Jatkokehitys kuten GPGPU ja rainbow-taulukot ovat tarjonneet hyökkääjille etuja. GPGPU esimerkiksi voi tuottaa yli 500 miljoonaa salasanaa sekunnissa. Riippuen ohjelmistosta rainbow-taulukot voivat murtaa 14-merkkisen aakkosnumeerisen salasanan noin 160 sekunnissa. Nyt tarkoitukseen on rakennettu myös FPGA-kortit, jotka voivat tarjota kymmenkertaisen suorituskyvyn. Tavallisella salasana tietokannalla ei yksinään ole mitään mahdollisuksia tämmöisiä menetelmiä vastaan. (Rouse, M. 2015)

Virukset ja haittaohjelmat yrittävät urkkia käyttäjän salasanoja, mutta suurin huolenaihe on, miten tiedät, että salasana on vaarantunut. Suojauslokista voi osoittaa, kun onnistunut kirjautuminen on tapahtunut. Mutta voitko todella todistaa, kuka oli tämän kirjautumisen takana. Kun laittaa tämän oikeisiin mittasuhteisiin niin salasanat ovat todella uhattuina.

Multifactor authentication (MFA) yhdistää kahta tai useampaa erillistä käyttäjätietoa. Mitä käyttäjä tietää (salasana), mitä käyttäjällä on (pankkikortti) ja mitä käyttäjä on (biometrinen tunnistus). Tavoitteena MFA:lla on luoda kerroksellinen puolustus ja täten vaikeuttaa luvatonta käytöönottoa kuten fyysinen sijainti, tietokone, verkko tai tietokanta. Jos yksikin tekijä vaarantuu tai on rikki, on hyökkääjällä vielä ainakin yksi este ennen onnistunutta tunkeutumista kohteeseen. (Rouse, M. 2015)

Tyypillisiä MFA skenaarioita ovat:

- Kortin lukeminen ja PIN-koodi.
- Kirjautumalla verkkosivulle käyttäjää pyydetään antamaan kertakäyttöinen salasana, minkä sivuston autentikointipalvelin on lähetänyt joko puhelimeen tai sähköpostiin.
- Lataamalla VPN-clientin, jolla on voimassa oleva digitaalinen sertifikaatti ja käyttäjän täytyy kirjautua ensin VPN:ään ennen kuin myönnetään pääsy verkkoon.
- Kortin lukeminen, sormenjäljen skannaus ja vastaus turvakysymykseen.

(Rouse, M. 2015)

3.23 Sähköposti

Tässä kappaleessa käymme läpi sähköpostipalvelimen toiminnan ja miten sähköposti liikkuu käyttäjältä toiselle. Koska toimintaperiaate on helpoin esitellä kuvalla, käymme läpi kuvan avulla, miten sähköposti toimii. Ensin kuitenkin avaamme muutaman perustermin, jota käytämme.

UA, eli Mail User Agency = Keskustelee suoraan käyttäjän kanssa. Käyttäjä voi olla viestin vastaanottaja tai lähettilä. Esimerkinä Gmail ja Outlook, koska näiden kautta käyttäjä tekee kaiken sähköpostiinsa liittyen.

MTA, eli Mail Transfer Agent = MTA:n tehtävä on siirtää asiakkaan lähetämä viesti lähtevältä sähköpostipalvelimelta aina vastaanottajan palvelimelle. Tähän käytetään esimerkiksi postfix- ohjelmaa, josta puhumme myöhemmin lisää.

MDA, eli Mail Delivery Agent = MDA määrittää vastaanottajan kansion palvelimessa, joka otti vastaan viestin.

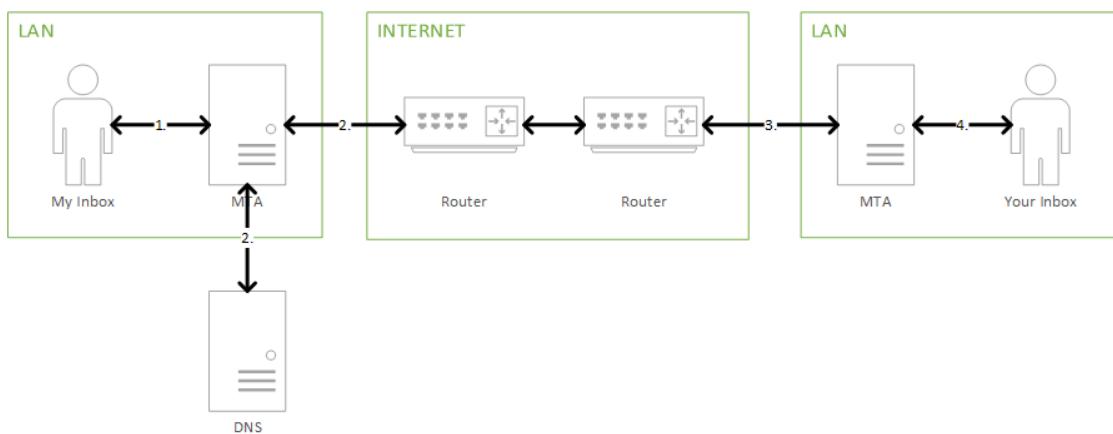
POP/IMAP = Molemmat protokollat siirtävät saapuneen postin käyttäjän MUA:an.

MX, eli Mail Exchanger Record = MX kirjaaa ylös postipalvelimien DNS- tiedot. Rekisteriin on kirjattu ylös arvo, joka tietyllä palvelimella on. Mitä pienempi arvo on kyseessä, sitä korkeampi prioriteetti kyseisellä palvelimella on.

Allaolevassa kuviossa 9 esittelemme sähköpostiviestin liikettä lähettiläiltä vastaanottajalle.

1. Kirjoitan sähköpostiviestin Gmailissani (MUA). Annan lähettiläjn osoitteeksi testi@posti.com ja tämän jälkeen painan lähetä. MUA siirtää lähetettävän viestin sähköpostipalvelimelle.
2. Sähköpostipalvelin kysyy DNS palvelimelta, missä kyseinen posti.com sijaitsee. Kun sähköpostipalvelin on vastaanottanut DNS palvelimelta vastauksen posti.com:in sisäinnista, lähettilä se SMTP protokolla käyttäen kyseisen paketin posti.com palvelimelle.
3. Lähettilä sähköposti saapuu posti.com palvelimelle. MDA päivittää käyttäjän testi saapuneiden sähköpostien listan ja testi saa ilmoituksen, että hänelle on saapunut sähköposti.
4. Testi käyttäjä käyttää POP tai IMAP protokollaa katsoakseen sähköpostinsa.

Näin viesti on kulkenut lähettiläiltä vastaanottajalle. (Xmodulo.com. 2017)



Kuvio 9. Sähköpostin liikenne

3.24 IGP

Interior Gateway Protocol (IGP) on protokolla mitä käytetään jakamaan reititystietoja asiakaslaitteiden ja reittimien välillä. Tämä tehdään autonomisten verkkojen sisällä eli paikallisissa verkoissa. Reititystietoja käyttävät verkkoprotokollat, kuten IP, joiden avulla määritellään, kuinka lähetysteet reititetään. Yleisempä IGP reititys protokollia ovat Routing Information Protocol (RIP) ja Open Shortest Path First (OSPF). (Rouse, M. 2007)

3.24.1 OSPF

Reittimet yhdistävät verkkoja käyttäen IP ja OSPF protokollia. OSPF nimensä mukaisesti etsii parhaan reitin, jota kautta lähettää paketteja yhdistettyjen verkkojen lävitse. OSPF on IETF suunnittelema verkkoprotokolla, jonka tarkoitus on liikennöidä autonomisten järjestelmä verkkojen lävitse, kuin ne olisivat yksi iso verkko, jotka voivat koostua monesta erillisestä Local Area Networkista (LAN), jotka on linkitetty reittimien avulla. (Rouse, M. 2015)

OSPF on suurimmaksi osaksi syrjäytänyt vanhemman RIP protokollan yritysverkossa. Reitin, joka käyttää OSPF protokollaa, oppii muutokset reititystaulussaan tai huomaa muutoksen verkossaan lähettää heti monilähetyksellä tiedot muille OSPF-palvelimille verkossaan, jotta kaikilla on samat reittitiedot tauluissaan. Toisin kuin

RIP, joka tarvitsee reitittimiltä koko reititystaulun jokaiselta naapuriltaan 30 sekunnin ajoin. OSPF lähettää ainoastaan muuttuneet kohdat ja ainoastaan silloin kun muutoksia on tullut. Reittien muuttuessa käytetään uusien reittien löytämiseen kuluvasta ajasta termiä convergence time. (Rouse, M. 2015)

OSPF määrittelee parhaat reittinsä ”link states” avulla, joiden avulla saadaan enemmän tietoja verkosta, kuten reiteille annettuja arvoja, joiden avulla voidaan antaa joillekin reitille isompi arvo, kuin normaalisti olisi. Esimerkiksi voidaan antaa satelliitti yhteydelle isompi arvo kuin langattomalle WAN yhteydelle. OSPF versio 2 on laajasti käytössä enterprise reittimissä. IPv6 uudistus tähän standardiin on tullut uudemman OSPF versio 3 mukana. Vaikka OSPF on tarkoitustsyrjäyttää RIP, on siinä vieläkin RIP tuki, jolla saadaan reitin isäntä kommunikointi toimimaan ja yhteensopivuus vanhempien verkkojen kanssa, jotka käyttävät RIP pääasiallisena protokollanaan. (Rouse, M. 2015)

3.25 BGP

BGP (Border Gateway Protocol) on reititysprotokolla, jota käytetään kaikkialla Internetissä. Tästä syystä se on myös tärkeä protokolla, jonka toimintaa voi olla vaikea ymmärtää. BGP:llä on merkitystä suurten organisaatioiden verkkojen ylläpitäjille, joiden tarvitsee yhdistää useampia ISP (Internet Service Providers) verkkojen. Jos BGP on konfiguroitu väärin se aiheuttaa saatavuus- ja turvallisuusongelmia. Vuonna 2003 tehtiin useita hyökkäyksiä BGP:hen. joissa modifioitu BGP- reitti salli tuntemattomien hyökkääjien suunnata suuria määriä liikennettä niin, että se kulki ensiksi reitittimien kautta, jotka olivat fyysisesti joko Valko-Venäjällä tai Islannissa ja vasta sen jälkeen liikenne lähetettiin määränpäähäänsä. (Schluting, C. 2014)

BGP maailmassa kuka reititys tunnistetaan verkkotunnuksella, jota kutsutaan myös AS (Autonomous System) nimellä. Kun BGP on käytössä niin reitin vetää listan reittejä sinun BGP naapureiltasi. Sen jälkeen tarkastellaan niitä, jotta löydetään lyhin AS-polku. Nämä laitetaan reitittimen reititystaulukkoon. Yleensä reitin käytää lyhyintä AS-polku, mutta ei aina. (Schluting, C. 2014)

Reittipäivitykset tallennetaan RIB:iin (Routing Information Base). Reititystaulukko tulee tallentaa vain yksi reitti per kohde, mutta RIB sisältää yleensä useita polkuja määäränpähän. Reitin päättää minkä reitin se lisää reititystaulukkoon ja mitä se käyttää. Siinä tapauksessa että reitti peruuutetaan, toinen reitti voidaan katsoa suoraan RIB:istä. Muuten RiBiä käytetään reittien seuraamiseen, joita voisi mahdollisesti käyttää. Jos reitin peruuntuminen vastaanotetaan ja se on olemassa vain RIB:issä niin se ainoastaan poistetaan sieltä. Tästä ei lähetetä päivityksiä kenellekään. RIB merkinnät ovat voimassa rajoittamattoman ajan. (Schluting, C. 2014)

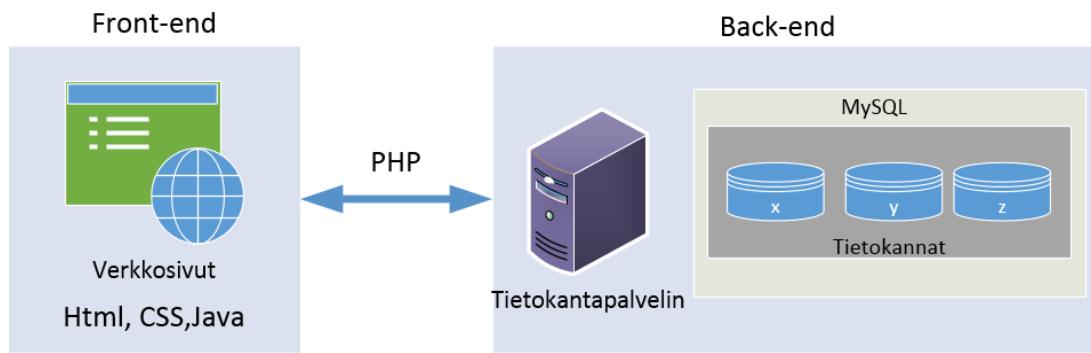
Monissa tapauksissa tulee olemaan useita reittejä tiettyyn kohteeseen. BGP käyttää tästä syystä path-attribuuttia päättämään, miten liikenne reititetään tiettyihin verkkoihin. Origin-attribuutti kertoo alkuperäisen reitityksen tekijän. (Schluting, C. 2014)

3.26 Tietokantapalvelin

Tietokanta on kokoelma informaatiosta, joka on järjestelty niin että sitä käsittelevä tietokone pystyy helposti hakemaan, hallitsemaan sekä päivittämään sen sisältämää dataa. Tiedot sijaitsevat taulukoidussa ympäristössä, joissa yksittäiset solut muodostavat rivejä ja sarakkeita (Webopedia.N.d.). Tietokanta luodaan hallitsemaan jonkin tietyn palvelun tai tarkoitukseen edaksi esimerkiksi se voi käsitteää esimerkiksi väestörekisterin, tuotetietokanta tai tilitiedot. (Jaakkola, T. Sarja, J.2006)

Tietokantapalvelin on kokonaisuus, joka hallitsee ns. Back-endinä eli taustalla olevien resurssien toimivien tietokantojen sisältämää informaatiota jollakin tietokantojen hallintasovelluksella esimerkiksi MySQL:llä, ja näin ollen pystyy tarjoamaan dataa Front-end rajapinnan eli visuaalisesti nähtävissä olevan ohjelman pyytäessä.

Alla olevassa kuviossa 10 on havainnollistettu miten yksinkertaisesti tietokantarajapinnat toimivat yhteen esimerkiksi jonkin verkkosivun pyynnöstä. Käytännössä käyttäjä hakee dataa verkkosivujen hakupalkista, jolloin PHP-ohjelmointikieli, joka yhdistää tietokannat ja Front-end:n mahdollistamalla datan hakemisen. Tietokantapalvelimella sijaitseva MySQL-sovellus tekee SQL (Structured Query Language)-kyselyn ja palauttaa PHP (Hypertext Preprocessor):n avulla datan käyttäjälle.



Kuvio 10. Tietokantarajapintojen toiminta

3.27 Lightweight Directory Access Protocol

Lightweight Directory Access Protocol (LDAP) on internet protokolla, jota sähköposti ja muut ohjelmat käyttävät informaation etsimiseen servereiltä. LDAP on käytössä keskikoisista isoihin yrityksiin asti ja sitä käytetään yhteystietojen tapaisen tiedon etsimiseen. Sähköpostipalveluissa sillä pystytään löytämään vastaanottajan tiedot, vaikka ei oltaisi kyseiseltä henkilöltä ennen sähköpostia vastaanotettu. (What is LDAP?. n.d.) Parhaiten tätä voi havainnollistaa meille tutulla Jyväskylän ammattikorkeakoulun (JAMK) sähköpostipalvelulla, joka pystyy löytämään yhteystiedot pelkän sukunimen tai etunimen perustella, vaikka kyseisen henkilön kanssa ei oltaisikaan ai-kaisemmin oltu yhteydessä.

LDAP serverit indeksoivat kaiken syötetyn datan ja filttereiden avulla voidaan valita haluttu informaatio, kuten ryhmät tai henkilöt. LDAP ei ole rajoittunut pelkästään yhteysinformaation etsimiseen tai edes ihmisiin kohdistuvan informaation etsimiseen. LDAP käytetään salattujen sertifikaattien löytämiseen, tulostinten löytämiseen ja muiden verkkopalveluiden löytämiseen. LDAP antaa myöskin pääsyn moneen palveliun yhdellä salasanalla syöttämällä, eli se jakaa sisäänkirjautumisen monen palveliun kanssa. LDAP suositellaan käytettäväksi minkä tahansa hakemisto tapaisen tiedon kanssa, jotka tekevät nopeita hakuja ja harvalleen tapahtuvia päivityksiä. (What is LDAP?. n.d.)

Protokollana LDAP ei määrittele miten ohjelmat toimivat serveri tai asiakas puolella. Se määrittelee millä ”kielellä” asiakas ohjelma keskustelee serverin kanssa ja LDAP tekee saman asian servereiden välisessä kommunikoinnissa. Asiakaspualella ohjelma voi olla esimerkiksi sähköposti ohjelma, tulostimen etsimiseen tehty ohjelma tai osoitteiden säilömiseen tehty ohjelma. Serveri puolella LDAP hoitaa ainoastaan kommunikoinnin tai vaihtoehtoisesti käytetään muita menetelmiä datan vastaanottamiseen/lähettämiseen ja LDAP lisätään perään. (What is LDAP?. n.d.)

LDAP myöskin määrittelee käyttöoikeudet, jotka järjestelmän ylläpitäjä on määritellyt ja halutessa voidaan määritellä datan yksityisyys. LDAP myöskin määrittelee, mitä formaattia ja attribuutteja servereilla oleva data käyttää. (What is LDAP?. n.d.)

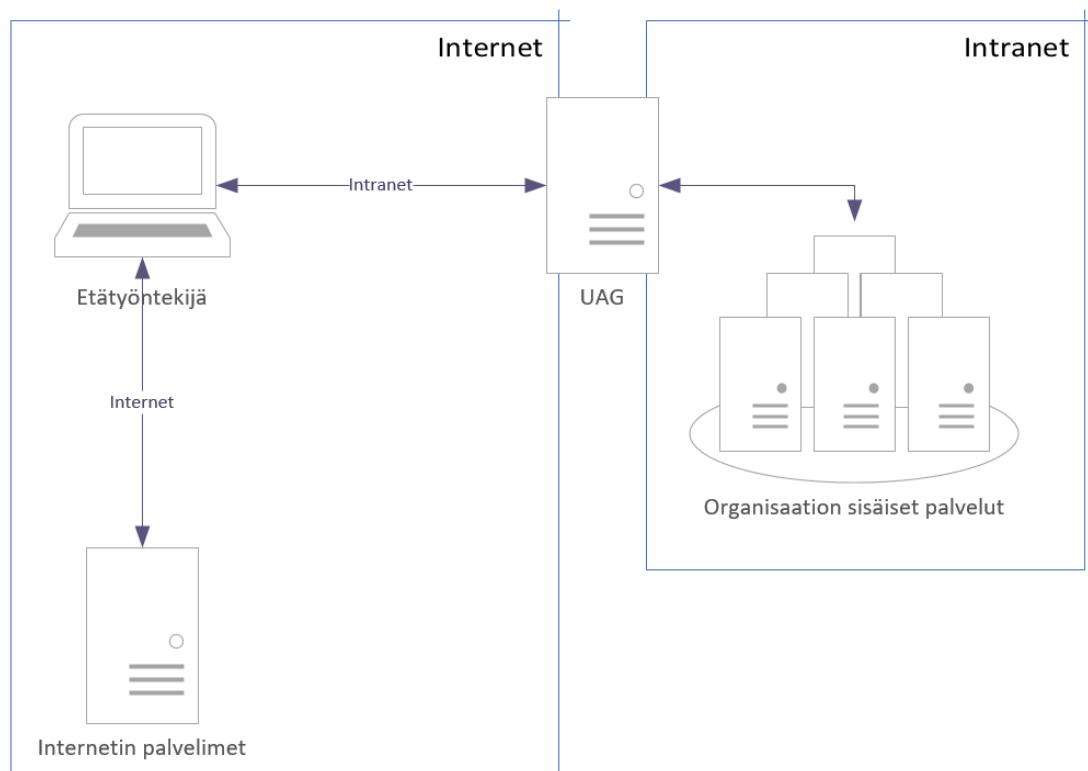
3.28 Intranet

Intra, Intranet ja Internal Network. Kaikilla näillä tarkoitetaan yrityksen tai muun organisaation sisäistä sivustoa. Toisin, kuin Internetsivuilla, tähän sivustoon on pääsy vain henkilökunnalla. Kyseisen organisaation intranet mukautuu yleensä yritysten tarpeiden ja tavoitteiden mukaan ja näitä tarpeita pyritään ratkaisemaan intranetin luomilla mahdollisuksilla parantaa yrityksen sisäistä kommunikointia ja tiedonjakoa. (Steven, L. 1998)

Syy intranetin hankkimiselle voi olla monia syitä. Intranetissä pystytään helposti yhdistämään kaikki organisaation palvelut samaan portaalipiiriin. Tämä helpottaa paljon organisaatiota juuri silloin, jos palveluita on enemmän, kuin 1-2, jolloin erilaisten sivujen ja salasanojen muistaminen ja aktiivinen seuraaminen voi jäädää. Lisäksi intraan pystytään lisäämään helposti erilaisia pieniä yksityiskohtia, jotka parantavat organisaation tuottavuutta. Näitä ovat esimerkiksi foorumi, jossa työntekijät voivat kommentoida ja keskustella organisaation sisäisistä tapahtumista, mutta myös yhteinen kalenteri ja uutisikkuna, josta henkilö näkee kaikki tärkeimmät tapahtumat heti. (Christian, M. 2009)

Intranet pohjaksi löytyy monta hyvää vaihtoehtoa, joista kolme yleisintä ovat Wordpress, Joomla ja Drupal. Työssämme käytämme Wordpress- vaihtoehtoa sen yksinkertaisuuden ja laajan suosion vuoksi. Jos organisaatio haluaa jotain lisää, eikä raha ole ongelma, löytyy vaihtoehtoja enemmän. (Mening, R. 2017)

Alla olevassa kuviossa 11 havainnollistetaan intranetin ja internetin ero. Tässä etätyöntekijä on poissa organisaation tiloista, mutta haluaa silti päästää käsiksi organisaation yhteisiin tiedostoihin. Tämä onnistuu UAG- palvelimen kautta, johonka yhdistetään päästäään kirjautumisen jälkeen käsiksi haluttuihin tiedostoihin. Intranet on siis eristyksissä muusta internetistä ja näin tiedostot ovat suoressa. (Technet. 2014.)



Kuvio 11. Etätyöntekijän yhteys intraan

3.29 Palomuuri

Palomuuria tarvitaan julkisesta internetistä tulevilta hyökkäyksiltä suojautumiseen. Palomuurin toiminta perustuu sääntöihin, joilla suodatetaan sisään tulevista yhteyksistä kaikki ylimääräinen pois. Useasti myös ulospäin suuntautuvaa liikennettä suodatetaan. Näin varmistumme siitä, ettei sisäverkon asiakkaat häiriköi muiden ulkoverkkojen asiakkaita. Yrityksissä on hyvin usein käytössä useampi palomuuri. Hyökkääjän päästessä ensimmäisen palomuurin läpi, hänen aiketaan ei käytännössä pysty enää estämään tämän jälkeen. Tästä syystä käytetään Demilitarized Zone:a (DMZ), joka sijaitsee julkisen internetin ja yrityksen sisäverkon välissä. Tälle alueelle sijoitetaan julkiset palvelimet, joihin halutaan päästä käsiksi ulkoverkosta. Yleensä palomuurit sijoitetaan DMZ:n molemmille puolille, eli ennen julkisia palvelimia, sekä niiden jälkeen ennen yrityksen sisäverkkoa. Näin pystytään hankaloittamaan hyökkäysten läpääsyä sisäverkkoon.

Palomuurit voivat yksinkertaisimillaan olla pelkkiä pakettisuodattimia, jotka suodattavat lähde- ja kohdeosoitteet sekä liikennöitäävät portit. Pakettisuodattimeen perustuvat palomuurit toimivat verkon kuljetuskerroksella. Tämän tyypisiä palomuureja on kahdenlaisia, tilattomia (stateless) sekä tilallisia (stateful).

Tilaton (stateless): Vertaa jokaista pakettia palomuurin staattisiin sääntöihin. Mikäli paketti ei ole sallittu, sitä ei välitetä eteenpäin. Tilattoman palomuurin ongelmana on, ettei kaikkien paluupakettien tarkkoja portteja tiedetä tiettyjen protokollien tapauksissa. Tilattomia palomuureja voivat olla myös Access-listat yritysten reittiämissä.

Tilallinen (stateful): Vertaa liikennettä staattiseen konfiguraatioon, mutta kykenee dynaamisesti antamaan lupia saapuvalle liikenteelle. Pitää kirja muodostetuista Transmission Control Protocol (TCP)- ja User Datagram Protocol (UDP)-yhteyksistä ja sallii näihin olemassa oleviin yhteyksiin kuuluvat paketit. TCP-yhteyksistä tarkistetaan myös ovatko yhteydet sallittuja. Mikäli yhteys on sallittu, se lisätään palomuurin yhteyslistaan ja tähän yhteyteen liittyvät paketit päästetään jatkossa läpi. Myös kaikki hyväksyttyihin yhteyksiin liittyvät Internet Control Message Protocol (ICMP)-sano-

mat päästetään läpi. Yhteyden ollessa käytämättömänä (idle) tietyn ajan, tai yhteyden sulkeuduttua, tiedot poistetaan yhteyslistalta ja paketteja poistettuihin yhteyksiin ei enää sallita.

Sovelluspalomuurit voivat suodattaa liikennettä sen sisällön perusteella. Mikäli paketeista löytyy esimerkiksi tunnettuja turvallisuusaukkoja hyödyntäviä murto-tyrkisiä, ne voidaan estää niiden pääsemättä sisäverkkoon asti. Sovelluspalomuurit toimivat verkon sovelluskerroksella. Nykyisin työasemakohtaisesti yleisimmin käytössä ovat sovellus- ja tilallisen palomuurin yhdistelmät. Näin tiedetään tarkkaan mitkä palvelut ovat työasemalla sallittuja ja mitkä yhteydet kohdistuvat juuri tähän kyseiseen työasemaan.

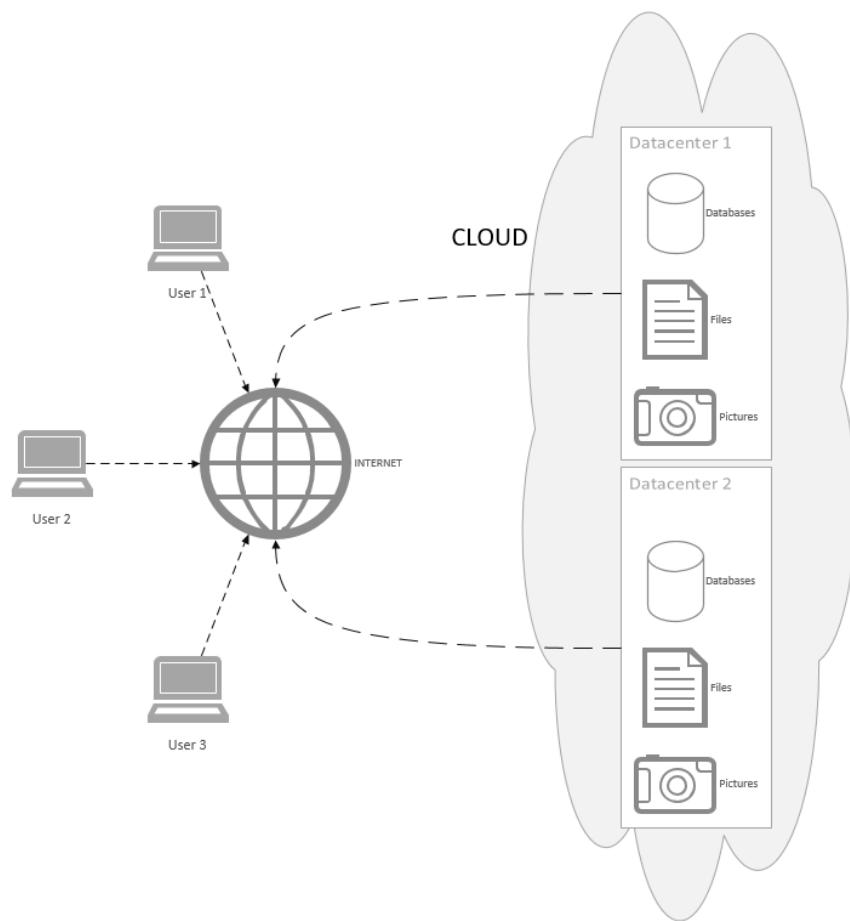
Palomuurauksen tarkoituksena on estää arkaluontoisten päätelitteiden ja sovellusten näkyvyys epäluotetuille käyttäjille. Mahdollisten käyttötörjestelmän vikojen hyväksikäyttö estetään rajaamalla verkon liikennettä. Tarkasti suunnitellut palomuurisäännöt tekevät verkon suojauksesta yksinkertaista ja tarvittaessa skaalautuvaa.

Palomuurien heikkoutena pidettäköön niiden kykyä suodattaa ainoastaan läpikulkevaa liikennettä. Verkkoon voi päästä käsiksi esimerkiksi langattoman lähiverkon tukiaseman, valmiiksi saastuneen työaseman kautta, tai pahimmillaan hyökkääjän päästessä fyysisesti verkkolaitteisiin kiinni. Palomuurit eivät myöskään pysty suodattamaan IPSec-tunnelin kautta kulkeavaa liikennettä, joissa kohdeporttia tai edes kohde-laitetta ei näy selkokielisenä. Tästä syystä VPN-liikenne kuljetetaan yleensä yrityksen DMZ:lle, josta se viedään salaamattomana palomuurin läpi sisäverkkoon. (Tech-faq.com, 2016)

3.30 Pilvipalvelut

Pilvipalvelulla tarkoitetaan palvelua, jota käyttäjä voi käyttää internetin välityksellä. Eriisia pilvipalveluita on monta ja niitä käytetään esimerkiksi tiedostonjakoon ja ison datamäären analysointiin. Pilvipalvelulla halutaan mahdollistaa pääsy dataan asiakkaan sijainnista riippumatta. Daten sijoittaminen on myös redundantista, sillä tiedostot on yleensä sijoitettu moneen eri kohteeseen yhtä aikaa, jolla vähennetään riskiä datan häviämisestä tai tuhoutumisesta. Kuviossa 12 on esitelty pilvipalvelun

paikka internetissä. Daten sijoittaminen pilveen vapauttaa myös resursseja itse käytäjältä. Kun käytetään muualla olevia resursseja, välttyy käyttäjä itse laitteiden hullostaa, rikkoutumisesta ja kalliilta sähkö ja laitekustannuksilta. Suojassa pidettävää tai herkkää dataa kuitenkaan harvoin säilötään pilveen sen helpon saatavuuden takia. Tässäkin täytyy muistaa, että data ei ole "mystisessä pilvessä" vaan pilvi on jonkin muun tietokone. (Webopedia.2014)



Kuvio 12. Käyttäjän ja pilvi

3.31 Monitorointi

Verkon monitorointi on osa verkonhallintaa ja sillä kerätään tietoja verkon toiminnasta. Käytännössä verkonmonitorointityökalut keräävät verkonhallintaohjelmilta hyödyllistä informaatiota monesta eri verkon osa-alueesta. Verkkojen koko ja monimutkaisuus on kasvanut huomattavasti internetin kasvun myötä, joten niiden hallinnoinnista on tullut entistä haastavampaa. Tämän takia kehitettiin verkonmonitorointityökaluja, joiden avulla pystytään toimivasti hallinnoimaan ja ylläpitämään korkean tason verkkoja, vaikka ne olisivatkin hajotettuna etäisiin sijainteihin. (Wong, E. 1997)

Toimenpiteitä mitä verkonvalvonnassa tehdään, on havainnollistettu alla olevassa lisässä.

- Valvotaan verkon tilaa.
- Ennalta määritetyt verkon vaatimukset täyttyvät.
- Suorituskyvyn ja käyttöasteen monitorointi ja määrittelyt.
- Epänormaalien toiminnan huomaaminen.
- Luvattomien muutoksienvaihtoehdot.
- Verkon Sääntöjen valvonta.
- Tuotoksien jäljitys ja laatuvaatimusten varmistus.
- Suorituskyvyn datan huomiointi. (Rantonen, M. 2017)

Monitorointi tavat vaihtelevat paikkakohtaisesti ja oikean tyylin valitseminen on silloin tärkeää. Neljä eri monitorointitapaa ovat Aktiivinen monitorointi, Passiivinen monitorointi, Reaktiivinen monitorointi ja Proaktiivinen monitorointi. (Rantonen, M. 2017)

Aktiivisella monitoroinnilla tarkoitetaan järjestelmän tai laitteiden jatkuvaan monitorointiin, jolla määritellään niiden tilat. Valvontaohjelmistot jatkuvasti pyytävät tietoja laitteilta näiden tilasta ja tämän tavan haittamuodostumisen on resurssien kova kulutus. Aktiivisella tavalla valvotaan kriittisiä laitteita tai järjestelmiä. Diagnostiikassa aktiivinen tapa on myösken yleinen. (Rantonen, M. 2017)

Passiivinen monitorointi on yleisempi menetelmä ja se käyttää tarkkailuagentteja, jotka lähettävät verkonvalvontaohjelmistolle keräämänsä tiedot. Passiivinen tapa tarvitsee hyvin määritellyt kohteet ja arvot, milloin hälytyksiä tehdään. Hälytys arvoista

käytetään sanaa triggers, eli milloin arvot laukaisevat hälytys informaation lähetysten. (Rantonen, M. 2017)

Reaktiivisella monitoroinnilla käynnistetään tietty toiminto, kun tapahtuma tai virhe tapahtuu. Esimerkkinä laiteen suoritusteho saattaa huonontua ja se johtaa laitteen uudelleenkäynnistykseen. Pääosin käytetään virheiden sattuessa, mutta voidaan käyttää myöskin sarjassa ajettavien toimintojen kanssa. Ennakointi ei onnistu tällä menettely tavalla, mutta kun tarvitaan korjaustoimenpiteitä ne tapahtuvat nopeammin. (Rantonen, M. 2017)

Proaktiivisella monitoroinnilla ennakoitaan korjaustoimenpiteitä, kun havaitaan, että joku entuudestaan tuttu tapahtuma on tullut ja järjestelmälle saattaa tulla tämän takia ongelmia. Käytössä kehittyneemmissä ympäristöissä, missä selkeitä trendejä pysyytään vetämään vertailua varten. Tähän menettelytapaan yhdistetään korjaava toimenpide ja ylläpidon ei tarvitse silloin tehdä sitä. (Rantonen, M. 2017)

Mittaamisella organisaation tai palvelun suuntaviivat määritellään. Nämä vaihtelevat paljon organisaation tai palvelun suhteesta. Mittareiden suhteesta on tärkeää määritellä, mitä ja miten mitataan. Tärkeitä toimintoja mittareille ovat selkä tuloksiensa esittäminen, tulosten perusteella tehtävät toimenpiteet ja suunnittelun organisaatio kohdaisesti. Esimerkkinä voidaan esitellä suorituskykymittareita, kuten SQL-serveri vastaan HTTP-serveri. (Rantonen, M. 2017)

Raportoinnilla pyritään saamaan toimintasuunnitelmia, joilla saavutetaan tuloksia. Mikäli raporttien pohjalta ei ryhdytä toimenpiteisiin, niin tämä on hyvä merkki toimimattomasta organisaatiosta. Tärkeitä asioita monitoroinnilla ovat kontrollointi, koska ilman sitä monitorointi on täysin merkityksetöntä ja tehotonta. Selkeä tarkoitus järjestelmän tai palvelun valvomiselle on pakollinen, koska mikäli sitä ei ole, niin järjestelmää ei pitäisi valvoa. (Rantonen, M. 2017)

3.31.1 Zenoss Core

Zenoss Core on avoimenlähdekoodiin pohjautuvat verkon monitorointi järjestelmä, jota pääsee muokkaamaan nettipohjaisen käyttöliittymän kautta. Sen kautta voidaan hallinnoida, monitoroida ja raportoida verkon voimavarojia. Zenos Core tuo verkon hallinnointiin pisteen, jonka kautta voidaan nähdä kaikki reitittimet, serverit ja yleinen ympäristö. (Badger, M. 2008)

Zenos Core on kirjoitettu Python-ohjelmointikielellä. Zenos Core on Linux-pohjainen, mutta sen asentamiseen ja käyttöön ei tarvita Linux administraattoria. Zenos Core on mahdollista asentaa VMware Playerille tai VMware Serverille. Zenos Core kehittyi koko ajan ja sen asentamista Linux-käyttöjärjestelmille helpotetaan koko ajan. Alla olevassa taulukossa 2 on listattu Zenoss Core:n ominaisuudet. (Badger, M. 2008)

Taulukko 2. Zenoss Core:n ominaisuuksia

Serverit, varastointi, verkot ja käyttöjärjestelmä	Kyllä
Yhdistetty monitorointi	Rajatusti
Tapahtumien hallinnointi	Rajatusti
Juurisyidenanalyysi (root cause analysis)	Rajatusti
Avoimenlähdekoodin ZenPackit	Kyllä
Raportointi	Rajatusti
Avoimuus ja lisäomaisuuksien tuki (Open and Extensible)	Rajatusti
Tekninen tuki	Yhteisö tuki
Laitteiden määrä	1,000

3.31.2 OpenNMS

OpenNMS on yritystason, integroitu ja avoimeen lähdekoodiin pohjautuva ohjelmisto, jolla saadaan verkon monitorointi ratkaisuja. Järjestelmä sisältää tuen alan standardi verkonhallinta protokollille, agentteille ja järjestelmän, joka voidaan ohjelmoida palveluille. OpenNMS saa teknistä tukea yhteisön puolelta. OpenNMS käyttää ReST API:a, jota on mahdollista muokata. OpenNMS toimii Zenoss Core:n tavoin VMware alustoilla. (The Platform. N.d.)

OpenNMS sisältää ilmoitusjärjestelmän, jonka avulla voidaan lähetä ilmoituksia, mikäli järjestelmässä tulee ongelmia. Esimerkiksi sähköpostilla, Slackin kautta tai tekemällä omia scriptejä. Tiketöinnin integraatio järjestelmän avulla voidaan ohjelmisto lisätä valmiina olevaan tiketöintijärjestelmään tai tehdä kokonaan uusi, jonka avulla verkonvalvonta saa tietoja itselleen. Hälytysten uudelleenlähetys on keino millä määrin hälytykset voidaan lähetä eri ohjelmistoille. Järjestelmällä voidaan käyttää järjestelmän resursseista mittauksia ja lokitiedostoja verkko laitteilta ja ohjelmistoilta. Käyttöjärjestelmä toimii Java pohjaisesti. (The Platform. N.d.)

3.31.3 Vertailu OpenNMS vs Zenoss Core

Molempien ohjelmistojen tukimahdolisudet vaikuttivat olevan erittäin samanlaiset, joista niistä en suoranaista voittajaa löytänyt. OpenNMS parempia puolia ovat sen yritysmalli, jonka avulla saadaan kaikki palvelut käyttöön eikä mitään ole piilotettu maksuseinän taakse, toisin kuin Zenoss Core:ssa. OpenNMS löytyy myöskin paremat integraatio mahdolisudet, kuten esimerkiksi Request Tracker ja ConcoursSuite. OpenNMS myöskin vaikutti olevan paljon joustavampi tikettijärjestelmä, jossa voit avata, päivittää tai sulkea tikettejä. Hälytysten suhteen OpenNMS vaikutti olevan enemmän joustavuutta, miten ja milloin niitä vastaanotetaan.

Zenoss Core:ssa saadaan perusominaisuudet, mitä verkonvalvontaan tarvitaan ja kaikki hienoudet löytyvät maksullisten versioiden takaa. OpenNMS yritysratkaisut veivät sen voittoon, koska he saavat tulonsa kouluttamalla tai antamalla teknistä tukea, joten heidän ei tarvitse lukita mitään ominaisuuksia maksumuurin taakse.

OpenNMS suurin heikkous on sen raskaus ja tämän takia on suositeltavaa asentaa se omalle serveri koneelle.

3.32 Tikettijärjestelmä

Tikettijärjestelmä yleensä sidotaan ITIL:n (Information Technology Infrastructure Library) elinkaarimallin palveluntuotantoon. Palvelutuotannossa määritellyn palvelupisten tehtäviin kuuluu toimien koordinointi tietyllä yrityksen tasolla asiakkaan kanssa, sekä prosessien täytäntöönpanoon sekä palveluiden tuottaminen tehokkaasti (Nummela, J. 2013).

Tikettijärjestelmät ovat tietokantoja jotka ylläpitävät ja hallitsevat incidenttejä, joita ovat esimerkiksi palvelussa ilmenneet ohjelmistoviat, palvelupyyynnöt, asiakaan lähetämät kyselyt. Incidentti on suunnittelematon palvelunlaadun heikkeneminen tai häiriö IT-palveluissa.

Palvelupisteen tiketointijärjestelmässä on kuvattu jo ennalta tapahtumien polut eli elinkaari incidenttien prosessointikaaviossa mitä jokaisen tapahtuman löytämisestä sen lopetukseen ja mahdolliseen ratkaisuun mahdollisine variaatioineen riippuen incidenttien tyypistä tapahtuu (Bertram, D. 2009).

Tässä toimeksiannossa oli tehtävänpäätä tutkia kolmea eri tiketointijärjestelmää ja valita sopivin vaihtoehto omaan yrityksen verkkoon toimimaan palvelupisteenä asiakkaalle sekä yrityksen sisäiseen tapahtumien hallintaan. Verrattavina järjestelminä oli OSTR, OsTicket sekä yksi vapaa valintainen järjestelmä, joka valikoitui Request Tracker:ksi.

OTRS tukee UNIX- sekä Windows-pohjaisia järjestelmiä vaatien tietokannan sekä web palvelin-ohjelman, kuten taulukosta nähdään. Active Directory sekä OpenLDAP palvelut ovat mahdollisia. Palvelu on tarjolla myös suomen kielellä. OTRS:n verkkosivulta voi ohjelmistoa kokeilla asiakkaan sekä service managerin osalta. (Who uses the Support Desk Software OTRS. N.d)

Asiakkaan näkökulmasta tiketin luonti yksinkertainen toiminto, jonka jälkeen tiketin tilaa pystyy seuraamaan keskitetysti. Service managerin näkökulmasta hallintapanee-liin on koottu tiketit sekä tilastointi luoduista sekä suljetuista tiketeistä. Hallintapaneeli on yksinkertainen ja selkeästi jäsennelty.

OsTicket on helpdesk ohjelma sekä asiakaspalveluun kehitetty ratkaisu pienille ja keskisuurille organisaatioille. Toimii myös Unix ja Windows-pohjaisilla palvelimilla varten Apache tai IIS ratkaisun sekä PHP että MySQL-tietokannan. Mahdollistaa tiketeistä kerätyn datan kustomoimisen, jotta ongelmien ratkaisu nopeutuu. HTML email-tuki sekä tikettien suodatus oikeisiin osastoihin tai henkilökunnalle. (OsTicket Features. N.d)

OsTicket-ohjelmistosta löytyi demo, joka on asiakkaan näkökulmasta yksinkertainen ja ei sisällä turhia hienouksia. Järjestelmänvalvojan kannalta ulkoasu on selkeä ja toimiva. Ohjelma on myös saatavilla suomenkielellä.

Request Tracker on vapaanlähdekodeerin omaava tikettienhallintaohjelma, joka tukee vain Unix-tyyppisiä järjestelmiä. Avainkohdat ohjelmanmassa on tikettien hallinta sähköpostilla tai ohjelman käyttöliittymän kautta. Ohjelma mahdollistaa sähköpostista tulleiden tikettien automatisoidun vastauksen sekä vastauspohjan muokkaamisen. (Key Features and Functionality. N.d

Verkosta löydetyn demon mukaan käyttöliittymä vaikuttaa hieman levinneeltä kaikkeine listoineen ja hakupalkkeineen. Tiketin luonti oli verrattain selkeää, vaikkakin tikettien seuranta ei ehkä ole optimoitu parhaiten.

3.33 IDS vs. IPS

Monissa organisaatiossa yksi vaikeammista tehtävistä on kun täyttyy ymmärtää IDS:ää (Intrusion Detection System) ja IPS:ää (Intelligent Protection System). Täyttyy pystyä ymmärtämään, että kumpaa käytetään, ja milloin tarvitaan mitäkin sen toimintoja. Organisaatio voi myös tutkia voiko se korvata IDS:n IPS:llä tai toisinpäin. (Jabbusch, J. 2009)

Niille jotka eivät ole perehtyneet IDS tekniikkaan, niin se on ohjelmisto tai laite, joka tarkkailee verkon toimintaa. Käytämällä esikonfiguroituja säätöjä IDS voi tarkastaa konfiguraatioiden lopputuloksista, että voivatko ne olla alittiita hyökkäyksille. Se voi tallentaa tapahtumia verkon kautta ja verrata niitä tunnettuihin hyökkäyksiin tai hyökkäyskuviioihin. (Jabbusch, J. 2009)

IPS ei voi vain havaita liikennettä, vaan se voi myös ryhtyä toimiin verkon suojelemiseksi. Voi tuntua, että käyttäjän verkossa ei ole mitään arvokasta, mutta rikolliset voivat käyttää automaattisia skannauksia ja tehdä luetteloa haavoittuvuuksista myöhempää käyttöä varten. (Jabbusch, J. 2009)

Hyvin viritetty IDS tai IPS voi tehokkaasti tunnistaa haittaohjelmat, ennen kuin ne aiheuttavat häiriötä. IDS/IPS teknologiat voivat älykkäämmin estää vaarallisia hyötykuormia, vaikka hyökkääjä käyttäisi epämuodostunutta tai out-of-order- pakettia naamoidakseen hyökkäyksen. (Jabbusch, J. 2009)

3.34 Lähiverkon koventaminen

3.34.1 BPDU Guard

Bridge Protocol Data Unit:it (BPDU) ovat paketteja joita Spanning Tree Protokolla (STP) käyttää havaitakseen verkossa olevien kytkinten väliset loopit eli tilanteet, jolloin kahden päätepisteen välisiä reittejä on useampi kuin yksi. Loopit aiheuttavat broadcast myrskyjä verkkoon, joka voidaan estää sulkemalla verkon yksi portti, jolloin verkkolaitteiden välille jäää vain yksi aktiivinen polku. (Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches.2006)

STP-protokollan keskeinen asia on root kytkimen valinta, joka tapahtuu vertaamalla millä kytkimellä on pienin Bridge ID eli prioriteettiarvo, joka muodostuu kytkimen MAC-osoitteesta sekä Switch Priority:stä, joka on standardissa oletuksena 32,768. Verkon kytkimet keskustelevat toistensa kanssa välittäen BPDU-paketteja keskenään.

Eri STP protokollat kuten Rapid STP ja VLAN STP käyttävät eri BPDU-paketteja, joiden tehtäväն on päätää, mikä portti suljetaan, ja mikä portti osoittaa Root kytkintä.

Kytkimiin liitettyt PC:t voivat myös lähettää BPDU paketteja, jotka mahdollistavat kytkimelle saapuessaan protokolla ongelmia STP:lle tai verkon jumiutumisen. (Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches.2016)

Tätä tarkoitusta varten BPDU Guard on kehitettyä, estämään tietystä PortFast-portista BPDU-pakettien saapumisen, sammuttamalla portin, kun se vastaanottaa pakettin. Näin ollen STP-topologiaan ei pystytä vaikuttamaan. Portin sammutuksen jälkeen se joudutaan manuaalisesti nostamaan takaisin pystyn. (Chapter: Optional STP Features.N.d.)

3.34.2 DHCP Snooping

DHCP snooping on tietoturvaominaisuus, joka toimii access layer kytkimellä ”palomuurina” ns. epäluotettavan ja luotetun päätelaitteen ja DHCP palvelimen välillä. Luotettu päätelaite on mikä tahansa laite, mikä on verkon järjestelmänvalvojen hallittavissa mm. kytkimet, reitittimet, palvelimet. Kaikki laitteet kytkimen verkon ulkopuolella luokitellaan näin ollen epäluotettaviksi laitteiksi. (Catalyst 6500 Release 12.2SX Software Configuration Guide. 2013)

DHCP snooping estää ominaisuksillaan näin ns. rogue DHCP-palvelinten mahdollisuuden jakaa IP-osoitteita päätelaitteille. Tällaisia laitteita usein käytetään Denial of Service (DoS) hyökkäyksissä tai man-in-the-middle hyökkäyksissä. (Banks, E.2012)

Pääpiirteittäin DHCP snooping suorittaa DHCP-viestien tarkastusta tuntemattomilta verkkolaitteilta ja pudottaa viestit tarvittaessa rajoittaa DHCP-liikennettä luotetuista ja tuntemattomista lähteistä. Ylläpitää tietokantaa epäluotettavista lähteistä ja niiden IP-osoitteista. Myös luotettujen päätelaitteiden MAC-osoitteet, IP-osoite, VLAN, lease time ja portti on talletettuna tietokannassa. (Catalyst 6500 Release 12.2SX Software Configuration Guide.2013)

3.34.3 Control Plane Protection

Ohjaustason suojaaminen on valvonta ominaisuus, mitä tarjotaan ohjaustason valvontaan. Ohjaustason valvonta mahdollistaa QoS valvonnан ohjaustason liikenteestä

reitittimelle. Se suojaa ohjaus- ja hallintotasoa yläpitämällä näin reitityksen vakauden, verkon tavoitettavuuden ja pakettien toimittamisen. Ohjaustason suojaus käytännössä suojaa verkon infrastruktuuria DoS hyökkäyksiltä mahdollistamalla ohjaustason selvemmän valvonnan ja haluttaessa rajoittamalla tietyn tyypistä liikennettä. (Understanding Control Plane Protection.N.d.)

Tarjoaa mekanismin, jolla suljettuihin TCP/UDP portteihin saapuvat paketit pudottetaan. Tarjoaa mahdollisuuden rajoittaa protokolla jonojen käyttöä, niin että yksi protokolla tulva ei ylikuormita sisään menevää rajapintaa. Kategorisoi ohjaustason raja-pinnan suodatuksen kolmeen host, transit ja CEF-exception. (Understanding Control Plane Protection.N.d)

3.34.4 CDP / LLDP hardening

Cisco Discovery Protocol (CDP) on siirtoyhteyskerros protokolla, jota Ciscon verkkolaitteet käyttävät. CDP mahdollistaa verkkotyökalujen oppia mitä laitteeseen suoraan kytketyt laitteet ovat. CDP:llä voidaan määrittää, miten rajapintoihin kytketyt laitteet ovat konfiguroitu, sekä miten eri siirtoyhteytason protokollia käyttävät laitteet voivat tutkia toisiaan. (Chapter: Configuring Cisco Discovery Protocol.2013)

Link Layer Discovery Protocol (LLDP) on protokolla, mitä käytetään samaan tarkoitukseen kuin CDP:tä mutta vain ei Cisco Systemsin verkkolaitteille.LLDP vaihtaa mainostusviestejä verkkolaitteiden välillä ja tallentaa tiedot laitteen Management Information Base (MIB)-tietokantaan. LLDP käyttää Type Length value (TLV) viestejä mainostessaan laitteita. (Orbitco.2016)

Näiden protokollien ominaisuuksien ansiosta on mahdollista, että niitä voidaan käyttää luvattomien käyttäjien toimesta esimerkiksi verkon kartoitukseen ja tiedusteluun, jolloin olisi suositeltavaa, että CDP/LLDP-protokollia ei käytettäisi tai rajapinnat, jotka ovat yhteydessä ulkoverkkoon evät käyttäisi näitä protokolia. (Cisco Guide to Harden Cisco IOS Devices.2016.)

3.35 Haavoittuskannaus

Haavoittumisen testaamisella tarkoitetaan tietokonejärjestelmän, erilaisten verkkojen tai sovellusten testaamista käytännössä. Tarkoituksena on etsiä aukkoja, joita mahdollinen hyökkääjä voisi hyödyntää. Kyseisen testauksen ja cräkkeröinnin ero on siinä, että mitä tiedoilla tehdään ja onko se luvanvaraista. (Holvitie, V.2014)

Tunkeutumistestausta voidaan tehdä joku manuaalisesti tai automaattisesti erinäisten sovellusten avulla. Prosessiin kuuluu tietojen keräämistä ennen kyseisen kohteen testausta sekä tiedustelua. Tällä tarkoitetaan sitä, että tunnistetaan reittejä kohdeverkkoon tai järjestelmään. (Holvitie, V.2014)

Yleensä on monia syitä miksi testausta suoritetaan, mutta yksi tärkeimmistä syistä on havaita mahdolliset haavoittuvuudet ja korjata ne ennen kuin joku ulkopuolin taho pääsee niihin käsiksi. Joskus testauksessa käytetään ulkopuolista tahoa, että yrityksen johto voisi vapauttaa resursseja kyseisten ongelmien korjaamiseen. (Holvitie, V.2014)

Tunkeutumistestaukset jaetaan yleensä kahteen kategoriaan: ilmoitettuun ja ilmoittamattomaan. Ilmoitettu testaus tarkoittaa sitä, että yritetään päästää käsiksi ja saada haltuun etukäteen sovittuja tiedostoja. Ilmoittamattoman testaamisen tarkoituksena, että vain yrityksen johdolla on tietoa tästä etukäteen. Tarkoituksena on siis testata nykyistä tilannetta niin infrastruktuurin kuin tietoturvahenkilöstönkin osalta. (Holvitie, V.2014)

3.36 802.1x

802.1X on IEEE standardi, käyttää portti-porttipohjaista verkonsisänpääsyn hallinnointia. IEEE 802 LAN:ia käytetään tuomaan fyysisen sisänpääsyn ominaisuudet, jonka avulla saadaan järjestelmään autentikointi ja auktorisointi. Järjestelmällä saadaan LAN-portteihin point-to-point yhteyksien ominaisuudet ja sisänpääsyn estämisken porteissa, missä autentikointi tai auktorisointi epäonnistuu. Portti on tässä kontekstissa liitääntärajapinta LAN infrastruktuuriin. (Snyder, J. 2010)

802.1X käyttää kolmea termiä, jotka täytyy tietää ymmärtääkseen sen toimintaa. Käyttäjästä tai asiakasta, joka haluaa autentikoitua, käytetään nimitystä supplicant. Authentication serveri on tyypillisesti RADIUS-palvelin, joka hoitaa autentikaation. Authenticator nimitystä käytetään laitteesta, joka on näiden kahden välissä, kuten wireless access point. 802.1x ei tarvitse paljoa muistia tai prosessointitehoa, joten se sopii hyvin käytettäväksi langattomissa verkoissa. (Snyder, J. 2010)

Protokollaa mitä 802.1X käyttää on Extensible Authentication Protocol Encapsulation over LANs (EAPOL). Se on tällä hetkellä määritelty Ethernet-tyyppisille LANeille mu-kaan lukien 802.11 langaton standardi ja Token Ring LAN:it, kuten Fiber Distributed Data Interface (FDDI). Käytännössä EAPOL on ainoastaan kapseloitu versio Extensible Authentication Protocollasta (EAP). (Snyder, J. 2010)

3.37 Lokit

Loki on dokumentti jostakin tapahtuneesta tietyllä hetkellä, mikä tapahtuu organisaation järjestelmissä tai ympäristössä. Näitä lokitietoja voidaan kerätä tärkeistä järjestelmistä käyttäen esimerkiksi yleisiä SNMP- ja Syslog- protokollia ja Windowssissa käytössä olevaa Event Logia. Logeilla voidaan seurata järjestelmien toimintaa ja niiden eheyttä. Myös häiriöiden ilmoitukset ovat tärkeitä, jotta niiden korjaaminen pystytään aloittamaan heti vian ilmettyä. Lokit ovat myös tärkeitä tietoturvan suhteeseen, sillä niillä pystytään havaitsemaan tietomurtoja tai niiden yrityksiä. Logiformaatit ovat yleensä ASCII- tekstinä. Tämä helpottaa niitten lukemista, sillä niihin ei tarvitse erillistä editoria. Osa lokijärjestelmistä kuitenkin käyttää logeissaan binääriä. Logien käsittelyyn tarkoitettut ohjelmat kuitenkin pystyvät lukemaan tätä.

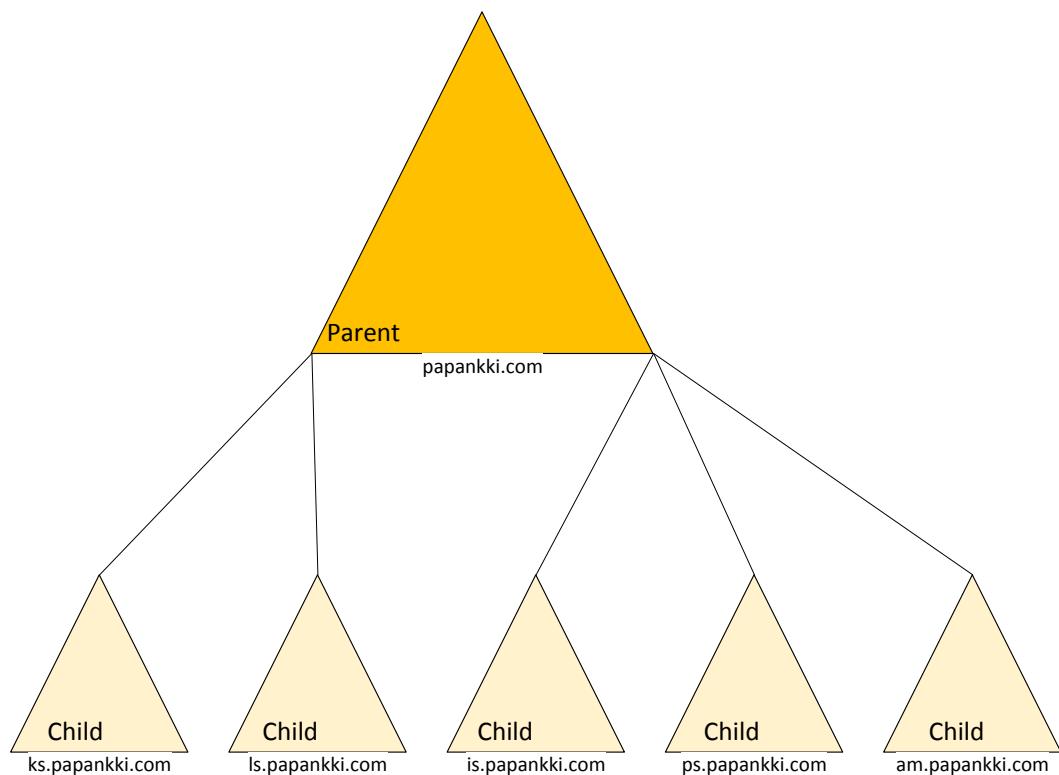
3.38 Auditointi

Auditoinnilla tarkoitetaan palvelun tai muun asian tarkastelua, jossa pyritään selvittämään, onko palvelussa tavoitettu asetetut tavoitteet. Auditointeja voidaan tehdä myös sertifikaatteja varten. Tällä halutaan varmistaa, jos palvelu tavoittaa tietyt sertifikaatin asettamat tavoitteet. Auditoinnin suorittaa aina joku muu henkilö, kuin palvelun toteuttanut henkilö.

4 Suunnitelma

4.1 AD-looginen rakenne

Päätimme tehdä organisaatiomme parent/child periaatteella, pääkonttori toimii Parent-domainina ja kaikki muut sivukonttorit ovat Child-domaineja. Organisaatio rakennettamme on havainnollistettu kuviossa 13. Päädyimme tähän ratkaisuun, koska ryhmän jäsenillä on eniten kokemusta AD-rakenteen toteutuksista. Organisaationsamme tulee olemaan neljä OU:ta, jotka ovat Johtajat, ATK-tuki, Konttori ja Ekonoministit.



Kuvio 13. Organisaatio rakenne

4.2 DHCP-suunnitelma ja MAC-Binding

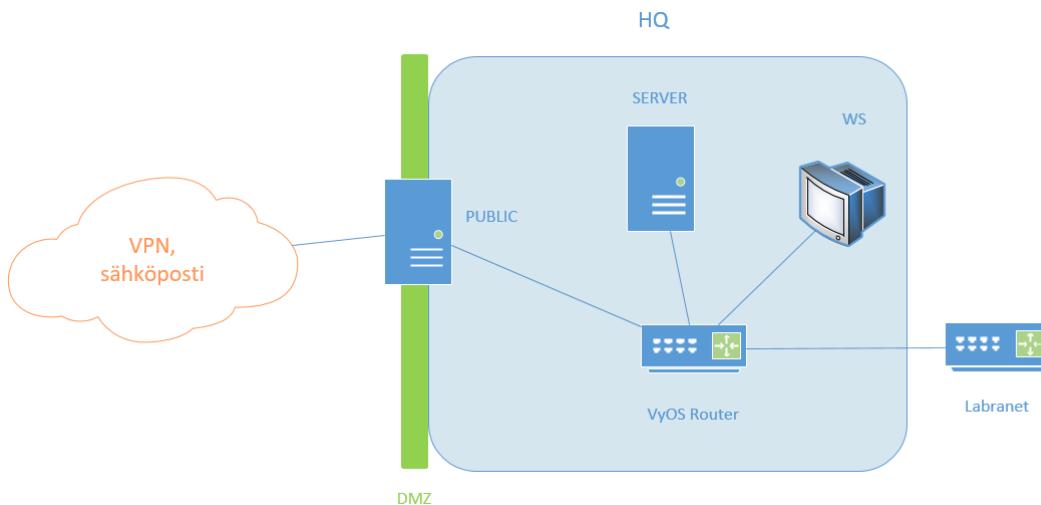
Suunnittelimme pääkonttorin ohjainpalvelimille sekä tiedostopalvelimille IPv4-osoiteistuksen noudattamaan 10.100.0.X/24 verkkoa. Yrityksen pienemmille toimipaikoilla käytetään 10.200.X.Y/24 verkotusta kuten liitteessä (Liite 1) on taulukoitu. DHCP:tä ajetaan jokaisen toimipaikan omassa VyOS reitittimessä. Toimeksiannossa oli myös määritelty käytettäväksi IP-osoitteiden jako MAC-osoitteiden mukaan eli ns. MAC-Binding. Alla olevasta taulukosta (Taulukko 3) nähdään, kuinka ajattelimme toteuttaa päätoimipaikan työasemien osoitejaon MAC-osoitteen mukaan.

Taulukko 3. MAC-Binding taulukko työasemille

Nimi	IP-osoite	MAC-osoite
HQ-WS1	10.0.0.10	00:0c:29:f6:30:5c
HQ-WS2	10.0.0.11	00:0c:29:64:8a:ff
HQ-WS3	10.0.0.12	00:0c:29:be:73:b9
HQ-WS4	10.0.0.13	00:0c:29:1d:44:6b

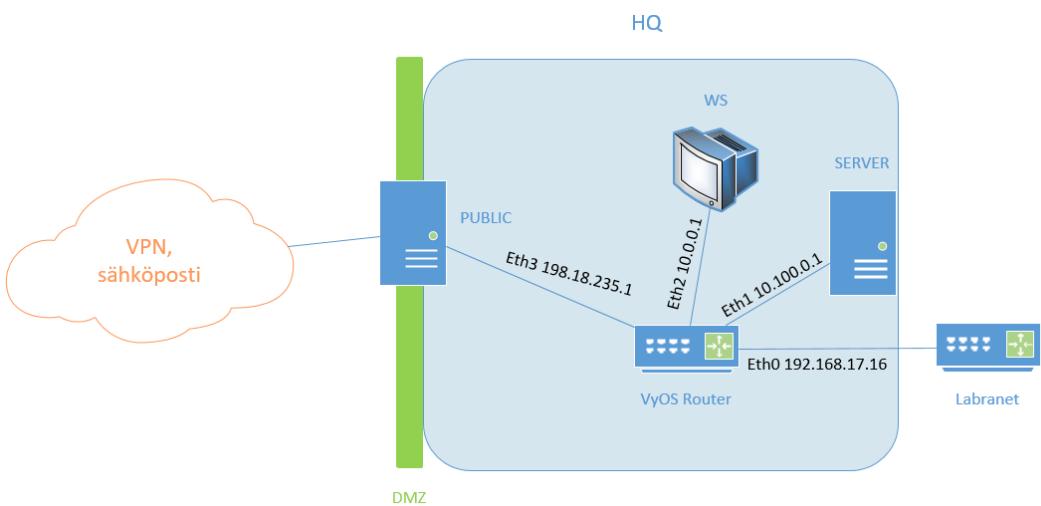
4.4 HQ Fyysinen ja looginen topologia

Kuviossa 14 on esitetty pääkonttorin HQ fyysinen topologia, sekä toimipaikan VLANit.



Kuvio 14. Pääkonttori HQn fyysinen topologia

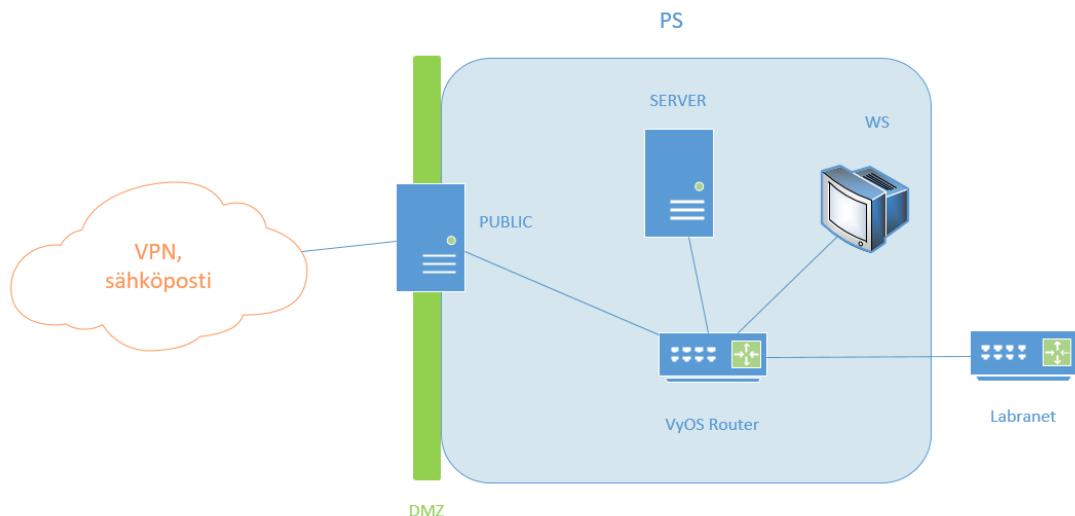
Kuviossa 15 on esitetty pääkonttorin HQ looginen topologia, sekä käytettävät IP-osoitteet.



Kuvio 15. Pääkonttori HQn looginen topologia

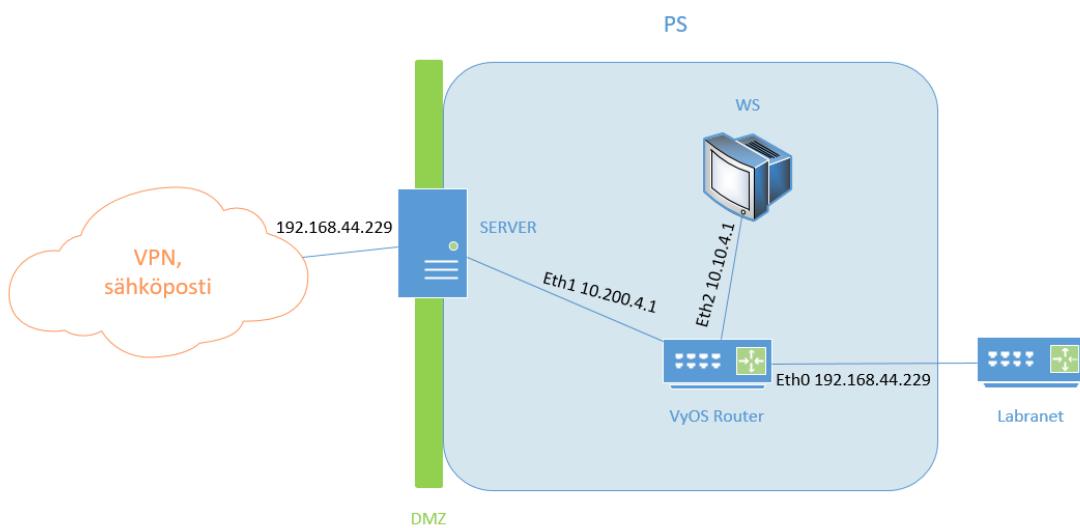
4.5 Pohjois-Suomen (PS) fyysinen ja looginen topologia

Kuviossa 16 on esitetty Pohjois-Suomen PS fyysinen topologia, sekä toimipaikan VLANit.



Kuvio 16. Pohjois-Suomen PS fyysinen topologia

Kuviossa 17 on esitetty Pohjois-Suomen PS looginen topologia, sekä käytettävät IP-osoitteet.



Kuvio 17. Pohjois-Suomen PS looginen topologia

4.6 Salasanakäytänteiden toteutus

Salasanojen suhteen tulemme käyttämään viestintäviraston suosituksia. Salasanojen minimi koko vähintään 15 merkkiä ja erikoismerkkejä pitää käyttää. Uuden käyttäjän tullessa järjestelmään annetaan hänen väliaikainen salasana mikä täytyy vaihtaa ensimmäisen sisäänkirjautumisen yhteydessä. Salasanakäytänteissä ei laiteta salasanoja vanhentumaan, koska niistä syntyy käyttäjille turhaa tekemistä ja uusimpien tutkimusten mukaan ne eivät juurikaan auta. (Cranor, L. 2016.)

Salasanat tullaan säilömään tiivisteinä tietoturvan lisäämiseksi ja käytettävä algoritmi on bcrypt. Lookup tables ja rainbow tables hyökkäysten estämiseksi suolaamme vielä käytetyt salasanat. Tätä ei vielä suoriteta Toimeksianto 1, vaan jätetään suorittavaksi tulevissa toimeksiantoissa.

4.7 Käyttäjien profiilit, kotihakemistot ja backup

Käyttäjät pystyvät kirjautumaan omaan profiliinsa mistä tahansa yrityksen työasemasta, sijainnista riippumatta. Työntekijöiltä poistetaan käytöstä palvelut ja ohjelmat joita he eivät tarvitse työskennellessään. Omien ohjelmien asennus ja työpöydän muokkaaminen estetään. Kotihakemiston koko tulee olemaan yksi gigatavu. Käyttäjän sähköpostiin lähetetään ilmoitus, jos levytilan käyttö ylittää 85%.

Kotikansiot varmuuskopioidaan joka yö klo. 01.00. Näin välttyään tärkeiden tietojen menetykseltä mahdollisen laiterikon sattuessa. Valittuna ajankohtana kenenkään työntekijän ei pitäisi olla töissä. Öisin ei myöskään tarvitse miettiä kaistankäyttöä tai laitteiston resurssien käyttöä varmuuskopioinnin aikana. Työntekijöillä on käytössään kaksi gigatavua yhteistä levyjakoa. Tämä väliaikaiseen käyttöön tarkoitettu tallennustila tyhjennetään joka yö klo. 24.00. Yleistä levyjakoa ei varmuuskopioida, eikä siellä tulisi säilyttää mitään tärkeitä tiedostoja. Toimipaikkojen ohjainpalvelimet on kahdennettu, joten DC1lle tehdyt muutokset replikoituu automaattisesti DC2lle.

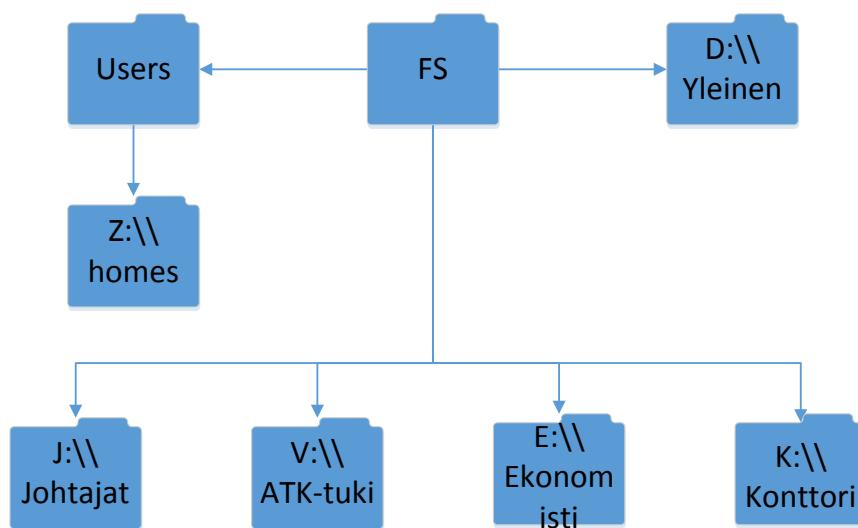
4.8 Levyjaot

Levyjaot toteutetaan siten, että kaikilla on oikeudet yleiseen kansioon, johon voi laittaa mitä vain koko päivän ajan, mutta se tyhjennetään joka päivä klo 00:00. Jokaiselle työntekijälle tehdään oma kotikansio, johon ainoastaan työntekijä itse pääsee käsiksi. Osoitteet kotikansioille tulevat olemaan esimerkiksi \\hq\Users\Johtaja\\$username periaatteella. Jokaiselle ryhmälle annetaan omat kansiot ja niihin pääsee käsiksi tauukon 4 mukaisesti.

Taulukko 4. Levyjakojen oikeudet

Kansiot	Ryhmat			
	Johtajat	Ekonomistit	Konttori	ATK
Johtajat	FC			FC
Ekonomistit	R	FC	RW	FC
Konttori	R	RW	FC	FC
ATK	R			FC
Yhteinen	FC	FC	FC	FC

Käyttäjälle tulee näkymään oma verkkolevy ja Yleinen, joka on ainoastaan HQ tiedostopalvelimella. Yleinen on jaettuna kaikkien sivukonttorien välillä. Levyjakoja havainnollistetaan Kuviossa 18.



Kuvio 18. Levyjaot

4.9 Toiminnallisuustasot

Toiminnallisuustasolla tarkoitetaan palveluita, jotka ovat käytössä koko infran alueella. Toiminnallisuustaso riippuu aina vanhimasta käytössä olevasta palvelinkäytöjärjestelmästä, joka määräää mitä palveluita verkossa voidaan käyttää. Esimerkiksi verkossa olevat Windows Server 2008 ja 2012 R2 palvelimet toimivat version 2008 tukemien palveluiden ehdolla. Tästä syystä paras tilanne olisi, jos kaikki verkon palvelimet käyttäisivät samaa versiota käyttöjärjestelmästä. Vanhempi versioita voi myös käyttää, mutta palveluita luodessa on oltava tietoinen mitä palveluita voidaan käyttää.

Omassa toteutuksessamme käytämme Windows Server 2012 R2 käyttöjärjestelmää kaikilla verkon palvelimilla. Näin vältämme toiminnallisuustasoista johtuvat ongelmat ja voimme käyttää kaikkia tarvitsemiamme palveluita.

4.10 NTP suunnitelma

NTP tullaan toteuttamaan siten, että HQ-VyOS saa aikatietonsa suoraan meille annetusta 192.168.17.2 osoitteessa olevassa NTP-palvelimelta. Tämän jälkeen HQ-DC1 ottaa aikatietonsa HQ-VyOS:ltä, jonka jälkeen se synkronisoituu automaattisesti suoraan muille brancheille oikeat aikatiedot. Brancheilla toimivat VyOS reitittimet täytyy konfiguroida saamaan aikatietonsa HQ-DC1:ltä. NTP asetusten muuttaminen pitää tehdä komento tulkin kautta Windows Server 2012 R2 versiossa, joten tulemme käyttämään Windows Powershell:iä näiden komentojen ajamiseen. Nämä komennot täytyvät jaa Käyttäjällä, jolla on riittävät oikeudet ja tässä tullaan käyttämään Administrator tiliä.

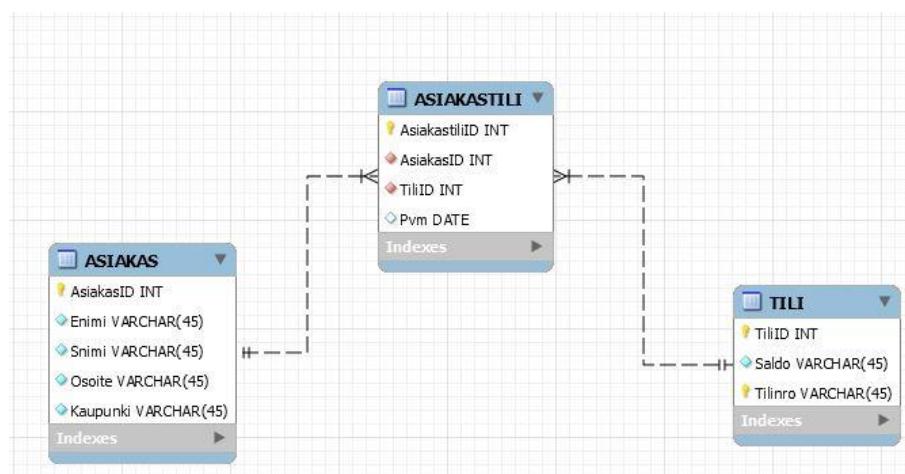
4.11 Palveluiden Autentikointi

Palvelut liitetään AD-ympäristöön, jotta pääsemme käsiksi haluttuihin palveluihin AD:ssa määritellyillä käyttäjillä. Liittäessämme palveluita ympäristöömme tulemme ensimmäiseksi lisäämään järjestelmän domainimme ja LDAP yhteyksillä hakemaan

käyttäjätiedot AD-palvelimilta. Domainiin liittyessämme saamme varmennettua käytäjät domainin kautta. LDAP yhteydellä saamme käyttäjien tiedot tuotua järjestelmään. Sähköposti palvelussa tulemme toteuttamaan AD/LDAP-integraation, jossa nähdään sen toiminta käytännössä.

4.12 Tietokantapalvelin

Pystytetään pankille MySQL-relaatiotietokanta Ubuntu 16.04.2 serverille, jossa ylläpidetään tietokantaa pankin asiakkaista (Kuvio 19.). Nostetaan palvelin Domainiin ja luodaan sille sertifikaatti. Muodostetaan suojaattu yhteys SQL-kyselyille sekä varmuuskopioidaan tietokanta.



Kuvio 19. Tietokannan käsitemalli

4.13 IGP Kovennukset

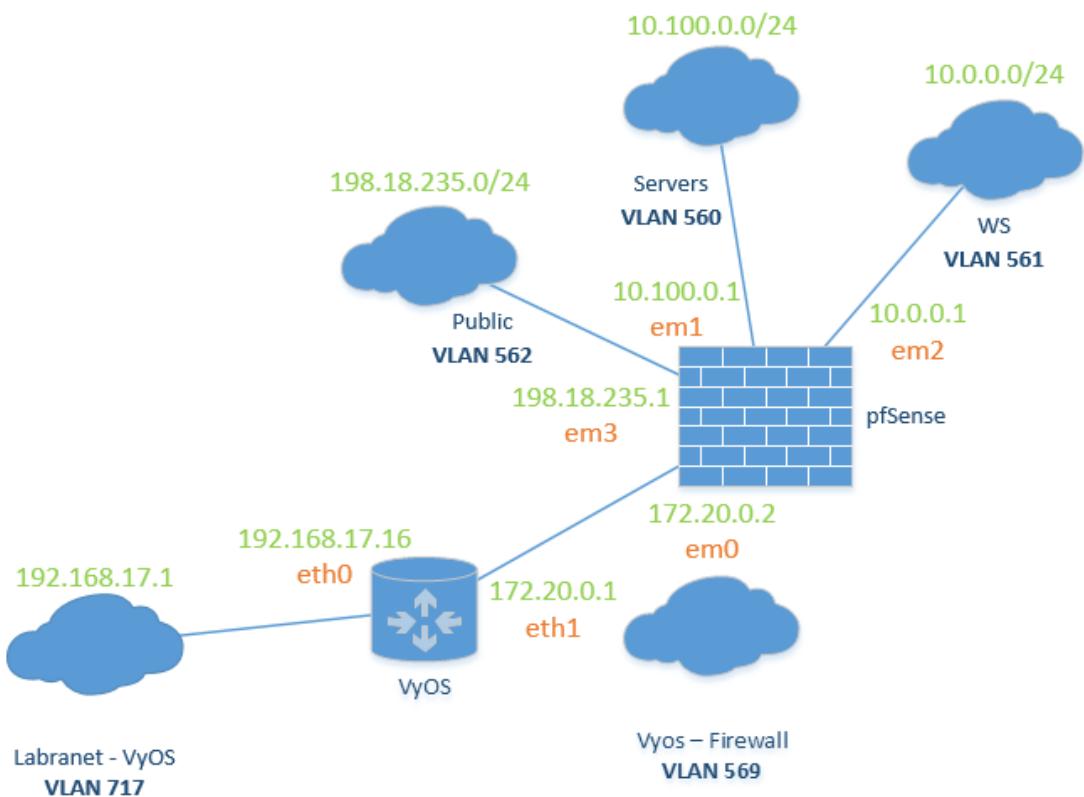
Yrityksemme käyttää OSPF:ää hoitamaan sisäverkkojen reitityksen. OSPF tietoturvaa tullaan parantamaan lisäämällä portit passiivisiksi. Tällä estämme luvattomat yhteydet portteihin ja turhien reititys protokollien jakamisen. Ainoat portit, mitä tulemme tarvitsemaan, poistetaan passive tilasta, kuten ulkoverkkoon menevä portti ja IPSec tunnelit. Laitamme OSPF:än käyttämään MD5 salausta.

4.14 DNS

Pääkonttorin ohjainpalvelin DC1 toimii sisäverkon osoitteiden selvittäjänä. Osoitteet, joita DC1 ei tunne, ohjataan DMZ-alueella sijaitsevalle DNS-palvelimelle. Tuntemat osoitekyselyt ohjataan DMZ:ltä ulkoverkossa oleville DNS-palvelimille. DNS-palvelimena toimii Ubuntu 16.04 käyttöjärjestelmällä varustettu palvelin ja nimipalvelinohjelmistona Bind9.

4.15 Palomuuri

Yrityksemme palomuuri on sijoitettu VyOS-reitittimen ja sisäverkon laitteiden väliin. Palomuurin tehtävänä on estää haitallinen liikenne yrityksemme verkkoon. Kaikki sisään ja ulostuleva liikenne yrityksessä ohjataan palomuurin kautta. Pystymme hallinnoimaan suodatettavaa liikennettä, sekä monitoroimaan yrityksen verkkoa. Verkon monitoroinnilla pystymme havaitsemaan mahdollisesti saastuneet laitteet ja mahdolliset hyökkäykset verkon ulkopuolelta. Kuviossa 20 on havainnollistettu palomuurin sijaintia verkossa.



Kuvio 20. Palomuurin sijainti verkossa

Palomuurin lisääminen aiheutti pieniä muutoksia verkon topologiaan, sekä reitittimen konfiguraatioihin. VyOS- reitittimen eth0 rajapinta on suoraa kiinni ulkoverkossa ja eth1- rajapinta palomuurissa. Reitittimeltä suljettiin käyttämättömäksi jääneet rajapinnat. VyOS:n ja palomuurin väliseksi verkoksi valitsimme privaatin 172.20.0/24-verkon. Palomuurin sisäverkon rajapintojen osoitteiksi asetettiin oletusyhdyksäytävien osoitteet.

Mitataan verkon Baseline ja kirjataan ylös, millaista liikennettä verkossa kulkee. Verkkoliikenteestä selvitetään liikenteen tyyppi, lähde- ja kohdeportit. Karttoituksen perusteella luodaan palomuuriin säännot kullekin verolle. Liikenne sallitaan vain, jos se täsmää luotuihin sääntöihin. Baseline- mittaus suoritettiin Public-, WS-, Servers ja WAN- verkoista. Liitteestä 3 selviää palomuuriin tehdyt säännot, portit, lähtevä- sekä kohdeverkko.

Valitsimme palomuurituotteeksemme ilmaisen PfSense- ohjelmiston. Valintaperusteenamme oli erittäin kattava dokumentaatio verkossa, mahdollisuus asentaa monia

Iisäosia, sekä mielestämme erittäin selkeä selaimen kautta hallittava käyttöliittymä. Valintaamme vaikutti myös SNORT-integraatio, joka helpotti tunkeutumisen testausta huomattavasti.

4.16 Tikettijärjestelmä

Tiketöintijärjestelmän vaatimusmäärittelyn mukaan järjestelmän kuuluu olla AD/LDAP-integroitavissa. Sekä tikettien jonot ja tikettien tekeminen sähköpostilla, että itse järjestelmässä. Tikitin luonnista tulisi tulla ilmoitus tekijän sähköpostiin. Palvelimelle myös sertifikaatti sekä tikettien luonti mahdollisuus ulko- ja sisäverkosta.

Aiemmin tehdysä ohjelmistovertailussa olevista ohjelmista valitaan OsTicket-ohjelma, koska käyttöliittymä vaikutti yksinkertaiselta ja verkosta löydyn demon perusteella helppokäytöinen. Asennetaan ohjelma Ubuntu 16.04 palvelimelle, toimialueen DMZ alueeseen eli VLAN 562:en.

4.17 Sähköposti

Sähköpostipalvelin tulee toimimaan erillisellä sähköpostipalvelimella HQ:ssa. Palveluun pystyy kirjautumaan omalla nimellä ja salasanalla, eli samoilla, joilla kirjaudutaan domainiin. Sähköpostit tallentuvat sähköpostipalvelimelle ja kirjautumistiedot haetaan DC1:llä.

4.18 Pilvipalvelu

Pilvipalvelussa haluttiin luoda yrityksen sisäinen pilvipalvelu helpottamaan yrityksen sisäistä tiedon tallennusta ja jakamista. Palveluun tullaan kirjautumaan AD-tunnuksienvälistä käyttäen omaa nimeään muodossa EtunimiSukunimi ja käyttäen samaa salasanaa, kuin käyttäjälle kirjauduttaessa. Koska toimeksiannossa haluttiin juuri oma sisäinen pilvipalveluratkaisu, palveluun ei pääse käsiksi ulkoverkosta. Tämä on turvalista myös tietoturvan kannalta, koska pankin tiedonjakoon ei haluta kenenkään pääsevän pankin ulkopuolelta.

4.19 Monitoroinnin suunnitelma

Monitoroinnissa tulemme käyttämään OpenNMS ohjelmistoa. Järjestelmän tulemme liittämään AD/LDAP-autentikoinnilla järjestelmäämme. Tulemme mittamaan järjestelmämme verkkoliikenteen toimivuutta pääkonttorin alueella, mihin kaikki palvelumme ovat tehty. Lisäksi tulemme valvomaan kiintolevyn täytymistä tarjoamissa palveluissamme. Kiintolevyn täytymisen rajat määritellään 90%, jonka jälkeen lähetetään hälytykset hallinnasta vastaaville sähköpostilla. OpenNMS käyttää Simple Network Management Protokollaa (SNMP) huomatakseen määriteltyjen arvojen ylityksen, joten se täytyy asentaa hallinnoitaville Linux laitteille. Toimiakseen SNMP tarvitsee UDP-portteja 161 ja 162, jotka avataan järjestelmien palomuureista.

4.20 Lähiverkon kovennus

BPDU-guard:n käyttöönotto suoritetaan Spidernetin kytkimiin WGx-SW1 -SW4 asettamalla Spanning-tree protokolla kytkinten rajapintoihin, jotka ovat yhteydessä toisiin kytkimiin. Koska toimeksiannossa on määritetty, että verkkomme VLAN:it vastaanotetaan kytkimen WGx-Sw2 portista 8, asetetaan tämä linkkiväli trunk-tilaan, kuin myös kytkinten väliset linkit. Mahdolliset hallintaverkon yhteydet toimivat Access-portteina. Access-portteihin asetetaan Portfast toiminto, joka mahdollistaa rajapinnan välittömän forwarding tilan, ilman että rajapinta toimisi ensin listening- ja learning- tilassa. BPDU-guard asetetaan rajapintoihin päälle, jolloin kun porttiin saapuu BPDU-viestejä, rajapinta muuttuu automaattisesti errdisable-tilaan. Lähempi tar-kastelu porteista ja laitteista löytyy Liitteestä 8.

DHCP-snooping:ssa määritellään luotetuksi porteiksi kaikki portit, mitkä osoittavat DHCP-palvelimelle tai ovat yhteydessä toiseen työryhmän kytkimeen. Asetetaan kytkinten portit, jotka eivät ole kohti toista työryhmän kytkintä tai DHCP-palvelinta epäluotettavaksi ja määritellään portteihin rate limit, estää näin ylimääräisten DHCP-viestien tulvituksen rajapintaan.

Control Plane Protection:n osalta asetetaan Spidernetin kytkimille access-list komennolla rajoituksia, jotka estävät esimerkiksi telnet ja SSH-yhteyden kaikista muista osoitteista paitsi hallintaverkon osoitteista.

CDP/LLDP kovennus toteutetaan enabloimalla DDP Ciscon kytkinten rajapintojen välille. LLDP asetetaan Extreme- ja HP laitteiston rajapintojen väliin sekä Cisco- ja Extreme laitteiden välille. Muuten muissa rajapinnoissa ei käytetä CDP:tä tai LLDP:tä.

4.21 Haavoittuvuusskannaus

Tarkoituksena on asentaa zenmap Keski-Suomen branchille ja lähteä sieltä tarkastelemaan kohderyhmän julkisia ip-osoitteita. Tarkoituksena on selvittää käyttöjärjestelmiä ja sitä minkälaisia palveluita ryhmällä on käytössä. Tarkoituksena on asentaa myös Kali, koska se on erittäin käytökelpoinen tämän tyylisissä skannauksissa. Kaliissa on myös useita hyviä ohjelmistoja juuri tästä käyttötarkoitusta varten.

Tarkoituksena on myös kokeilla ssh-yhteyttä ja yrittää oletusalasanoilla kirjautus esim. VyOSille ja muille vastaaville. Työkaluina käytetään varmasti ainakin zenmapia, koska se on kohtuullisen laaja nmap-sovellus ja tietysti Kalin dig-komentoja, jos se on mahdollista.

Zenmapilla pystyy saamaan selville ainakin sen, että pyöriikö kyseinen virtuaalikone linuxin vai jonkun muun OS:llä.

4.22 Etäyhteys

Etäyhteys tullaan toteuttamaan käyttäen OpenVPN palvelua, Debian pohjaisella palvelimella. Tulemme luomaan sertifikaatit serverille ja sieltä ne jaetaan käyttäjille.

Etäyhteyden konfiguroinnissa on 10 askelta, jotka menevät seuraavasti:

1. OpenVPN asennus
2. Konfigurointi
3. Pakettien forwardoinnin salliminen
4. Palomuurin konfigurointi
5. CA:n konfigurointi
6. Certifikaatin ja avaimen luonti serverille
7. Certin ja avaimen siirtäminen oikeaan paikkaan
8. Certin ja avainten luonti käyttäjille
9. Yhdistetyn OpenVPN profiiliin luonti asiakaslaitteille
10. Asiakas profiilin asennus

4.23 802.1x autentikaatio

Ensimmäisenä joudumme luomaan Radius-serverin ympäristöömme, koska tehtäväni ykkösessä epäonnistuimme sen tekemisessä. Radius pitää konfiguroida ottaamaan vastaan EAP liikennettä. Supplicant täytyy konfiguroida käyttämään portti pohjaista 802.1X autentikaatiota. Radius serverin ja supplicantin välillä tulee olemaan Ciscon kytkin, joka täytyy konfiguroida liitteen 9 mukaisesti. 802.1x konfiguraation pohjana tullaan käyttämään kovennuksessa tehtyjä konfiguraatioita.

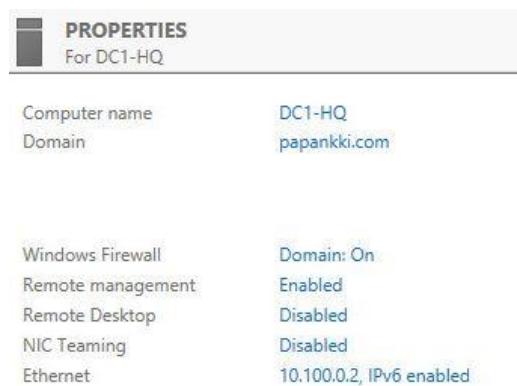
4.24 Lokienhallinta

Lokeja säilytetään graylog- palvelimella. Tärkeimmät palvelut säilytetään seuraavat puoli vuotta, niin kuin Katakri, vaatii kansallisessa tuvallisuusauditointikriteeristössä. Lokit haetaan DC1, DC2, FS1, www ja web palvelimilta, jotka sijaitsevat päätoimipisteellä.

5 Toteutus

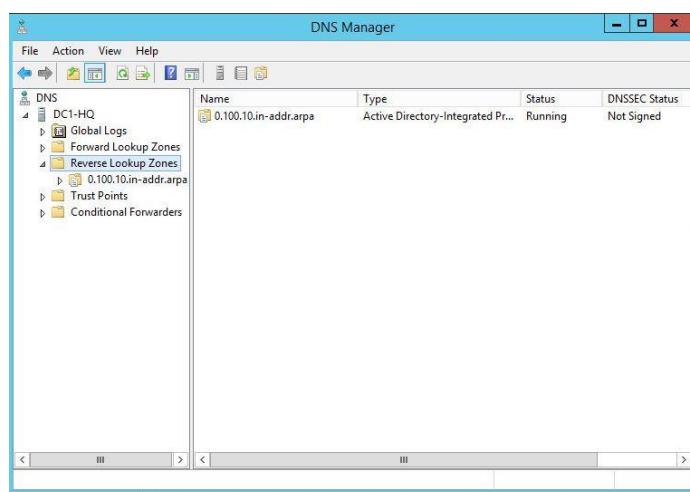
5.1 Pääkonttorin ohjainpalvelin DC1 ja DC2

Projekti toteutus aloitettiin asentamalla pääkonttoriin ohjainpalvelimet DC1 ja DC2. Ohjainpalvelimet nostettiin papankki.com domainiin ja annettiin staattiset IP-osoitteet. (kts. Kuvio 21)



Kuvio 21. Ohjainpalvelin nostettu domainiin ja annettu IP-osoite

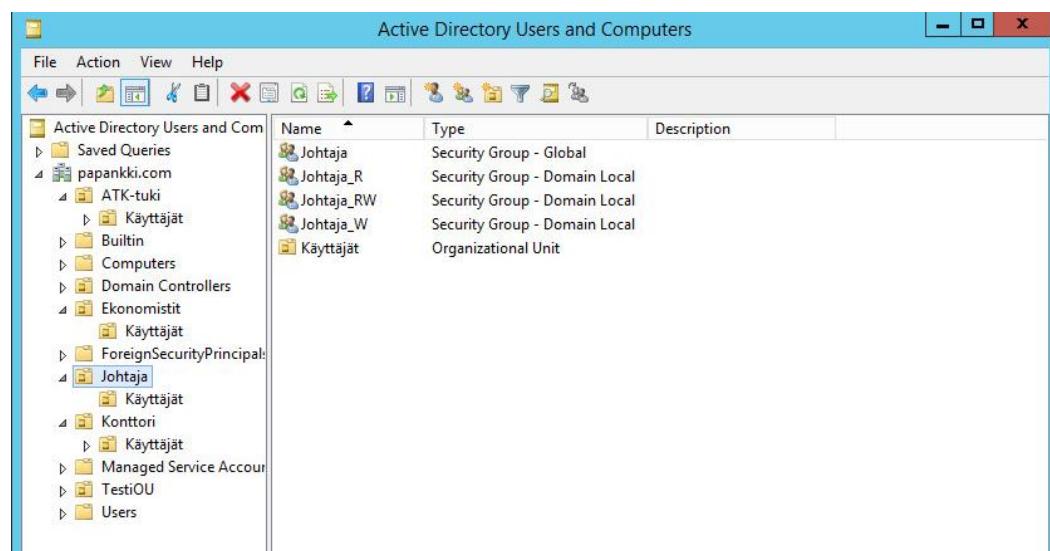
Pääkonttorin DC1:lle luotiin Reverse Lookup Zone, jotta nimikyselyt toimivat. (kts. Kuvio 22)



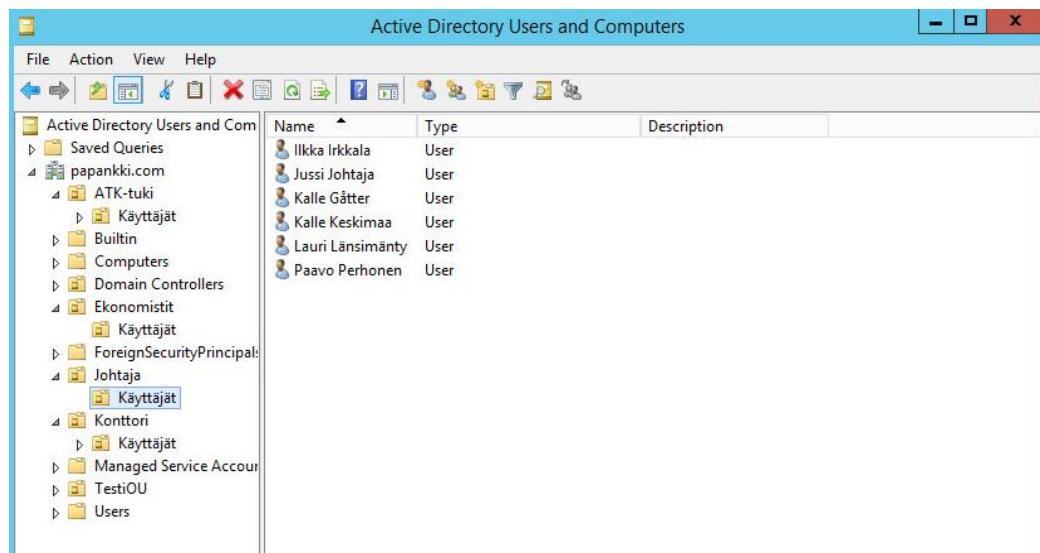
Kuvio 22. DC1:lle luotu Reverse Lookup Zone

5.1.1 Käyttäjien luonti

DC1:lle luotiin suunnitellut käyttäjät ja ryhmät, jotka pystyvät käyttämään palveluita. Tämä toteutettiin niin, että jokaiselle ryhmälle tehtiin oma Organization Unit, jonka sisälle tehtiin yksi globaali ryhmä, johon sijoitettiin kaikki käyttäjät. Tämän jälkeen kolme lokaalia ryhmää, joilla oli joko luku, kirjoitus tai luku ja kirjoitusoikeudet. Tämän lisäksi oma unit, johon luotiin itse käyttäjät. Tämä toteutettiin jokaiselle ryhmälle. (Kts. Kuviot 23 ja 24)



Kuvio 23. Globaalit ja lokaalit ryhmät



Kuvio 24. Johtaja- ryhmän käyttäjät

5.1.2 Replikointi ja DNS

Ohjainpalvelin DC1 replikoidaan DC2:lle mahdollisten laiterikkojen aiheuttamien katojen välttämiseksi. DC1:n AD tiedot replikoituvat automaattisesti. Myös DNS kyseilyt ohjautuvat DC2:lle tarvittaessa. (kts. Kuvio 25)

```
C:\>repadmin /syncall
CALLBACK MESSAGE: The following replication is in progress:
  From: 7cf39bf-b-ce12-4ee5-b84e-2fb448ef321d._msdcs.papankki.com
  To : 4588b4aa-ddcc-474c-aeff-f085026a3979._msdcs.papankki.com
CALLBACK MESSAGE: The following replication completed successfully:
  From: 7cf39bf-b-ce12-4ee5-b84e-2fb448ef321d._msdcs.papankki.com
  To : 4588b4aa-ddcc-474c-aeff-f085026a3979._msdcs.papankki.com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.
```

```
C:\>
```

Kuvio 25. Pääkonttorin ohjainpalvelimen DC1 replikointi

Testasimme replikoinnin toimintaa katkaisemalla DC1:ltä yhteyden verkkoon. (kts. Kuvio 26)

```

Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\TatuTarha>ping 10.100.0.2

Pinging 10.100.0.2 with 32 bytes of data:
Reply from 10.0.0.1: Destination host unreachable.

Ping statistics for 10.100.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
C:\Users\TatuTarha>_

```

Kuvio 26. DC1 yhteys katkaistu

Kirjauduimme pankin työntekijän käyttäjätilille ja tarkistimme miltä ohjainpalvelimelta ryhmäkäytänteet, profili ja levyjaot on haettu. DC2 toimii suunnitellusti. (kts.

Kuvio 27 ja 28

USER SETTINGS

```

CN=Tatu Tarha,OU=Käyttäjät,OU=Ekonomistit,DC=papankki,DC=com
Last time Group Policy was applied: 31.1.2017 at 15:13:25
Group Policy was applied from:      DC2-HQ.papankki.com
Group Policy slow link threshold:   500 kbps
Domain Name:                      PAPANKKI
Domain Type:                       Windows 2000

```

Applied Group Policy Objects

```

Default Domain Policy
Ryhämäkäytänteet

```

```
The following GPOs were not applied because they were filtered out
```

```

Yleinenlevy
Filtering: Disabled (GPO)

```

```

Local Group Policy
Filtering: Not Applied (Empty)

```

```
The user is a part of the following security groups
```

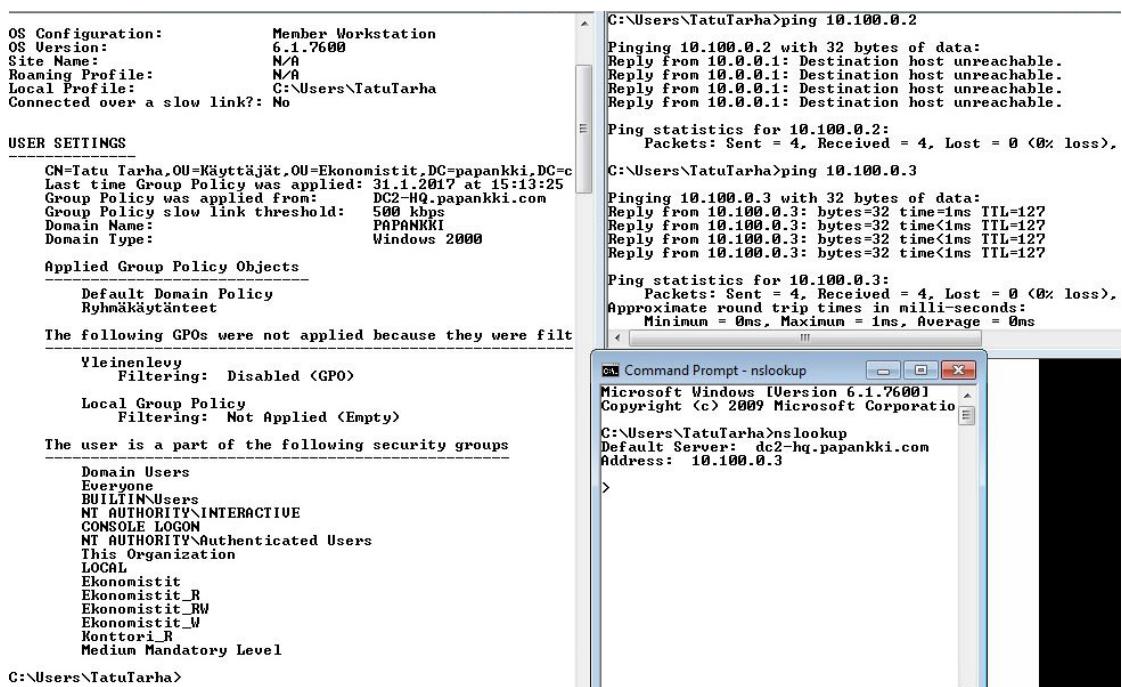
```

Domain Users
Everyone
BUILTIN\Users
NT AUTHORITY\INTERACTIVE
CONSOLE LOGON
NT AUTHORITY\Authenticated Users
This Organization
LOCAL
Ekonomistit
Ekonomistit_R
Ekonomistit_RW
Ekonomistit_W
Konttori_R
Medium Mandatory Level

```

```
C:\Users\TatuTarha>_
```

Kuvio 27. DC2 toiminta AD:na laiterikon sattuessa



Kuvio 28. Käyttäjän profiili ladattu DC2:ltä

Testasimme myös DNS:n toimintaa DC1:n ollessa pois verkosta. Nimikyselyt ohjautuvat suunnitellusti DC2:lle ja nslookup-komennolla saamme varmistuksen. (kts. Kuvio 29 ja 30)

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation

C:\Users\TatuTarha>nslookup
Default Server: dc2-hq.papankki.com
Address: 10.100.0.3

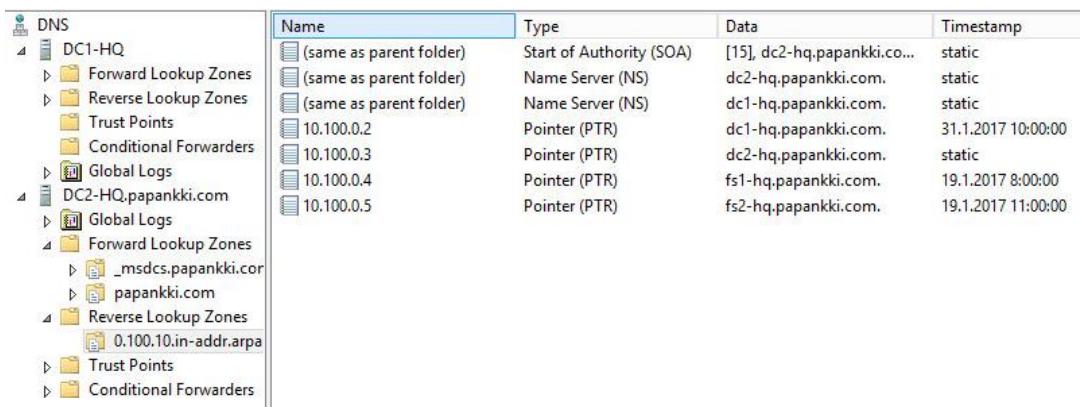
> dc1-hq
Server: dc2-hq.papankki.com
Address: 10.100.0.3

Name: dc1-hq.papankki.com
Address: 10.100.0.2

> fs1-hq
Server: dc2-hq.papankki.com
Address: 10.100.0.3

Name: fs1-hq.papankki.com
Address: 10.100.0.4
```

Kuvio 29. Työasemalta todennettu DNS:n toiminta DC2:lla



The screenshot shows the Windows DNS Management console. On the left, the DNS tree is displayed with nodes for DC1-HQ and DC2-HQ.papankki.com. The DC2 node has sub-nodes for Global Logs, Forward Lookup Zones (containing _msdcs.papankki.com and papankki.com), Reverse Lookup Zones (containing 0.100.10.in-addr.arpa), Trust Points, and Conditional Forwarders. On the right, a table lists DNS records:

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[15], dc2-hq.papankki.co...	static
(same as parent folder)	Name Server (NS)	dc2-hq.papankki.com.	static
(same as parent folder)	Name Server (NS)	dc1-hq.papankki.com.	static
10.100.0.2	Pointer (PTR)	dc1-hq.papankki.com.	31.1.2017 10:00:00
10.100.0.3	Pointer (PTR)	dc2-hq.papankki.com.	static
10.100.0.4	Pointer (PTR)	fs1-hq.papankki.com.	19.1.2017 8:00:00
10.100.0.5	Pointer (PTR)	fs2-hq.papankki.com.	19.1.2017 11:00:00

Kuvio 30. DNS DC2:lla

5.1.3 RADIUS

Atk-tukeen kuuluvat työntekijät pystyvät kirjautumaan pääkonttorin reitittimeen etänä ja tekemään mahdollisia korjauksia konfiguraatioon tarvitsematta olla fyysisesti laitteen äärellä. Reitin kysyy ohjainpalvelimelta varmennusta, löytyykö laitteelle kirjautuva henkilö palvelimen AD:sta. Kuviossa 31 on todennettu Atk-tuen työntekijän käyttäjätunnus reitittimelle.

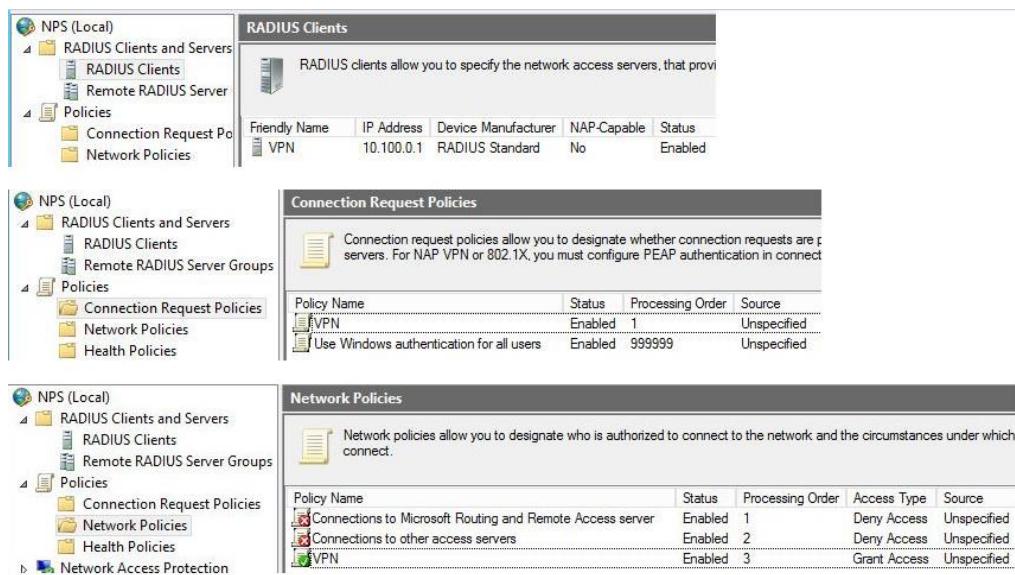
```

}
host-name R1-HQ
login {
    radius-server 10.100.0.2 {
        secret Kissai23
    }
    user kaijakuitu {
        authentication {
            encrypted-password $6$aVpkEFFjLHSx$Bfp4B1cuFsRHUzLVkIzxT3051x0m
yurqWi1K/BFJgRcPEBd0I7Pf2k9R3WjZYb3y5exFaoINUml5BeHi2YEof0
            plaintext-password ""
        }
        level admin
    }
}

```

Kuvio 31. VyOS:lle määritetty RADIUS-palvelimen osoite ja salasana

Asensimme DC1:lle Network Policy Server palvelun, josta löytyy RADIUSsta koskevat policyt. (kts. Kuvio 32)



Kuvio 32. Ohjainpalvelimelle luodut Policyt

Kirjauduimme HQ-PC4:ltä Atk-tukeen kuuluvan Kaija Kuidun tunnuksilla reitittimelle.
(kts. Kuvio 33)

The image shows two terminal windows side-by-side:

- Left Terminal (HQ-PC4):**

```
Z:>ipconfig /all
Windows IP-määritykset

  Isäntänimi : HQ-PC4
  Ensisiainen DNS-liite : papankki.com
  Sisäntyyppi : Hybriidi
  IP-osoite käytössä : Ei
  WINS-määrityspalvelin käytössä : Ei
  DNS-liitteiden etsintälüettelo : papankki.com

Ethernet-sovitin Lähiverkkoyhteys:
  Yhteyskohainen DNS-liite : papankki.com
  Kuvaus : Intel(R) PRO/100
  IP-osoite . . . . . : 00-0C-29-1D-44-6
  DHCP käytössä : Kyllä
  Automaattinen määritys käytössä : Kyllä
  Linkin palkallinen IPv6-osoite . . . : fe80::657d:2250:6e83:
>  IPv4-osoite . . . . . : 10.0.0.13(Ensisiainen
  Oliverkon peite . . . . . : 255.255.255.0
  Määttäluupa nyönnetty . . . . . : 7. helinkuuta 20
  Käyttäluupa vanhenee . . . . . : 8. helinkuuta 2017
  Oletusyhdykskäytävä . . . . . : 10.0.0.1
  DHCP-palvelin . . . . . : 10.0.0.1
  DHCPv6-IAID : 234894137
  DHCPv6-asiaan DUID-tunnus : 00-01-00-01-20-22-7D-
  DNS-palvelimet : 10.100.0.2
  NetBIOS TCP/IP:n päällä . . . . . : Käytössä

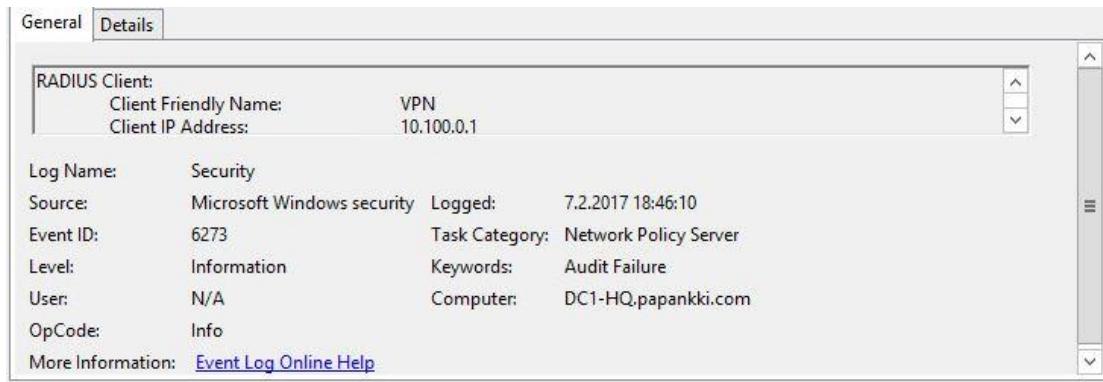
Tunneliosivitin istapapankki.com:
  Laiteen tila : Ei kytkeytyy
  Yhteyskohainen DNS-liite : papankki.com
  Kuvaus : Microsoft ISATAP
  Fyysisen osoite . . . . . : 00-00-00-00-00-0
  DHCP käytössä : Ei
  Automaattinen määritys käytössä : Kyllä

Z:>
```
- Right Terminal (VyOS Router):**

```
kaijakuitu@R1-HQ: ~
server 2.pool.ntp.org {
}
package {
    auto-sync 1
    repository community {
        components main
        distribution helium
        password ""
        url http://packages.vyos.net/vyos
        username ""
    }
}
syslog {
    global {
        facility all {
            level notice
        }
        facility protocols {
            level debug
        }
    }
}
time-zone UTC
vpn {
    pptp {
        remote-access {
            authentication {
                mode radius
                radius-server 10.100.0.2 {
                    key Kissai23
                }
            }
            client-ip-pool {
                start 10.0.0.1
                stop 10.0.0.254
            }
        }
    }
}
[edit]
kaijakuitu@R1-HQ#
```

Kuvio 33. Todennus radiuksen toiminnasta HQ-PC1:ltä

DC1 Event Viewer:llä näemme lokin, ketkä ovat yrittäneet kirjautua reitittimelle. Kuviossa 34 käyttäjä on syöttänyt virheellisen käyttäjätunnuksen, josta on jänyt ohjainpalvelimelle lokitieto.



Kuvio 34. DC1 Event Viewer tieto väärästä käyttäjätunnuksesta kirjautuessa etänä reitittimelle

5.1.4 Kerberos

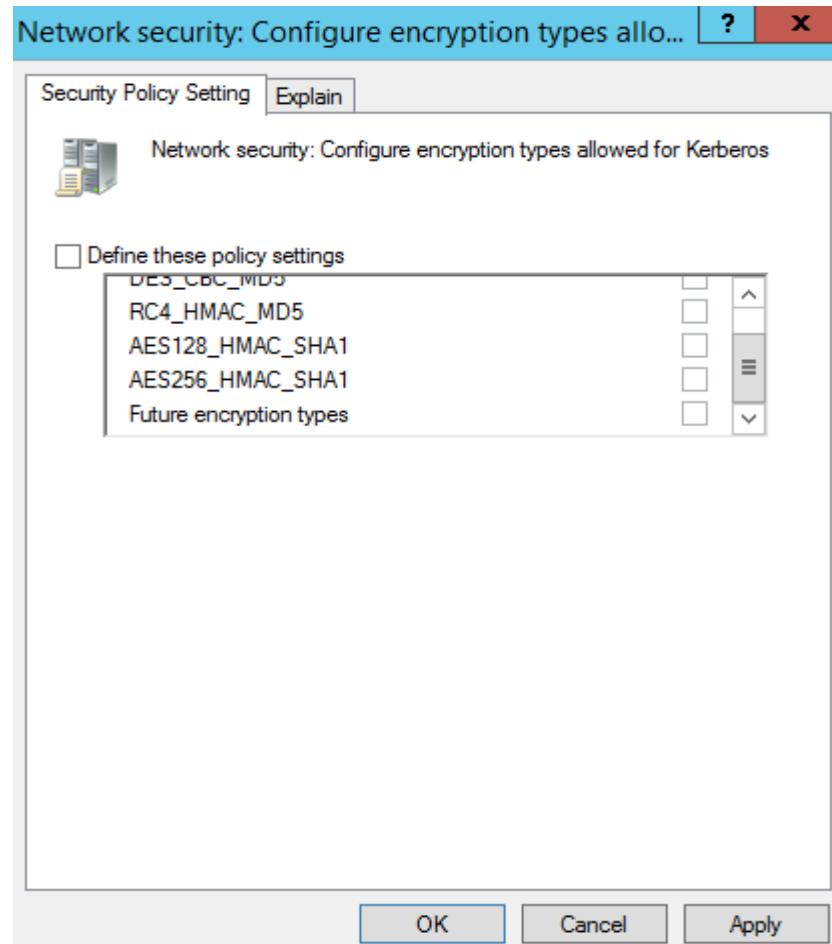
Tavoitteena oli osoittaa mistä Kerberoksen salausta voi muuttaa. Kuviossa 35 on ensin määritelty klist-komennolla saatu tuloste ja kuviossa 36 on taas määritetty, miten Kerberoksen salausta voi muuttaa. Kerberoksessa oli jo uusin salaus käytössä, joten muutoksia ei tarvinnut tehdä.

```
Cached Tickets: (2)

#0> Client: Administrator @ PAPANKKI.COM
Server: krbtgt/PAPANKKI.COM @ PAPANKKI.COM
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent nameCanonicalize
Start Time: 1/27/2017 11:24:39 <local>
End Time: 1/27/2017 21:24:39 <local>
Renew Time: 2/3/2017 11:24:39 <local>
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x1 -> PRIMARY
Kdc Called: DC1-HQ

#1> Client: Administrator @ PAPANKKI.COM
Server: host/dc1-hq.papankki.com @ PAPANKKI.COM
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegation nameCanonicalize
Start Time: 1/27/2017 11:24:39 <local>
End Time: 1/27/2017 21:24:39 <local>
Renew Time: 2/3/2017 11:24:39 <local>
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
```

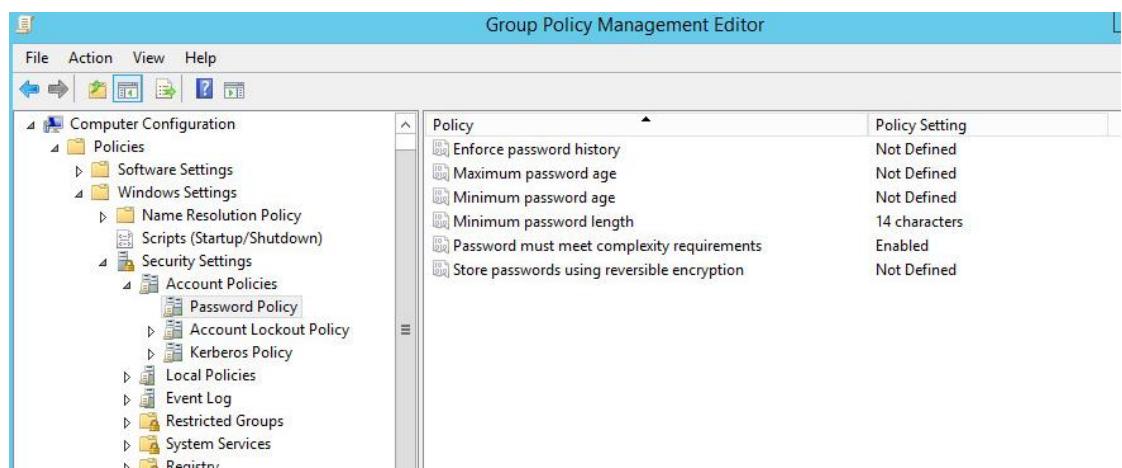
Kuvio 35. Klist komento



Kuvio 36. Kerberoksen salauksen muuttaminen

5.1.5 Salasanakäytänteiden todennus

Salasanakäytänteiden osalta teimme salasanasta minimissään 14 pituisen, koska Windows ei salli sitä pidempiä salasanoja. Complexity requirementsit laitettiin päälle, eli pitää olla isoja ja pieniä kirjaimia erikoismerkkejä ja numeroita. Todennus kuviossa 37.



Kuvio 37. Salasanakäytänteiden todennus

5.2 Pääkonttorin työasemat

Jokainen pääkonttorin työasema nostettiin papankki.com domainiin. Tämän jälkeen käyttäjien tileille pystytiin kirjautumaan ja tiedot haettiin ohjainpalvelimelta. (kts.

Kuvio 38 ja 39)

Computer name, domain, and workgroup settings

Computer name:	HQ-PC1
Full computer name:	HQ-PC1.papankki.com
Computer description:	
Domain:	papankki.com

Kuvio 38. Ensimmäinen pääkonttorin työasema nostettu domainiin



Kuvio 39. Käyttäjän kirjautuminen papankki.com domainiin

Tietoturva silmällä pitäen pääkonttorin työasemat on määritetty MAC-osoitteen perusteella saamaan niille ennalta määritellyt IP-osoitteet. Kuviossa 40 on esitetty HQ-PC1 saama IP-osoite. MAC-Binding toimii oikein ja jakaa ennalta määritellyn IP-osoitteen kullekin työasemalle.

```
C:\Users\KalleKytkin>ipconfig /all
Windows IP Configuration

Host Name . . . . . : HQ-PC1
Primary Dns Suffix . . . . . : papankki.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : papankki.com

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . . . : papankki.com
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-F6-30-5C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::cde4:d0e9:a19f:def0%11(PREFERRED)
IPv4 Address . . . . . : 10.0.0.10(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 3. helmikuuta 2017 10:11:16
Lease Expires . . . . . : 4. helmikuuta 2017 10:59:41
Default Gateway . . . . . : 10.0.0.1
DHCP Server . . . . . : 10.0.0.1
DHCPv6 IAID . . . . . : 234884137
DHCPv6 Client DUID. . . . . : 00-01-00-01-20-1B-30-6B-00-0C-29-F6-30-5C

DNS Servers . . . . . : 10.100.0.3
                           10.100.0.2
NetBIOS over Tcpip. . . . . : Enabled

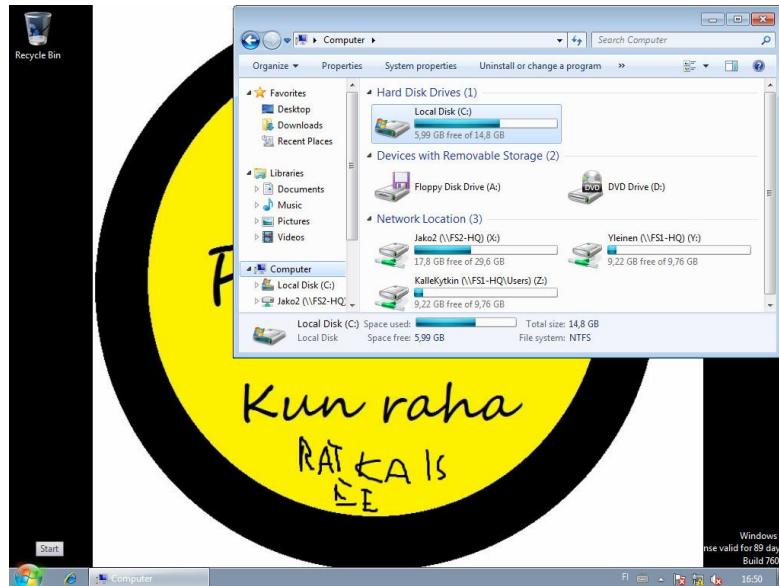
Tunnel adapter isatap.papankki.com:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : papankki.com
Description . . . . . : Microsoft ISATAP Adapter #2
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes

C:\Users\KalleKytkin>
```

Kuvio 40. Todennus MAC-Binding toiminnasta pääkonttorin työasemalta

Kuviossa 41 on esitetty ryhmäkäytänteiden toimintaa. Taustakuva on pankin logo, joka latautuu jokaiselle käyttäjälle. Myös verkkolevyt näkyvät käyttäjille.



Kuvio 41. Ryhmäkäytänteissä ennalta määritelty taustakuva ja levyjaot

5.3 Pääkonttorin tiedostopalvelimet FS1 ja FS2

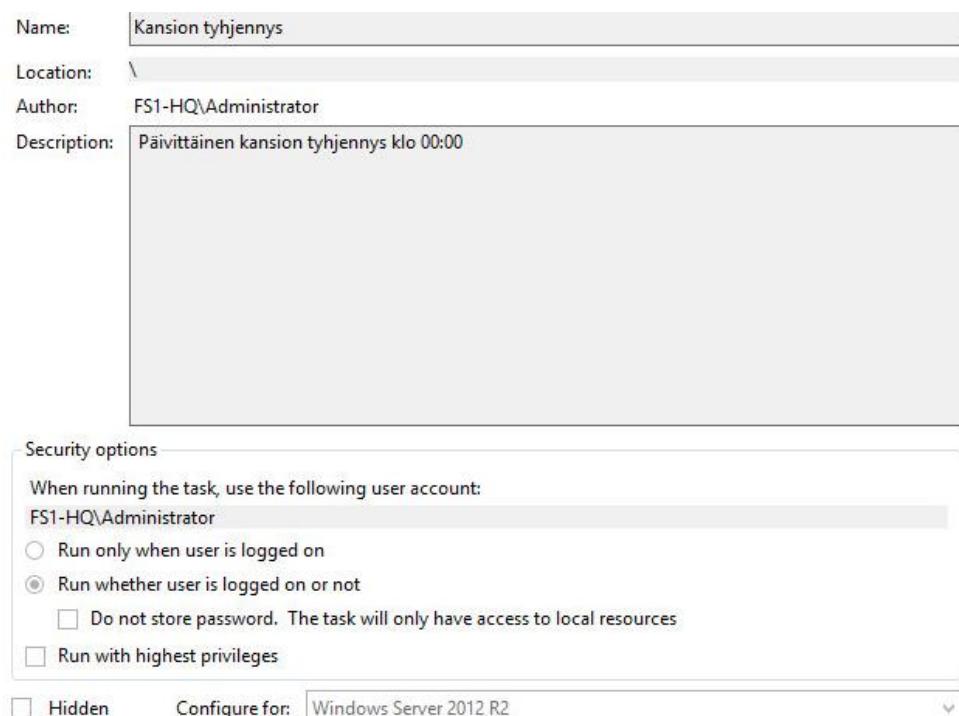
5.3.1 Yleisen levyjaon tyhjennys

Tyhjennys suoritettiin tekemällä simppeli Windows Powershell scripti, joka laitettiin osoittamaan oikeaan kansioon ja poistamaan kaikki tiedostot kyseistä kansiosta. Todennus on kuviossa 42.

```
poisto - Notepad
File Edit Format View Help
Remove-Item E:\Shares\Yleinen\* -recurse
```

Kuvio 42. Yleinen kansion tyhjennys scripti

Käyttäämme Windowsin Task Scheduleria laitoimme sen ajamaan edellä mainitun scrip-
tin joka päivä klo 00:00. Käyttäjien ei tarvitse olla kirjautuneena koneelle, jotta tyh-
jennys alkaisi. Todennukset löytyvät kuvioista 43 ja 44. Todennukset otettiin Task
Schedulerista.



Kuvio 43. Käyttäjän sisäänkirjautumisen todennus

Trigger	Details	Status
Daily	At 0:00 every day	Enabled

Kuvio 44. Ajastimen todennus

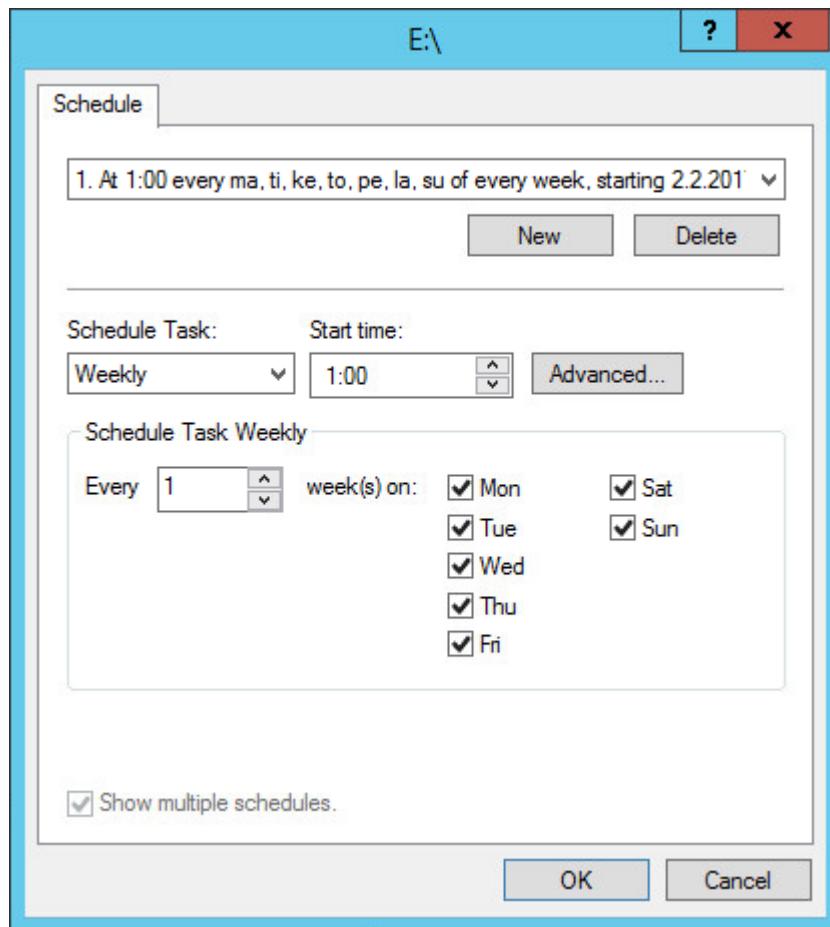
Alla olevasta kuvista 45 löytyy todennus Powershellin ajamisesta ja mikä scripti aje-
taan. Määrittelimme, että task scheduler avaa ohjelman Powershell ja käyttää lisä ar-
gumenttia poisto.ps1 scriptiä.

Action	Details
Start a program	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe C:\scripts\poisto.ps1

Kuvio 45. Todennus ajettavista toiminnoista

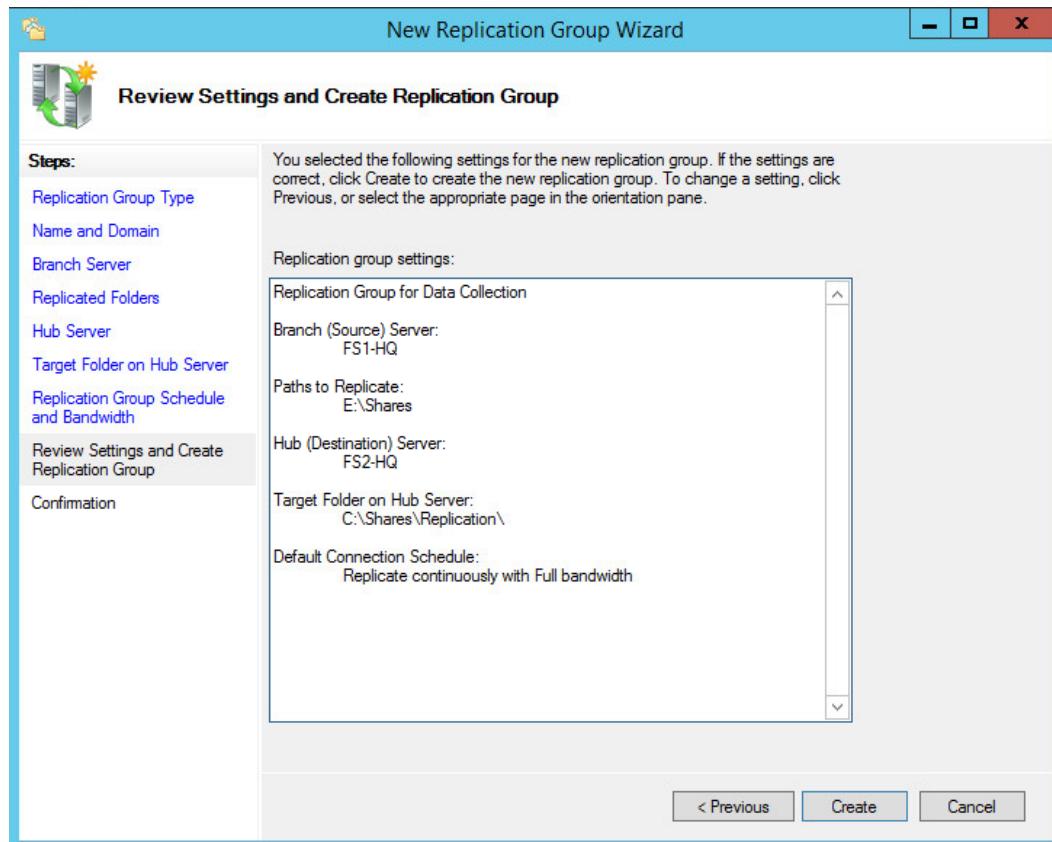
5.3.2 Tiedostopalvelimen FS1 backup

Tiedostopalvelin FS1:lle luotiin Volume Shadow Copy, jolla jaossa olevien kansioiden varmuuskopiointi ajoitettiin klo.01.00 joka yö. Varmuuskopiosta tulee vain paikallinen, joten se ei ole laiterikon sattuessa turvallisimpien vaihtoehto. (kts. Kuvio 46)



Kuvio 46. Volume Shadow Copy ajoitettu joka yö klo.01.00

FS2:lle luotiin replikointi käyttäjien ja ryhmien levyjaoista, jotka sijaitsevat FS1:llä. Pystymme varmistamaan tiedostojen säilymisen, vaikka FS1 hajoaisi kokonaan. (kts. Kuvio 47)



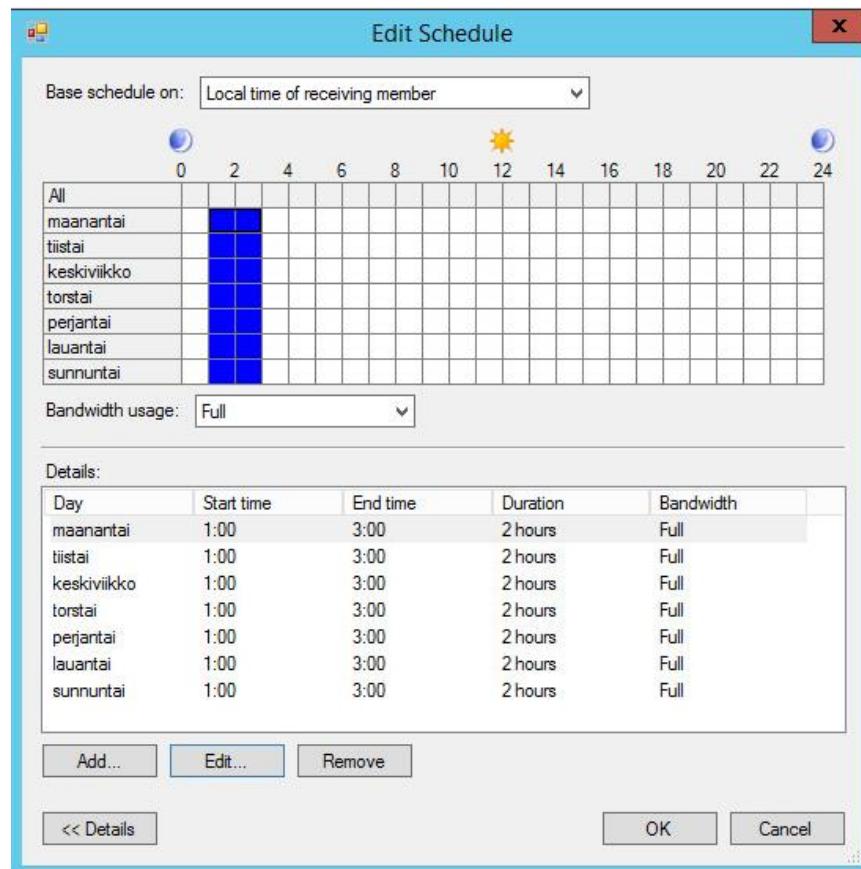
Kuvio 47. FS1 replikointi FS2:lle

Kuviossa 48 on esitetty replikoitava asema, sekä kohdeserveri.

Fileservu1 (papankki.com)					
Memberships	Connections	Replicated Folders	Delegation		
2 entries					
State	Local Path	Membership Status	Member	Replicat...	Staging Qu...
■ State: Normal (2 items)					
	E:\Shares	Enabled	FS1-HQ	Shares	4,00 GB
	C:\Shares\Replication\Shares	Enabled	FS2-HQ	Shares	4,00 GB

Kuvio 48. Todennus replikoinnista

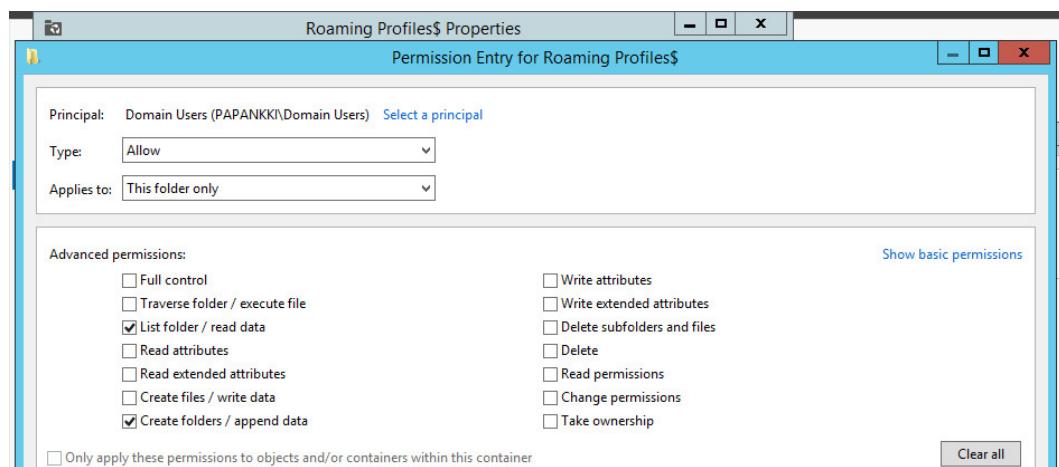
Replikointi on ajoitettu jokaiselle viikonpäivälle klo.01.00. Yöllä saamme kaiken kais-tan käyttöömme replikoinnin nopeuttamiseksi. Tänä ajankohtana yrityksessä ei myöskään työskentele ketään. (kts. Kuvio 49)



Kuvio 49. Replikointi ajoitettu klo.01.00 joka päivä

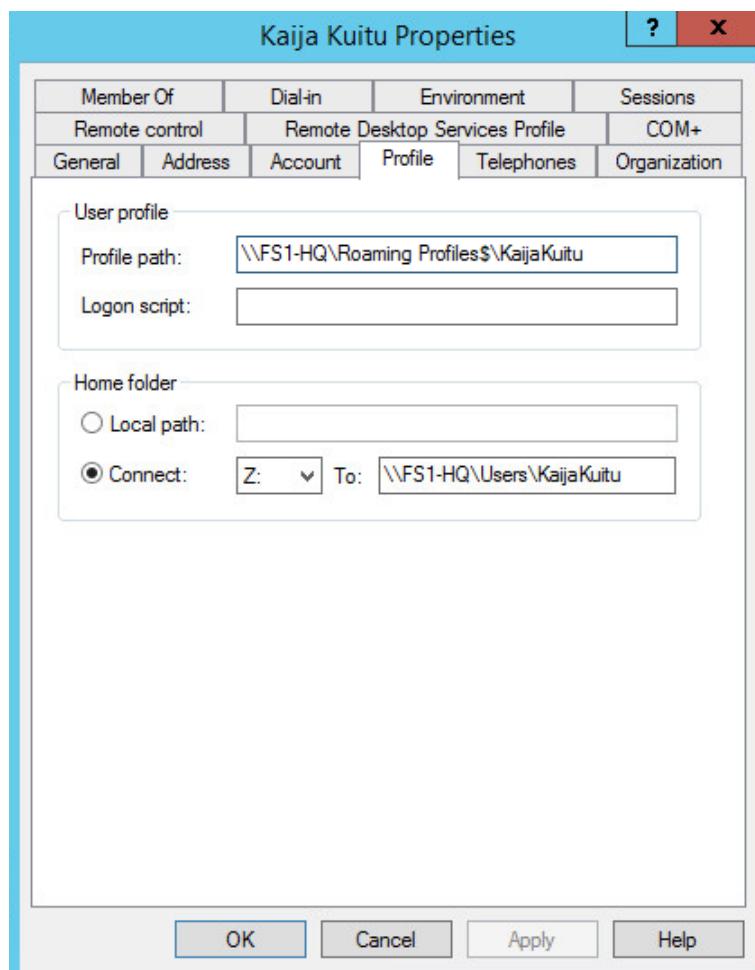
5.3.3 Roaming User

Roaming- profiles palvelun teko aloitettiin tekemällä Roaming- profiles kansio FS1-HQ- palvelimelle ja asettamalla oikeudet kansioon. Tätä on havainnollistettu kuviossa 50.



Kuvio 50. Roaming profiles kansio tehty FS1-HQ:lle

Tämän jälkeen asetetaan kansion asetukset käyttäjän profiiliin DC1-HQ palvelimella (kts. Kuvio 51).



Kuvio 51. Kansiopolun liittäminen

Lopuksi kirjauduttiin Kaija Kuidun käyttäjällä Windows 7- työasemalle ja luotiin työpöydälle testitiedosto. Tämän jälkeen kirjauduttiin uudelleen toiselle työasemalle ja tiedosto latautui automaattisesti työpöydälle. Tämän jälkeen Profile path liitettiin jo-kaiseen käyttäjään. (kts. Kuvio 52 ja 53).



Kuvio 52. Testitiedosto säilynyt työpöydällä konetta vaihdettaessa

```

RSOP data for PAPANKKI\KalleKytkin on HQ-PC2 : Logging Mode
-----
OS Configuration: Member Workstation
OS Version: 6.1.7600
Site Name: N/A
Roaming Profile: \\FS1-HQ\Roaming Profiles$\KalleKytkin.U2
Local Profile: C:\Users\KalleKytkin
Connected over a slow link?: No

USER SETTINGS
-----
CN=Kalle Kytkin,OU=Käyttäjät,OU=ATK-tuki,DC=papankki,DC=com
Last time Group Policy was applied: 3.2.2017 at 9:43:29
Group Policy was applied from: DC1-HQ.papankki.com
Group Policy slow link threshold: 500 kbps
Domain Name: PAPANKKI
Domain Type: Windows 2000

Applied Group Policy Objects
-----
Default Domain Policy
Ryhmäkäytänteet
Konttori-levyjako
ATK-levyjako
Ekonomistit-levyjako
Johtajat-levyjako

The following GPOs were not applied because they were filtered out
-----
Yleinenlevy
Filtering: Disabled (GPO)

Local Group Policy
Filtering: Not Applied (Empty)

The user is a part of the following security groups
-----
Domain Users
Everyone
BUILTIN\Users
NT AUTHORITY\INTERACTIVE
CONSOLE LOGON
NT AUTHORITY\Authenticated Users
This Organization
LOCAL
ATK-tuki
UPN Users
Ekonomistit_RW
Konttori_RW
^ATV_L1_2017

```

Kuvio 53. Roaming profiilin haun todennus

5.4 VyOS

VyOS on avoimeen lähdekoodiin perustuva käyttöjärjestelmä, joka voidaan asentaa fyysiseen laitteistoon, virtuaalikoneelle tai pilveen. Se perustuu GNU/Linuxiin ja siihen liittyy sovelluksia esim. Quagga, ISC DHCPD, OpenVPN ja StrongS/WAN. (VyOS. N.d.)

VyOS muistuttaa enemmän perinteistä reititintä, joka keskittyy antamaan dynaamista tukea kattaville reititys ominaisuuksille, kuten dynaaminen reititysprotokolla ja komentorivi rajapinta. (VyOS. N.d.)

VyOS backupin tekeminen aloitettiin ensin scriptistä ja tuon jälkeen määritettiin task schedulerilla, miten usein backupit haluttiin tehdä. Nämä on todennettu kuvioissa 54 ja 55.

```
#!/bin/vbash
source /opt/vyatta/etc/functions/script-template

run show configuration commands > ${HOME}/$(date +%Y%m%d-%H%M%S)_${(hostname)}.txt
cat /config/config.boot > /home/vyos/$(date +%d%m%y)_${(hostname)}_config.boot.txt
```

Kuvio 54. VyOs backup scripti

```
vyos@R1-HQ# ls -l /home/vyos
total 16
-rw-rw-r-- 1 vyos vyattacfg 0 Feb 2 07:23 020217-072125_R6-HQ.config.boot.tx
t
-rw-rw-r-- 1 vyos vyattacfg 3508 Feb 2 07:21 020217-072125_R6-HQ.txt
-rw-rw-r-- 1 vyos vyattacfg 3807 Feb 2 07:31 02022017-073117_R6-HQ.config.boot.
txt
-rw-rw-r-- 1 root root 4753 Feb 7 00:00 07021486425608_R6-HQ.config_boot.t
xt
[edit]
vyos@R1-HQ# _____
```

Kuvio 55. VyOs backup todennus

5.5 VyOS NAT

VyOS konfiguraatioon luotiin NAT-säännöt sisäverkosta tuleville IP-osoitteille. Sääntöjen mukaan kaikki ulosmenevät yhteydet muutetaan operaattorilta saamaamme 192.168.17.16 osoitteeseen. Riippumatta siitä, mistä VLAN:sta liikennöidään, ulospäin näkyy vain yrityksen julkisen osoitteen liikennöinti. (kts. Kuvio 56)

```

vyos@R1-HQ# show nat
source {
    rule 10 {
        description NAT-to-SRV
        outbound-interface eth0
        source {
            address 10.100.0.0/24
        }
        translation {
            address masquerade
        }
    }
    rule 20 {
        description NAT-to-WS
        outbound-interface eth0
        source {
            address 10.0.0.0/24
        }
        translation {
            address masquerade
        }
    }
    rule 30 {
        description NAT-to-DMZ
        outbound-interface eth0
        source {
            address 192.18.235.0/24
        }
        translation {
            address masquerade
        }
    }
}

```

Kuvio 56. VyOS:lle luodut NAT-säännöt

5.6 Public Key Infrastructure avainten luonti ja sertifikointi

Päätteliin käyttää OpenSSL ohjelmaa julkisten ja privaattien avainten luontiin sekä sertifikaattipyyntöjen tekemiseen. Luomme jokaiselle ryhmämme jäsenelle omat avainparit käyttäen Rivest Shamir Adleman (RSA) salausalgoritmia. Samalla myös luotiin käyttäjien sertifikaattipyyntö, johon määriteltiin jäsenien tietoja (Kuvio 57). Kuviossa 58 kuvataan kaikkien jäsenten avain- ja csr-tiedostot.

```

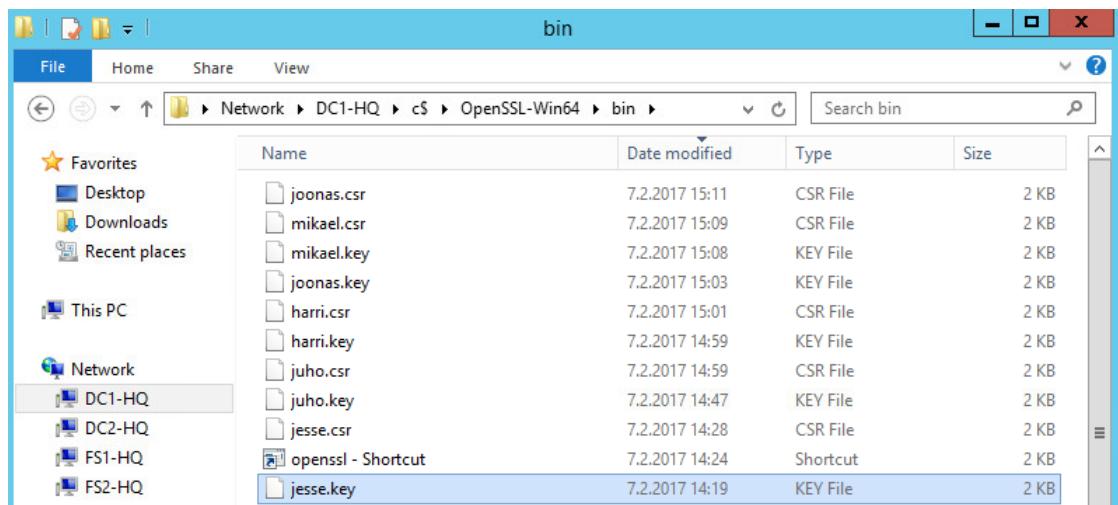
OpenSSL> genrsa -out harri.key 2048
Generating RSA private key, 2048 bit long modulus
.....+
.....+
e is 65537 <0x010001>
OpenSSL> req -new -key harri.key -out harri.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:FI
State or Province Name (full name) [Some-State]:Lansi-Suomi
Locality Name (eg, city) []:Seinajoki
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Papankki.com
Organizational Unit Name (eg, section) []:ATK-tuki
Common Name (e.g. server FQDN or YOUR name) []:Harri
Email Address []:harri@papankki.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Kissa123
An optional company name []:Papankki.com
OpenSSL> -

```

Kuvio 57. Harrin RSA-avainparin luonti ja sertifikaattipyyntö



Kuvio 58. Jäsenten avaimet ja csr-tiedostot

Luotiin CA avain papankki.ca.key jolla allekirjoitetaan käyttäjien csr pyynnöt jatkossa sekä papankki.ca.csr sertifointipyyntö, joka allekirjoitetaan itse papankki.ca.key tiedostolla luoden näin itseallekirjoitettu sertifikaatti (Kuvio 59). Seuraavaksi allekirjottiin käyttäjän harri.csr sertifointipyyntö papankki.ca.key avaimella luoden näin harri.crt tiedoston. Lähempä tarkastelu harri.cert sertifikaatin sisällöstä kuviossa 60.

```

OpenSSL> req -new -key papankki.ca.key -out papankki.ca.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name <2 letter code> [AU]:FI
State or Province Name <full name> [Some-State]:KS
Locality Name <eg, city> []:JKL
Organization Name <eg, company> [Internet Widgits Pty Ltd]:papankki
Organizational Unit Name <eg, section> []:papankki
Common Name <e.g. server FQDN or YOUR name> []:papankki
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:papankki
OpenSSL> x509 -req -days 100 -in papankki.ca.csr -signkey papankki.ca.key -out p
apankki.crt
Signature ok
subject=C = FI, ST = KS, L = JKL, O = papankki, OU = papankki, CN = papankki
Getting Private key

```

Kuvio 59. Papankki sertifikaatin luonti

```

OpenSSL> x509 -in harri.crt -text -noout
Certificate:
Data:
Version: 1 (0x0)
Serial Number:
    06:5B:64:89:8F:65:14:8d
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = FI, ST = Lansi-Suomi, L = Seinajoki, O = Papankki.com, OU =
ATK-tuki, CN = Harri, emailAddress = harri@papankki.com
Validity
    Not Before: Feb 15 10:36:51 2017 GMT
    Not After : May 26 10:36:51 2017 GMT
Subject: C = FI, ST = Lansi-Suomi, L = Seinajoki, O = Papankki.com, OU =
ATK-tuki, CN = Harri, emailAddress = harri@papankki.com
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
            Modulus:
                00:d3:96:36:91:2f:78:79:41:21:97:09:df:56:4e:
                30:ad:4b:75:57:c1:d2:d3:e1:7a:78:62:6e:21:20:
                c7:5e:b2:de:fc:13:eb:58:6d:75:0d:ab:29:8b:53:
                b3:3f:91:ce:26:85:98:89:d1:bd:f6:fe:98:5e:74:
                a0:1e:cc:28:b6:d3:7f:7e:41:7d:fe:54:12:51:
                2b:1b:25:a0:a9:94:65:6f:2d:f0:6e:7a:0d:4b:
                c6:6a:4e:eb:53:c1:3f:3a:ee:0f:05:dc:28:a7:8e:
                11:12:b8:91:eb:0f:7e:37:77:ad:ac:7b:8a:d8:85:
                0d:23:73:00:df:ca:2d:0b:91:48:ab:ab:7a:1e:5c:
                c1:96:6c:98:41:97:79:a7:47:15:b4:f0:b2:e6:20:
                5b:dd:dd:6:24:4e:d1:fc:19:a9:8:f:d:c4:3e:5b:
                3a:5d:d3:b4:6:9e:6a:5a:64:e2:b7:ec:74:16:8e:
                af:4a:26:a3:c6:ab:91:91:a9:49:f2:53:ec:c1:9:
                df:6c:46:54:53:c7:ed:78:45:4d:bf:f2:48:d:00:
                39:1e:47:c9:9c:cd:af:1:e7:3f:0e:62:6b:dc:ce:66:
                49:0e:0f:df:b4:1a:as:05:26:0:43:47:ff:53:21:
                9:c:ac:0e:id:72:90:a9:03:af:17:04:03:a3:0d:1e:
                fc:af
            Exponent: 65537 (0x10001)
Signature Algorithm: sha256WithRSAEncryption
    a2:8d:4d:3:84:d3:1a:10:35:ee:ba:e5:f6:eb:47:50:47:34:
    91:2d:98:e4:57:d6:20:c6:66:10:48:18:7e:7a:ae:da:e0:97:
    cc:ae:34:53:99:dd:3:32:a3:97:ff:49:46:f4:ed:1b:98:86:
    04:b7:9c:d0:9b:22:f0:27:ae:04:69:c0:40:50:51:52:d2:bd:
    a1:if:18:12:f5:17:el:54:7b:85:74:d6:f1:8a:ee:84:5d:2e:
    4f:18:10:ff:7:4:e:03:df:64:de:f6:2b:41:e1:88:31:h1:dh:
    34:94:9a:48:5:d:d0:aa:06:97:31:c6:08:e1:7:b7:e0:f4:d2:
    00:44:bc:ee:8:e:7:b:bd:4d:61:52:18:32:40:40:ce:5c:9b:ec:
    e0:e5:45:57:07:e6:74:ab:e2:ad:1:2f:7f:31:c7:70:28:23:
    00:02:01:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
    21:72:13:1a:90:ab:01:da:d2:f5:be:2a:64:2e:40:9a:20:5c:
    76:4d:1f:cc:eb:8c:cf:f9:72:68:90:9a:f1:71:0b:57:s2:
    ba:cb:ca:6f:20:db:0d:2c:66:cb:fb:0b:bd:40:e8:71:8c:93:
    b3:41:cf:9b:80:e1:7a:fa:a5:b7:a7:a7:b5:14:ff:22:ef:2d:
    9e:7f:fc:44

```

Kuvio 60. Harri.crt tarkastelu

5.6.1 Certification Authority

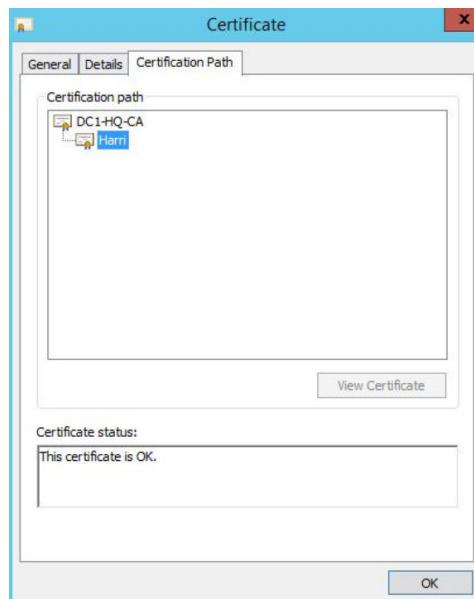
Kokeiltiin myös Windows Server 2012 R2 Certification Authority roolia sertifikaattien tekemiseen, jota varten HQ-DC1:stä tehtiin Root CA, joka vastaa tällä kertaa sertifiointipyynnöistä. Tätä varten roolin asennuksessa luotiin DC1:lle oma yksityinen

avain, sekä sertifikaatti. Kun CA:n sertifikaatti on luotu, tehdään uusi sertifikaattipohja käyttäjille user templatesta, jota jaetaan tuleville käyttäjille (Kuvio 61).

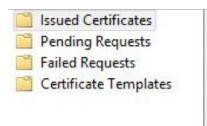
Name	Intended Purpose
Kayttajat	Client Authentication, Secure Email, Encrypting File System
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentication, Smart Card Logon
Kerberos Authentication	Client Authentication, Server Authentication, Smart Card Logon
EFS Recovery Agent	File Recovery
D:\var\ccc	Encrypting File System

Kuvio 61. Kayttajat sertifikaattipohja

Seuraavaksi käydään käyttäjänä pyytämässä sertifikaattia certmgr.msc työkalulla, jolloin valitaan luotu Kayttajat sertifikaattipohja ja lähetään pyyntö CA:lle, joka hyväksyy sertifikaattipyynnön ja lisää sen issued certificates kansioonsa. Esimerkkinä Harrin sertifikaatin sertifointipolku kuviossa 62. Näin tehtiin kaikille ryhmän jäsenille, joka voidaan todentaa katsomalla DC1-HQ-CA:n Issued Certificates-listaa (Kuvio 63.).



Kuvio 62. Harrin sertifikaattipolku



5	PAPANKKI\harri	-----BEGIN CERTI...	Kayttajat (1.3.6.1.4.1....	1300000005d31...	15.2.2017 12:44		15.2.2018 12:44
6	PAPANKKI\juho	-----BEGIN CERTI...	Kayttajat (1.3.6.1.4.1....	130000000682c...	15.2.2017 12:53		15.2.2018 12:53
7	PAPANKKI\jesse	-----BEGIN CERTI...	Kayttajat (1.3.6.1.4.1....	13000000072ae...	15.2.2017 12:55		15.2.2018 12:55
8	PAPANKKI\joonas	-----BEGIN CERTI...	Kayttajat (1.3.6.1.4.1....	1300000008b16...	15.2.2017 12:56		15.2.2018 12:56
9	PAPANKKI\mikael	-----BEGIN CERTI...	Kayttajat (1.3.6.1.4.1....	1300000009161...	15.2.2017 12:57		15.2.2018 12:57

Kuvio 63. Käyttäjien sertifikaatit

5.7 Tietokantapalvelin

Pystytettiin Ubuntu 16.04-palvelin ja luotiin suunnitelman mukainen MySQL-tietokanta taulukoineen Asiakas, Asiakastili sekä Tili (Kuvio 64.). Palvelin nostettiin myös papankki.com toimialueeseen, käyttäen mm krb5-user, sssd, samba sekä ntp-applikaatioita (Kuvio 65.).

```
Database changed
mysql> show tables;
+-----+
| Tables_in_PANKKI |
+-----+
| ASIAKAS          |
| ASIAKASTILI      |
| TILI              |
+-----+
3 rows in set (0.06 sec)

mysql> exit
Bye
ubuntu@HQ-SQL:/etc$ _
```

Kuvio 64. MySQL tietokanta palvelimella

```
ubuntu@HQ-SQL:/etc$ sudo net ads info
LDAP server: 10.100.0.2
LDAP server name: DC1-HQ.papankki.com
Realm: PAPANKKI.COM
Bind Path: dc=PAPANKKI,dc=COM
LDAP port: 389
Server time: Tue, 28 Feb 2017 13:28:39 EET
KDC server: 10.100.0.2
Server time offset: 0
ubuntu@HQ-SQL:/etc$
```

Kuvio 65. Ubuntu-palvelin nostettu papankki domainiin

Alla olevassa kuviossa todennus SQL-palvelimella olevasta varmuuskopointi scriptistä (Kuvio 66.). Määriteltiin crontab -e tiedostoon scriptin ajohetkeksi, joka päivä klo 02:00 lisäämällä alla oleva rivi tiedostoon.

```
00 2 * * * /home/bin/backup.sh
```

```
GNU nano 2.5.3                               File: backup.sh

#!/bin/bash
user="root"
password="Kissa123"
host="localhost"
db_name="PANKKI"
backupfolder="/home/backups/mysql"
date=$(date +"%d-%m-%Y")
logfile="$backupfolder/backup_log/backup_log_${date}_%d-%m-%Y"
mysqldump --user=$user --password=$password --host=$host $db_name > $backupfolder/$db_name:$date.sql
echo "mysql varmuuskopointi aloitettu ($date)" >> $logfile
echo "mysql varmuuskopointi lopetettu ($date)" >> $logfile
```

Kuvio 66. Backup.sh scripti

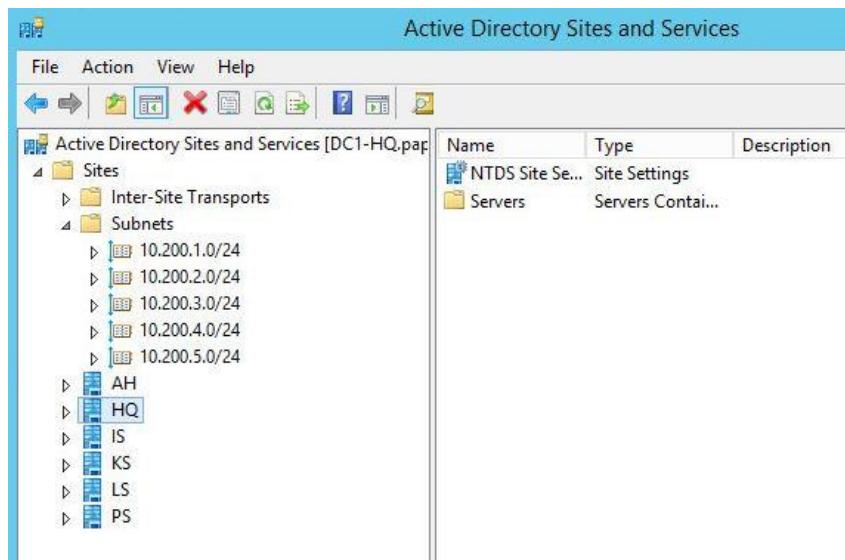
Alla todennus (Kuvio 67.) että varmuuskopointi on toimiva ja varmuuskopio tietokannan joka päivä.

```
ubuntu@HQ-SQL:/home/backups/mysql$ ls -l
total 88
drwxr-xr-x 2 root root 4096 Mar 29 02:00 backup_log
-rw-rw-rwx 1 root root 467 Mar  9 22:32 backup.sh
-rw-r--r-- 1 root root 3643 Mar 10 09:18 PANKKI:10-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 11 02:00 PANKKI:11-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 12 02:00 PANKKI:12-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 13 02:00 PANKKI:13-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 14 02:00 PANKKI:14-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 15 02:00 PANKKI:15-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 16 02:00 PANKKI:16-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 17 02:00 PANKKI:17-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 18 02:00 PANKKI:18-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 19 02:00 PANKKI:19-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 20 02:00 PANKKI:20-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 21 02:00 PANKKI:21-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 22 02:00 PANKKI:22-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 23 02:00 PANKKI:23-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 24 02:00 PANKKI:24-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 25 02:00 PANKKI:25-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 26 02:00 PANKKI:26-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 27 02:00 PANKKI:27-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 28 02:00 PANKKI:28-03-2017.sql
-rw-r--r-- 1 root root 3643 Mar 29 02:00 PANKKI:29-03-2017.sql
```

Kuvio 67. Varmuuskopointi todennus

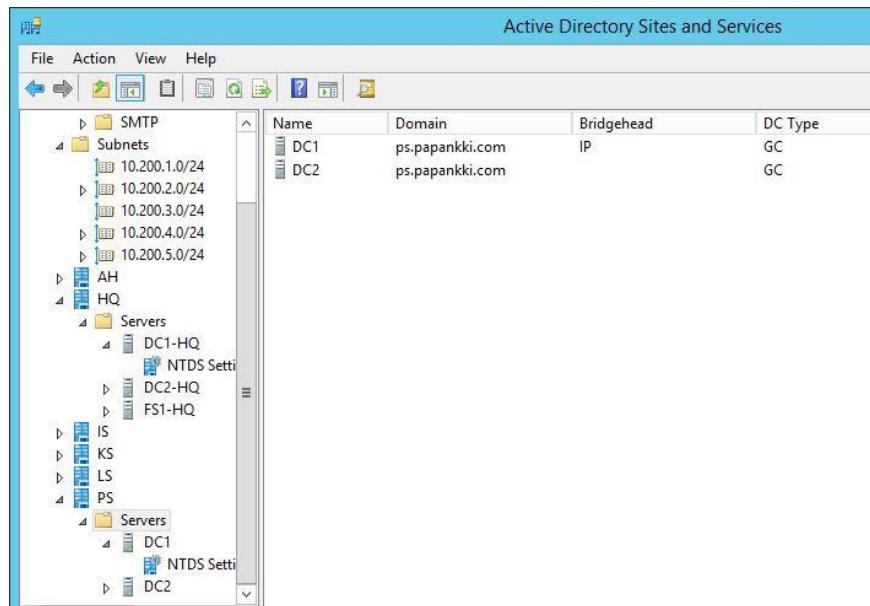
5.8 Branchien pystytyks

Pääkonttorin ohjainpalvelimelle luotiin jokaista branchia varten oma subnet. Myös jokainen branch on lisätty ohjainpalvelimelle omana Site:na (kts. Kuvio 68).



Kuvio 68. Branchille luodut subnetit

Branchien ja pääkonttorin välille luotiin Bridgehead Server- yhteydet, jotta replikoinnin yhteydessä ei syntyisi ongelmia (kts. Kuvio 69).



Kuvio 69. Pääkonttorin ja branchien välille luodut Bridgehead Serverit

Taulukossa 5 on esitetty pää- ja sivukonttorien välille luotavaa IPSec- tunnelia varten suunnittelimme privaatti osoitejako, tunnelin numero ja Router ID.

Taulukko 5. Toimipaikkojen IPSec- tunnelin osoitteet, tunnelin nro ja Router ID

	KS:	LS:	IS:	AH:	PS:
HQ router	172.16.1.1	172.16.2.1	172.16.3.1	172.16.4.1	172.16.5.1
Branch router	172.16.1.2	172.16.2.2	172.16.3.2	172.16.4.2	172.16.5.2
Tunnel nro.	1	3	4	5	0
Router ID	4.4.4.4	7.7.7.7	3.3.3.3	5.5.5.5	9.9.9.9

Kuviossa 70 on esitetty pääkonttorin HQ ja branchien väliset IPSec-tunnelit.

```
192.168.44.227                               192.168.17.16

Tunnel  State  Bytes Out/In   Encrypt  Hash    NAT-T  A-Time  L-Time  Proto
-----  -----  -----  -----  -----  -----  -----  -----  -----
 3      up     364.9K/453.6K  aes128  md5    no     3932   86400   gre

Peer ID / IP                                Local ID / IP
-----
192.168.44.228                               192.168.17.16

Tunnel  State  Bytes Out/In   Encrypt  Hash    NAT-T  A-Time  L-Time  Proto
-----  -----  -----  -----  -----  -----  -----  -----  -----
 4      up     315.1K/376.1K  aes128  md5    no     3344   86400   gre

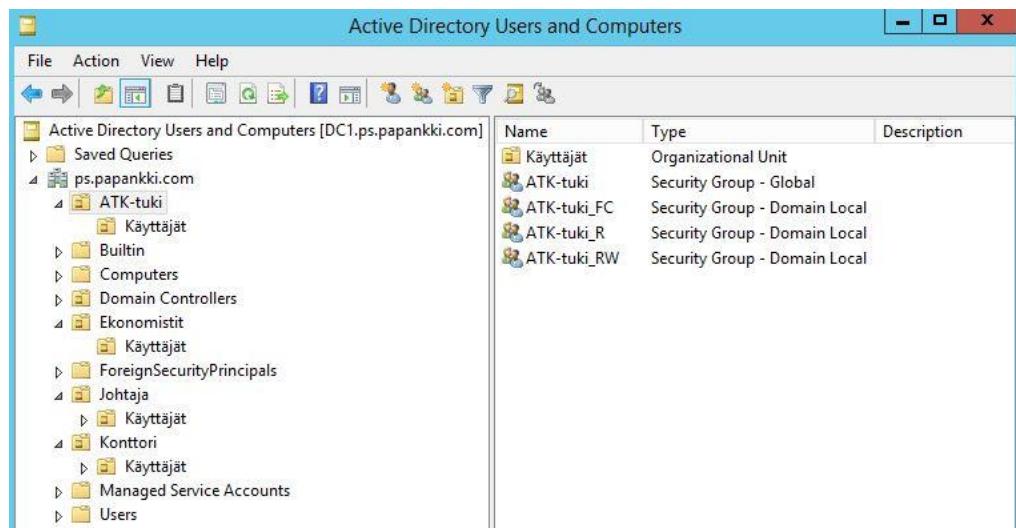
Peer ID / IP                                Local ID / IP
-----
192.168.44.229                               192.168.17.16

Tunnel  State  Bytes Out/In   Encrypt  Hash    NAT-T  A-Time  L-Time  Proto
-----  -----  -----  -----  -----  -----  -----  -----  -----
 0      up     1.1M/916.4K   aes128  md5    no     4286   86400   gre
```

Kuvio 70. Pääkonttorin ja branchien väliset IPSec-tunnelit

5.9 Pohjois-Suomen PS ohjainpalvelimet DC1 ja DC2

Pohjois-Suomen konttorin pystytys aloitettiin asentamalla ohjainpalvelimet DC1 ja DC2. Ohjainpalvelin nostettiin papankki.com domainiin ja annettiin staattiset IP-osoitteet. Ohjainpalvelin DC1:lle luotiin käyttäjät Kuvion 71 mukaisesti.



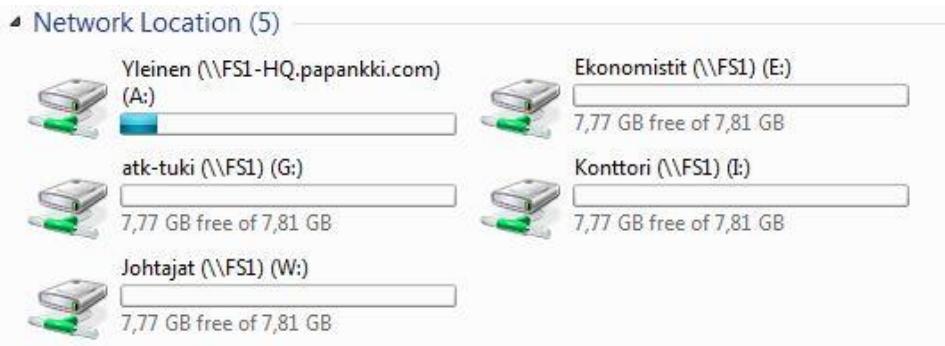
Kuvio 71. Pohjois-Suomen käyttäjät

Testasimme toimintaa Pohjois-Suomen työasemalta kirjautumalta, joka on nostettu papankki.com domainiin. Testikäyttäjänä toimii RoopeRamppi (kts. Kuvio 72).



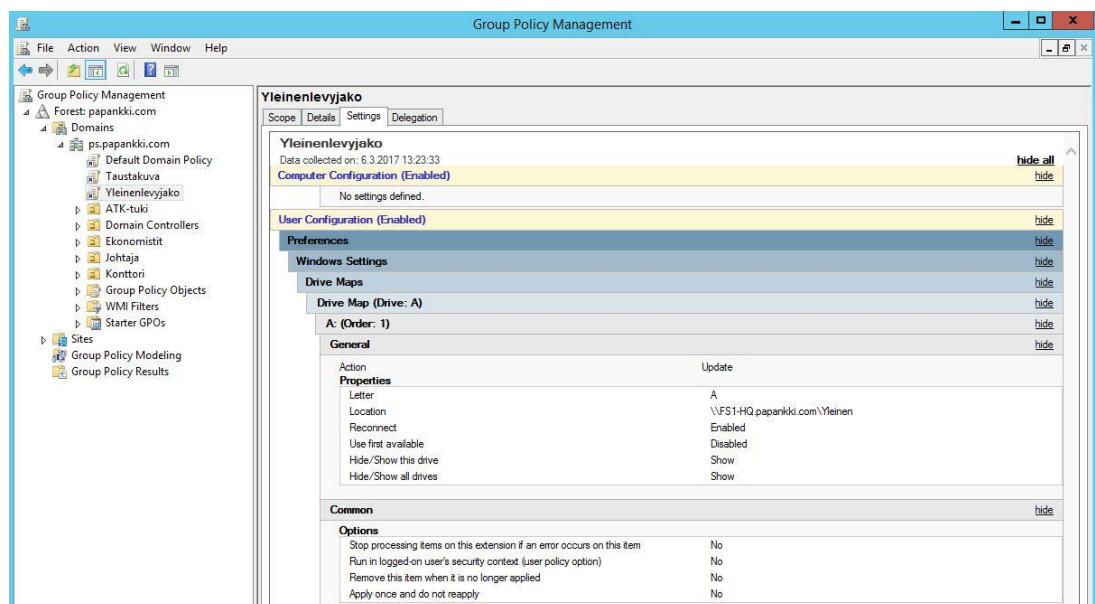
Kuvio 72. Käyttäjän kirjautuminen ps.papankki.com domainiin.

Pohjois-Suomen käyttäjille luotiin levyjaot Taulukko 4 mukaisesti. Yleinen levyjako näkyy kaikille käyttäjille pää- ja sivukonttoreilla. Yleinen levyjako (kts. Kuvio 73) määritettiin näkymään kaikille käyttäjillä Group Policy Managerin kautta.



Kuvio 73. Yleinen levyjako

Kuviossa 74 on esitetty yleiselle levyjaolle luotu GPO. Levyjako sijaitsee pääkonttorin tiedostopalvelin FS1:llä ja se on määritetty näkymään jokaisen sivukonttorin työntekijällä.



Kuvio 74. Yleisen levyjaon GPO Pohjois-Suomen ohjainpalvelin DC1:ltä

Kaikille yrityksen työntekijöille määritettiin sama työasemien taustakuva, joka latautuu oman toimipaikan tiedostopalvelimelta (kts. Kuvio 75). Taustakuva ei jostain mystisestä syystä latautunut käyttäjien työpöydälle, mutta näkyi Windowsin teemoissa normaalisti. Todennus otettu tästä syystä Windowsin teemoista.

Change the visuals and sounds on your computer

Click a theme to change the desktop background, window color,



Kuvio 75. PS toimipisteen käyttäjän taustakuva

5.9.1 Pohjois-Suomen IPSec tunneli

Jokaisen toimipisteen ja pääkonttorin välille on luotava IPSec-tunneli, jotta ne voivat liikkennöidä keskenään. PS:n ja HQ:n välille luotiin tunneli ja annettiin molempien päihin sama salausavain. Tunnelin toimivuus voidaan testata molempien päiden VyOS-reitittimiltä show vpn ipsec sa-komennolla (kts. Kuvio 76).

```
vyos@R1-PS# run show vpn ipsec sa
Peer ID / IP                                Local ID / IP
-----                                         -----
192.168.17.16                               192.168.44.229

Tunnel  State   Bytes Out/In    Encrypt  Hash      NAT-T   A-Time   L-Time   Proto
-----  -----   -----          -----   -----      -----   -----   -----   -----
  0      up      4.1M/3.4M    aes128   md5       no      13660   86400   gre
```

Kuvio 76. Todennus PS:n IPSec tunnelin toimivuudesta.

IPSec-tunnelin luonnin jälkeen testasimme pingata pääkonttorin ohjainpalvelin DC1:tä. Tunneli toimi oikein ja pääkonttorin ohjainpalvelin vastasi pingiin (kts. Kuvio 77).

```
C:\Users\Administrator>ping 10.100.0.2

Pinging 10.100.0.2 with 32 bytes of data:
Reply from 10.100.0.2: bytes=32 time=1ms TTL=126

Ping statistics for 10.100.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Administrator>
```

Kuvio 77. Ping pääkonttorin ohjainpalvelimelta

Jokaiselle sivukonttorille on määritetty OSPF mainostamaan omia sisäverkkojaan, sekä IPSec-tunnelin privaattia osoitetta. Jokaisen sivukonttorin reititin vastaanottaa OSPF-mainostukset ja saa tiedon muista verkoista. Kuviossa 78 Pohjois-Suomen työasemalta on ajettu tracert komento, jossa kysytään reittiä Itä-Suomen ohjainpalvelin DC1:lle.

```
C:\Users\PaavoPerhosjoki>tracert 10.200.3.2

Tracing route to DC1-IS [10.200.3.2]
over a maximum of 30 hops:
  1    <1 ms      <1 ms      <1 ms  10.10.4.1
  2    <1 ms      <1 ms      <1 ms  172.16.5.1
  3      1 ms      1 ms      1 ms  172.16.3.2
  4      1 ms      1 ms      1 ms  DC1-IS [10.200.3.2]

Trace complete.
```

Kuvio 78. Tracert Itä-Suomen ohjainpalvelimelle

5.10 Keski-Suomen KS ohjainpalvelimet DC1 ja DC2

Keski-Suomen konttorin pystytys aloitettiin asentamalla ohjainpalvelimet DC1 ja DC2.

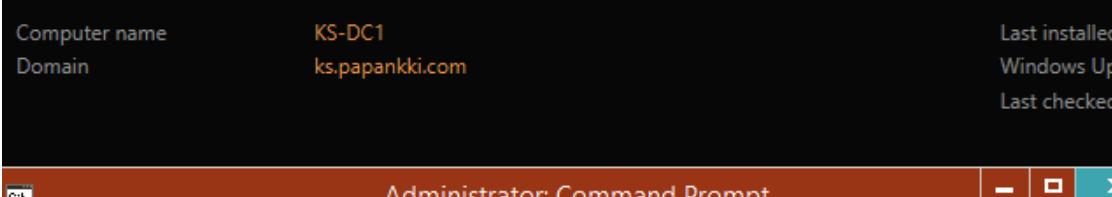
Ohjainpalvelin nostettiin papankki.com domainiin ja annettiin staattiset IP-osoitteet.

(Kts. Kuvio 79)

PROPERTIES				TASKS
For KS-DC1				
Computer name	KS-DC1	Last installed updates	Never	
Domain	ks.papankki.com	Windows Update	Not configured	
		Last checked for updates	Never	
Windows Firewall	Domain: On	Windows Error Reporting	Off	
Remote management	Enabled	Customer Experience Improvement Program	Not participating	
Remote Desktop	Disabled	IE Enhanced Security Configuration	On	
NIC Teaming	Disabled	Time zone	(UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius	
Ethernet	10.200.1.2, IPv6 enabled	Product ID	00252-10000-00000-AA228 (activated)	
Ethernet 2	IPv4 address assigned by DHCP, IPv6 enabled			
Operating system version	Microsoft Windows Server 2012 R2 Standard Evaluation	Processors	Intel(R) Core(TM) i7 CPU	920 @ 2.67GHz
Hardware information	innotek GmbH VirtualBox	Installed memory (RAM)	2 GB	
		Total disk space	24.66 GB	

Kuvio 79. DC1 domain

Kuviossa 80 todennetaan että yhteys toimii Keski-Suomen ja HQ:n välillä.



```

Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 10.100.0.4

Pinging 10.100.0.4 with 32 bytes of data:
Reply from 10.100.0.4: bytes=32 time=1ms TTL=126

Ping statistics for 10.100.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Administrator>

```

Kuvio 80. Ping KS-DC1 to HQ-FS1

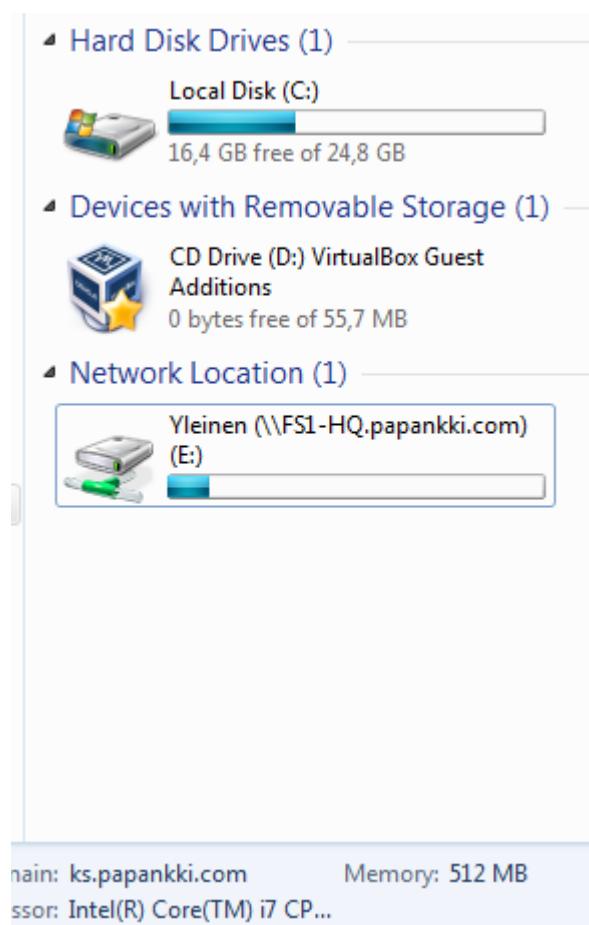
Kuviossa 81 on haettu aika NTP-palvelimelta.

```
vyos@vyos:~$ show date  
Mon Feb 27 13:44:17 EET 2017  
vyos@vyos:~$ _
```



Kuvio 81. NTP KS-VyOS

Kuviossa 82 on kirjauduttu KS-WS1:lle Kalle Keskimaan tunnuksilla.



Kuvio 82. Yleinen levyjako todennus

5.11 Ahvenanmaan palveluiden pystytyks

Omassa branchissä toteutettiin R1-AH, DC1-AH, DC2-AH, FS1-AH, FS2-AH ja Workstation. Ensiksi laitteet pystytettiin ja liitettiin domainiin. Tätä todennetaan kuviossa 83.

```
C:\Users\Administrator>hostname
DC1-AH

C:\Users\Administrator>ping ah-dc2
Pinging AH-DC2.ah.papankki.com [10.200.5.3] with 32 bytes of data:
Reply from 10.200.5.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.200.5.3:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping fs1-ah
Pinging FS1-AH [fe80::9d22:a7fd:ee79:8112%12] with 32 bytes of data:
Reply from fe80::9d22:a7fd:ee79:8112%12: time<1ms
Reply from fe80::9d22:a7fd:ee79:8112%12: time<1ms
Reply from fe80::9d22:a7fd:ee79:8112%12: time<1ms
Reply from fe80::9d22:a7fd:ee79:8112%12: time<1ms

Ping statistics for fe80::9d22:a7fd:ee79:8112%12:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

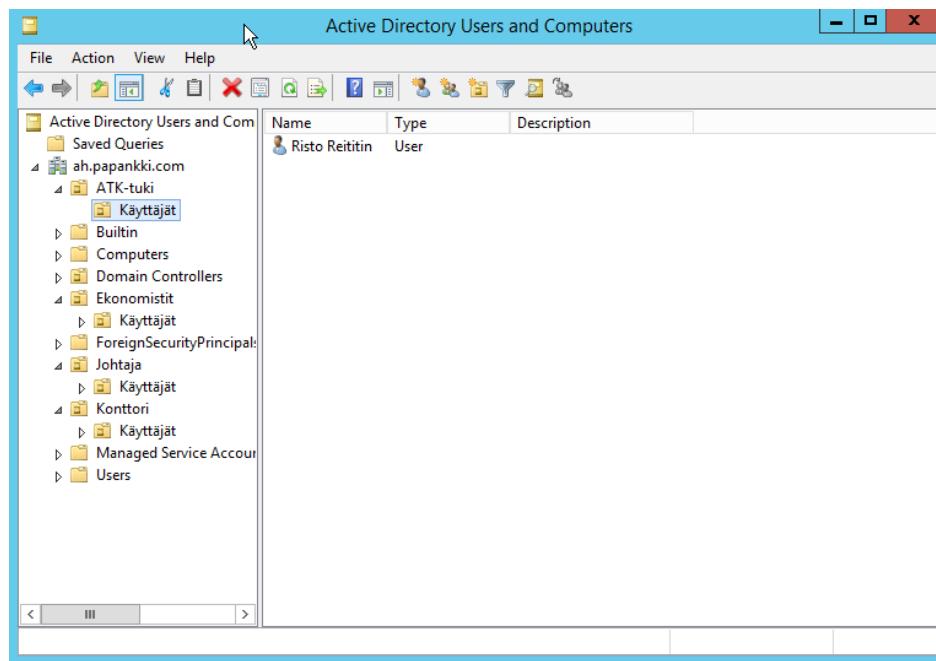
Kuvio 83. Ahvenanmaan palvelinten pingaus.

Seuraavaksi yhdistettiin branch IPSec-tunnelilla päätöimipisteeseen. Tätä todennetaan kuviossa 84.

Peer ID / IP		Local ID / IP							
-----		-----							
192.168.17.16		192.168.44.225							
Tunnel	State	Bytes Out/In	Encrypt	Hash	NAT-T	A-Time	L-Time	Proto	
5	up	1.5M/702.4K	aes128	md5	no	5972	86400	gre	

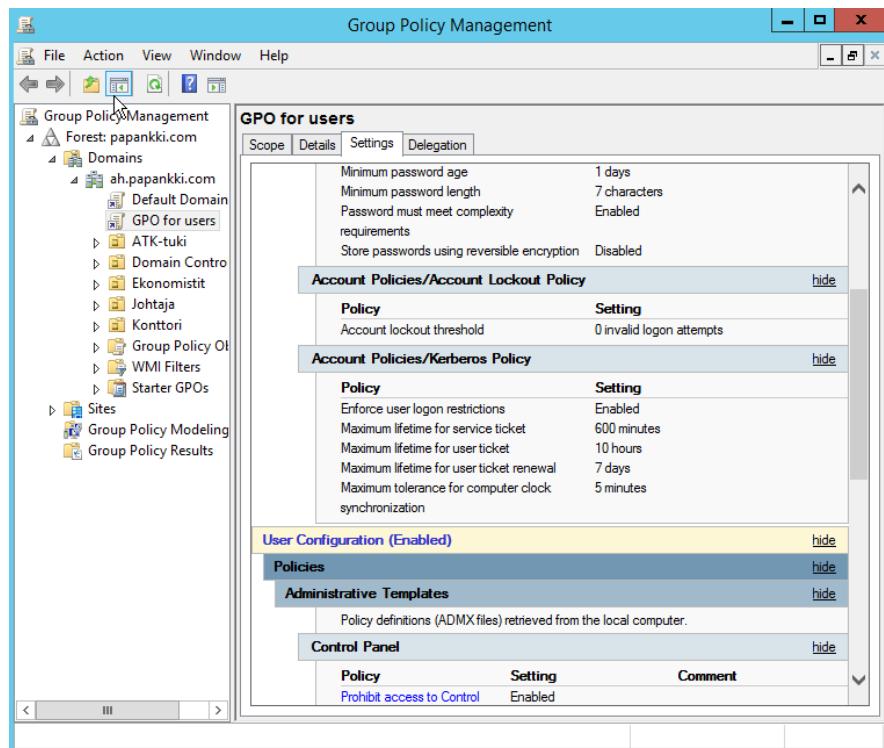
Kuvio 84. IPSec tunneli toiminnassa

Ahvenanmaan DC1:lle lisättiin myös käyttäjät, jota todennetaan kuviossa 85



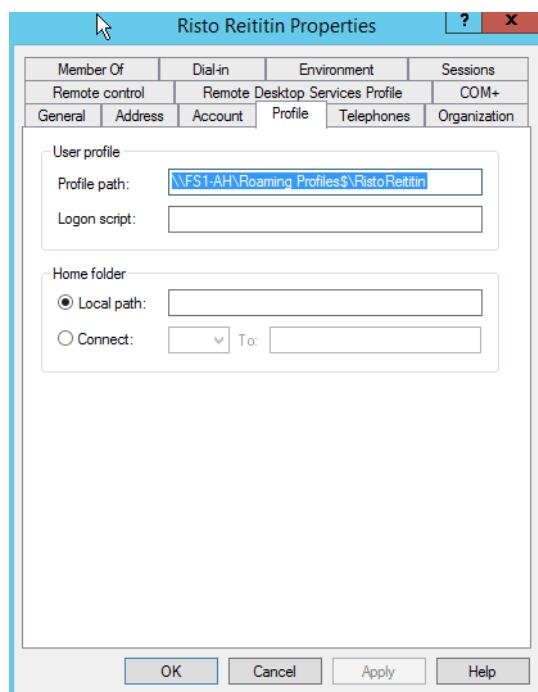
Kuvio 85. Käyttäjät lisätty Ahvenanmaahan

Seuraavaksi lisättiin käyttäjille oikeat oikeudet, jota todennetaan kuviossa 86.



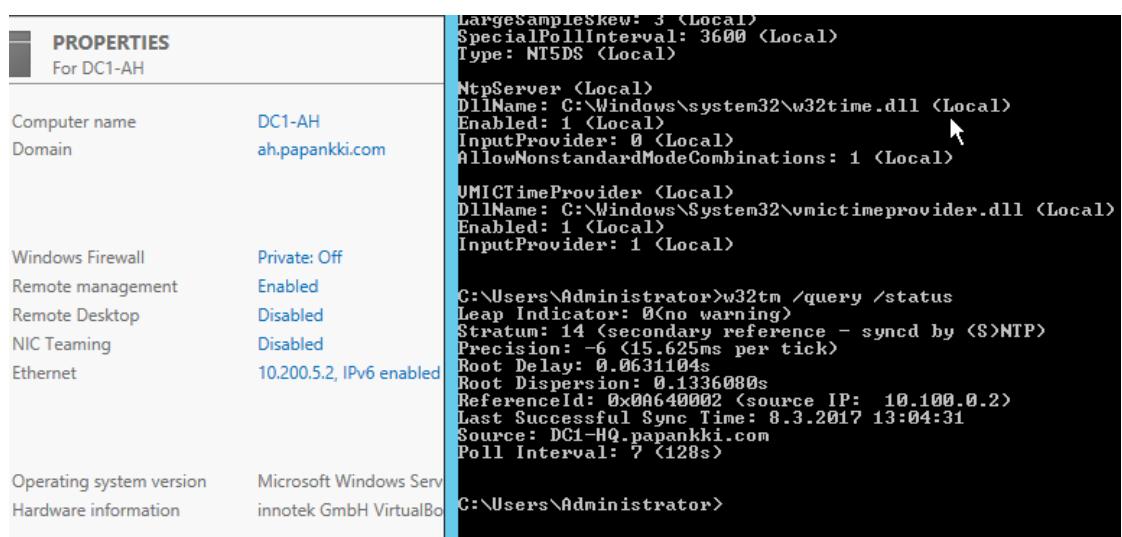
Kuvio 86. Ahvenanmaan käyttäjien oikeudet

Koska käyttäjien pitää pystyä käyttämään tiliään joka puolella yritystä, luotiin heille roaming profilet. Tätä todennetaan kuviossa 87.



Kuvio 87. Ahvenanmaan Roaming profilet

Lopuksi testattiin myös NTP:n toimivuus, jota todennetaan kuviossa 88.



Kuvio 88. Ahvenanmaan DC1 hakee HQ:ltä ajan

5.12 Itä-Suomen IS ohjainpalvelinten pystytys

Itä-Suomen lapsitoimialueen nimeksi asetettiin is.papankki.com joiden Domain Controllerina toimivat DC1-IS ja DC2-IS-palvelimet, lisäksi asennettiin kaksi tiedostopalvelinta FS1 ja FS2. Toimialueeseen kuuluvat myös työntekijöiden työasemat, joita nostettiin Domainiin kaksi kappaletta WS1-IS ja WS2-IS. Toimialueen liikennöinnin reitityksestä huolehtii VyOS-reititin, joka vastaa DHCP, NAT, OSPF sekä IPSec-VPN-palveluista. Alla todennus DC1-IS:n toimialueeseen nostosta (Kuvio 89.).

Computer name	DC1-IS
Domain	is.papankki.com
<hr/>	
Windows Firewall	Public: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet	10.200.3.2, IPv6 enabled

Kuvio 89. DC1 domainissa

Ohjainpalvelimelle DC1-IS luotiin OU rakenne sekä ryhmärakenne (Kuvio 90.). tavalla, jossa yrityksen tietyn sektorin OU:n sisälle luodaan globaali ryhmä, jonka käyttäjät OU:sta lisätään käyttäjiä, jotka sitten lisätään jäseniksi Domain Localeihin ryhmiin FC, RW ja R

Name	Type	Description
Johtaja	Security Group - Global	
Johtaja_FC	Security Group - Domain Local	
Johtaja_R	Security Group - Domain Local	
Johtaja_RW	Security Group - Domain Local	
Käyttäjät	Organizational Unit	

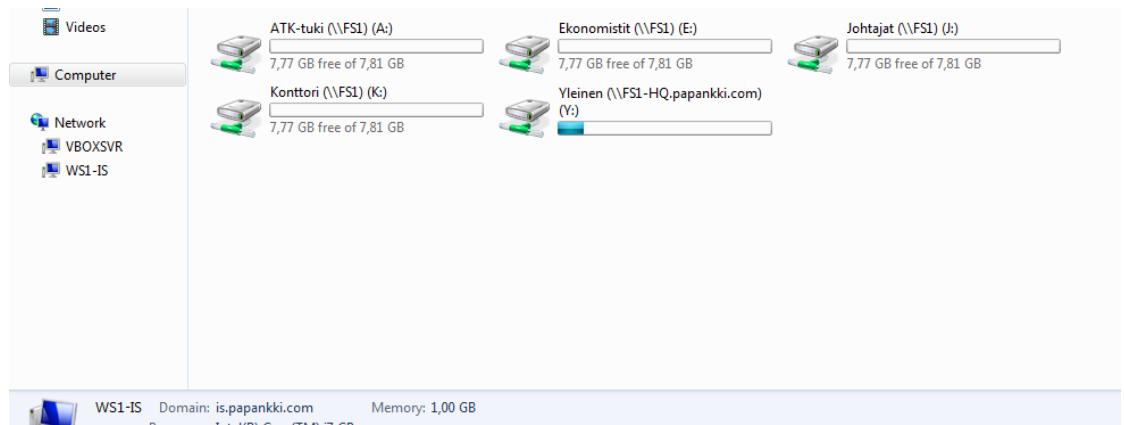
Kuvio 90. IS-DC1 OU- ja ryhmärakenne

DC1-IS ohjainpalvelimelle konfiguroitiin ryhmäkäytäntöön taustakuva sekä osasto-kohtainen levyjako tiedostopalvelin IS-FS1:ltä, sekä yleinen levyjako päätoimipaikan tiedostopalvelin FS1-HQ:ltä (Kuvio 91.).

Action	Properties	Update
Letter	Y	
Location	\\\FS1-HQ.papankki.com\Yleinen	
Reconnect	Enabled	
Use first available	Disabled	
Hide/Show this drive	Show	
Hide/Show all drives	Show	

Kuvio 91. GPO-rakenne

Alla myös todennus levyjakojen toimivuudesta työasemalta WS1-IS, jossa on kirjaututtu johtajat käyttäjällä, jolle näkyy kaikkien osastojen levyjaot (Kuvio 92.).



Kuvio 92. Levyjako todennus

Ohjainpalvelin IS-DC1:lle asetettiin NTP-palvelimeksi päätoimipaikan DC1-HQ ohjainpalvelin, jolta se saa nyt ajan (Kuvio 93.). Kuviossa todennetaan myös IS-DC1:n IP-osoite.

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 14 (secondary reference - syncd by ($NTP))
Precision: -6 (15.625ms per tick)
Root Delay: 0.0630341s
Root Dispersion: 0.1565473s
ReferenceId: 0x0A640002 (source IP: 10.100.0.2)
Last Successful Sync Time: 6.3.2017 13:52:58
Source: DC1-HQ.papankki.com
Poll Interval: 9 (512s)

PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . . . . . : fe80::30ae:b78:1398:d4d7%12
  Link-local IPv6 Address . . . . . : 10.200.3.2
  IPv4 Address . . . . . : 10.200.3.2
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.200.3.1

Tunnel adapter isatap.{6358E2AC-3E54-4953-BAC6-76F18A1982C5}:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
PS C:\Users\Administrator>
```

Kuvio 93. NTP- ja IP-osoite

5.12.1 Itä-Suomen Tiedostopalvelimet

Tiedostopalvelimille luotiin levyjaot niin kuin aikaisemmassa johtajan levyjako-kuviossa nähtiin. Sekä määriteltiin kuinka levyt näkyvät käyttäjille ja myös ryhmäkohtaiset oikeudet taulukon 3 mukaisesti. Alla esimerkki ekonomistien levyjaosta, jossa ATK-tuella sekä ekonomisteilla on Full Control sekä konttori-osaston työntekijöillä luku- ja kirjoitusoikeudet, unohtamatta johtajia jotka pystyvät lukemaan levyn sisältöä (Kuvio 94.).

Name: E:\Shares\Ekonomitit
Owner: Administrators (FS1\Administrators) [Change](#)

Permissions	Share	Auditing	Effective Access	
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).				
Permission entries:				
Type	Principal	Access	Inherited from	Applies to
Allow	Administrators (FS1\Administ...	Full control	None	This folder, subfolders and files
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	CREATOR OWNER	Full control	None	Subfolders and files only
Allow	Ekonomitit_FC (IS\Ekonomis...	Full control	None	This folder, subfolders and files
Allow	ATK-tuki_FC (IS\ATK-tuki_FC)	Full control	None	This folder, subfolders and files
Allow	Konttori-RW (IS\Konttori-RW)	Read, write & execute	None	This folder, subfolders and files
Allow	Johtaja_R (IS\Johtaja_R)	Read & execute	None	This folder, subfolders and files

[Add](#) [Remove](#) [Edit](#)

Kuvio 94. Ekonomistien levyn oikeusmäärittely

5.12.2 Itä-Suomen VyOS

VyOS-reitittimelle konfiguroitiin OSPF-reititys area 0.0.0.0:na, jossa mainostetaan palvelinten, työasemien sekä IPSec-tunnelin verkkoja. Alla (Kuvio 95.) reitittimen reitystaulu, josta nähdään kuinka muiden toimialueiden verkot mainostuvat tälle reittimelle.

```

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.16.3.1, tun4, 00:03:29
O  1.1.1.1/32 [110/20] via 172.16.3.1, 00:03:29
C>* 1.1.1.1/32 is directly connected, lo
O>* 10.0.0.0/24 [110/20] via 172.16.3.1, tun4, 00:03:30
S  10.0.0.0/24 [1/0] via 172.16.0.7 inactive
O  10.10.3.0/24 [110/10] is directly connected, eth2, 00:04:20
C>* 10.10.3.0/24 is directly connected, eth2
O  10.100.0.0/24 [110/20] via 172.16.3.1, 00:03:30
S>* 10.100.0.0/24 [1/0] via 172.16.3.1, tun4
O  10.200.3.0/24 [110/10] is directly connected, eth1, 00:04:20
C>* 10.200.3.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.1.0/30 [110/20] via 172.16.3.1, tun4, 00:03:30
O>* 172.16.2.0/30 [110/20] via 172.16.3.1, tun4, 00:03:30
O  172.16.3.0/30 [110/10] is directly connected, tun4, 00:04:20
C>* 172.16.3.0/30 is directly connected, tun4
O>* 172.16.4.0/30 [110/20] via 172.16.3.1, tun4, 00:03:30
O>* 172.16.5.0/30 [110/20] via 172.16.3.1, tun4, 00:03:30
S>* 192.168.17.0/24 [1/0] via 192.168.44.1, eth0
C>* 192.168.44.0/24 is directly connected, eth0
[edit]
vyos@vyos# _____

```

Kuvio 95. VyOS reititystaulu

Alla on myös (Kuvio 96.) show ip ospf database-komennolla saadut reitittimet, mitkä löytyvät samalta OSPF-alueelta.

```

OSPF Router with ID (3.3.3.3)

        Router Link States (Area 0.0.0.0)

Link ID      ADV Router      Age  Seq#      CkSum  Link count
1.1.1.1      1.1.1.1        185  0x800000014 0x2135 7
3.3.3.3      3.3.3.3        289  0x80000000f 0xc7b7 3
4.4.4.4      4.4.4.4        185  0x800000008 0xc0c5 3
7.7.7.7      7.7.7.7        844  0x800000007 0x3535 3
9.9.9.9      9.9.9.9        175  0x800000003 0xc094 3

        Net Link States (Area 0.0.0.0)

Link ID      ADV Router      Age  Seq#      CkSum
172.16.1.2   4.4.4.4        186  0x800000001 0x3d3c
172.16.2.1   1.1.1.1        953  0x800000001 0x2d4c
172.16.3.2   3.3.3.3        279  0x800000003 0xf6e
172.16.5.2   9.9.9.9        1935 0x800000001 0x75d7

```

Kuvio 96. OSPF database

IPSec-tunnelilla saatiaan luotua site-to-site yhteys päätoimialueen VyOS:lle. Sekä yhteys muihin toimialueisiin. Konfiguroitiin esp- ja ike-group asetukset samoiksi kuin

päätoimialueen VyOS:lla sekä pre-shared-key. Alla (Kuvio 97.) todennus Itä-Suomen IPSec tunnelin 4 toiminnasta.

```
Peer ID / IP                               Local ID / IP
-----                                     -----
192.168.17.16                           192.168.44.228

Tunnel  State   Bytes Out/In   Encrypt  Hash    NAT-T   A-Time   L-Time   Proto
-----  -----   -----          -----   -----   -----   -----   -----   -----
  4      up      1.2M/1010.4K  aes128  md5     no      10881   86400   gre

[edit]
vyos@vyos#
```

Kuvio 97. IPSec-tunnelin todennus

5.13 Länsi-Suomen palveluiden pystytys

Länsi-Suomen lapsitoimialueen nimaksi laitettiin ls.papankki.com ja sinne asennettiin Domain Controllereiksi LS-DC1 ja LS-DC2-palvelimet. Tiedostopalvelimia asennettiin 2 kappaletta, FS1 ja FS2. Toimialueelle lisättiin työasemia, joiden avulla voitiin testata toimivuutta. Näiden nimet menevät mallia LS-WS1, LS-WS2 ja niin edespäin.

Yhteydet HQ:n ja muiden branchien välillä hoidettiin VyOS reitittimellä. Ensiksi tehtiin IPSec tunneli HQ:n reitittimen välillä ja tätä on todennettu kuviossa 98.

```
vyos@vyos:~$ show vpn ipsec sa
Peer ID / IP                               Local ID / IP
-----                                     -----
192.168.17.16                           192.168.44.227

Tunnel  State   Bytes Out/In   Encrypt  Hash    NAT-T   A-Time   L-Time   Proto
-----  -----   -----          -----   -----   -----   -----   -----   -----
  3      up      401.4K/345.5K  aes128  md5     no      3188    86400   gre
```

Kuvio 98. LS IPSec tunneli

Tämän jälkeen tehtiin OSPF reititys kuntoon, jotta saatettiin yhteydet muille brancheille. Tätä todennetaan Kuviossa 99, ottamalla trace route Itä-Suomen DC1:lle.

```
C:\Users\Administrator>tracert 10.200.3.2
Tracing route to DC1-HQ [10.200.3.2]
over a maximum of 30 hops:
  1  <1 ms    <1 ms    <1 ms  10.200.2.1
  2  <1 ms    <1 ms    <1 ms  172.16.2.1
  3  1 ms     1 ms     1 ms  172.16.3.2
  4  1 ms     1 ms     1 ms  DC1-HQ [10.200.3.2]

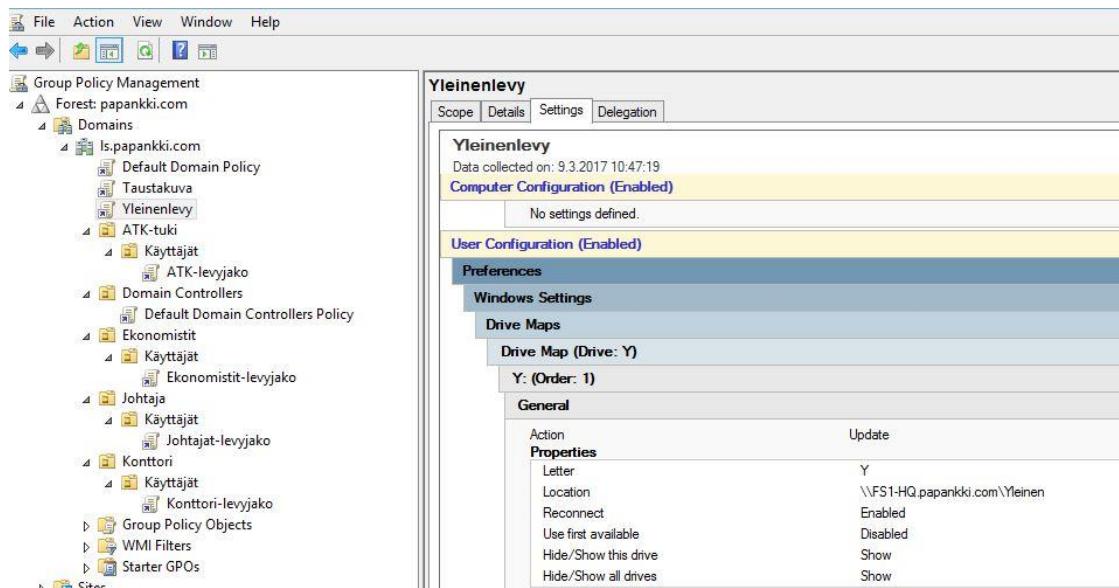
Trace complete.

C:\Users\Administrator>tracert 10.100.0.2
Tracing route to dc1-hq.papankki.com [10.100.0.2]
over a maximum of 30 hops:
  1  <1 ms    <1 ms    <1 ms  10.200.2.1
  2  1 ms     <1 ms    <1 ms  172.16.2.1
  3  1 ms     <1 ms    <1 ms  dc1-hq.papankki.com [10.100.0.2]

Trace complete.
```

Kuvio 99. LS Yhteyksien todennus

Loimme tarvittavat GPO:t, jotta saimme tehtyä taustakuvan ja levyjaot onnistuneesti. GPO:ta on havainnollistettu kuviossa 100.



Kuvio 100. GPO todennus LS

Määrittelimme levyjaoille oikeudet taulukon 3 mukaisesti. Tätä todennetaan kuviossa 101.

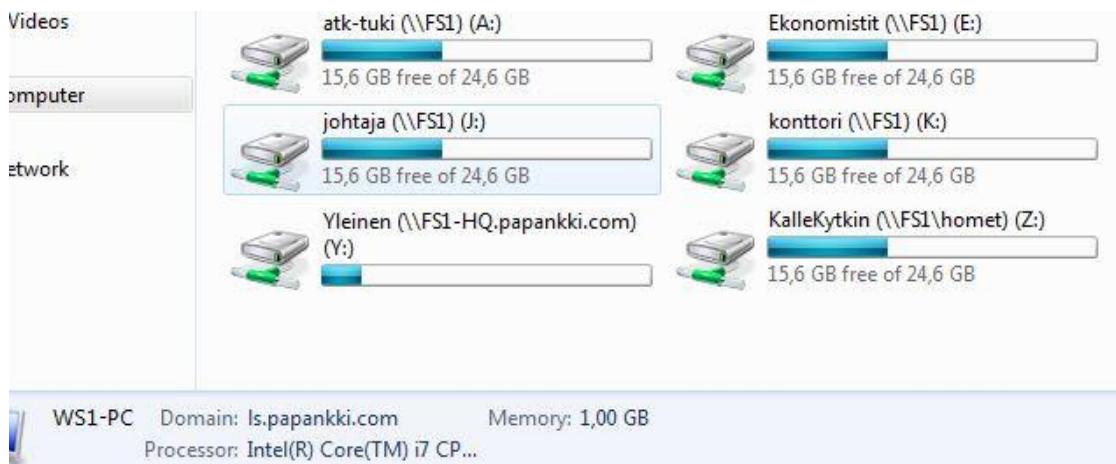
Name: C:\jaot\konttori
Owner: Administrators (FS1\Administrators) [Change](#)

Permissions	Share	Auditing	Effective Access	
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).				
Permission entries:				
Type	Principal	Access	Inherited from	Applies to
Allow	Johtaja_R (LS\Johtaja_R)	Read	None	This folder, subfolders and files
Allow	Ekonomistit_RW (LS\Ekonomi...)	Read, write & execute	None	This folder, subfolders and files
Allow	Konttori_FC (LS\Konttori_FC)	Full control	None	This folder, subfolders and files
Allow	ATK-tuki-FC (LS\ATK-tuki-FC)	Full control	None	This folder, subfolders and files
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrators (FS1\Administ...)	Full control	None	This folder, subfolders and files
Allow	CREATOR OWNER	Full control	None	Subfolders and files only

[Add](#) [Remove](#) [View](#)

Kuvio 101. Levyjakojen oikeudet LS

Levyjakojen todennuksen testasimme menemällä KalleKytkimellä WS1 sisään ja tarkistamalla näkyvätkö levyjaot. Tästä todennus kuviossa 102.



Kuvio 102. Levyjaot LS

NTP:n toteutuksesta löytyy kattavammat ohjeet 5.14 osiosta, joten kuviossa 103 vain todennetaan LS-DC1:n NTP tietoja.

```
PS C:\Users\Administrator> w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 14 (secondary reference - syncd by (S)NTP)
Precision: -6 (15.625ms per tick)
Root Delay: 0.0630646s
Root Dispersion: 7.8797730s
ReferenceId: 0x0A640002 (source IP: 10.100.0.2)
Last Successful Sync Time: 9.3.2017 11:18:09
Source: 10.100.0.2
Poll Interval: 8 (256s)

PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . . . . . : fe80::d148:d613:2a83:cd83%12
  Link-local IPv6 Address . . . . . : 10.200.2.2
  IPv4 Address . . . . . : 10.200.2.2
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.200.2.1
```

Kuvio 103. NTP DC1-LS

5.14 NTP toteutus

HQ:lle ajettiin tarvittavat komennot Windows Powershell:in kautta, jotka löytyvät kuviosta 104. Ensimmäinen komento loppui /update kohtaan, mutta luettavuuden parantamiseksi pilkoin sen kahdelle riville.

```
w32tm /config /manualpeerlist:10.100.0.1
/syncfromflags:manual /reliable:yes /update
Stop-Service w32time
Start-Service w32time
```

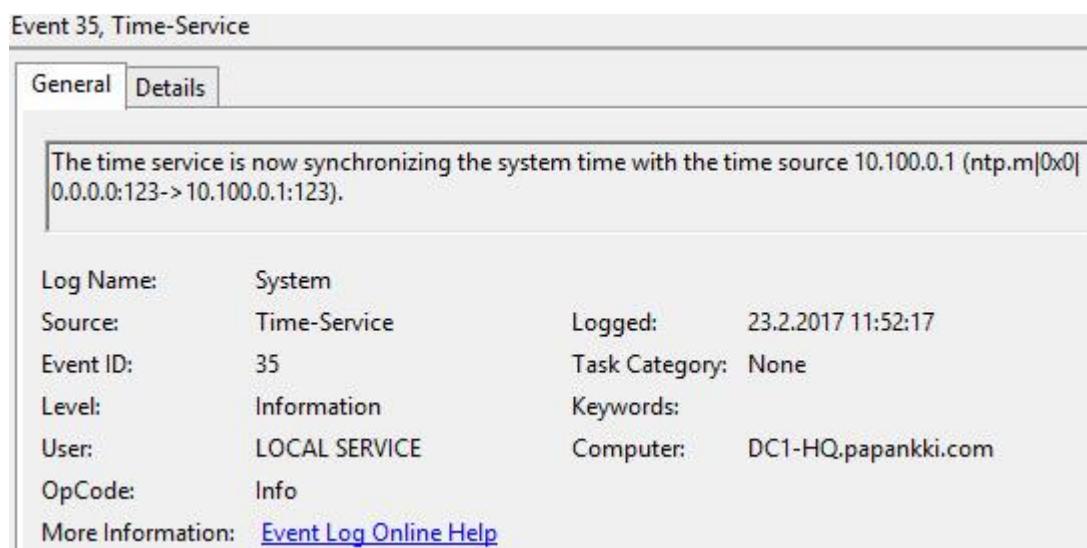
Kuvio 104. Powershell- komennot

Varmistaaksemme, että saimme oikean NTP-palvelimen laitettua onnistuneesti, ajoimme vielä w32tm /query /status komennon, jonka tiedot löytyvät kuviosta 105.

```
PS C:\Users\Administrator> w32tm /query /status
Leap Indicator: 0 (no warning)
Stratum: 13 (secondary reference - synced by ($)NTP)
Precision: -6 (15.625ms per tick)
Root Delay: 0.0317230s
Root Dispersion: 0.0457980s
ReferenceId: 0x0A640001 (source IP: 10.100.0.1)
Last Successful Sync Time: 23.2.2017 12:04:17
Source: 10.100.0.1
Poll Interval: 7 (128s)
```

Kuvio 105. HQ NTP status

Vielä varmistaaksemme NTP:n toimivuuden kävimme läpi Event Viewerin Windows Logs, System välilehden ja varmistimme että Event ID: 47 ei löytynyt. Event Vieweristä täytyy löytyä samalta välilehdeltä Event ID: 35, joka todentaa NTP toimivuuden. Event ID:35 otettiin todennus kuvio 106.



Kuvio 106. Event Viewer todennus

HQ VyOS konfiguroitiin saamaan aikatietonsa NTP-palvelimelta, joka meille oltiin annettu tehtävänanossa, eli osoitteesta 192.168.17.2. Todennus konfiguraatiosta kuviossa 107.

```

        }
    ntp {
        server 192.168.17.2 {
    }
vyos@R1-HQ:~$ _
```

Kuvio 107. HQ vyOS konfiguraatio

NTP tiedot pystytettiin varmistamaan show ntp -komennolla, joka on todennettu kuviossa 108.

```

vyos@R1-HQ:~$ show ntp
      remote           local      st poll reach   delay   offset   disp
=====
*192.168.17.2     192.168.17.16   11   128   377  0.00053 -0.001471  0.08455
```

Kuvio 108. NTP todennus HQ VyOS

NTP konfiguraatiot pystytettiin tekemään kahdella eri tavalla. HQ VyOS konfiguraatiot tehtiin poistamalla muut NTP-palvelin merkinnät, lisättiin haluttu NTP-palvelinosoite ja laitettiin oikea aikavyöhyke. Käytettyjä komentoja voi tarkastella kuvista 109.

```

set system time-zone Europe/Helsinki
set system ntp server 192.168.17.2
delete system ntp server 0.pool.ntp.org
delete system ntp server 1.pool.ntp.org
delete system ntp server 2.pool.ntp.org|
```

Kuvio 109. HQ VyOS komennot

Branchien VyOS:it täytyi lisätä ottamaan aikansa HQ-DC1:ltä. Tämä tehtiin käyttämällä prefer termiä tehdessämme konfiguraatiota. Tämän avulla meidän ei tarvinnut poistaa vanhoja NTP-palvelin merkintöjä. Käytetyt komennot löytyvät kuvista 110.

```
set system time-zone Europe/Helsinki
set system ntp server 10.100.0.2 'prefer'
```

Kuvio 110. Branchien VyOS komennot

Branchien VyOS saavat NTP-tiedot HQ-DC1, eli osoitteesta 10.100.0.2. Tätä todennetaan Länsi-Suomen branchin VyOS konfiguraatiolla kuviossa 111.

```
ntp {
    server 0.pool.ntp.org {
    }
    server 1.pool.ntp.org {
    }
    server 2.pool.ntp.org {
    }
    server 10.100.0.2 {
        prefer
    }
```

Kuvio 111. Länsi-Suomi branchin VyOS NTP konfiguraatio

Varmistamme vielä show ntp –komennolla, että branchin NTP on toiminnassa oikeilla osoitteilla ja tästä on todennus Länsi-Suomen branchilta kuviossa 112.

```
vyos@vyos:~$ show ntp
      remote           local      st  poll  reach   delay   offset   disp
=====
*10.100.0.2      10.200.2.1      13 128  377  0.00113  0.011564 0.14577
vyos@vyos:~$ _
```

Kuvio 112. Show ntp Länsi-Suomen branchilta

Kuviossa 113 Pohjois-Suomen reititin saa aikatiedot pääkonttorin ohjainpalvelimelta

```
vyos@R1-PS# run show date
Mon Feb 27 13:44:05 EET 2017
[edit]
vyos@R1-PS#
```

Kuvio 113. Pohjois-Suomen reitittimen NTP-aika

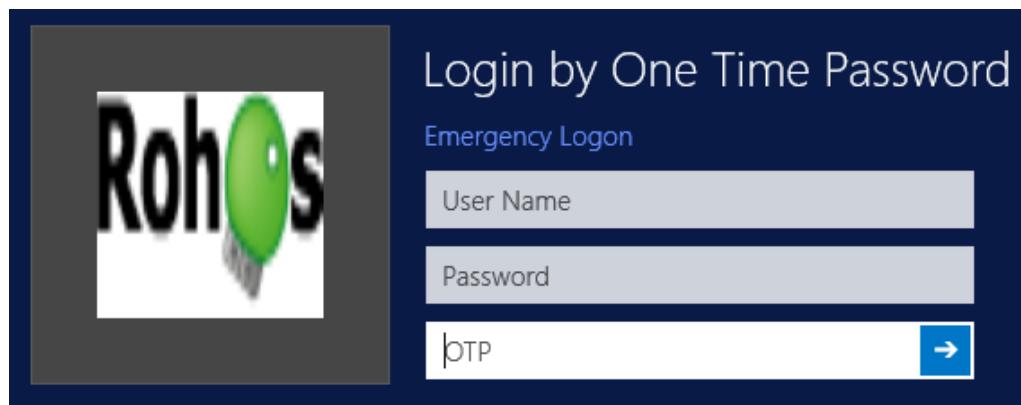
Branchit saavat NTP tietonsa automaattisesti HQ-DC1:ltä. Tarkistimme Event Vie-
weristä, oliko Event ID: 47 tai 35 ja näitä ei löytynyt varmaan sen takia, koska aika tie-
dot synkronoitiin suoraan HQ-DC1:ltä. Alhaalla olevassa kuviossa 114 on todennus
NTP:n toimivuudesta.

```
PS C:\Users\Administrator> w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 14 (secondary reference - syncd by ($)NTP)
Precision: -6 (15.625ms per tick)
Root Delay: 0.0629120s
Root Dispersion: 0.8585858s
ReferenceId: 0x0A640002 (source IP: 10.100.0.2)
Last Successful Sync Time: 23.2.2017 11:56:05
Source: DC1-HQ.papankki.com
Poll Interval: 10 (1024s)

PS C:\Users\Administrator>
```

Kuvio 114. Branch DC:n NTP todennus

Multifactor authentikointia käytetään niin, että kirjautuminen tapahtuu ROHOS-ohjelmalla, mutta authentikointi tapahtuu käyttäen Google-tiliä. Puhelimessa on Google authenticator ja tämä antaa 20 sekuntia voimassa olevia kertakäyttöisiä koodia jotka syötetään OTP-kenttään Kuviossa 115.



Kuvio 115. MFA todennus

HQ:n DC1 määriteltiin Conditional Forwardseihin (kts. Kuvio 116) kaikki yritykset paitsi BBA, jonka domain nimeä ei löytynyt mistään.

Name	Type
PS.PAPANKKI.COM	Conditional ...
Idil.com	Conditional ...
logistiikkaa.fi	Conditional ...
mutrof.com	Conditional ...
enok.com	Conditional ...
paperproducts.com	Conditional ...
kipito.fi	Conditional ...

Kuvio 116. DNS Conditional Forwarders

Kuviossa 117 on määritetty BGP asetukset HQ:n VyOSille. Tämän lisäksi jokaiselle naapuruudelle määriteltiin MD5-authentikaatio komennolla: set protocols bgp <AS numero> neighbor <neighbor IP> password <passwd>

```

bgp 65250 {
    neighbor 192.168.17.11 {
        remote-as 65000
        update-source 192.168.17.16
    }
    neighbor 192.168.17.12 {
        remote-as 65050
        update-source 192.168.17.16
    }
    neighbor 192.168.17.13 {
        remote-as 65100
        update-source 192.168.17.16
    }
    neighbor 192.168.17.14 {
        remote-as 65150
        update-source 192.168.17.16
    }
    neighbor 192.168.17.15 {
        remote-as 65200
        update-source 192.168.17.16
    }
    neighbor 192.168.17.17 {
        remote-as 65300
        update-source 192.168.17.16
    }
}

```

Kuvio 117. BGP asetukset

Show ip bgp – komennolla on saatu esiin BGP- reitit. (Kts. kuvio 118)

```

vyos@R1-HQ:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.17.16
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop            Metric LocPrf Weight Path
*  192.0.2.0        192.168.17.11          0 65300 65050 65000 i
*>  192.168.17.11          192.168.17.11          0 65050 65000 i
*  198.51.100.0     192.168.17.13          0 65300 65050 65000 6
5100 i
*>  192.168.17.13          192.168.17.13          0 65050 65000 65100 i

Total number of prefixes 2
vyos@R1-HQ:~$ _

```

Kuvio 118. Show ip bgp

5.15 Sähköpostipalvelimen toteutus

Papankin sähköpostipalvelin koostuu lähetyks (Postfix) ja vastaanotto (Dovecot) osista. Nämä ovat eri ohjelmia, joten niitten asennus käydään vaiheittain.

5.15.1 Dovecot

Seuraavaksi asennettiin Dovecot. Dovecot on vastuussa sähköpostin vastaanottamisesta. Kuvassa on esitetty polku, johon postit saapuvat. Tällöin Dovecot tietää, mistä saapuvat postit haetaan. (Katso kuvio 119)

```
# Protocols we want to be serving.
protocols = imap pop3
protocol imap {
mail_location = maildir:~/mail
}
pop3_uidl_format = %08Xu%08Xv
```

Kuvio 119. Sähköpostien sijainti

5.15.2 Postfix

Sähköpostipalvelimen luominen aloitettiin päivittämällä palvelin ja asentamalla apache 2 ja php5. Kun alkuvalmistelut oltiin tehty, asennettiin postfix. Asennusten jälkeen säädettiin palvelimen tiedot (Katso kuvio 120).

```

myhostname = mail.papankki.com
mydomain = papankki.com
myorigin = $mydomain
home_mailbox = mail/
mynetworks = 10.100.0.0/24
inet_interfaces = all
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
smtpd_sasl_auth_enable = yes
smtpd_sasl_type = cyrus
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_authenticated_header = yes
smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination
smtpd_tls_auth_only = no
smtp_use_tls = yes
smtpd_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtpd_tls_key_file = /etc/postfix/ssl/smtpd.key
smtpd_tls_cert_file = /etc/postfix/ssl/smtpd.crt
smtpd_tls_CAfile = /etc/postfix/ssl/cacert.pem
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom

```

Kuvio 120. Postfixin konfigurointitiedosto

Tähän luotiin myös sertifikaatti openssl:n avulla. Katso kuvio 121.

```

[root@web ssl]# openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 1024
0 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
Enter pass phrase for smtpd.key:
Verifying - Enter pass phrase for smtpd.key:
[root@web ssl]#

```

Kuvio 121. SSL:n luonti postfixille

5.15.3 Squirrelmail

Lopuksi asennettiin Squirrelmail, joka vastaa loppukäyttäjän miellyttävästä käytöstä. Squirrelmailissa käyttäjä pystyy kirjautumaan graafisen käyttöliittymän kautta webseleimella sähköpostiin, lähettilä ja vastaanottaa postea. Asennuksen jälkeen asetettiin palvelimelle nimi. (Katso kuvio 122)

```
GNU nano 2.0.9          File: /etc/httpd/conf/httpd.conf

# <VirtualHost> definition. These values also provide defaults for
# any <VirtualHost> containers you may define later in the file.
#
# All of these directives may appear inside <VirtualHost> containers,
# in which case these default settings will be overridden for the
# virtual host being defined.
#
#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed. This address appears on some server-generated pages, such
# as error documents. e.g. admin@your-domain.com
#
ServerAdmin root@localhost
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If this is not set to valid DNS name for your host, server-generated
# redirections will not work. See also the UseCanonicalName directive.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
# You will have to access it by its address anyway, and this will make
# redirections work in a sensible way.
#
# ServerName www.mail.papankki.com:80
#
# UseCanonicalName: Determines how Apache constructs self-referencing
# URLs and the SERVER_NAME and SERVER_PORT variables.
[ Wrote 1009 lines ]
```

Kuvio 122. Palvelimen nimen asetus

Squirrelmailn konfiguraatiotiedostosta annettiin palvelulle domain nimi, määriteltiin käytettävät portit ja palvelut. (Katso kuvio 123)

```
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Organization Preferences
1. Organization Name      : papankki.com
2. Organization Logo     : 1
3. Org. Logo Width/Height : (308/111)
4. Organization Title    : SquirrelMail $version
5. Signout Page          :
6. Top Frame              : _top
7. Provider link          : http://squirrelmail.org/
8. Provider name          : SquirrelMail

R  Return to Main Menu
C  Turn color off
S  Save data
Q  Quit

Command >> _
```

Kuvio 123. Squirrelmailn konfiguraatiotiedosto

Tämän jälkeen loimme kaksi testikäyttäjää. Kissa ja Koira. Käytämme näitä käyttäjiä palvelun demoamiseen, kunnes palveluun pystyy kirjautumaan domainin tunnuksilla. Jos kaikki on mennyt oikein, pitäisi sähköposti näyttää tältä. Kuvassa näkyy myös vastaanotettuja viestejä. (Katso kuvio 124)

The screenshot shows the SquirrelMail web interface. The left sidebar has 'Folders' with 'INBOX (7)' selected, and links for Drafts, Sent, and Trash. The main area shows the 'INBOX' folder with 7 messages. The header row includes columns for 'From', 'Date', and 'Subject'. The messages listed are:

From	Date	Subject
<input type="checkbox"/> koira@papankki.com	4:35 pm	Le EBIN
<input type="checkbox"/> koira@papankki.com	4:31 pm	asd
<input type="checkbox"/> kissa@papankki.com	4:28 pm	asd
<input type="checkbox"/> koira@papankki.com	4:27 pm	asd
<input type="checkbox"/> koira@papankki.com	4:23 pm	asd
<input type="checkbox"/> kissa@papankki.com	4:10 pm	asd
<input type="checkbox"/> koira@papankki.com	3:56 pm	asd

Buttons at the top right include 'Sign Out', 'SquirrelMail', 'Compose', 'Addresses', 'Folders', 'Options', 'Search', 'Help', 'Move Selected To' (with 'INBOX' dropdown), 'Forward', 'Transform Selected Messages' (with 'Read', 'Unread', 'Delete' buttons), 'Viewing Messages: 1 to 7 (7 total)', and 'Toggle All'.

Kuvio 124. Kissaa@papankki.com saapuneet viestit

Avasimme Kissa- käyttäjän saaman viestin, joka oli saapunut osoitteesta [koira@papankki.com](#). Asetetut tiedot ovat oikein ja viesti kulkee hyvin perille. Tätä todennettiin kuviossa 125.

The screenshot shows the SquirrelMail message view for a specific email. The left sidebar is identical to the inbox view. The main area shows the message details for an email from 'koira@papankki.com' to 'kissa@papankki.com' on March 2, 2017, at 4:35 pm. The subject is 'Le EBIN'. The message content is 'IT JUST WORKS'. Navigation buttons at the top right include 'Sign Out', 'SquirrelMail', 'Compose', 'Addresses', 'Folders', 'Options', 'Search', 'Help', 'Message List', 'Unread', 'Delete', 'Previous', 'Next', 'Forward', 'Forward as Attachment', 'Reply', and 'Reply All'.

Kuvio 125. Testiviesti vastaanotettu

5.15.4 AD/LDAP-integraatio

Käytimme Winbind:a lisätäksemme palvelimen domainiimme ja saimme käyttäjät tuotua sen kautta järjestelmään. Todennukset kuvioissa 126 ja 127.

```
[root@web ~]# net ads info
LDAP server: 10.100.0.2
LDAP server name: DC1-HQ.papankki.com
Realm: PAPANKKI.COM
Bind Path: dc=PAPANKKI,dc=COM
LDAP port: 389
Server time: Wed, 05 Apr 2017 14:44:58 EEST
KDC server: 10.100.0.2
Server time offset: 0
```

Kuvio 126. Domainiin liittyminen

```
[root@web ~]# wbinfo -u
administrator
guest
krbtgt
tatutarha
patepalvelin
jussi.johtaja
lassilammas
ps§
harri
jesse
joonas
juho
mikael
ks§
is§
ls§
ah§
testikäyttäjä
ldap
```

Kuvio 127. Domainin käyttäjät

Emme onnistuneet saamaan LDAP yhteyttä toimimaan kunnolla, joten jouduimme tekemään scriptin, jolla teimme käyttäjille kotikansiot. Todennus kuviossa 128.

```
[root@web ~]# cat addmailuser.sh
#!/bin/bash

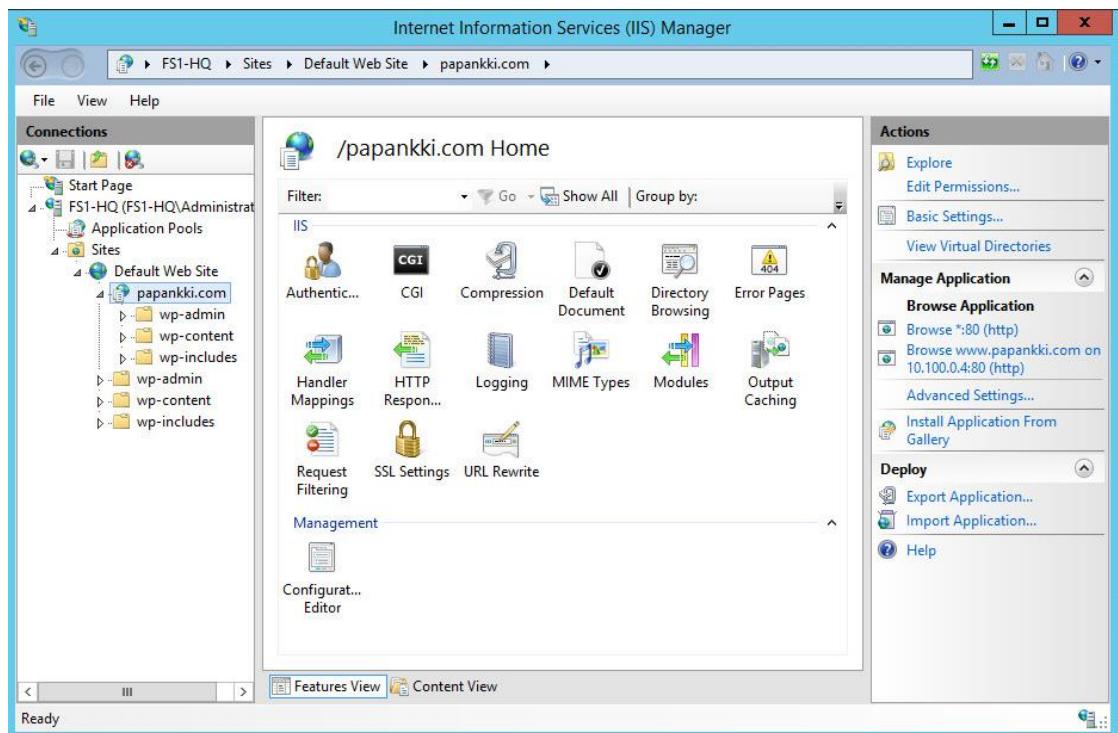
echo -n "Enter the AD login ID : "
read i
su - $i << PAPANKKI
exit
PAPANKKI
echo "$i User's Mail Box has been created"
[root@web ~]#
```

Kuvio 128. Scripti millä tehdään kotikansiot

Tämä ratkaisu ei ole pidemmän päälle toimiva ratkaisu, koska mitä enemmän ihmisiä tulee domainiin käyttäjinä, sitä enemmän tulee rasitusta IT-henkilökunnalle ylläpitää järjestelmää. Tämän takia yritymme saada LDAP yhteyttä toimimaan kunnolla, mutta siinä emme loppujen lopuksi onnistuneet tekemään. LDAP yhteyttä käytäen olisimme myöskin saaneet sähköpostin osoitekirjan jaettua käyttäjien kesken.

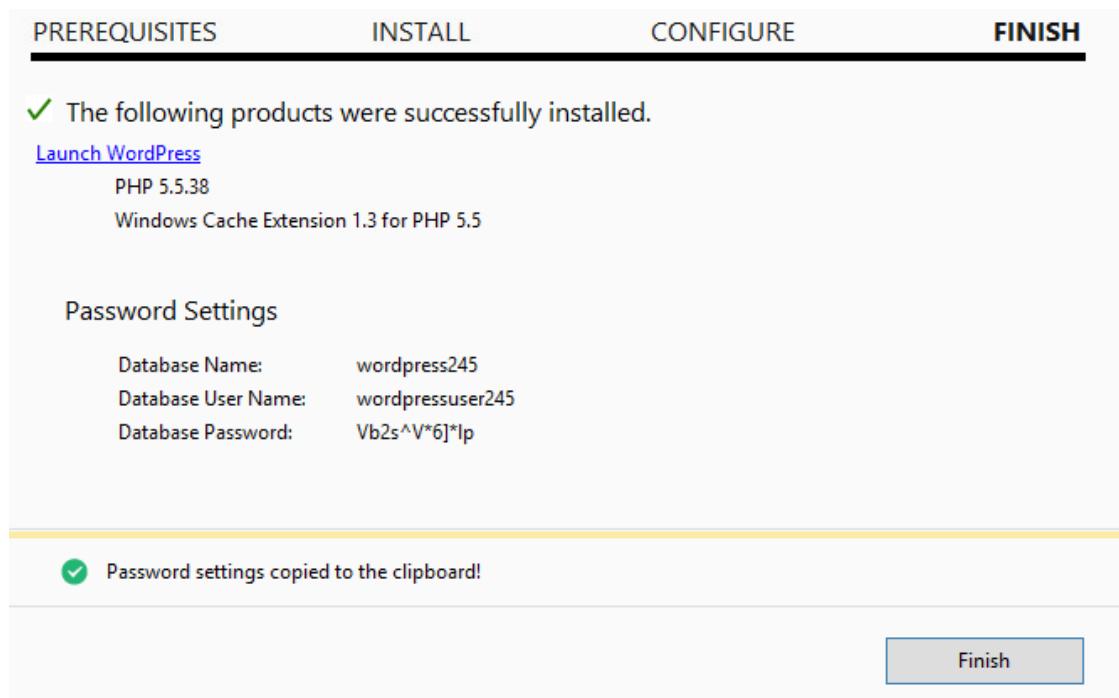
5.16 Intra

Wordpress päättiin asentaa päätöimipisteen tiedostopalvelimelle, koska tässä arvioitiin olevan vähinten kuormaa. Alkuperäinen suunnitelma oli rakentaa palvelu erilliselle CentOS- palvelimelle. Tästä kuitenkin luovuttiin Linux:n yhteistyön hankaluuskien vuoksi. FS1- palvelimelle asennettiin Internet Information Services (IIS) palvelu, jonka pääälle rakennettiin Wordpress- sivu. Todennus tästä kuviossa 129.



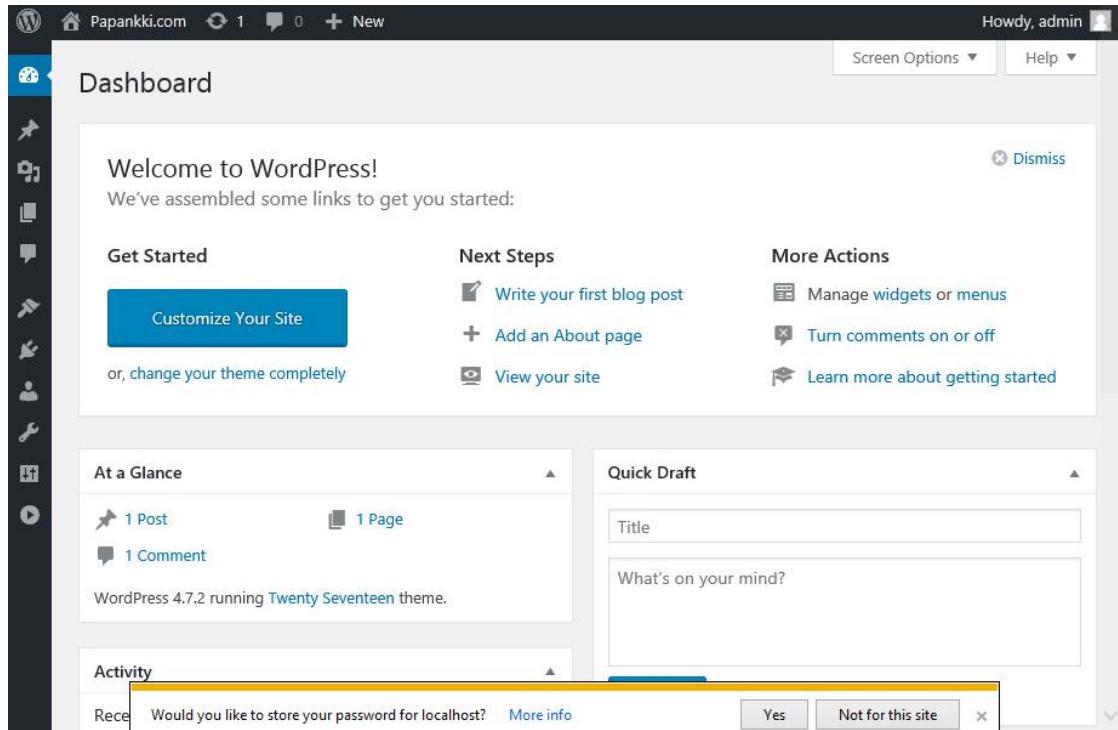
Kuvio 129. ISS:n alkuvalikko

Wordpress asennettiin onnistuneesti ja tietokanta luotiin ilman ongelmia. Todennus tästä iloisesta tapahtumasta löytyy kuviossa 130.



Kuvio 130. Wordpress ja sille tietokanta asennettu

Wordpress- adminsivulle pääsi kirjautumaan helposti käyttämällä localhost osoitetta. (Katso kuvio 131) Tällöin kaikki palvelut toimivat moitteettomasti ja säätöjä pystytiin tekemään.



Kuvio 131. Wordpress adminsivu

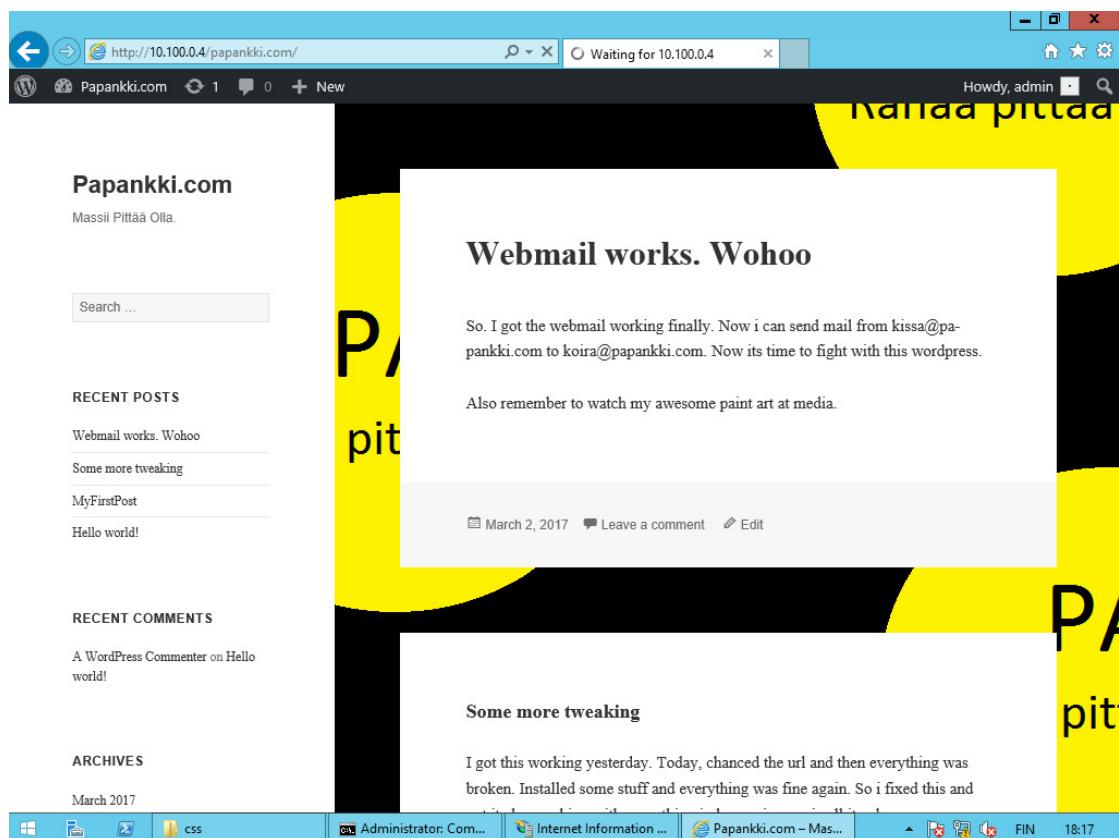
Wordpressn asetuksista säädettiin niin, että palveluun pääsi myös muualta, kuin palvelun sisältävältä koneelta. Tämä toteutettiin antamalla palvelulle toimiva osoite (10.100.0.4) Localhost osoitteen sijaan. Todennus kuviossa 132.

General Settings

Site Title	Papankki.com
Tagline	Massii Pittää Olla. <i>In a few words, explain what this site is about.</i>
WordPress Address (URL)	http://10.100.0.4/papankki.com
Site Address (URL)	http://10.100.0.4/papankki.com
Email Address	admin@papankki.com <i>This address is used for admin purposes, like new user notification.</i>

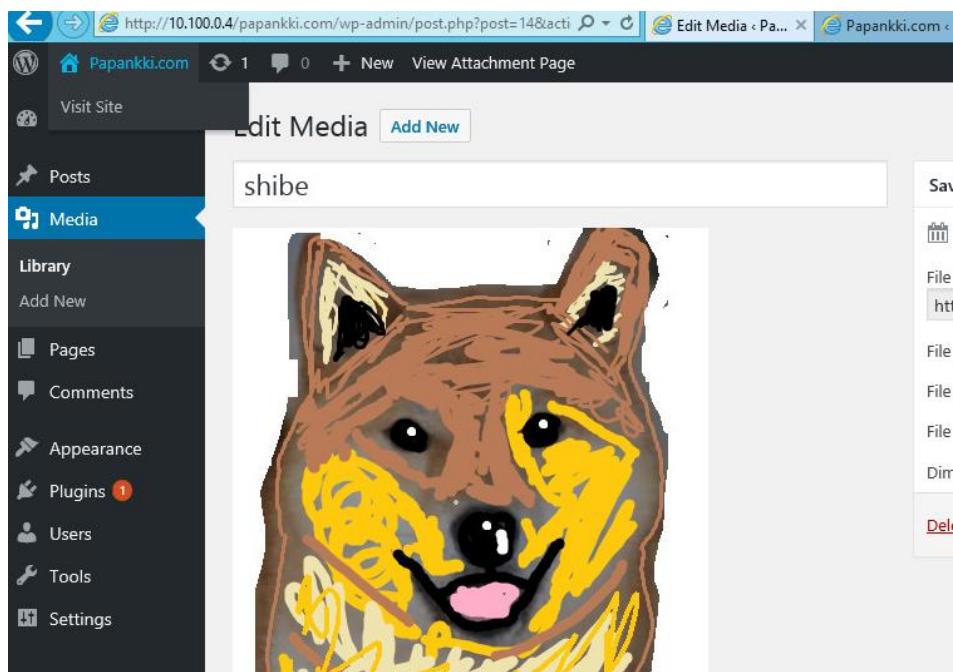
Kuvio 132. URL:n asettaminen Wordpressiin

Lopuksi kirjoitettiin päivitys intran sivulle ja testattiin myös palveluun pääsy multa lähiverkossa olevilta koneilta. Tämä onnistui, vaikka sivu ei hyvältä näyttänytkään. (Katso kuvio 133)



Kuvio 133. Intrasivun etusivu

Testasimme myös median lisäämistä intraan. Tämä toimi moitteetta. Tiedosto ladattiin palveluun samalta palvelimelta, jossa itse palvelu oli. (Katso kuvio 134)



Kuvio 134. Kuvien lataus sivulle toimii

5.17 Intran varmenne

Pystytettiin IIS palvelin HQ-FS1 palvelimelle, joka mainittiin, jo aikaisemmin. Tätä varten HQ-FS1:lle vaadittiin oma palvelin sertifikaatti, joka saatettiin Autoenrollment GPO:n kautta. Tätä on havainnollistettu kuviossa 135.

Policy	Setting
Automatic certificate management	Enabled
Option	Setting
Enroll new certificates, renew expired certificates, process pending certificate requests and remove revoked certificates	Enabled
Update and manage certificates that use certificate templates from Active Directory	Enabled

Public Key Policies/Automatic Certificate Request Settings

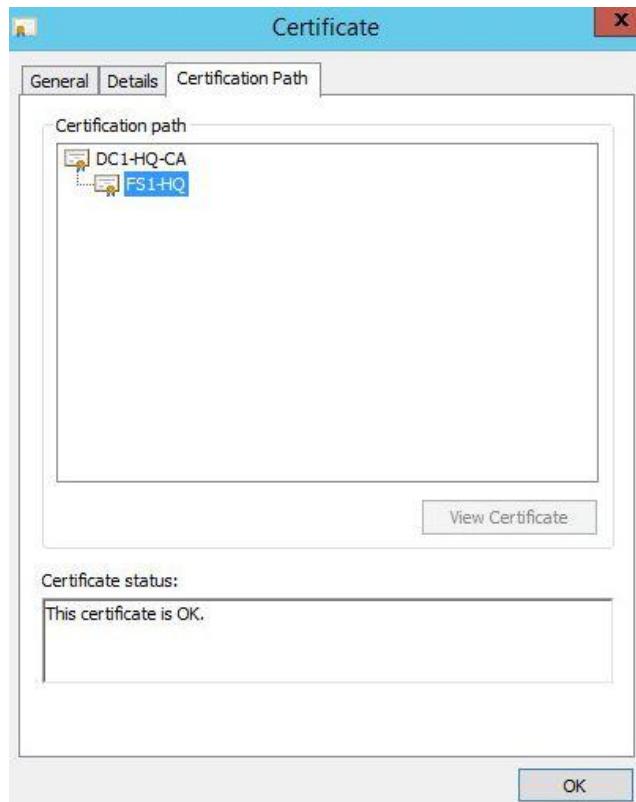
Automatic Certificate Request

Computer

For additional information about individual settings, launch the Local Group Policy Object Editor.

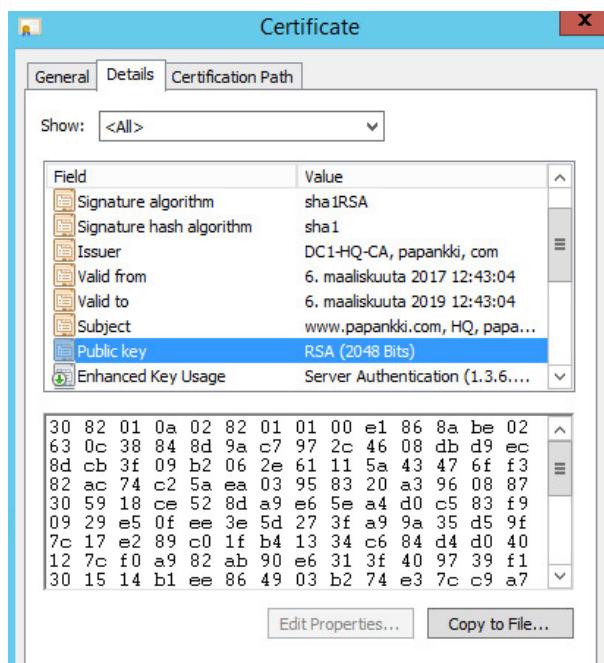
Kuvio 135. AutoEnrollment GPO

Sertifikaatilla pystytään autentikoimaan palvelin CA:lle, kun intralle haetaan SSL-sertifikaattia. Kuten alla olevasta kuvista 136 huomataan. FS1-HQ on saanut allekirjoitetun varmenteen DC1-HQ:ltä.



Kuvio 136. FS1-HQ sertifikaatti

Intran varmenne haettiin käyttämällä DC1-HQ:n CertServ manageria, jonne sertifiointipyynnön voi ladata ja valita millä sertifointi pohjalla haluaa allekirjoituksen CA:ltä. Intralle valittiin Web Server pohja ja 2048 bittinen RSA-kryptausavain. Kuviossa 137 on tästä todennettu.



Kuvio 137. Intran varmenne

Lisättyin intran bindingeihin https, jolle valittiin CA:ltä saama SSL-sertifikaatti www.papankki.com. Alla olevassa kuvio 138 on todennus HTTPS-yhteyden toimivuudesta, mikä kertoo, että sivusto on varmennettu DC1-HQ-CA:lla. HTTPS-yhteys jostain syystä ei anna ladata sivun CSS-muotoiluja, kuten alla oleva kuvio näkee.

The screenshot shows a browser window with the URL https://www.papankki.com. The page content includes a 'Skip to content' link, the logo 'Papankki.com', and a search bar. To the right, a sidebar titled 'Tietoja sivusta - https://www.papa...' provides details about the site's security: it lists icons for Yleiset (General), Media, Syötteet (Input), Oikeudet (Rights), and Turvallisuus (Security). It also shows the following information: Sivuston identiteetti (Site's identity), WWW-sivusto: www.papankki.com, Omistaja: Sivustoon ei liity tietoa omistajasta (The owner of the website is not listed), and Varmentaja: CN=DC1-HQ-CA,DC=papankki,DC=com.

Kuvio 138. HTTPS-yhteys intraan

5.18 IGP kovennuksen toteutus

Muokkasimme OSPF:n asetuksia ensimmäisenä HQ:n reitittimellä laittaen kaikki portit passiiviksi ja poistimme sen ainoastaan IPSec tunneleista ja rajapinnasta, joka menee ulkoverkkoon eli eth0:sta. Tämän jälkeen lisäsimme OSPF:n käyttämään MD5 varmennetta plain textin sijaan. Tästä todennukset HQ:n VyOSIta kuviossa 139.

```
vyos@R1-HQ# show protocols ospf
area 0.0.0.0 {
    authentication md5
    network 10.0.0.0/24
    network 10.100.0.0/24
    network 172.16.5.0/30
    network 172.16.1.0/30
    network 172.16.2.0/30
    network 172.16.3.0/30
    network 172.16.4.0/30
    network 172.16.0.0/30
}
default-information {
    originate {
        always
        metric 10
        metric-type 2
    }
}
log-adjacency-changes {
}
parameters {
    abr-type cisco
    router-id 1.1.1.1
}
passive-interface default
passive-interface-exclude eth0
passive-interface-exclude tun0
passive-interface-exclude tun1
passive-interface-exclude tun3
passive-interface-exclude tun4
passive-interface-exclude tun5
redistribute {
    connected {
        metric-type 2
        route-map CONNECT
    }
}
[edit]
```

Kuvio 139. OSPF kovennukset HQ

Tämän jälkeen ajoimme samat komennot, mutta ainoastaan pienemmässä mittakaavassa lapsidomainien reitittimille. Tämä todennetaan kuviossa 140.

```
vyos@LS-vyos# show protocols ospf
area 0.0.0.0 {
    authentication md5
    network 172.16.0.0/30
    network 10.200.2.0/24
    network 10.10.2.0/24
}
log-adjacency-changes {
}
parameters {
    abr-type cisco
    router-id 7.7.7.7
}
passive-interface default
passive-interface-exclude eth0
passive-interface-exclude tun3
redistribute {
    connected {
        metric-type 2
        route-map CONNECT
    }
}
```

Kuvio 140. LS OSPF

5.19 DNS

Ubuntu 16.04 palvelimelle asennettiin Bind9 nimipalvelinohjelmisto selvittämään ulkoverkon osoitteita. Rajapinnoille asetettiin osoitteet Liitteen 1 mukaisesti. Ens32-rajapinta määritettiin kuulumaan sisäverkon VLAN 562:een (kts. Kuvio 141).

```
auto ens32
iface ens32 inet static
    address 198.18.235.2
    netmask 255.255.255.0
    network 198.18.235.0
    gateway 198.18.235.1
```

Kuvio 141. DNS- palvelimen rajapinnan osoitteet

Bind9 konfiguroinnissa tarvittavat tiedostot on esitetty Kuviossa 142.

```
/etc/resolv.conf
/etc/bind/named.conf
/etc/bind/named.conf.options
/etc/bind/named.conf.local
```

Kuvio 142. Bind9 konfiguraatiotiedostot

Db.papankki.com tiedostoon määritettiin Public verkossa sijaitsevien laitteiden nimet sekä julkiset IP-osoitteet (kts. Kuvio 143).

```
GNU nano 2.5.3                               File: /etc/bind/db.papankki.com

; BIND data file for local loopback interface
;
$TTL    604800
@      IN      SOA     papankki.com.   root.papankki.com. (
                      2           ; Serial
                      604800      ; Refresh
                      86400       ; Retry
                     2419200     ; Expire
                     604800 )    ; Negative Cache TTL
;
@      IN      NS      dns-virtual-machine.papankki.com.
dns-virtual-machine.papankki.com.      IN      A      198.18.235.2
www.papankki.com.                      IN      A      198.18.235.3
tiketti.papankki.com.                  IN      A      198.18.235.4
```

Kuvio 143. Db.papankki.com tiedostoon lisättyt laitteet ja julkiset osoitteet

Named.conf.options- tiedostoon lisättiin zone papankki.com ja määritettiin polku osoittamaan db.papankki.com tiedostoon (kts. Kuvio 144).

```
GNU nano 2.5.3          File: /etc/bind/named.conf.options

options {
    directory "/var/cache/bind";

    recursion no;
    auth-nxdomain no;      # conform to RFC1035
    listen-on-v6 { any; };

};

zone "papankki.com" {
    type master;
    file "/etc/bind/db.papankki.com";
};
```

Kuvio 144. Ulkoverkon DNS- palvelinten osoitteet

Kuviossa 145 todennettuna Zone- tiedoston lisäys Bind9:n. Zonen nimaksi määritettiin db.10.

```
GNU nano 2.5.3          File: /etc/bind/named.conf.local

zone "235.18.198.in-addr.arpa" {
    type master;
    notify no;
    file "/etc/bind/db.10";
};
```

Kuvio 145. Zone db.10

Db.10 tiedostoon määritettiin papankki.com domain, sekä DNS- palvelimen nimi (kts. Kuvio 146).

```
GNU nano 2.5.3                               File: /etc/bind/db.10

; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     papankki.com.  root.papankki.com. (
                      1           ; Serial
                      604800      ; Refresh
                      86400       ; Retry
                     2419200     ; Expire
                     604800 )    ; Negative Cache TTL
;
@       IN      NS      dns-virtual-machine.papankki.com.
198.18.235.2   IN      PTR     dns-virtual-machine.papankki.com.
198.18.235.4   IN      PTR     tiketti.papankki.com.
```

Kuvio 146. db.10- tiedosto

Kaikki tarvittavat konfiguraatiot on tehty ja sisäverkon nimenselvitystä testattiin dig @localhost www.papankki.com- komennolla. Kuviossa 147 todennettuna papankki.com osoitteen selvitys sisäverkosta.

```
dns@dns-virtual-machine:~$ dig @localhost www.papankki.com

; <>> DIG 9.10.3-P4-Ubuntu <><> @localhost www.papankki.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 446
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.papankki.com.          IN      A

;; ANSWER SECTION:
www.papankki.com.      604800  IN      A      198.18.235.3

;; AUTHORITY SECTION:
papankki.com.          604800  IN      NS     dns-virtual-machine.papankki.com.

;; ADDITIONAL SECTION:
dns-virtual-machine.papankki.com. 604800 IN A  198.18.235.2

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Mar 24 11:19:04 EET 2017
;; MSG SIZE  rcvd: 111
```

Kuvio 147. Nimikyselyn testaus

5.20 Palomuuri

5.20.1 Pääkonttorin VyOS-reititin

VyOS- reititin vaati konfiguraatiomuutoksia palomuurin lisäämisen jälkeen. Reitittimestä poistettiin käytöstä ylimääräiseksi jäneet rajapinnat ja eth1- rajapinnalle annettiin IP-osoite kuvion 20 mukaisesti. Kuviossa 148 on esitetty rajapintojen osoitteet konfiguraatiomuutoksen jälkeen.

```
interfaces {
    ethernet eth0 {
        address 192.168.17.16/24
        description OUTSIDE
        duplex auto
        hw-id 00:0c:29:a1:1e:84
        smp_affinity auto
        speed auto
    }
    ethernet eth1 {
        address 172.20.0.1/24
        description INSIDE
        duplex auto
        hw-id 00:0c:29:a1:1e:8e
        smp_affinity auto
        speed auto
    }
}
```

Kuvio 148. Rajapintojen osoitteet muutoksen jälkeen

Reittimelle lisättiin staattisiksi reiteiksi Server, WS ja Public- verkkojen osoitteet. Verkot löytyvät nyt palomuurin takaa, jota on havainnollistettu kuviossa 149.

```
static {
    route 10.0.0.0/24 {
        next-hop 172.20.0.2 {
        }
    }
    route 10.100.0.0/24 {
        next-hop 172.20.0.2 {
        }
    }
    route 198.18.235.0/24 {
        next-hop 172.20.0.2 {
        }
    }
}
```

Kuvio 149. Uudet staattiset reitit

5.20.2 pfSense asennus ja konfigurointi

Asennuksen jälkeen pfSensen:n rajapinnat määritetään käyttöön ja annetaan ennalta suunnitellut osoitteet kuvion 20 mukaisesti. Todennus rajapintojen osoitteista kuvossa 150.

```
*** Welcome to pfSense 2.3.2-RELEASE (amd64 full-install) on pfSense ***
WAN (wan)      -> em0          -> v4: 172.20.0.2/24
LAN (lan)      -> em1          -> v4: 10.100.0.1/24
OPT1 (opt1)    -> em2          -> v4: 10.0.0.1/24
OPT2 (opt2)    -> em3          -> v4: 198.18.235.1/24
```

Kuvio 150. pfSense rajapinnat

LAN-rajapinnan määritysten jälkeen pääsemme tekemään konfiguraatiomuutoksia nettiselaimella käyttämällä WebGUI:ta. Palomuurin hallintasivulle pääsee servereidens oletusyhdykskäytävän IP-osoitteella 10.100.0.1. Aloitussivua havainnollistettu kuvossa 151.

The screenshot shows the pfSense 2.3.2-RELEASE dashboard. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area has two sections: 'System Information' and 'Interfaces'.

System Information:

System Information	
Name	pfSense.papanetti.com
Version	2.3.2-RELEASE (amd64) built on Tue Jul 19 12:44:43 CDT 2016 FreeBSD 10.3-RELEASE-p5
Unable to check for updates	
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU E5420 @ 2.50GHz
Uptime	23 Hours 16 Minutes 41 Seconds
Current date/time	Sat Mar 18 13:15:08 EET 2017
DNS server(s)	• 127.0.0.1 • 10.100.0.2 • 10.100.0.11
Last config change	Sat Mar 18 10:57:19 EET 2017
State table size	1% (316/47000) Show states
MBUF Usage	6% (1776/29666)
Load average	0.03, 0.04, 0.04
CPU usage	0%
Memory usage	16% of 477 MiB

Interfaces:

Interfaces			
WAN	1000baseT <full-duplex>	172.20.0.2	
LAN	1000baseT <full-duplex>	10.100.0.1	
OPT1	1000baseT <full-duplex>	10.0.0.1	
OPT2	1000baseT <full-duplex>	198.18.235.1	

Kuvio 151. pfSense aloitussivu

System- valikon alta löytyvään General Setup sivulle pääsemme määrittämään domain-nimen, DNS-palvelinten osoitteet, sekä NTP-palvelimen osoitteen (kts. Kuvio 152).

The screenshot shows the pfSense General Setup configuration page. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled "System / General Setup".

System

- Hostname:** pfSense (input field)
- Domain:** papankki.com (input field)

DNS Server Settings

DNS Server	Address	Gateway
1	10.100.0.2	none
2	10.100.0.11	none
3	DNS Server	none
4	DNS Server	none

DNS Server Override checkbox is checked. A note below it states: "If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). However, they will not be assigned to DHCP and PPTP VPN clients."

Disable DNS Forwarder checkbox is unchecked. A note below it states: "By default localhost (127.0.0.1) will be used as the first DNS server where the DNS Forwarder or DNS Resolver is enabled and set to listen on Localhost, so system can use the local DNS service to perform lookups. Checking this box omits localhost from the list of DNS servers."

Localization

- Timezone:** Europe/Helsinki (dropdown menu)
- Timeservers:** 10.100.0.2 (input field)

Kuvio 152. Domain, DNS ja NTP

VyOS-reitin hoittaa DHCP:n roolia, joten se on kerrottava pfSense:lle Services valikon alta löytyvälle DHCP Server välilehdelle. DHCP palvelu sidotaan palomuurin rajapintaan em1. Todennus kuviossa 153.

Services / DHCP Server / OPT1

WAN LAN OPT1 OPT2

General Options

Enable	<input checked="" type="checkbox"/> Enable DHCP server on OPT1 interface
Deny unknown clients	<input type="checkbox"/> Only the clients defined below will get DHCP leases from this server.
Ignore denied clients	<input type="checkbox"/> Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Subnet	10.0.0.0
Subnet mask	255.255.255.0
Available range	10.0.0.1 - 10.0.0.254
Range	From: 10.0.0.10 To: 10.0.0.254

Additional Pools

Add	Add pool
If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.	

Pool Start	Pool End	Description	Actions

Servers

WINS servers	WINS Server 1
	WINS Server 2
DNS servers	10.100.0.2
	10.100.0.3
	DNS Server 3
	DNS Server 4
Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.	

Other Options

Gateway	10.0.0.1
The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.	
Domain name	papankki.com
The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.	

Kuvio 153. DHCP asetus pfSense:ssä

Palomuurissa on oletuksena NAT päällä, joten se on myös kytkettävä pois päältä.

Emme tarvitse palomuurista löytyvää NAT:a, koska pääkonttorin VyOS- reititin hoittaa NAT:n roolia. NAT asetukset löytyvät Firewall- valikosta (kts. Kuvio 154).

Firewall / NAT / Outbound

Port Forward 1:1 Outbound NPt

General Logging Options

Mode	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> Disable Outbound NAT rule generation.
Automatic outbound		Hybrid Outbound	Manual Outbound	
NAT rule generation.		NAT rule generation.	NAT rule generation.	
(IPsec passthrough included)		(Automatic Outbound NAT + rules below)	(AON - Advanced Outbound NAT)	(No Outbound NAT rules)

Kuvio 154. NAT kytketty pois päältä

Sallimme myös SSH- yhteyden palomuuriin, jonka määritykset löytyvät System – Advanced valikosta (kts. Kuvio 155).

Secure Shell

Secure Shell Server Enable Secure Shell

Authentication Method Disable password login for Secure Shell (RSA/DSA key only)
When enabled, authorized keys need to be configured for each user that has been granted secure shell access.

SSH port
Note: Leave this blank for the default of 22.

Kuvio 155. SSH päälle

Varmistaaksemme verkon toiminnan ennen palomuurisääntöjen tekemistä, joudumme luomaan Floating säädön, joka sallii kaiken liikenteen. Tästä löytyy todennus kuviossa 156.

Edit Firewall Rule

Action Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Quick Apply the action immediately on match.
Set this option to apply this action to traffic that matches this rule immediately.

Interface
Choose the interface(s) for this rule.

Direction

Floating

Address Family
Select the Internet Protocol version this rule applies to.

Protocol
Choose which IP protocol this rule should match.

Source

Source Invert match. /

Destination

Destination Invert match. /

Kuvio 156. Floating any säätö

5.20.3 Palomuurisäännöt

Verkkomme Baselinen mukaisesti luodut säännöt on esitetty Kuvioissa 157 - 161. Kuviosta selviää myös portit, lähde- ja kohdeverkot. Jokaisen sisäverkon sääntölistan loppuun luotiin Deny-sääntö. Sen tehtävänä on estää liikenne, ellei mihinkään edellä oleviin sääntöihin osuta.

The screenshot shows the 'Floating' tab selected in the Firewall / Rules interface. The rules table has the following data:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓ 0 /0 B	IPv4 TCP	*	*	PUBLIC net	22 (SSH)	*	none		SSH	
<input type="checkbox"/> ✓ 0 /0 B	IPv4+6 *	*	*	*	*	*	none			
<input type="checkbox"/> ✓ 2 /1 KiB	IPv4 ICMP any	*	*	*	*	*	none		Ping	

Kuvio 157. Floating säännöt

The screenshot shows the 'PUBLIC' tab selected in the Firewall / Rules interface. The rules table has the following data:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> ✓ 0 /6 KB	IPv4 TCP	PUBLIC net	*	SERVERS net	25 (SMTP)	*	none			
<input checked="" type="checkbox"/> ✓ 0 /0 B	IPv4 TCP	PUBLIC net	*	SERVERS net	265	*	none			
<input checked="" type="checkbox"/> ✓ 0 /0 B	IPv4 TCP	PUBLIC net	53 (DNS)	*	53 (DNS)	*	none			
<input checked="" type="checkbox"/> ✓ 0 /0 B	IPv4 TCP	PUBLIC net	123 (NTP)	SERVERS net	123 (NTP)	*	none			
<input checked="" type="checkbox"/> ✓ 0 /0 B	IPv4 TCP	PUBLIC net	*	Sivukonttorit	389 (LDAP)	*	none			
<input checked="" type="checkbox"/> ✓ 0 /0 B	IPv4 TCP	PUBLIC net	*	Sivukonttorit	3268	*	none			
<input checked="" type="checkbox"/> ✓ 0 /0 B	IPv4 TCP	PUBLIC net	5355	*	5355	*	none			
<input checked="" type="checkbox"/> ✓ 0 /0 B	IPv4 TCP	PUBLIC net	49000-65535	*	49000-65535	*	none			
<input checked="" type="checkbox"/> ✓ 0 /2.10 MiB	IPv4 TCP	PUBLIC net	*	SERVERS net	389 (LDAP)	*	none			
<input checked="" type="checkbox"/> ✓ 0 /0 B	IPv4 TCP	PUBLIC net	*	SERVERS net	3268	*	none			
<input checked="" type="checkbox"/> ✘ 0 /0 B	IPv4 *	*	*	*	*	*	none		Block All	

Kuvio 158. Public säännöt

Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/8.21 MiB	*	*	*	SERVERS Address	80 22	*	*		Anti-Lockout Rule	
✓ 0/43.94 MiB	IPv4 *	SERVERS net	*	*	*	*	*	none	Default allow LAN to any rule	
✓ 0/0 B	IPv6 *	SERVERS net	*	*	*	*	*	none	Default allow LAN IPv6 to any rule	
✓ 0/0 B	IPv4 TCP	SERVERS net	53 (DNS)	*	53 (DNS)	*	none			
✓ 0/0 B	IPv4 TCP	SERVERS net	5355	*	5355	*	none			
✓ 0/0 B	IPv4 TCP	SERVERS net	*	PUBLIC net	80 (HTTP)	*	none			
✓ 0/0 B	IPv4 TCP	SERVERS net	*	PUBLIC net	443 (HTTPS)	*	none			
✓ 0/0 B	IPv4 TCP	SERVERS net	67	SERVERS net	67-68	*	none			
✓ 0/0 B	IPv4 TCP	SERVERS net	123 (NTP)	SERVERS net	123 (NTP)	*	none			
✓ 0/0 B	IPv4 TCP	SERVERS net	*	SERVERS net	389 (LDAP)	*	none			
✓ 0/0 B	IPv4 TCP	SERVERS net	*	SERVERS net	3268	*	none			
✓ 0/0 B	IPv4 TCP	SERVERS net	*	Sivukonttorit	389 (LDAP)	*	none			
✓ 0/0 B	IPv4 TCP	SERVERS net	*	Sivukonttorit	3268	*	none			
✓ 0/0 B	IPv4 TCP	SERVERS net	49000-65535	*	49000-65535	*	none			
✗ 0/0 B	IPv4 *	*	*	*	*	*	*	none	Block All	

Kuvio 159. Servers säänot

Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/0 B	IPv4 TCP	WS net	53 (DNS)	*	53 (DNS)	*	none			
✓ 0/0 B	IPv4 TCP	WS net	5355	*	5355	*	none			
✓ 0/3.07 MiB	IPv4 TCP	WS net	*	*	80 (HTTP)	*	none			
✓ 0/1.12 MiB	IPv4 TCP	WS net	*	*	443 (HTTPS)	*	none			
✓ 0/0 B	IPv4 TCP	WS net	67-68	SERVERS net	67-68	*	none			
✓ 0/0 B	IPv4 TCP	WS net	123 (NTP)	SERVERS net	123 (NTP)	*	none			
✓ 0/901 KB	IPv4 TCP	WS net	*	SERVERS net	389 (LDAP)	*	none			
✓ 0/0 B	IPv4 TCP	WS net	*	SERVERS net	3268	*	none			
✓ 0/469 KB	IPv4 TCP	WS net	*	SERVERS net	88	*	none			
✓ 0/46 KB	IPv4 TCP	WS net	*	SERVERS net	135	*	none			
✓ 0/1.18 MiB	IPv4 TCP	WS net	*	SERVERS net	137-139	*	none			
✓ 0/1.38 MiB	IPv4 TCP	WS net	*	SERVERS net	445 (MSDS)	*	none			
✓ 0/195 KB	IPv4 TCP	WS net	49000-65535	SERVERS net	49000-65535	*	none			
✗ 0/0 B	IPv4 *	*	*	*	*	*	*	none	Block All	

Kuvio 160. WS säännöt

Rules (Drag to Change Order)											Actions
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	Sivukonttorit	53 (DNS)	*	53 (DNS)	*	none	DNS	
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	Sivukonttorit	5355	*	5355	*	none	DNS	
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	Sivukonttorit	49000 - 65535	*	49000 - 65535	*	none	DNS	
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	Sivukonttorit	53 (DNS)	PUBLIC net	53 (DNS)	*	none	DNS	
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	Sivukonttorit	*	PUBLIC net	5355	*	none	DNS	
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	Sivukonttorit	49000 - 65535	PUBLIC net	49000 - 65535	*	none	DNS	
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	Sivukonttorit	123 (NTP)	SERVERS net	123 (NTP)	*	none	NTP	
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	Sivukonttorit	*	SERVERS net	389 (LDAP)	*	none	LDAP	
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	Sivukonttorit	3268	SERVERS net	3268	*	none	LDAP	
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	*	*	PUBLIC net	443 (HTTPS)	*	none	HTTP	
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	*	*	PUBLIC net	80 (HTTP)	*	none	HTTP	
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	Sivukonttorit	*	SERVERS net	135	*	none		
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	Sivukonttorit	*	SERVERS net	137 (NetBIOS-NS)	*	none		
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	Sivukonttorit	*	SERVERS net	138 (NetBIOS-DGM)	*	none		
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	Sivukonttorit	*	SERVERS net	139 (NetBIOS-SGN)	*	none		
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	Sivukonttorit	*	SERVERS net	445 (MS-DP)	*	none		
<input checked="" type="checkbox"/>	0 / 0 B	IPv4 *	*	*	*	*	*	*	none	Block All	

Kuvio 161. WAN säännöt

Loimme sivutoimipaikoista oman ns. aliaksen, ettei jokaisen konttorin verkolle tarvitse tehdä omia sääntöjä. Aliaksen voi luoda Firewall – Aliases valikosta. Sivukonttoreiden alias on esitetty Kuviossa 162.

Firewall / Aliases / IP			
IP	Ports	URLs	All
Firewall Aliases IP			
Name	Values	Description	Actions
Sivukonttorit	10.200.1.0/24, 10.10.1.0/24, 10.200.2.0/24, 10.10.2.0/24, 10.200.3.0/24, 10.10.3.0/24, 10.200.4.0/24, 10.10.4.0/24, 10.200.5.0/24, 10.10.5.0/24	Kaikki sivukonttorit	

Kuvio 162. Sivutoimipaikkojen alias

5.20.4 Palomuurisääntöjen todennus

Palomuurisääntöjä testattiin estämällä ICMP- liikenne verkossa. Tilatonta palomuuria pystytään näin testaamaan helposti pelkillä sääntömuutoksilla. Kuvioissa 163 ja 164 ICMP- liikenteen salliva sääntö on päällä. Aiemmin luotu kaiken liikenteen salliva sääntö käännettiin pois päältä palomuurisääntöjen luonnin jälkeen.

Floating	WAN	SERVERS	WS	PUBLIC						
Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓	0 /0 B	IPv4 TCP	*	*	PUBLIC net	22 (SSH)	*	none	SSH	 
<input type="checkbox"/> ✓	0 /0 B	IPv4+6	*	*	*	*	*	none		 
<input type="checkbox"/> ✓	0 /240 B	IPv4 ICMP any	*	*	*	*	*	none	Ping	 

Kuvio 163. ICMP- liikenne sallitaan

The screenshot shows the 'Edit Firewall Rule' configuration page. The 'Action' dropdown is set to 'Pass'. A note explains the difference between 'block' and 'reject': 'Hint: the difference between block and reject is that with reject, the packet is returned to the sender, whereas with block the packet is dropped.' Below this, there are two sections: 'Disabled' (unchecked) and 'Quick' (unchecked). The 'Interface' dropdown menu includes 'WAN', 'SERVERS', 'WS', and 'PUBLIC', with 'WAN' currently selected. A note below the interface dropdown says 'Choose the interface(s) for this rule.'

Kuvio 164. ICMP- liikenne sallittu kaikkiin rajapointoihin

Kuviossa 165 on vielä todennettu ICMP- liikenteen toimivuus pingaamalla pääkonttorin ohjainpalvelin DC1:tä työasemalta.

```
C:\Users\JussiJohtaja>ping 10.100.0.2
Pinging 10.100.0.2 with 32 bytes of data:
Reply from 10.100.0.2: bytes=32 time<1ms TTL=127
Reply from 10.100.0.2: bytes=32 time<1ms TTL=127
Reply from 10.100.0.2: bytes=32 time<1ms TTL=127
Reply from 10.100.0.2: bytes=32 time=1ms TTL=127

Ping statistics for 10.100.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Kuvio 165. Ping työasemalta ohjainpalvelimelle onnistuu

ICMP- liikenne todettiin aiemmin toimivaksi, joten seuraavaksi sääntö kielletään palomuurin Floating säädöissä. Tästä todennus kuvioissa 166 ja 167.

Floating	WAN	SERVERS	WS	PUBLIC						
Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓ 0 /0 B	IPv4 TCP	*	*	PUBLIC net	22 (SSH)	*	none		SSH	
<input type="checkbox"/> ✓ 0 /0 B	IPv4+6 *	*	*	*	*	*	none			
<input type="checkbox"/> ✗ 0 /240 B	IPv4 ICMP any	*	*	*	*	*	none		Ping	

Kuvio 166. Block ICMP

Firewall / Rules / Floating / Edit

Edit Firewall Rule

Action: Block ▼
 Choose what to do with packets that match the criteria specified.
 Hint: the difference between block and reject is that with reject the packet is returned to the sender, whereas with block the packet is dropped.

Disabled: Disable this rule
 Set this option to disable this rule without removing it from the configuration.

Quick: Apply the action immediately on match.
 Set this option to apply this action to traffic that matches this rule.

Interface: WAN
SERVERS
WS
PUBLIC ^ ▼
 Choose the interface(s) for this rule.

Kuvio 167. ICMP blokattu kaikissa rajapinnoissa

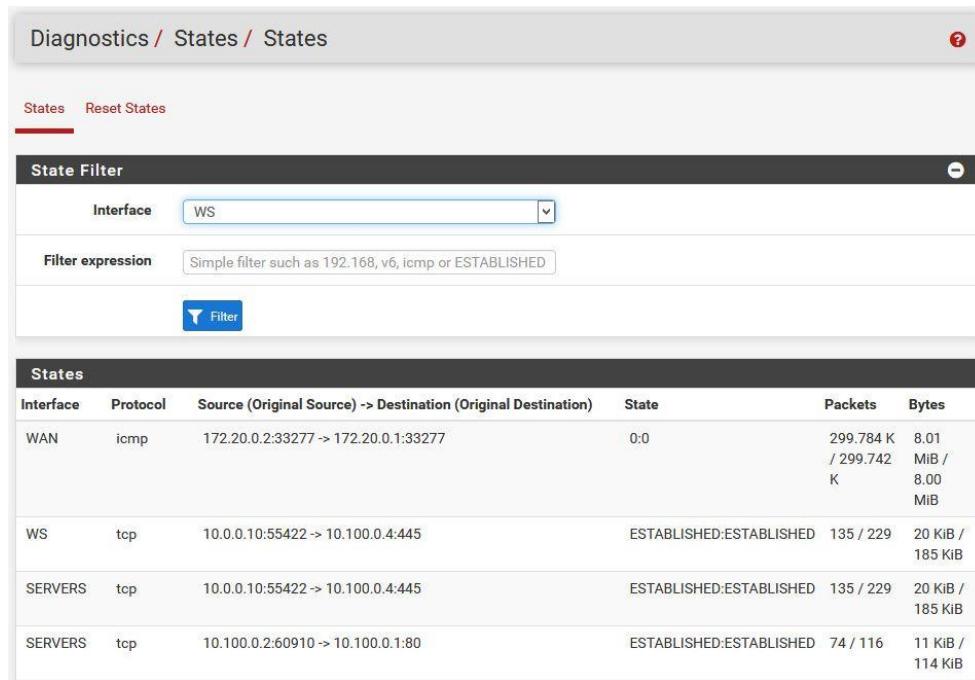
Sääntömuutoksen jälkeen työasemalta yritettiin uudestaan pingata pääkonttorin ohjainpalvelin DC1:tä. Kuviosta 168 selviää, että ping ei mene läpi, jonka edellä tehty sääntömuutos estää.

```
C:\Users\JussiJohtaja>ping 10.100.0.2
Pinging 10.100.0.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.100.0.2:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Kuvio 168. ICMP- todennus sääntömuutoksen jälkeen

Palomuurin Diagnostics – States välilehdeltä löytyy myös tilataulu, joka kertoo tapahtuneesta liikenteestä. Taulusta löytyy lähde-, kohdeverkot ja portit molempien suuntiin. Kuviossa 169 osa palomuurin tilataulusta edellä tehdyin sääntöjen testailun ja todennuksen jäljiltä.



The screenshot shows the 'Diagnostics / States / States' interface. At the top, there are 'States' and 'Reset States' buttons. Below is a 'State Filter' section with an 'Interface' dropdown set to 'WS', a 'Filter expression' input field containing 'Simple filter such as 192.168, v6, icmp or ESTABLISHED', and a 'Filter' button. The main table has a header 'States' and columns: Interface, Protocol, Source (Original Source) -> Destination (Original Destination), State, Packets, and Bytes. The data rows are:

Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
WAN	icmp	172.20.0.2:33277 -> 172.20.0.1:33277	0:0	299.784 K / 299.742 K	8.01 MiB / 8.00 MiB
WS	tcp	10.0.0.10:55422 -> 10.100.0.4:445	ESTABLISHED:ESTABLISHED	135 / 229	20 KIB / 185 KIB
SERVERS	tcp	10.0.0.10:55422 -> 10.100.0.4:445	ESTABLISHED:ESTABLISHED	135 / 229	20 KIB / 185 KIB
SERVERS	tcp	10.100.0.2:60910 -> 10.100.0.1:80	ESTABLISHED:ESTABLISHED	74 / 116	11 Kib / 114 Kib

Kuvio 169. PfSense tilataulu

5.21 Owncloud toteutus ja LDAP- integraatio

Owncloudin toteuttaminen aloitettiin asettamalla repoon reitti, mistä Owncloudin saa asennettua. Kuviossa 170 on kyseinen reitti.

```
nano 2.6.3                                         File: owncloud.list

deb https://download.owncloud.org/download/repositories/stable/Ubuntu_16.04/ /
```

Kuvio 170. Kohdepolku, mistä Owncloud pystyy lataamaan halutut paketit

Tämän jälkeen päivitettiin järjestelmä ja asennettiin Owncloudin paketti. Asennuksen jälkeen Owncloudille tarvittiin tietokanta. Kuviossa 171 tietokannan luonti.

```
pekka@CLOUD:/$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5
Server version: 5.7.17-0ubuntu0.16.10.1 (Ubuntu)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

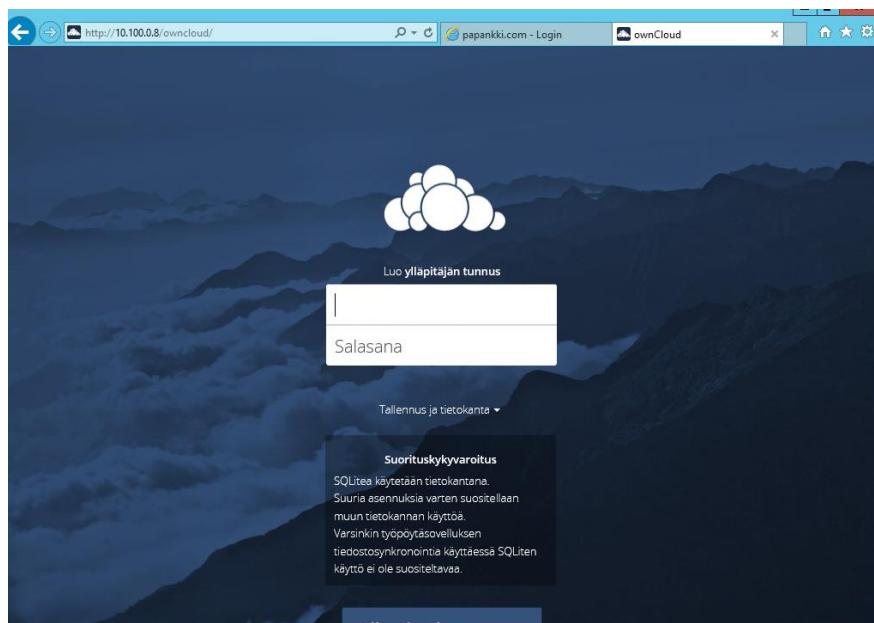
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE DATABASE owncloud;
```

Kuvio 171. Tietokannan luonti Owncloudille

Tämän jälkeen päästään näkemään owncloudin etusivu asettamalla verkkoselaimseen IP/owncloud. Aluksi luotiin admin-käyttäjä, jolla pystytiin muokkaamaan owncloudin asetuksia selaimen kautta. Kuviossa 172 näkyy ADMIN- käyttäjän luonti.



Kuvio 172. Admin käyttäjän luonti asennuksen jälkeen

Kirjautumisen jälkeen päästiin luomaan testikäyttäjät kissa ja koira kuviossa 173.

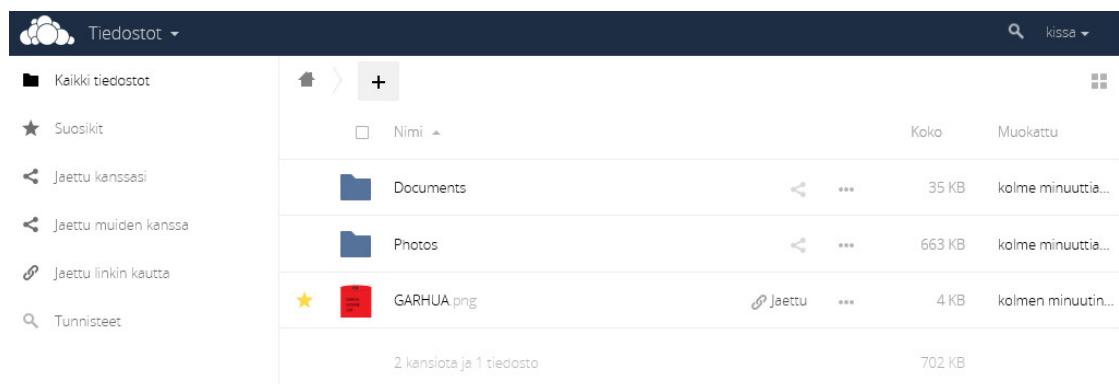
The screenshot shows the "Käyttäjät" (Users) page in the OwnCloud settings. The URL is http://10.100.0.8/owncloud/index.php/settings/users. On the left, there are filters for "Käyttäjätunnus" (Username), "Salasana" (Password), "Testieläimet" (Groups), and a "Luo" (Create) button. The main table lists three users:

	Käyttäjätunnus	Koko nimi	Salasana	Testieläimet	Ryhmat	Ryhmyläpätevät
3	admin	admin	*****	admin	admin	ei ryhmää
1	A					
2	kissa	kissa	*****	Testieläimet	Testieläimet	ei ryhmää
2	koira	koira	*****	Testieläimet	Testieläimet	ei ryhmää

On the right, a sidebar menu is open with options: Henkilökohtainen (Personal), Käyttäjät (Users), Ohje (Help), Ylläpito (Maintenance), and Kirjaudu ulos (Logout). The "admin" user is currently selected.

Kuvio 173. Testikäyttäjien luonti

Tämän jälkeen kirjauduttiin käyttäjällä kissa ja ladattiin tiedosto testaten näin toimivuutta. Ladattiin GARHUA.png tiedosto ja sen lataamisessa tai jakamisessa ei ollut ongelmia. Kuviossa 174 näemme GARHUA-tiedoston.



Kuvio 174. Tiedoston lisääminen pilveen onnistui

Seuraavaksi haluttiin liittää palvelu Windows AD:hen, jotta käyttäjät pystyivät kirjautumaan palveluun omilla tunnuksillaan. Asennettiin paketit krb5-user, winbind, samba, ntpdate ja libpam-modules. Tämän jälkeen tarkistettiin vielä toimivuus DC1:lle ja lisättiin NTP hakemaan aika DC1:ltä 5 minuutin välein. Tämän komennon näemme kuviossa 175.

```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *      * * *    root    cd / && run-parts --report /etc/cron.hourly
25 6      * * *    root    test -x /usr/sbin/anacron || ( cd / && run-parts
47 6      * * ?    root    test -x /usr/sbin/anacron || ( cd / && run-parts
52 6      1 * *    root    test -x /usr/sbin/anacron || ( cd / && run-parts
*/5 *     * * *    root    ntpdate dc1-ah.papankki.com
#
```

Kuvio 175. NTP:n asettaminen

Tämän jälkeen kuviossa 176 asetettiin kerberoksen konfiguraatio-tiedostoon palvelimen asetukset

```
[domain_realm]
.mit.edu = ATHENA/MIT.EDU
mit.edu = ATHENA/MIT.EDU
.media.mit.edu = MEDIA-LAB/MIT.EI
media.mit.edu = MEDIA-LAB/MIT.EI
.csail.mit.edu = CSAIL/MIT.EDU
csail.mit.edu = CSAIL/MIT.EDU
.whois.edu = ATHENA/MIT.EDU
whois.edu = ATHENA/MIT.EDU
.stanford.edu = stanford.edu
.slac.stanford.edu = SLAC.STANFORD.EDU
.toronto.edu = UTORONTO.CA
.utoronto.ca = UTORONTO.CA
.papankki.com = PAPANKKI.COM
papankki.com = PAPANKKI.com

[login]
krb4_convert = true
krb4_get_tickets = false
```

Kuvio 176. Konfiguraatioiden asettaminen palvelimen löytämiseksi

Tämän jälkeen testattiin konfiguraatiota kinit-komennolla kuviossa 177. Koska virheilmoitusta ei tullut, yhteys toimii.

```
pekka@CLOUD:/etc/network$ kinit Administrator@PAPANKKI.COM
Password for Administrator@PAPANKKI.COM:
pekka@CLOUD:/etc/network$ _
```

Kuvio 177. Yhteys DC1:seen testattui

Seuraavaksi tarkistettiin sambaan asetetut konfiguraatiot (Kuvio 178.). Virheilmoitukset eivät tullut, joten voidaan edetä.

```
pekka@CLOUD:~$ testparm
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Processing section "[printers]"
Processing section "[print$]"
Loaded services file OK.
Server role: ROLE_DOMAIN_MEMBER

Press enter to see a dump of your service definitions
```

Kuvio 178. Samban konfiguraation testaus

Lopuksi samba- ja winbind- palvelut käynnistettiin uudelleen ja yhdistettiin Ubuntu AD:hen. (Kts. kuvio 179.)

```
pekka@CLOUD:/etc/network$ sudo net ads join -U administrator@PAPANKKI.COM
Enter administrator@PAPANKKI.COM's password:
Using short domain name -- PAPANKKI
Joined 'CLOUD' to dns domain 'papankki.com'
```

Kuvio 179. Ubuntu palvelin yhdistetään AD:hen

Jotta Owncloud pystyy löytämään käyttäjät AD:ltä, annettiin winbindille oikeudet kirjautua AD- tunnuksilla. (Kts. kuvio 180.)

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc-reference' and 'info' packages installed, try:
# 'info libc "Name Service Switch"' for information about this file.

passwd:      compat winbind
group:       compat winbind
shadow:      compat
gshadow:     files
```

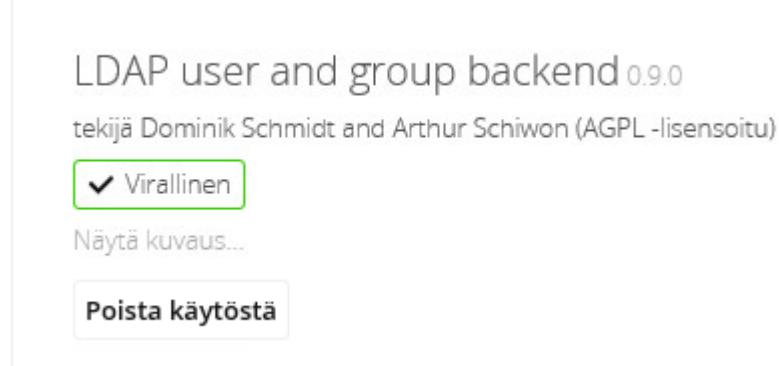
Kuvio 180. Winbind saa oikeudet kirjautua

Myös Linux koneeseen asetetaan pääsy tunnuksilla. Komennot asetettiin tiedostoihin common-auth, -account ja -session kuviossa 181.

```
# here are the per-package modules (the "Primary" block)
account sufficient      pam_winbind.so
account [success=1 new_authtok_reqd=done default=ignore]
# here's the fallback if no module succeeds
#
# here are the per-package modules (the "Primary" block)
auth    [success=1 default=ignore]      pam_unix.so nullok_
auth    sufficient      pam_winbind.so
# here's the fallback if no module succeeds
#
# here are the per-package modules (the "Primary" block)
session required      pam_mkhomedir.so
session [default=1]          pam_permit.so
# here's the fallback if no module succeeds
```

Kuvio 181. Winbind:n pääsy asetus kolmeen tiedostoon

Lopuksi tehtiin kotikansio AD käyttäjille ja asetettiin LDAP- lisäosa owncloudiin. (Kts. kuva 182.)



Kuvio 182. LDAP lisäosan ottaminen käyttöön

LDAP:n asetuksista syötettiin palvelimen asetukset ja testattiin niiden toimivuus kuvissa 183.

Kuvio 183. Owncloud LDAP asetukset

Käyttäjiksi ladattiin kaikki tarvittavat käyttäjät kuviossa 184 ja testattiin Jussi Johtajan kirjautumista. Määritykset olivat kunnossa ja Jussi Johtaja pystyi siis kirjautumaan ja määritykset näyttivät vihreää valoa.



Kuvio 184. Testikirjautuminen käyttäjällä JussiJohtaja

Tämän jälkeen hyväksyttiin kirjautuminen myös sähköpostin kautta, joka oli tyylilä etunimisukunimi@papankki.com. (Kts. kuvio 185.)

LDAP

Palvelin	Käyttäjät	Login Attributes	Ryhmät	Lisäasetukset	Expert
----------	-----------	------------------	--------	---------------	--------

When logging in, ownCloud will find the user based on the following attributes:

LDAP-/AD-
käyttäjätunnus:

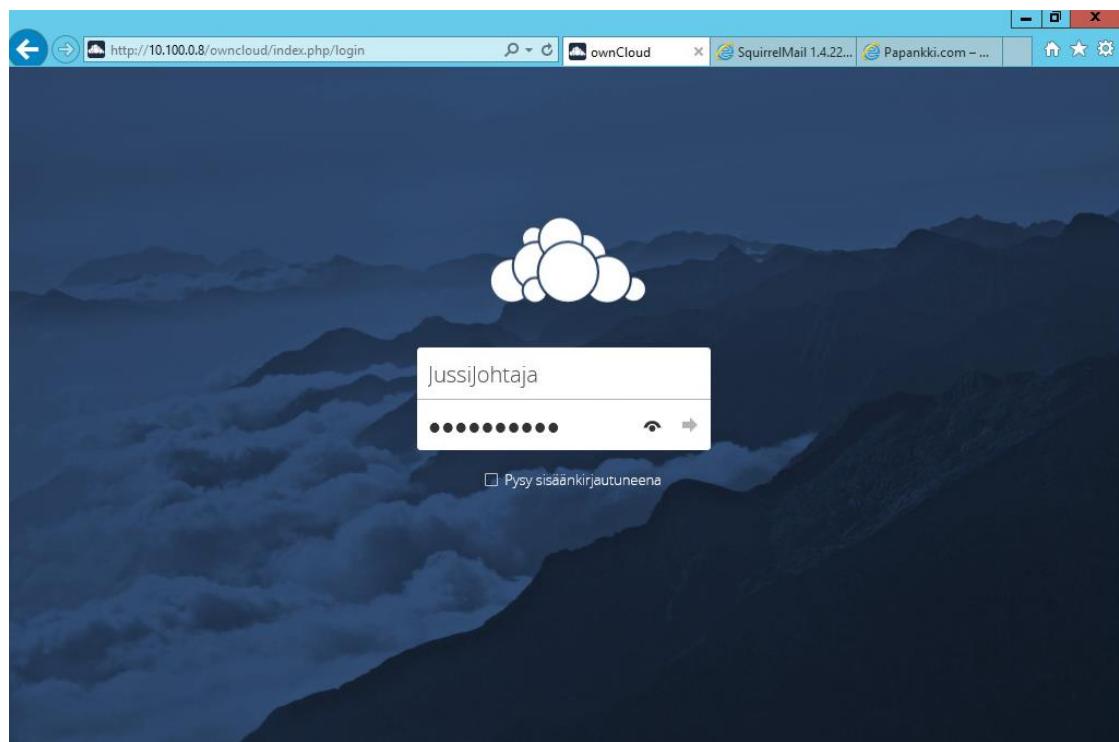
LDAP-/AD-
sähköpostiosoite:

Other Attributes:

[Muokkaa LDAP-kyselyä](#)

Kuvio 185. Kirjautumistapojen hyväksyminen

Lopuksi testataan, toimiiko kyseinen järjestelmä ja kirjaudutaan sisään käyttäjällä jussi johtaja kuviossa 186.



Kuvio 186. Jussi Johtajan kirjautumistiedot

Järjestelmä toimii ja päästään tiedostoihin, jotka näkyvät kuviossa 187.

Nimi	Koko	Muokattu
Documents	35 KB	neljän minuutin p...
Photos	663 KB	neljän minuutin p...

Kuvio 187. Jussi Johtajan tiedostot

Testataan vielä toista käyttäjää, joka on Pate Palvelin. Myös tämä käyttäjä pääsee kirjautumaan palveluun, joka tarkoittaa sitä, että palvelu toimii halutulla tavalla. (Kts. kuvio 188.)

	Nimi	Koko	Muokattu
	Documents	35 KB	neljän minuutin p...
	Photos	663 KB	neljän minuutin p...
	2 kansiota	698 KB	

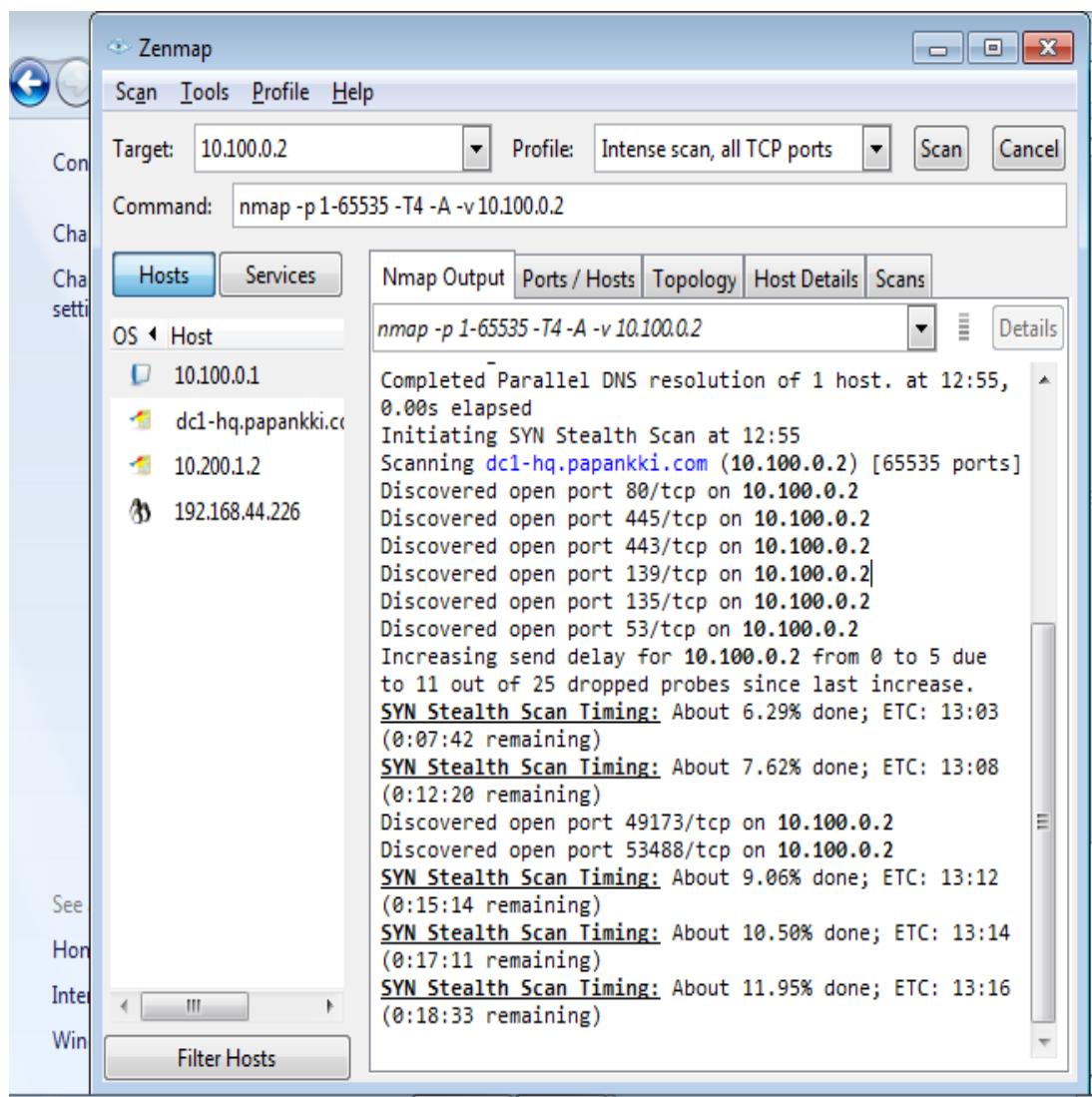
Kuvio 188. Pate Palvelimen kirjautuminen

5.22 Snort

Snorttia yrityttiin ensin toteuttaa Windowsille, mutta tämä epäonnistui koska Snort ei jostain syystä tunnistanut virtuaalikoneen rajapintoja. Tuon jälkeen Snortia yrityttiin asentaa Ubuntulle, mutta siinäkin kohdassa havaittiin ongelmia.

Sitten selvisi, että PfSense palomuuriin Snort on suhteellisen helppo asentaa ohelman oman paketinhallinnan kautta. Tämän jälkeen piti vielä ladata Snortille community säännöt, jotka ovat tietyn yhteisön ylläpitämät ilmaiset säännöt. Olisi ollut myös mahdollista ladata Snort VRT-ryhmän ylläpitämiä maksullisia sääntöjä, mutta niille ei ollut mitään tarvetta tässä.

Kun Snortin asetukset olivat kunnossa, niin tehtiin Zenmap skannaus IP-osoitteesta 10.10.1.12. (Kts. kuvio 189.)



Kuvio 189. Zenmap

Snort hälytti skannauksesta. (Kts kuvio 190.)

Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2017-03-24 12:51:10	3	TCP	Unknown Traffic	10.10.1.12	1573	10.100.0.2	80	119:31	(http_inspect) UNKNOWN METHOD
2017-03-24 12:49:43	3	TCP	Unknown Traffic	10.100.0.2	61439	10.100.0.1	80	119:31	(http_inspect) UNKNOWN METHOD
2017-03-24 --:--	3	TCP	Unknown	10.100.0.2	88	10.10.1.12	1409	120:3	(http_inspect) NO CONTENT-

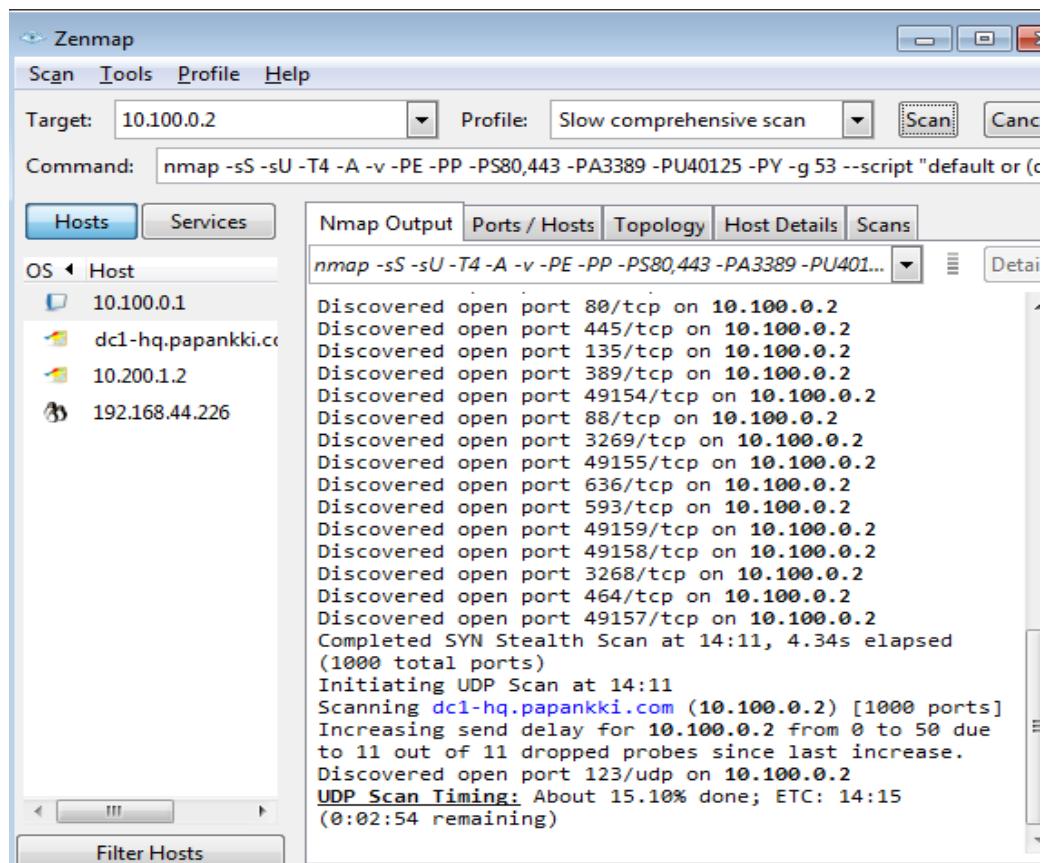
Kuvio 190. Snort Alert

Tämän jälkeen laitettiin IPS päälle, mutta jostain syystä "Which IP to Block" ei pystynyt vaihtamaan esimerkiksi Sourceen. (Kts. kuvio 191.)

Alert Settings	
Send Alerts to System Logs	<input type="checkbox"/> Snort will send Alerts to the firewall's system logs
Block Offenders	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Snort alert
Kill States	<input type="checkbox"/> Checking this option will kill firewall states for the blocked IP. Default is checked.
Which IP to Block	BOTH

Kuvio 191. Snort IPS

En tiedä johtuuko edellä mainitusta, mutta jostain syystä BLOCK-välilehden alle ei tulut mitään, mutta ei toisaalta tullut myöskään ALERT-välilehden alle, joten IPS toimii. (Kts. Kuviot 192. ja 193.)



Kuvio 192. Zenmap Snort IPS

Last 250 Alert Log Entries									
Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2017-03-24 14:02:20	3	TCP	Unknown Traffic	10.10.1.12	3291	10.100.0.2	80	119:31	(http_inspect) UNKNOWN METHOD
2017-03-24 14:01:03	3	TCP	Unknown Traffic	10.100.0.2	88	10.10.1.12	3128	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2017-03-24 14:00:57	3	TCP	Unknown Traffic	10.100.0.2	593	10.10.1.12	3111	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2017-03-24 13:57:39	3	TCP	Unknown Traffic	10.100.0.2	88	10.10.1.12	2809	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE

Kuvio 193. Snort ei hälytystä

5.23 Monitoroinnin toteutus

Pystytimme Centos 7.3-palvelimen ja asensimme sinne OpenNMS 19.0.1-ohjelmaan vaadittavat paketit. Lisäksi oli suositeltavaa asentaa jrrd2 ja iplike paketit, jotta saisimme helpotettua työskentelyämme OpenNMS parissa. Yllä mainitut paketit saatiiin helposti asennettua käyttämällä OpenNMS tarjoamaa repositorya yum install:in kautta. Asetimme palvelimelle osoitteen 10.100.0.9, jonka kautta pääsee verkkopohjaiseen käyttöjärjestelmään kiinni.

OpenNMS palvelussa ei ole sisäänrakennettua toimintaa, millä olisi pystynyt hakemaan käyttäjät AD:ltä, joten täytyi muokata konfiguraatio tiedostoja. Alla olevissa kuvioissa 194, 195 ja 196 on tämä todennettu ottamalla todennuksia activeDirectory.xml tiedostosta.

```
<beans:value>ldap://dc1-hq.papankki.com:389/</beans:value>
<beans:value>ldap://dc2-hq.papankki.com:389/</beans:value>
</beans:list>
```

Kuvio 194. LDAP servereiden osoitteet

```
<beans:bean id="authenticationSource" class="org.springframework.ldap.authentication.DefaultAuthenticationSource">
    <beans:property name="target" ref="springSecurityAuthenticationSource"/>
    <!-- Identify an unprivileged user for initial binding to the directory -->
    <!-- In some cases, expressing the user as an LDAP DN is the right way -->
    <beans:property name="defaultUser" value="CN=LDAP,CN=Users,DC=papankki,DC=com"/>
    <!-- In other cases, it's necessary to express it in user@domain format -->
    <!-- <beans:property name="defaultUser" value="opennms_bind@example.org"/> -->
    <!-- Specify the unprivileged bind user's password here -->
    <beans:property name="defaultPassword" value="Kissa123"/>
</beans:bean>
```

Kuvio 195. LDAP bind

```

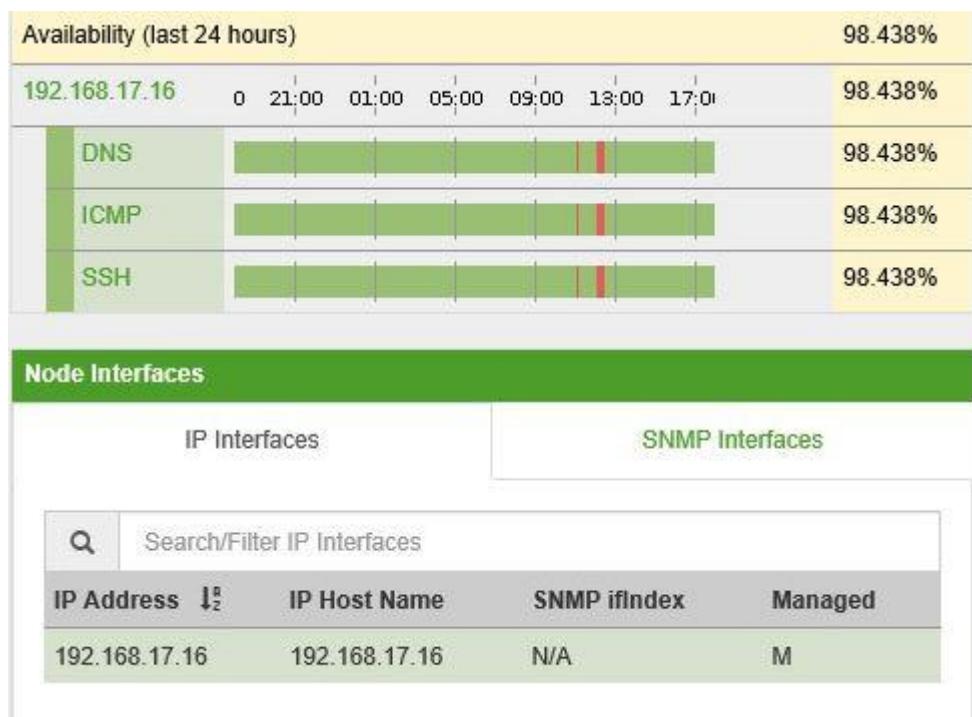
<beans:map>
  <beans:entry>
    <!-- Name of the AD group for normal (non-admin) OpenNMS users -->
    <beans:key><beans:value>ATK-tuki</beans:value></beans:key>
    <beans:list>
      <beans:value>ROLE_USER</beans:value>
      <!-- <beans:value>ROLE_DASHBOARD</beans:value> -->
    </beans:list>
  </beans:entry>
  <beans:entry>
    <!-- Name of the AD group for OpenNMS administrators -->
    <beans:key><beans:value>ATK-tuki</beans:value></beans:key>
    <beans:list>
      <beans:value>ROLE_USER</beans:value>
      <beans:value>ROLE_ADMIN</beans:value>
    </beans:list>
  </beans:entry>
</beans:map>
</beans:property>
</beans:bean>

</beans:beans>

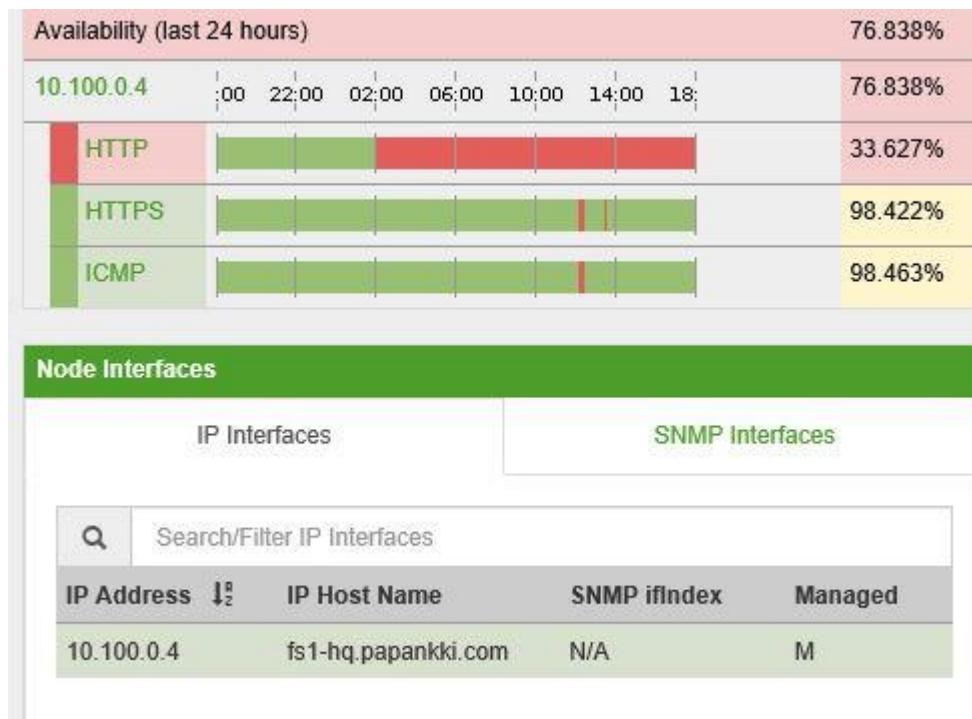
```

Kuvio 196. Ryhmät johon täytyy kuulua

AD käyttäjiä ei kuitenkaan saatu toimimaan kunnolla, joten jätimme sen aikaa säästääksemme pois käytöstä. Yhteystietojen monitorointi onnistui ongelmissa, ei tarvinnut kuin lisätä halutun järjestelmän IP ja tämän avulla pystyimme valvomaan, oliko järjestelmässämme ongelmia. Kuviossa 197 on todennettu HQ-VyOS reitittimen toimintaa ja Kuviossa 198 HTTP ongelmia FS1-HQ ongelmia.



Kuvio 197. Liikenne toimii HQ-VyOS



Kuvio 198. Ongelmia havaittu FS1-HQ

SNMP täytyi aktivoida laitteilla, joissa halusimme saada hälytyksiä. Todennus kuviossa 199 R1-HQ:ltä.

```
vyos@R1-HQ# show service snmp
community opennms {
    authorization rw
    client 10.100.0.9
}
[edit]
```

Kuvio 199. SNMP R1-HQ

SNMP täytyi ainoastaan laittaa päälle, mikäli halusimme kuviossa 200 todennetun hälytyksen toimivan.



Kuvio 200. Kovalevy liian täynnä

Kovalevy skannauksen toiminta vaati snmpd.conf muokkausta ja sinne täytyi tehdä alla olevassa kuviossa 201 todennettu rivi. Tämä täytyi tehdä kaikille laitteille, joille haluttiin kovalevyn monitorointi.

```
rocommunity MyCommunityString
disk /
```

Kuvio 201. SNMP konfigurointi HQ-WEB palvelimelta

Kaikista hälytyksistä tuli lähettilä sähköposti ylläpitäjille. Sähköposti hälytysten toimivuutta on todennettu kuviossa 202.

<input type="checkbox"/> OpenNMS	5:56 pm	Notice #6: node 192.168.17.216 down.
<input type="checkbox"/> jussijohtaja@papankki.com	4:53 pm	Kanaali
<input type="checkbox"/> OpenNMS	4:03 pm	Authentication Failed (Notice #5)
<input type="checkbox"/> OpenNMS	3:11 pm	RESOLVED: Notice #4: SSH down on OpenNMS.papankki....
<input type="checkbox"/> harri@papankki.com	Tue, 3:39 pm	ttest

[Toggle All](#) Viewing Messages: 1 to

Kuvio 202. Sähköposti harri@papankki.com

Kovalevy monitoroinnista ei saatu sähköpostia, vaikka muista laitteista tulikin sähköpostia, joten epäilemme, että sen toteutusta ei saatu kunnolla tehtyä loppuun asti.

5.24 Tikettijärjestelmä

Palvelimena käytetään Ubuntu 16.04-server käyttöjärjestelmää, jolle annettiin VLAN 562 alueen IP-osoite (Kuvio 203).

```
tiketti@osticket:/home$ ifconfig
ens32      Link encap:Ethernet HWaddr 00:0c:29:c2:db:9a
            inet addr:198.18.235.4 Bcast:198.18.235.255 Mask:255.255.255.0
```

Kuvio 203. Tikettijärjestelmän ifconfig-tiedot

OsTicket 1.10-ohjelma vaatimusten mukaisesti asennettiin palvelimelle Apache 2.4, php5.6 sekä MySql-server versio 5.7. Asennusten jälkeen haettiin Osticket-ohjelma wgetin avulla osticket.com sivustolta, jonka jälkeen tiedostot purettiin ja asetettiin var/www/html kansion alle. Muutettiin myös html-kansion omistajaksi www-data sekä kansio-oikeudet annettiin chmod 777-komennolla. (Kts kuvio 204.)

```
tiketti@osticket:/var/www/html$ ls -a
.           assets        file.php    login.php   open.php    scripts
..          avatar.php   images     logo.php    ost-config.php  secure.inc.php
account.php bootstrap.php include   logout.php  pages     tickets.php
ajax.php    captcha.php index.php  main.inc.php profile.php upload
api         client.inc.php js        manage.php  preset.php  view.php
apps        css          kb        offline.php  sep       web.config
```

Kuvio 204. Osticket-palvelimen /var/www/html-tiedosto

Osticket vaatii oman Mysql tietokannan ja käyttäjän tietokantaan. Luotiin osticket-tietokanta, jolle annettiin ost-käyttäjälle kaikki oikeudet grant all-komennolla (Kuvio 205.). OsTicketin installoinnin yhteydessä nämä tiedot eli tietokannan nimi ja käyttäjä sekä salasana on annettava vielä järjestelmälle.

```
+-----+  
| Grants for ost@localhost |  
+-----+  
| GRANT USAGE ON *.* TO 'ost'@'localhost'  
| GRANT ALL PRIVILEGES ON 'osticket'.* TO 'ost'@'localhost'  
+-----+  
2 rows in set (0.23 sec)
```

Kuvio 205. Osticket-palvelimen tietokanta

Osticket asennuksen jälkeen asennettiin AD/LDAP-lisäosa jotta AD-käyttäjät voivat kirjautua tiketöintijärjestelmään. Tätä varten haettiin Osticket-verkkosivulta auth-ldap.phar-tiedosto, joka asetettiin /var/www/html/include/plugins-kansion alle. Tämän seurauksena voidaan nyt käyttöliittymän kautta asentaa lisäosa. Alla (Kuvio 206.) on lisäosan asetuksista kuvio, jossa määritellään domainiksi papankki.com ja LDAP-palvelimeksi 10.100.0.2 eli DC1-HQ. Lisäksi asetettiin kaikki domainin OU:t käyttäjien etsintäperusteisiin.

Default Domain: Default domain used in authentication and searches	<input type="text" value="papankki.com"/>
DNS Servers: (optional) DNS servers to query about AD servers. Useful if the AD server is not on the same network as this web server or does not have its DNS configured to point to the AD servers	<input type="text" value="10.100.0.2"/>
Generic configuration for LDAP <i>Not necessary if Active Directory is configured above</i>	
LDAP servers: Use "server" or "server:port". Place one server entry per line	<input type="text" value="10.100.0.2"/> <small>[...]</small>
Use TLS:	<input checked="" type="checkbox"/> Use TLS to communicate with the LDAP server
Connection Information <i>Useful only for information lookups. Not necessary for authentication. NOTE that this data is not necessary if you searches</i>	
Search User: Bind DN (distinguished name) to bind to the LDAP server as in order to perform searches	<input type="text" value="CN=Administrator,CN=Users,DC=papankki,DC=co"/>
Password: Password associated with the DN's account	<input type="password"/>
Search Base: Used when searching for users	<input type="text" value="OU=ATK-tuki,OU=Johtaja,OU=Ekonomistit,OU=Konttori,DC=papankki,DC=co"/>
LDAP Schema: Layout of the user data in the LDAP server	<input type="text" value="Microsoft® Active Directory"/> <small>[▼]</small>

Kuvio 206. Osticket AD/LDAP-lisäosan asetukset

Tämän jälkeen otetaan lisäosa käyttöön ja testataan toimintaa. Kirjauduttiin ATK-tuen Pate Palvelin-käyttäjällä ja luotiin tiketti järjestelmään. (Kts kuvio 207.)

Email: _____
Client: Pate Palvelin

Help Topic
WWW-palvelu *

Ticket Details
Please Describe Your Issue

Issue Summary *
Ei toimi ei

Ei toimi ei

Drop files here or choose them

[Create Ticket](#) [Reset](#) [Cancel](#)

Kuvio 207. Tiketin lähetys Pate Palvelimella

Tiketti saatiin järjestelmään, ja sitä voidaan lähteä työstämään. (Kts kuvio 208.)

The screenshot shows the OSTicket interface. At the top, there's a logo of a kangaroo and the word "OSTicket". To the right, it says "Welcome, Admin. | Admin Panel | Profile | Log Out". Below the header, there are navigation tabs: Dashboard, Users, Tasks, Tickets (which is selected), and Knowledgebase. Under the Tickets tab, there are links for "Open (1)", "Closed", and "New Ticket". A search bar with an "advanced" link is followed by a "Sort" dropdown. Below this, a table titled "Open Tickets" lists one item:

Number	Last Updated	Subject	From	Priority	Assigned To
402234	3/27/17, 7:23 PM	Ei toimi ei	Pate Palvelin	Normal	

At the bottom left of the table, there are buttons for "Select: All", "None", and "Toggle".

Kuvio 208. Tiketin saapuminen

Seuraavaksi luodaan tiketöintijärjestelmälle oma sertifikaatti luomalla ensin 2048-bitinen rsa-avainpari Openssl-ohjelmalla. Avainparista luotiin sertifointipyyntö (Kuvio 209.) Tiketti.csr, joka allekirjoitetaan CA:n toimesta.

```
tiketti@osticket:/home$ sudo openssl req -text -noout -verify -in tiketti.csr
verify OK
Certificate Request:
Data:
Version: 0 (0x0)
Subject: C=FI, ST=FI, L=HQ, O=Internet Widgits Pty Ltd, CN=198.18.235.4
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
            Modulus:
                00:ad:6c:ac:8d:dc:4a:a8:a8:83:43:93:a5:d9:98:
                a6:92:ac:76:82:32:70:a8:12:22:9d:f9:78:21:89:
                8a:e4:52:9d:0e:de:5a:08:fc:f5:e9:11:f6:d9:53:
                62:af:d4:36:39:62:e4:cc:d0:5d:c4:92:55:66:51:
                02:7e:9a:b7:2c:88:63:0c:43:e8:21:1b:15:c8:e4:
                c6:fc:47:57:53:28:62:e9:3a:3b:a0:11:2e:42:60:
                a4:a8:4a:da:4e:96:b5:85:d0:9f:57:c9:15:20:7e:
                db:29:18:20:1d:1c:72:3c:37:28:f3:18:a6:56:95:
                89:d5:d5:5d:d6:f9:e6:34:dc:fc:2f:11:b6:23:97:
                f9:9e:bd:3f:e2:20:ac:96:06:d4:06:aa:6d:54:b2:
                1e:53:d4:19:5a:23:b2:26:3d:83:91:1f:6a:48:6b:
                a7:84:bd:79:ca:7a:15:e3:e2:18:cd:b8:90:47:00:
                87:35:f6:fe:39:cd:cb:d3:ac:87:4f:81:21:0a:d3:
                5e:11:ff:ac:5e:10:1b:e0:e6:76:0c:be:b8:ec:bc:
                7d:6c:86:7a:95:df:19:4b:38:4d:40:45:c9:56:b8:
                79:ac:68:09:bc:61:55:ef:d6:40:df:ca:c0:f7:d5:
                af:be:41:e5:26:37:ee:42:5b:84:30:a7:4f:89:11:
                61:6b
            Exponent: 65537 (0x10001)
-----
```

Kuvio 209. Tiketti.csr tiedosto

Sertifointipyyntö syötetään DC1-HQ:n CertSrv-palveluun, josta ladataan allekirjoitettu Base64-koodattu sertifikaatti. Sertifikaatti lähetetään takaisin palvelimelle, jonne lisätään DC1-HQ-CA-sertifikaatti CA-ksi /etc/ssl/certs-kansioon. Alla todennus allekirjoitetusta Tiketti.cer-tiedostosta. (Kts kuvio 210.)

```
tiketti@osticket:/home$ sudo openssl x509 -in Tiketti.cer -text -noout
Certificate:
Data:
    Version: 3 (0x2)
    Serial Number:
        13:00:00:00:2c:5b:fb:af:ca:15:ab:db:f1:00:00:00:00:00:2c
Signature Algorithm: sha1WithRSAEncryption
    Issuer: DC=com, DC=papankki, CN=DC1-HQ-CA
    Validity
        Not Before: Mar 28 21:28:36 2017 GMT
        Not After : Mar 28 21:28:36 2019 GMT
Subject: C=FI, ST=FI, L=HQ, O=Internet Widgits Pty Ltd, CN=198.18.235.4
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
        Modulus:
            00:ad:6c:ac:8d:dc:4a:a8:a8:83:43:93:a5:d9:98:
            a6:92:ac:76:82:32:70:a8:12:22:9d:f9:78:21:89:
            8a:e4:52:9d:0e:de:5a:08:fc:f5:e9:11:f6:d9:53:
            62:af:d4:36:39:62:e4:cc:d0:5d:c4:92:55:66:51:
            02:7e:9a:b7:2c:88:63:0c:43:e8:21:1b:15:c8:e4:
            c6:fc:47:57:53:28:62:e9:3a:3b:a0:11:2e:42:60:
            a4:a8:4a:da:4e:96:b5:85:d0:9f:57:c9:15:20:7e:
            db:29:18:20:1d:1c:72:3c:37:28:f3:18:a6:56:95:
            89:d5:d5:5d:d6:f9:e6:34:dc:fc:2f:11:b6:23:97:
            f9:9e:bd:3f:e2:20:ac:96:06:d4:06:aa:6d:54:b2:
            1e:53:d4:19:5a:23:b2:26:3d:83:91:1f:6a:48:6b:
            a7:84:bd:79:ca:7a:15:e3:e2:18:cd:b8:90:47:00:
            87:35:f6:fe:39:cd:cb:d3:ac:87:4f:81:21:0a:d3:
            5e:11:ff:ac:5e:10:1b:e0:e6:76:0c:be:b8:ec:bc:
            7d:6c:86:7a:95:df:19:4b:38:4d:40:45:c9:56:b8:
            79:ac:68:09:bc:61:55:ef:d6:40:df:ca:c0:f7:45:
            af:be:41:e5:26:37:ee:42:5b:84:30:a7:4f:89:11:
            61:6b
        Exponent: 65537 (0x10001)
X509v3 extensions:
```

Kuvio 210. Tiketti.cer tiedosto

Määritellään vielä /etc/apache2/sites-available/default-ssl.conf tiedostoon ssl-ase-tukset, jonka jälkeen https-yhteys tiketointijärjestelmään kuului onnistua. Kerrottiin mistä löytyy palvelimen sertifikaatti sekä mistä hakea CA-tiedot. (Kts kuvio 211.)

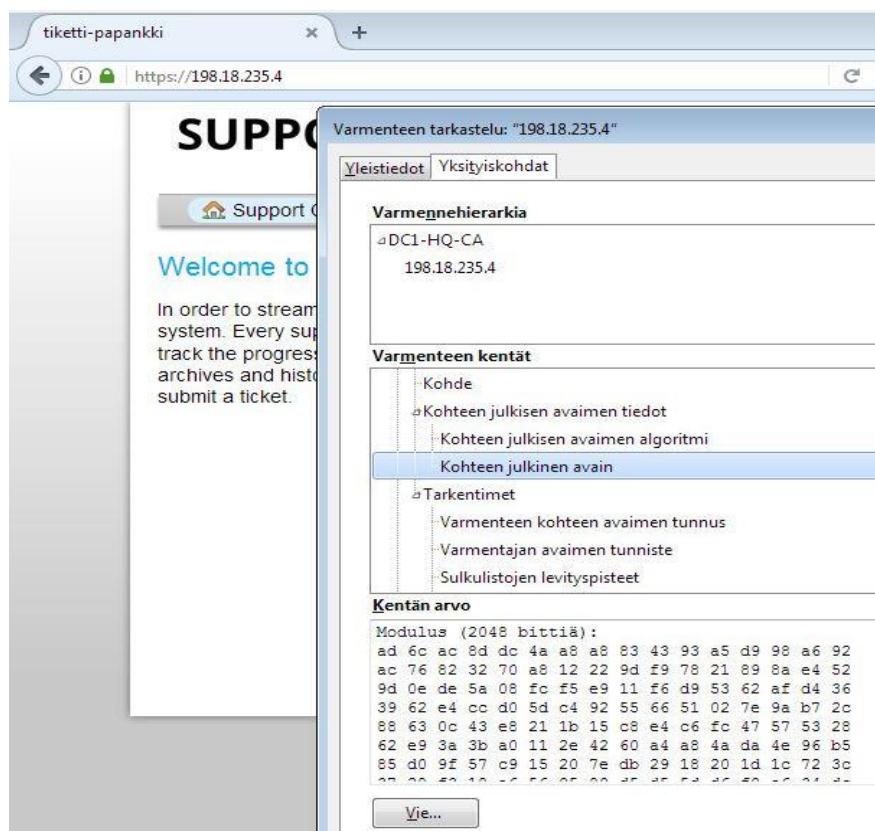
```
SSLCertificateFile      /etc/ssl/certs/Tiketti.cer
SSLCertificateKeyFile /etc/ssl/private/tiketti.key_
SSLCACertificatePath /etc/ssl/certs/
```

Kuvio 211. Apache2 default-ssl.conf tiedoston muutokset

Tämän jälkeen otettiin käyttöön ssl-moduuli sekä ssl-virtual host ja uudelleen käynnistettiin apache2 alla olevilla komennolla.

```
sudo a2enmod ssl
sudo a2ensite default-ssl
sudo /etc/init.d/apache2 restart
```

Alla (Kuvio 212.) todennus, että tiketöintijärjestelmään pääsee https-yhteydellä, sekä varmentaja ja julkinen avain.



Kuvio 212. OSticket:n HTTPS-varmenne

5.25 Lähiverkon kovennus

BPDU-guardin osalta saatiin Ciscon-laitteille asetettua halutuille rajapinnoille BPDU-guard päälle rajapintoihin ja Access-portit Portfast-tilaan. Extreme-laitteiden kanssa toteutus jäi spanning-tree tasolle. HP:n BPDU-konfiguraatiot saatiin bpdu-protection päälle. Tarkemmat konfiguraatiot löytyvät liitteistä (Liite 4, 5, 6 ,7).

Alla kuviossa (Kuvio 213.) todennetaan WG1-SW1 kytkimen VLAN asetukset, jossa kytkimelle on luotu VLAN 111 ns.blackhole vlaniks, jonka käyttämättömät rajapinnat implementoidaan sekä 563 Workstations että 563 Hallinta wlan.

WG1-SW1#sh vlan

VLAN	Name		Status	Ports		
1	default		active	Gi0/2,	Gi0/3	
111	VLAN0111		active	Gi0/1, Gi0/4, Gi0/5, Gi0/7	Gi0/8, Gi0/9, Gi0/10, Gi0/11	
561	Workstations		active	Gi0/12	Gi0/6	
563	Hallinta		active			
1002	fdmi-default		act/unsup			
1003	token-ring-default		act/unsup			
1004	fdnet-default		act/unsup			
1005	trnet-default		act/unsup			
VLAN	Type	SAID	MTU	Parent	RingNo BridgeNo Stp BrdgMode Trans1 Trans2	
1	enet	100001	1500	-	- - - - -	0 0
111	enet	100111	1500	-	- - - - -	0 0
561	enet	100561	1500	-	- - - - -	0 0
563	enet	100563	1500	-	- - - - -	0 0
1002	fdmi	101002	1500	-	- - - - -	0 0
1003	tr	101003	1500	-	- - - - -	0 0
1004	fdnet	101004	1500	-	- - - ieee -	0 0
VLAN	Type	SAID	MTU	Parent	RingNo BridgeNo Stp BrdgMode Trans1 Trans2	
1005	trnet	101005	1500	-	- - ibm - -	0 0
Remote SPAN VLANs						

Primary Secondary Type Ports

WG1-SW1#

Kuvio 213. WG1-SW1 vlanit

Alla kuviossa (Kuvio 214.) todennus kytkimen WG1-SW2 vlan-konfiguraatioista.

WG1-SW2#sh vlan

VLAN	Name		Status	Ports		
1	default		active	Fa0/1		
111	VLAN0111		active	Fa0/2, Fa0/3, Fa0/4, Fa0/5	Fa0/6, Fa0/7, Fa0/9, Fa0/10	
				Fa0/11, Fa0/12, Fa0/13, Fa0/14	Fa0/15, Fa0/16, Fa0/17, Fa0/18	
				Fa0/19, Fa0/20, Fa0/22, Fa0/23	Fa0/24	
561	Workstations		active	Fa0/21		
563	Hallinta		active			
1002	fdmi-default		act/unsup			
1003	token-ring-default		act/unsup			
1004	fdnet-default		act/unsup			
1005	trnet-default		act/unsup			
VLAN	Type	SAID	MTU	Parent	RingNo BridgeNo Stp BrdgMode Trans1 Trans2	
1	enet	100001	1500	-	- - - - -	0 0
111	enet	100111	1500	-	- - - - -	0 0
561	enet	100561	1500	-	- - - - -	0 0
563	enet	100563	1500	-	- - - - -	0 0
VLAN	Type	SAID	MTU	Parent	RingNo BridgeNo Stp BrdgMode Trans1 Trans2	
1002	fdmi	101002	1500	-	- - - - -	0 0
1003	tr	101003	1500	-	- - - - -	0 0
1004	fdnet	101004	1500	-	- - ieee -	0 0
1005	trnet	101005	1500	-	- - - ibm -	0 0
Remote SPAN VLANs						

Primary Secondary Type Ports

WG1-SW2#

Kuvio 214. WG1-SW2 vlanit

WG1-SW3 Extreme laitteelle asetettiin Hallinta vlan 563 ja Workstations vlan 561, kuten alla olevasta kuvista (Kuvio 215.) näkyy.

```
* X250e-24t.42 # show vlan
-----
```

Name	VID	Protocol	Addr	Flags	Proto	Ports	Virtual Active router /Total
Default	1				ANY	0 /0	VR-Default
Hallinta	563	192.168.0.4	/24		ANY	1 /2	VR-Default
Mgmt	4095				ANY	0 /1	VR-Mgmt
Mustareika	111				ANY	0 /23	VR-Default
temp	4092				ANY	0 /0	VR-Default
Workstations	561				ANY	2 /3	VR-Default

```
Flags : (B) BFD Enabled, (c) 802.1ad customer VLAN, (C) EAPS Control VLAN,
(d) NetLogin Dynamically created VLAN, (D) VLAN Admin Disabled,
(E) ESRP Enabled, (f) IP Forwarding Enabled,
(F) Learning Disabled, (i) ISIS Enabled, (I) Inter-Switch Connection VLAN for MLAG,
(L) Loopback Enabled, (l) MPLS Enabled, (m) IPmc Forwarding Enabled,
(M) Translation Member VLAN or Subscriber VLAN,
(n) IP Multinetting Enabled, (N) Network Login VLAN, (o) OSPF Enabled,
(O) Flooding Disabled, (p) PIM Enabled, (P) EAPS protected VLAN,
(r) RIP Enabled, (R) Sub-VLAN IP Range Configured,
(s) Sub-VLAN, (S) Super-VLAN, (t) Translation VLAN or Network VLAN,
(T) Member of STP Domain, (V) VPLS Enabled, (v) VRRP Enabled, (W) VPWS Enabled
```

```
Total number of VLAN(s) : 6
* X250e-24t.43 #
```

Kuvio 215. WG1-SW3 vlanit

WG1-SW4 HP:n kytkimelle asetettiin vlan:t samoilla spesifikaatioilla, kuten aikaisemmissakin kytkimissä. (Kts. Kuvio 216.)

```
WG1-SW4# show vlans
Status and Counters - VLAN Information

Maximum VLANs to support : 256
Primary VLAN : DEFAULT_VLAN
Management VLAN :

-----
```

VLAN ID	Name	Status	Voice	Jumbo
1	DEFAULT_VLAN	Port-based	No	No
111	Mustareika	Port-based	No	No
561	Workstations	Port-based	No	No
563	Hallinta	Port-based	No	No

```
WG1-SW4#
```

Kuvio 216. WG1-SW4 vlanit

DHCP-snooping saatiin sille tasolle, että Ciscon-laitteille asetettiin DHCP snooping halutulla tavalla. Alla kuviossa (Kuvio 217.) todennus WG1-SW1 kytkimen DHCP snooping asetuksista, jossa vain sisäverkon rajapinnat ovat luotettuja ja työaseman rajapinnan rate limit.

```

Insertion of option 82 is enabled
  circuit-id format: vlan-mod-port
  remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

```

Interface	Trusted	Rate limit (pps)
GigabitEthernet0/2	yes	unlimited
GigabitEthernet0/3	yes	unlimited
GigabitEthernet0/6	no	100

Kuvio 217. WG1-SW1 DHCP-snooping

Kuviossa (Kuvio 218.) todennus myös mitkä rajapinnat ovat luotettuja WG1-SW2 kytkimellä eli Fe0/1 rajapinta osoittaa WG1-SW1 kytkimelle ja Fe0/8, joka on yhteydessä yritysverkon palomuuriin.

```

Insertion of option 82 is enabled

```

Interface	Trusted	Rate limit (pps)
FastEthernet0/1	yes	unlimited
FastEthernet0/8	yes	unlimited
FastEthernet0/21	no	100

Kuvio 218. WG1-SW2 DHCP-snooping

Alla todennus (Kuvio 219.) WG-SW3 kytkimen DHCP-snooping aikaansaannoksista, jossa DHCP-palvelimiksi määritettiin DC1-HQ ja DC1-HQ palvelimet ja portti 1 luotetuksi portiksi.

```
* X250e-24t.48 # show ip-security dhcp-snooping vlan "Workstations"
Trusted Ports: 1
Trusted DHCP Servers: 10.100.0.2, 10.100.0.3
Bindings Restoration : Disabled
Bindings Filename :
Bindings File Location :
  Primary Server : None
  Secondary Server: None
Bindings Write Interval : 30 minutes
Bindings last uploaded at:
-----
Port          Violation-action
* X250e-24t.49 #
```

Kuvio 219. WG1-SW3 DHCP-snooping

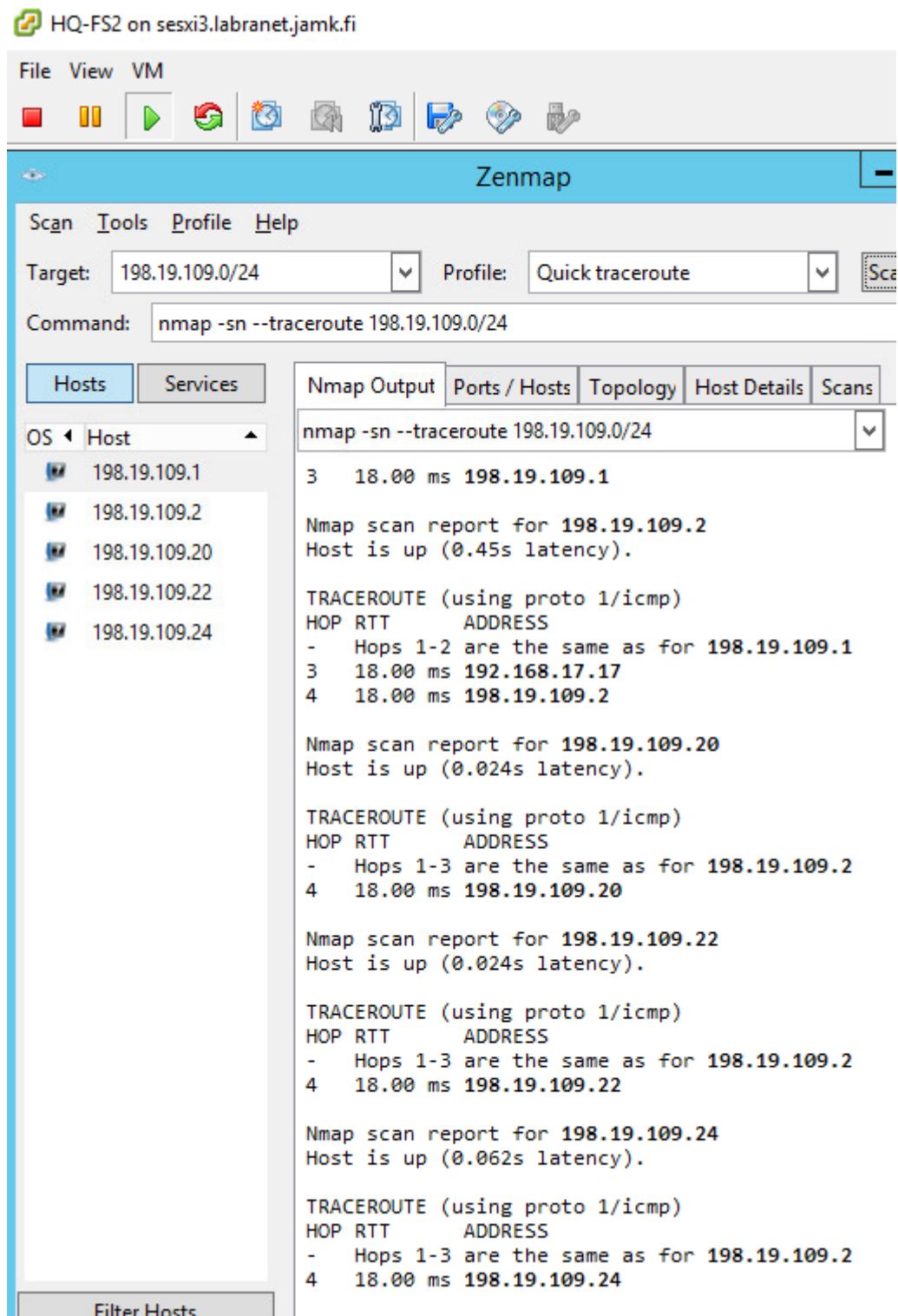
Saatiin rajoitettua CDP:n käyttöä Ciscon laitteilla eli rajoitettiin CDP toimimaan vain käytettyihin rajapintoihin ja multa rajapinnoilta myös Access-porteista pois päältä. WG1-SW1-laitteella ei LLDP:tä ollut tuettuna, joten sitä ei voitu konfiguroida. Externen laitteella oli oma Extreme Discovery Protocol, joka otettiin pois käytöstä rajapinnoilta ja vain portteihin 1 ja 2 aktivoitiin LLDP. HP:n kytkimellä otettiin CDP pois käytöstä kaikilta rajapinnoilta, mutta LLDP asetettiin porttiin 1. Tarkemmat tiedot konfiguraatioista liitteissä (Liite 4, 5, 6 ,7).

Control plane suojaus jäi vähemmälle, melkeinpä koska laitteista ei löydetty suoraan control plane protection asetuksia. Sen sijaan asetettiin ainakin Ciscon-laitteille consoli- ja telnet yhteyksile salasanat ja suojattiin salasanat service password-encryption. Lisäksi vielä asetettiin ilmoitus, banner motd-komennolla, kun käyttäjä kirjautuu laitteelle. Lisätietoa löytyy liitteistä (Liite 4, 5).

5.26 Haavoittuvuuskannaus

Toteutus meni kohtuu uusiksi, kun zenmap-skanneja ei pystynyt tekemään Keski-Suomen branchilta ilman muutoksia ja tämän takia zenmap asennettiin FS2:lle.

Aloitettiin skannaamalla ryhmä seiskan koko julkista aluetta. (Kts. kuvio 220)



Kuvio. 220 Zenmap Scan R7

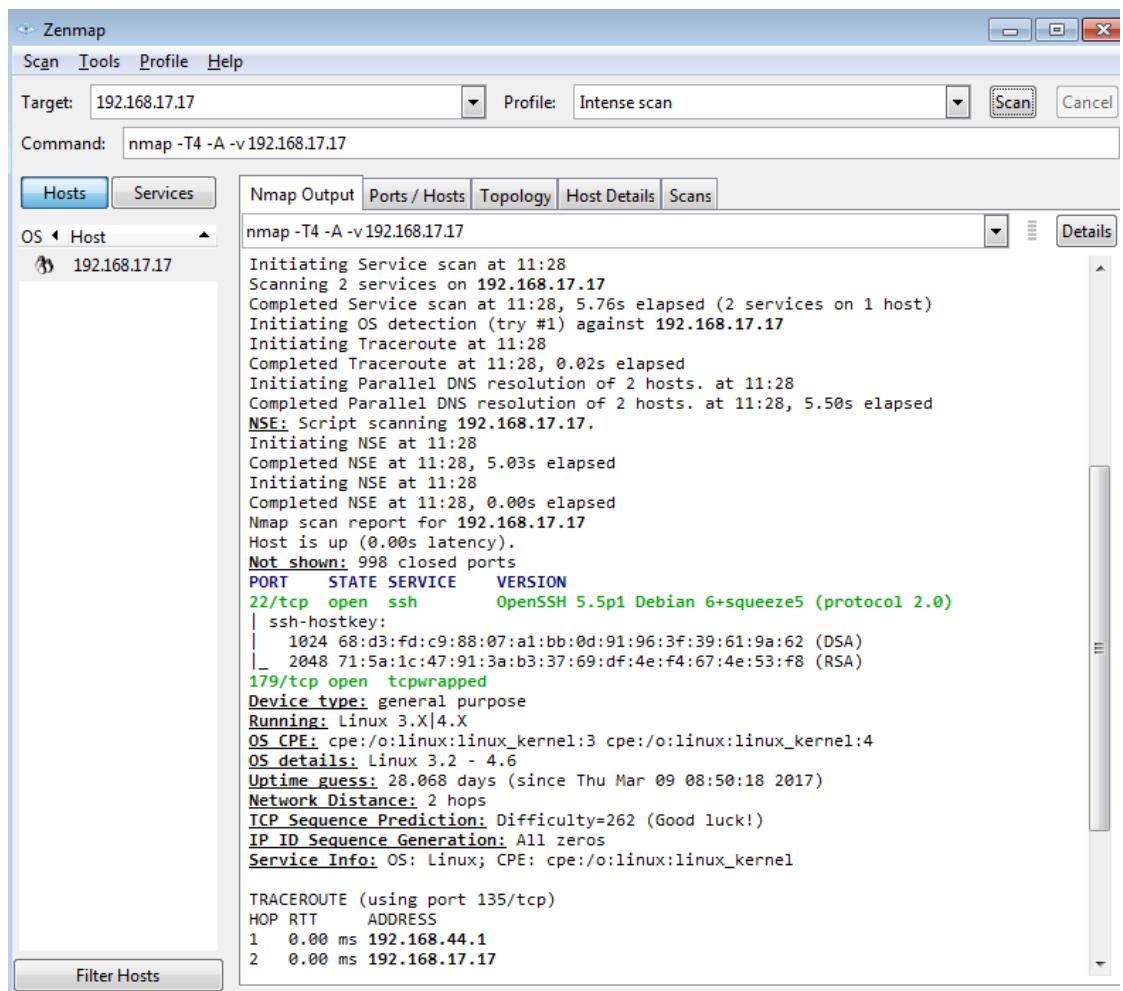
Tämän jälkeen Zenmap oli piirtänyt topologian ryhmä seiskan julkisesta verkosta.
(Kts. Kuvio 221) Kuvista käy myös ilmi eri osoitteiden käyttöjärjestelmät.



Kuvio. 221 Zenmap topologia

Seuraavaksi tarkasteltiin enemmän mahdollista VyOS-osoitetta eli 192.168.17.17.

(Kts. kuvio 222)



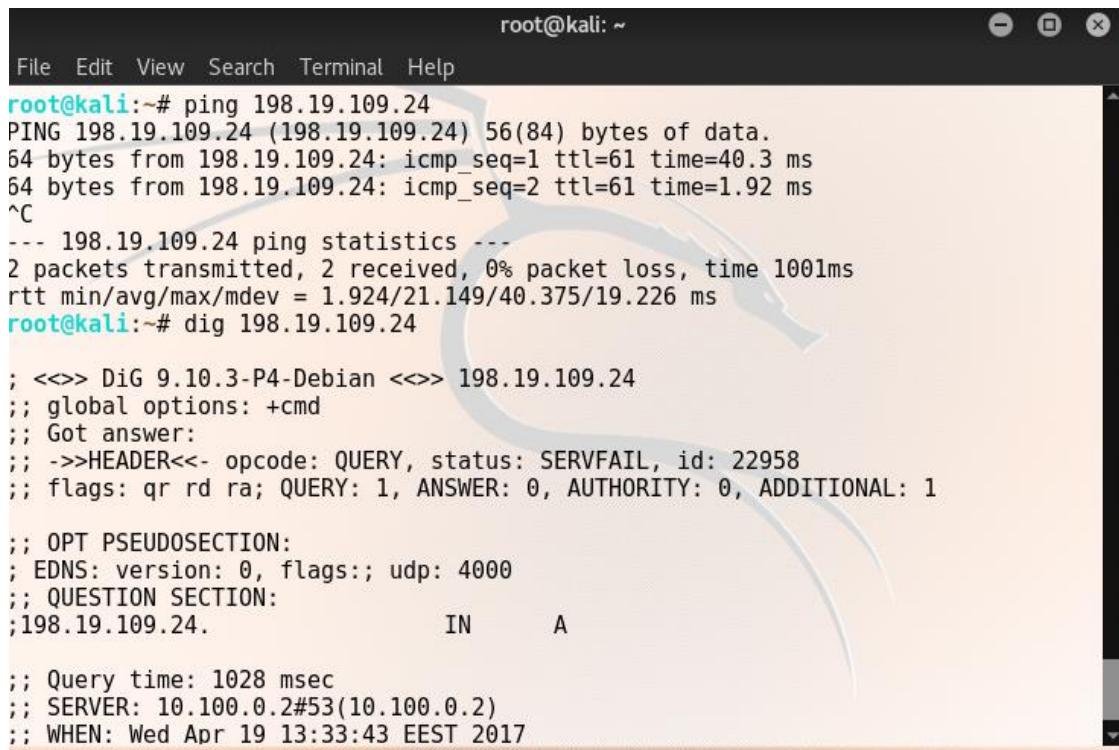
Kuvio. 222 Zenmap VyOS

Kävi siis selväksi että mm. ssh-portti on auki, joten seuraavaksi kokeiltiin ottaa SSH-yhteys. (Kts. Kuvio 223)

```
192.168.17.17 - PuTTY
login as: root
Welcome to VyOS
root@192.168.17.17's password:
Access denied
root@192.168.17.17's password:
Access denied
root@192.168.17.17's password: [REDACTED]
```

Kuvio. 223 VyOS SSH

Seuraavaksi päätimme kokeilla Kalin dig-skannia, mutta se ei tuottanut tulosta. (Kts. kuvio 224)



The screenshot shows a terminal window titled "root@kali: ~". The window contains the following text:

```
root@kali:~# ping 198.19.109.24
PING 198.19.109.24 (198.19.109.24) 56(84) bytes of data.
64 bytes from 198.19.109.24: icmp_seq=1 ttl=61 time=40.3 ms
64 bytes from 198.19.109.24: icmp_seq=2 ttl=61 time=1.92 ms
^C
--- 198.19.109.24 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.924/21.149/40.375/19.226 ms
root@kali:~# dig 198.19.109.24

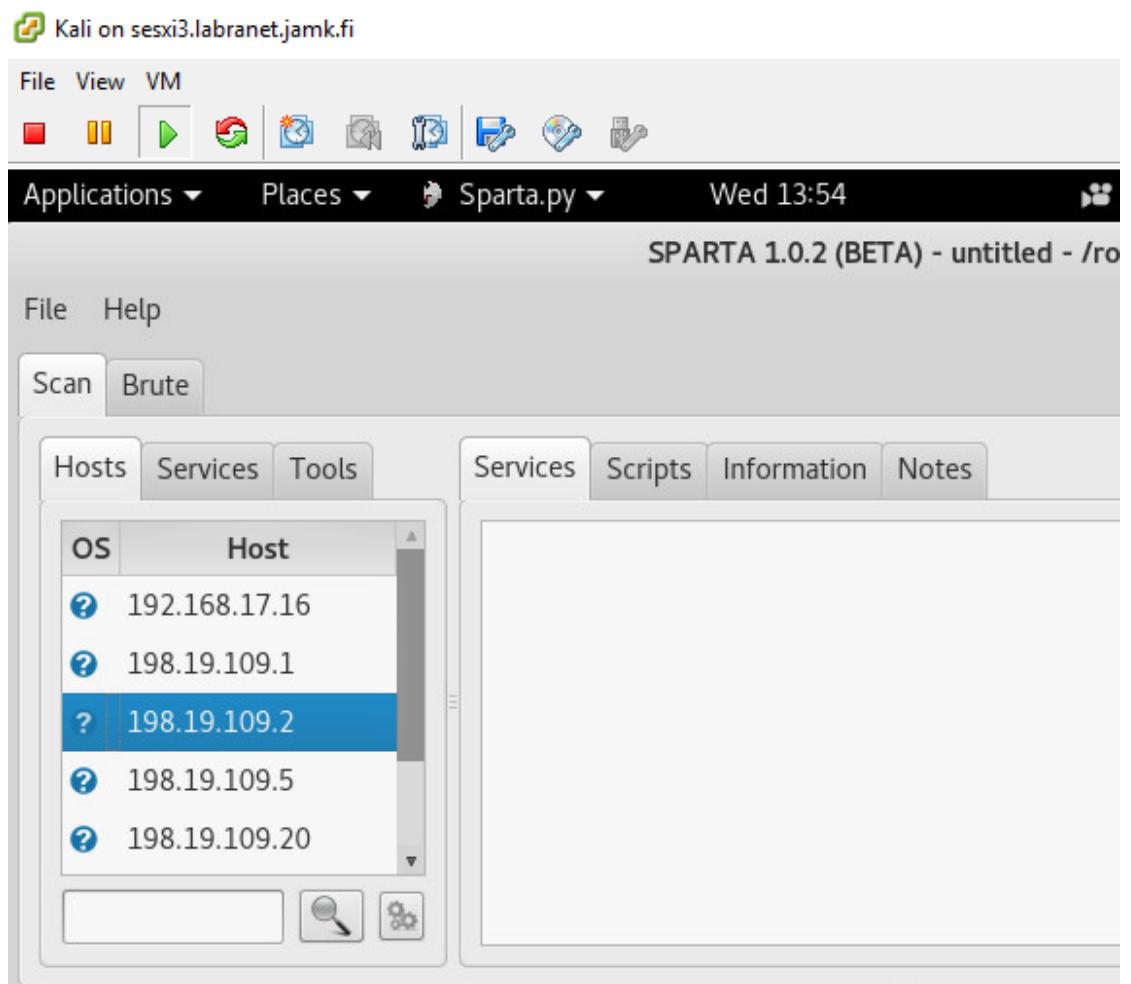
; <>> DiG 9.10.3-P4-Debian <>> 198.19.109.24
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 22958
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;198.19.109.24.           IN      A

;; Query time: 1028 msec
;; SERVER: 10.100.0.2#53(10.100.0.2)
;; WHEN: Wed Apr 19 13:33:43 EEST 2017
```

Kuvio. 224 Kali dig

Lopuksi päätettiin vielä kokeilla Kalin Sparta-ohjelmistoa. Sieltä paljastui yksi uusi osoite. Eli .5 loppuinen. (Kts. Kuvio 225)



Kuvio. 225 Kali Sparta

Loppuyhteenvetona voisi sanoa, että ryhmä seiskalla on tietoturva-asiat hyvin hallin-nassa, koska mahdollista tietoa oli todella niukasti saatavilla. Toki tähän vaikutti myös se, että verkkotunnusta ei ollut saatavilla. Tämä karsi joitakin työkaluja kokonaan pois, mutta niillä mentiin mitä oli käytössä.

5.27 Etäyhteys

Serveri konfiguroinnissa loimme vaadittavat certit ja avaimet, jotka löytyvät kuvista 226.

```
root@VPNserver:/etc/openvpn/easy-rsa/keys# ls /etc/openvpn/
ca.crt dh2048.pem easy-rsa server.conf update-resolv-conf VPN.crt VPN.key
```

Kuvio 226. Serveri Certit ja avain

OpenVPN konfigurointi onnistui ja saimme sen toimimaan ongelmitta. Tästä todennus kuviossa 227.

```
root@VPNserver:/etc/openvpn/easy-rsa/keys# service openvpn status
● openvpn.service - OpenVPN service
  Loaded: loaded (/lib/systemd/system/openvpn.service; enabled)
  Active: active (exited) since Tue 2017-04-18 21:31:56 EEST; 18h ago
    Main PID: 376 (code=exited, status=0/SUCCESS)
      CGroup: /system.slice/openvpn.service

Apr 18 21:31:56 VPNserver systemd[1]: Started OpenVPN service.
Apr 18 23:14:05 VPNserver systemd[1]: Started OpenVPN service.
root@VPNserver:/etc/openvpn/easy-rsa/keys#
```

Kuvio 227. OpenVPN toimii

Tässä ongelmat sitten alkoivatkin, sillä yhteydet eivät jostain syystä toimineet ja emme pystyneet lähettämään tarvittavia avaimia ja certtejä asiakaslaitteelle.

5.28 802.1x autentikaatio

Aluksi teimme Radius-palvelimen ja teimme vaadittavat konfiguraatiot. Tästä todennus kuviossa 228, jossa testaamme yhteyttä "testing" käytäjällä.

```

Sending Access-Request Id 24 from 0.0.0.0:60683 to 127.0.0.1:1812
  User-Name = 'testing'
  User-Password = 'testing123'
  NAS-IP-Address = 10.100.0.11
  NAS-Port = 0
  Message-Authenticator = 0x00
Received Access-Accept Id 24 from 127.0.0.1:1812 to 127.0.0.1:60683 length 28

```

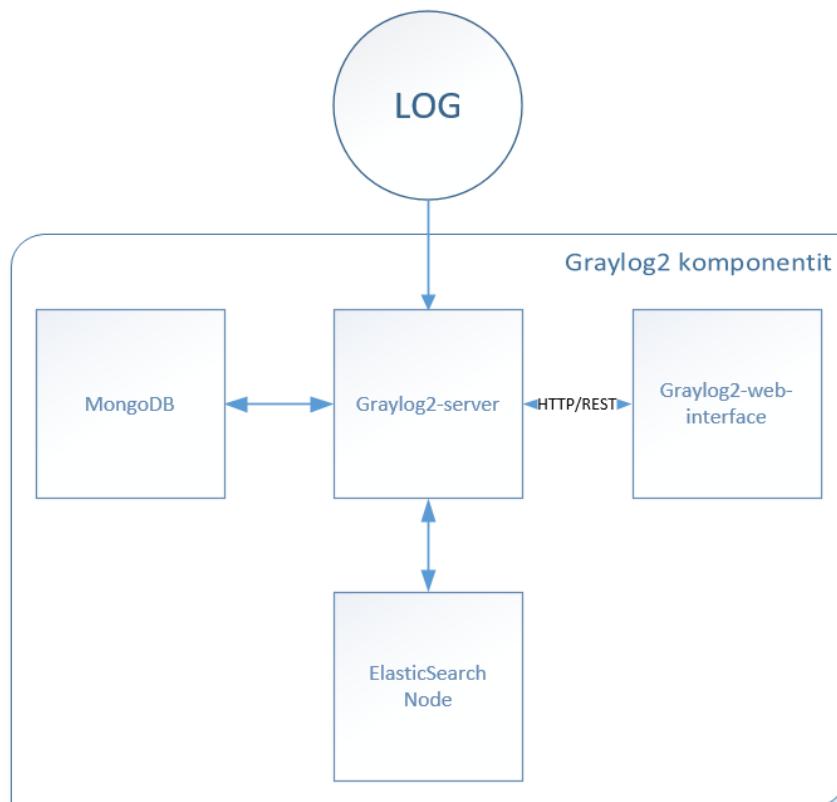
Kuvio 228. Radius-palvelimen testaus

802.1x konfigurointia Ciscon kytkimille oli tarkoitus käyttää lähiverkon kovennuksesta käytettyjä konfiguroointeja ja sitten lisätä liitteen 4 konfiguroinnit niiden päälle. Tässä ongelmaksi tuli se, että laitteille ei pääsyt kirjautumaan sisään, koska muilta ryhmiltä oli jäänyt autentikaatiot niihin päälle.

5.29 Lokienhallinta

Käytämme lokienhallinnan palvelimessa neljää palvelua. Nämä ovat Graylog2 Server node, Elasticsearch node, MongoDB ja Graylog2 Web Interface. Katso kuvio 229.

Graylog2 Server nodea. Tämä toimii palvelimena, joka vastaanottaa ja käsittelee saapuvat viestit. Palvelin keskustelee myös kaikkien muiden komponenttien kanssa. Nodeja voi olla monta, mutta yhden palvelimen täytyy toimia "Masterina", joka johtaa muita nodeja. Elasticsearch Node säilyttää kaikki lokit ja tiedot, jotka Graylog2 palvelin kerää. MongoDB Kerää metadatan, jota syntyy prosessissa. Web Interface on käyttäjän graafinen rajapinta palvelun käyttämiselle.



Kuvio 229. Lokien hallintapalvelimen osat

Järjestelmän asentaminen aloitettiin asentamalla MongoDB. Asentaminen oli hyvin yksinkertainen ja suoraviivainen. Tämän konfigurointitiedostoon ei tarvinnut siis koskea. Seuraavaksi kohteena oli Java 7. Graylog2 vaatii toimiakseen Javan, joten se asennettiin normaalisti sudo apt-get install oracle-java7-installer komennolla. Kuviossa 230 Javan asennus

```

Oracle Java 9 (for both Ubuntu and Debian): http://www.webupd8.org/2015/02/install-oracle-java-9-in-ubuntu-linux.html

For JDK9, the PPA uses standard builds from: https://jdk9.java.net/download/ (and not the Jigsaw builds!).
Important!!! For now, you should continue to use Java 8 because Oracle Java 9 is available as an early access release! You should only use Oracle Java 9 if you explicitly need it, because it may contain bugs and it might not include the latest security patches! Also, some Java options were removed in JDK9, so you may encounter issues with various Java apps. More information and installation instructions (Ubuntu / Linux Mint / Debian): http://www.webupd8.org/2015/02/install-oracle-java-9-in-ubuntu-linux.html
More info: https://launchpad.net/~webupd8team/+archive/ubuntu/java
Press [ENTER] to continue or ctrl-c to cancel adding it

gpg: keybox '/tmp/tmpuqcjltn/pubring.gpg' created
gpg: /tmp/tmpuqcjltn/trustdb.gpg: trustdb created
gpg: key C2518248EEA14806: public key "Launchpad VLC" imported
gpg: no ultimately trusted keys found
gpg: Total number processed: 1
gpg:                      imported: 1
OK

```

Kuvio 230. Javan asennus

Seuraava palvelu on elasticsearch. Asennuksen jälkeen configuroitiin clusterin nimi, palvelimen osoite, poistettiin dynaamiset scriptit käytöstä. Palvelimelle annettiin osoitteeksi localhost, jottei tähän päästä käsiksi ulkoverkosta. Kuviossa 231 tehdyt muutokset.

```

elasticsearch-0.90.10.de 100%[=====] 16.60M 8.13MB/s in 2.0s
2017-03-30 12:31:48 (8.13 MB/s) - 'elasticsearch-0.90.10.deb' saved [17403440/17403440]

pekka@Graylog:~$ sudo dpkg -i elasticsearch-0.90.10.deb
Selecting previously unselected package elasticsearch.
(Reading database ... 59456 files and directories currently installed.)
Preparing to unpack elasticsearch-0.90.10.deb ...
Unpacking elasticsearch (0.90.10) ...
Setting up elasticsearch (0.90.10) ...
Adding system user 'elasticsearch' (UID 112) ...
Adding new user 'elasticsearch' (UID 112) with group 'elasticsearch' ...
Not creating home directory '/usr/share/elasticsearch'.
Processing triggers for systemd (231-9ubuntu3) ...
Processing triggers for ureadahead (0.100.0-19) ...
pekka@Graylog:~$



##### Cluster #####
# Cluster name identifies your cluster for auto-discovery. If you're running
# multiple clusters on the same network, make sure you're using unique names.
#
cluster.name: graylog2

##### Network And HTTP #####
# ElasticSearch, by default, binds itself to the 0.0.0.0 address, and listens
# on port [9200-9300] for HTTP traffic and on port [9300-9400] for node-to-node
# communication. (the range means that if the port is busy, it will automatically
# try the next port).

# Set the bind address specifically (IPv4 or IPv6):
#
network.bind_host: localhost
script.disable_dynamic: true_

```

Kuvio 231. Elasticsearch asennus ja conffi

Seuraavaksi itse Graylog2 palvelimen asennus kuviossa 232.

```
Connecting to github-cloud.s3.amazonaws.com (github-cloud.s3.amazonaws.com) |52.216.81.0|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 57270187 (55M) [application/octet-stream]
Saving to: 'graylog2-server-0.20.2.tgz'

graylog2-server-0.20.2.t 69%[=====] 38.21M 7.65MB/s eta 3s
```

Kuvio 232. Graylog serverin asennus

Asennamme myös pwgen- nimisen ohjelman, jolla pystymme luomaan suojaatua salasanoja. Kuviossa luomme adminille salaisen avaimen ja luomme salasanasta Kissaa123 sha2 arvon kuviossa 233.

```
pekka@Graylog:/opt$ PASSWORD=$(echo -n Kissaa123 | shasum -a 256 | awk '{print $1}')
pekka@Graylog:/opt$ sudo -E sed -i -e 's/root_password_sha2 =.*$/root_password_sha2 = '$PASSWORD'/' /etc/graylog2.conf
```

Kuvio 233. Salasanan luonti

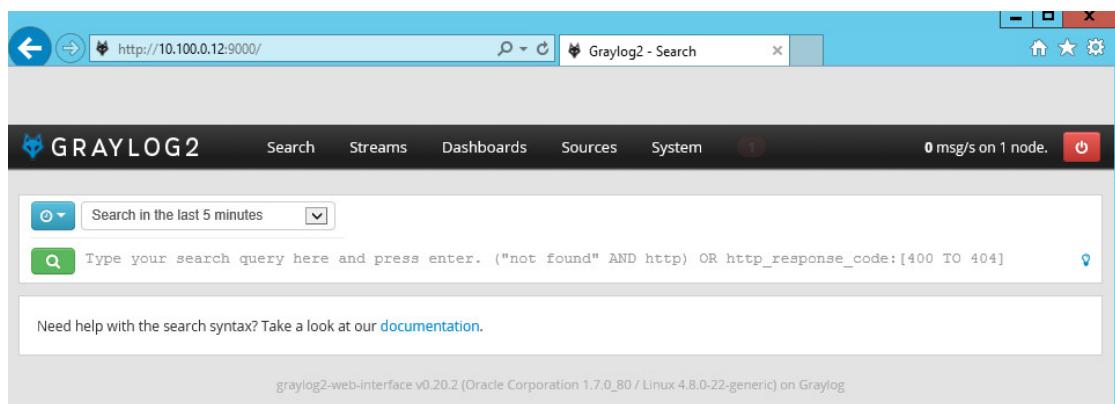
Lopuksi asensimme graylog2:en web interfacen. Kuviossa 234 palvelun asennus valmis. Seuraavaksi koitimme sisäänsijautumista palveluun ja pääsimme kirjautumaan palveluun kuviossa 235.

```
HTTP request sent, awaiting response... 200 OK
Length: 44756998 (43M) [application/octet-stream]
Saving to: 'graylog2-web-interface-0.20.2.tgz'

graylog2-web-interface-0 100%[=====] 42.68M 65.0KB/s in 3m 50s
2017-03-31 12:06:33 (190 KB/s) - 'graylog2-web-interface-0.20.2.tgz' saved [44756998/44756998]

pekka@Graylog:/opt$ _
```

Kuvio 234. Graylog Web- interfaces asennus



Kuvio 235. Graylog Web-interfaces aloitussivu

Tämä jälkeen lisäsimme portit, mistä vastaanotetaan logeja kuviossa 236. Koska 514 portti oli hiukan ronkeli hallittavuuden kanssa, käytettiin porttia 5140.

The screenshot shows the "Running local inputs" section of the Graylog2 web interface. It lists two inputs: "asd (GELF UDP)" and "syslog (Syslog UDP)".

- asd (GELF UDP)**: Started by **Administrator** on **3eb72ad7 / Graylog** 4 days ago. Status: **running**. Network IO: **0B** (total: **284.4MiB**). Configuration details:


```
port: 5140
bind_address: 10.100.0.12
recv_buffer_size: 1048576
```
- syslog (Syslog UDP)**: Started by **Administrator** on **3eb72ad7 / Graylog** 4 days ago. Status: **running**. Network IO: **0B** (total: **51.5MiB**). Configuration details:


```
allow_override_date: true
port: 514
bind_address: 10.100.0.12
recv_buffer_size: 1048576
```

Kuvio 236. Graylog- palvelimen kuuntelemat portit

Tämän jälkeen palvelimilta annettiin käsky, mihin lähetetään lokit ja ne näkivät palvelimella kuviossa 237.

Sources

All

This is a list of all sources that sent messages to Graylog2. Use it to quickly search for all messages of a specific source or get an overview of what systems are sending in how many messages. **Click on source name to prepare a query for it. Hold the Alt key while clicking to search right away.** Note that the list is cached for a few seconds so you might have to wait a bit until a new source appears.

Per page:

50

Search:

Source name	Message count
dc1-hq.papankki.com	227877
dc2-hq.papankki.com	64866
fs1-hq	4994
web	931
www	221
198.18.235.3	19

Showing 6 of 6 records

Previous **1** Next

Kuvio 237. Lähdelista

Seuraavaksi kuviossa 238 näkyy DC1 lähettämät logit.

Search results

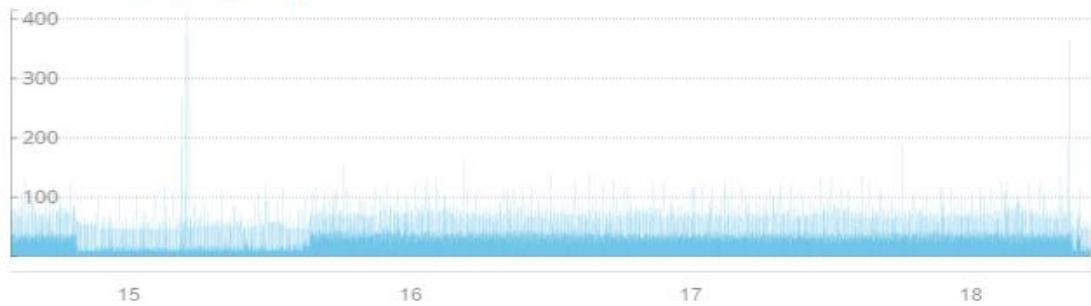
Found 227,879 messages. 



 Export

Save search

Total result histogram



Kuvio 238. DC1 saapuvat lokit

Kuviossa 239 Harri kirjautuu sähköpostiinsa. Kuviossa 240 Harri lähettää viestiä Jussi Johtajalle sähköpostistaan. Kuviossa 241 Harri kirjautuu pois sähköpostipalvelusta.

		ndd_cm.c:872(cm_prepare_connection)	ebadc1c0-2431-11e7-a08b-000c29f0723b
2017-04-18 14:39:58.833	web	-- cm_prepare_connection winbindd n: mutex grab failed for DC1-HQ.papanikki.com	Received by test@ on 3eb72ad7 / Graylog Timestamp: 2017-04-18 14:39:57.859 Index: graylog2_0
2017-04-18 14:39:58.680	web	-- [2017/04/18 14:39:58.5 winbindd 96536, 0] libutil.tdb.c:72 (tdb_chainlock_with_time_out_internal)	Actions
2017-04-18 14:39:58.680	web	-- tdb_chainlock_with_time_out_internal: alarm (40) timed out for key DC1-HQ.papanikki.com in tdb /var/lib/samba/mutex.tdb	application_name auth facility security/authorization level Notice [5] message -- pam_krb5[10976]: authentication succeeds for 'harry' (harry@PAPANKKI.COM) source web
2017-04-18 14:39:57.901	web	-- imap(harry): Disconnect dovecot ed: Logged out bytes=35 7/1551	
2017-04-18 14:39:57.890	web	-- imap-login: Login: user ==<harry>, method=PLAIN, rip=:1, lip=:1, mpid=1099 3, secured	
2017-04-18 14:39:57.882	web	-- pam_winbind(dovecot: auth account): user 'harry' granted access	
2017-04-18 14:39:57.859	web	-- pam_krb5[10976]: auth authentication succeeds for 'harry' (harry@PAPANKKI.CO	

Kuvio 239. Lokeja Harrin kirjautumisesta

2017-04-18 14:42:44.155	web	-- CFC77DF7A5: to=<jussij@papanikki.com>, relay=local, delay=7.9, bytes=3/4.3/0/0.7, dsn=2.0.0, status=sent (delivered to maildir)
2017-04-18 14:42:39.214	web	-- CFC77DF7A5: from=<harry@papanikki.com>, size=709, nrcpt=1 (queue active)
2017-04-18 14:42:38.967	web	-- disconnect from localhost[127.0.0.1]
2017-04-18 14:42:38.295	web	-- CFC77DF7A5: message-id=<24f61801cf6684dbe04c3eb3f0a51b8.squirrel@10.100.0.6>

Kuvio 240. Sähköpostin lähetysten lokit

✉ e16ecff0-2432-11e7-a08b-
000c29f0723b

Received by 🌐 testið on 3eb72ad7 / Graylog

Timestamp: 2017-04-18 14:46:50.167

Index: graylog2_0

Actions ▾

application_name

dovecot

facility

mail

level

Info [6]

message

- - imap(harri): Disconnected: Logged out

bytes=143/1795

source

web

Kuvio 241. Harrin uloskirjautumisen loki

6 Pohdinta

6.1 Toimeksianto 3

Toimeksianto kolmosessa ongelmia riitti edelleen. Palomuuri oli nostettava verkkoon heti ensimmäisellä tunnilla ja sen konfigurointi oli suoritettava pikkuhiljaan rikkomatta kaikkia ympärillä olevia palveluita. Kunnollista verkon Baseline mittausta ei kyetty suorittamaan riittävän aikaisin ja riittävän laajasti. Mittausta varten tarvittavat palvelut olivat joko kokonaan pysytämättä tai niin keskeneräisiä ettei niiden liikenne näkynyt mittauksen aikana. Google olikin ystävä palomuurisääntöjä luodessa ja suuria osa säännöistä jäi testaamatta kokonaan. Lähes täydellinen suunnittelun puute palveluita pystytettäessä hankaloittaa myös sääntöjen tekemistä. Esimerkiksi sähköpostipalvelin sijaitsee väärässä verkossa. Edellä mainituista syistä palomuurin säännöt on kytettävä pois päältä, jotta palvelut saadaan pystyyn ja toimiviksi.

Myös oman sisäisen pilvipalveluratkaisun pystyttämisessä koettiin hieman haasteita, mutta lopulta autentikointi toimi odotetusti. Myöskin epäselvyys täytyykö palveluun päästä ulkoverkosta vai vain sisäverkosta oli kysymys, mutta koska en ainoana ymärännyt sisäisen pilvipalveluratkaisun toimimista vain sisäisenä, päätin pitää palvelun tain.

Monitorointi ohjelma ei suostunut asentumaan kunnolla aluksi suunnitelmissa olleelle Debian palvelimelle, joten se täytyi vaihtaa Centos käyttöjärjestelmään. AD käyttäjien tuontiin ei taaskaan löytynyt suoraviivaista ohjetta tai järjestelmää, millä sen olisi voinut helposti toteuttaa, joten priorisoinnin nimissä jätimme sen takaaalle. Ongelmia kertyi ja niiden ratkaisemiseen ei riittänyt kaikki aika, mutta saimme tehtyä kuitenkin jonkinlaisen monitorointi ratkaisun. Viilattavaa vielä riittää paljonkin.

Tiketointijärjestelmästä saimme toteutettua sisäisen tiketinluonnon sekä AD/LDAP autentikoinnin. Myös palvelun varmenne saatuiin kuin saatinkin luotua. Aikaisempien ITIL-kokemuksien takia päätettiin jättää ITIL prosessikaavioit pois. Aikaa kului aluksi aikaisempien toimeksiantojen toteutuksien kanssa, jotka jäivät ainakin www-palvelimen kannalta vielä toteuttamatta erinäisten motivaatio sekä linux ongelmien takia.

6.2 Toimeksianto 4

Lähiverkon koventamisen osalta jäi hieman vajaaksi ainakin, kun control plane hardening:sta ei ollut suunnitelmassakaan varmaa tietoa, miten tulisi toteuttaa. Lisäksi Extremen-laitteella konfiguroiminen ei ollut kovin varmallalla pohjalla. Todennukset jäivät konfiguraatio tasolle, kun aika ei riittänyt Spidernetin tiloissa testaukseen. Lisäksi AAA konfiguraatiot hidastivat toimintaa, kun kytkin pystyi hallintayhteyden katketessa menemään lukkoon, jos autentikaatiota ei oltu konfiguroitu oikein.

802.1x toteutuksessa tuli juurikin se ongelaksi, että WG:llä ei päässyt käsiksi kytkimiin, koska ne olivat lukossa. Tämä tapahtui kahdella eri WG:llä ja aika ei enään antanut periksi lähteä muita ryhmiä kokeilemaan.

Lähteet

- Afterdawn.fi. 2017. NAT. Viitattu 14.2.2017. <http://fin.afterdawn.com/sanasto/selitys.cfm/nat>.
- Ala-Lahti, J & Malste, M & Nieminen, M. 2016. Harjoitustyö Palvelinkäyttöjärjestelmät. Windows. Viitattu 25.1.2017.
- Badger, M. 2008. Zenoss Core Network and System Monitoring. 16. Packt Publishing. Viitattu 22.3.2017. https://books.google.fi/books?id=B3YBMfU_u8sC&pg=PT15&lpg=PT15&dq=Zenoss+Core&source=bl&ots=WcAjq8Bjgl&sig=Zivr5-OpBGTJE6FjTmVOeGI_dbl&hl=fi&sa=X&ved=0ahUKEwjP8Lm76uXSAhVBpCwKHSmMCwgQ6AElbDAN#v=onepage&q&f=false.
- Banks, E. 25.9.2012. Five Things To Know About DHCP Snooping. Viitattu 4.4.2017. <http://packet-pushers.net/five-things-to-know-about-dhcp-snooping/>.
- Bertram, D. 2009. University of Calgary. The Social Nature of Issue Tracking in Software Engineering. Viitattu 21.3.2017. <https://pdfs.semanticscholar.org/e9df/1819e362adbf55e66a9a8a70ee1618a0fc1d.pdf>.
- Catalyst 6500 Release 12.2SX Software Configuration Guide Chapter: DHCP Snooping. 17.11.2013. Cisco verkkosivut. Viitattu 4.4.2017. <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html>.
- Chapter: Configuring Cisco Discovery Protocol. 30.10.2013. Cisco verkkosivut. Viitattu 4.4.2017. http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf015.html.
- Chapter: Optional STP Features. N.d. Ciscon verkkosivut. Viitattu 4.4.2017. www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/stp_enha.html#wp1020395%0A.
- Cisco Guide to Harden Cisco IOS Devices. 20.10.2016. Ciscon verkkosivut. Viitattu 4.4.2017. <http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>.
- Cloud Computing Explained. Viitattu 21.3.2017 http://www.webopedia.com/quick_ref/cloud_computing.asp
- Cranor, L. 2016. Time to rethink mandatory password changes. Federal Trade Commissionin artikkeli. Viitattu 8.2.2017. <https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes>.
- Folder Redirection Overview. N.d. Microsoft Technet verkkosivut. Viitattu 25.1.2017. [https://technet.microsoft.com/en-us/library/cc732275\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc732275(v=ws.11).aspx).
- Garman, J. 2003. Kerberos: The Definitive Guide.. Sebastopol, USA: O'Reilly Media, Inc. DirectAccess in Windows Server. Viitattu 1.3.2017. <https://technet.microsoft.com/library/dn636118.aspx>
- Holvitie, V. 2014 Tunkeutumistestaus geologatiopalvelimelle. Viitattu 19.4.2017. https://publications.theseus.fi/bitstream/handle/10024/77307/Valtteri_Holvitie.pdf?sequence=1
- How VPN Works. 2003. Microsoft Technet verkkosivu. Viitattu 8.3.2017. [https://technet.microsoft.com/en-us/library/cc779919\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc779919(v=ws.10).aspx).
- Jaakkola, T. Sarja, J. 2006. Mitä on tietokanta? Viitattu. 21.2.2017. <http://verkkopedagogi.net/vanhat/fi/sisalto/materiaalit/access2003/luku021c5a.html?C:D=419700&selres=419700>.
- Jabbusch, J. 2009. IDS vs. IPS. How to know when you need the technology. Viitattu 29.3. <http://searchsecurity.techtarget.com/tip/IDS-vs-IPS-How-to-know-when-you-need-the-technology>

- Jäntti, H & Viilos, M. 2016. Harjoitustyö Palvelinkäyttöjärjestelmät. Windows. Viitattu 18.1.2017.
- Karamanian, A. Tenneti, S. Dessart, F. 17.12.2010. PKI Uncovered Certificate-Based Security Solutions for Next-Generation Networks. Viitattu 5.2.2017.
- Key Features and Functionality. N.d. Request Tracker verkkosivut. Viitattu 21.3.2017. <https://bestpractical.com/request-tracker>.
- Krout, E. 2015 DNS Records: an Introduction. Viitattu 25.1.2017. <https://www.linode.com/docs/networking/dns/dns-records-an-introduction>.
- Lehtinen, M. 2007. Mikä on NTP? Network Time Protocol (NTP). Viitattu 17.1.2017. <http://www.slideserve.com/taini/ntp-mikko-lehtinen>.
- Lipponen, J & Tanninen, T. 2016. Harjoitustyö Palvelinkäyttöjärjestelmät. Windows. Viitattu 13.1.2017.
- Mason, A. 2002. VPNs and VPN Technologies. Viitattu 14.2.2017. <http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=6>.
- Mening, R. 25.2.2017. WordPress vs Joomla vs Drupal. Viitattu 1.3.2017. <https://websitesetup.org/cms-comparison-wordpress-vs-joomla-drupal/>
- Mitchell, B. 2017. What is a DNS Server. Viitattu 8.3.2017. <https://www.lifewire.com/what-is-a-dns-server-817513>.
- Nummela, J. 2013. Lahden Ammattikorkeakoulu. Tiketointijärjestelmän käyttöönotto. Viitattu 21.3.2017. https://www.theseus.fi/bitstream/handle/10024/56687/Nummela_Janne.pdf?sequence=1.
- Orbitco. 28.7.2016. What is Link Layer Discovery Protocol (LLDP). Viitattu 4.4.2017. <http://www.orbit-computer-solutions.com/link-layer-discovery-protocol-lldp/>.
- Orpana, P. 2014. Nimipalvelut ja DNSSEC. Viitattu 18.1.2017. <https://wiki.tut.fi/Tietoturva/Tutkielmat/DNSTietoturvallisuus>.
- OsTicket Features. N.d. OsTicket verkkosivut. Viitattu 21.3.2017. <http://osticket.com/features>
- Rantonen, M. 2017. Monitorointi. ITPH-TT-k2017 kurssin diat 7.3.2017. Viitattu 22.3.2017
- Roaming User Profiles. N.d. Microsoft Technet verkkosivut. Viitattu 24.1.2017. [https://technet.microsoft.com/en-us/library/hh848267\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh848267(v=ws.11).aspx).
- Rouse, M. 2007. RADIUS (Remote Authentication Dial-In User Service). Whatis Technet artikkeli. Viitattu 3.2.2017. <http://searchsecurity.techtarget.com/definition/RADIUS>.
- Rouse, M. 2007. IGP (Interior Gateway Protocol). Whatis Technet artikkeli. Viitattu 1.3.2017. <http://searchsecurity.techtarget.com/definition/IGP>.
- Rousse, M. 2009. SSL VPN (Secure Sockets Layer virtual private network. Viitattu 5.3.2017. <http://searchsecurity.techtarget.com/definition/SSL-VPN>
- Rouse, M. 2010. Authentication, authorization, and accounting (AAA). Whatis Technet artikkeli. Viitattu 3.2.2017. <http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting>.
- Rouse, M. 2015. Multifactor authentication (MFA). Whatis Technet artikkeli. Viitattu 15.2.2017. <http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA>.
- Rouse, M. 2015. OSPF (Open Shortest Path First). Whatis Technet artikkeli. Viitattu 1.3.2017. <http://searchenterprisewan.techtarget.com/definition/OSPF>.
- Sarmed Rahman. 2014. How a mail server works. Viitattu 21.2.2017. <http://xmodulo.com/how-mail-server-works.html>

- Schluting, C. 2014. Understanding BGP Routing. Viitattu 22.2.2017
<http://www.enterprisenetworkingplanet.com/netsp/article.php/3615896/Networking-101-Understanding-BGP-Routing.htm>
- Schneier, B. 1996. Applied Cryptography. Protocols, Algorithms, and Source Code in C. 2. painos. New York, USA: John Wiley & Sons, Inc.
- Snyder, J. 2010. What is 802.1X? Viitattu 19.4.2017. <http://www.networkworld.com/article/2216499/wireless/what-is-802-1x-.html>.
- Tech-faq.com. 2016. Firewalls. Viitattu 20.3.2017. <http://www.tech-faq.com/firewall.html>
- The Difference Between Internet, Intranet, And Extranet. Viitattu 1.3.2017
<http://www.iorg.com/papers/iw/19981019-advisor.html>
- The Platform. N.d. Open NMS-verkkosivut. Viitattu 22.3.2017.
<https://www.opennms.org/en/opennms/the-platform>
- Top 10 Countdown to Making the Most of Your Intranet. Viitattu 1.3.2017
<https://www.claromentis.com/blog/top-10-ideas-making-the-most-of-your-corporate-intranet/>
- Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches. 18.8.2006. Viitattu 4.4.2017. <http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html>.
- Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches. 12.8.2016. Juniper Networks. Viitattu 4.4.2017. https://www.juniper.net/techpubs/en_US/junos/topics/concept/spanning-trees-bpdu-protection-understanding-ex-series.html
- Understanding Control Plane Protection. N.d. Ciscon verkkosivut. Viitattu 4.4.2017. <http://www.cisco.com/c/en/us/about/security-center/understanding-cppr.html>.
- Viestintävirasto. 2014 A. Salasanat haltuun – Neuvaja salasanojen käyttöön ja hallin-taan (Joulukuun 2014 teeman koontijulkaisu). Viitattu 20.1.2017.
https://www.viestintavirasto.fi/attachments/tietoturva/Salasanat_haltuun.pdf.
- Viestintävirasto. 2014 B. Älä jätä oveasi lukeutumatta - käytä DNSSec-avainta. Viitattu 18.1.2017.
<https://www.viestintavirasto.fi/viestintavirasto/signaali/signaali22014/alajataoveasilukeutumatta-kaytadnssec-avainta.html>.
- VyOS. N.d. VyOS kotisivut. Viitattu 8.2.2017. <https://vyos.io/>.
- Webopedia. 2014. database. Viitattu 21.2.2017. <http://www.webopedia.com/TERM/D/database.html>.
- What is LDAP?. N.d. Artikkeli Gracion Software sivustolta. Viitattu 22.2.2017.
<http://www.gracion.com/server/whatldap.html>.
- Who uses the Support Desk Software OTRS. N.d. OTRS verkkosivut. Viitattu 21.3.2017. <https://www.otrs.com/who-uses-the-support-desk-software-otsr/>
- Wong, E. 1997. Network Monitoring Fundamentals and Standards. Viitattu 22.3.2017.
http://www.cse.wustl.edu/~jain/cis788-97/ftp/net_monitoring/.

Liitteet

Liite 1. Yrityksen laiteluettelo

Pääkonttorin laitelista (Domain: papankki.com)			
Laiteen nimi	IP-osoite	Käyttöjärjestelmä	Palvelu(t)
R1-HQ	192.168.17.16	VyOS 1.1.7	Reititys, IP Forwarding, DHCP
DC1	10.100.0.2	Windows Server 2012 R2	Ohjainpalvelin 1, PKI CA
DC2	10.100.0.3	Windows Server 2012 R2	Ohjainpalvelin 2
FS1	10.100.0.4	Windows Server 2012 R2	Tiedostopalvelin 1
FS2	10.100.0.5	Windows Server 2012 R2	Tiedostopalvelin 2
MAIL	10.100.0.6	Centos 6.8	Sähköposti
SQL	10.100.0.7	Ubuntu 16.04	SQL
CLOUD	10.100.0.8	Centos 6.7	Owncloud
OpenNMS	10.100.0.9	Centos 7.3	OpenNMS
VPN	10.100.0.10	Debian 8.7	VPN
RADIUS	10.100.0.11	Centos 7.3	FreeRadius
Graylog	10.100.0.12	Ubuntu 14.10	Graylog
DNS	198.18.235.2	Ubuntu 16.04	DNS
WWW	198.18.235.3	Ubuntu 16.04	WWW-palvelin
OsTicket	198.18.235.4	Ubuntu 16.04	Tikettijärjestelmä
pfSense		pfSense 2.3.2	Palomuuri
WS1	10.0.0.10	Windows 7 SP1	Host kone (DHCP)
WS2	10.0.0.11	Windows 7 SP1	Host kone (DHCP)
WS3	10.0.0.12	Windows 7 SP1	Host kone (DHCP)
WS(n)	10.0.0.254	Windows 7 SP1	Host kone (DHCP)

Keski-Suomen laitelista (Domain: ks.papankki.com)			
Laiteen nimi	IP-osoite	Käyttöjärjestelmä	Palvelu(t)
R1-KS	192.168.44.226	VyOS 1.1.7	Reititys, IP Forwarding, DHCP
DC1	10.200.1.2	Windows Server 2012 R2	Ohjainpalvelin 1
DC2	10.200.1.3	Windows Server 2012 R2	Ohjainpalvelin 2
FS1	10.200.1.4	Windows Server 2012 R2	Tiedostopalvelin 1
FS2	10.200.1.5	Windows Server 2012 R2	Tiedostopalvelin 2
WS1	10.10.1.10	Windows 7 SP1	Host kone (DHCP)
WS2	10.10.1.11	Windows 7 SP1	Host kone (DHCP)
WS3	10.10.1.12	Windows 7 SP1	Host kone (DHCP)
WS(n)	10.10.1.254	Windows 7 SP1	Host kone (DHCP)

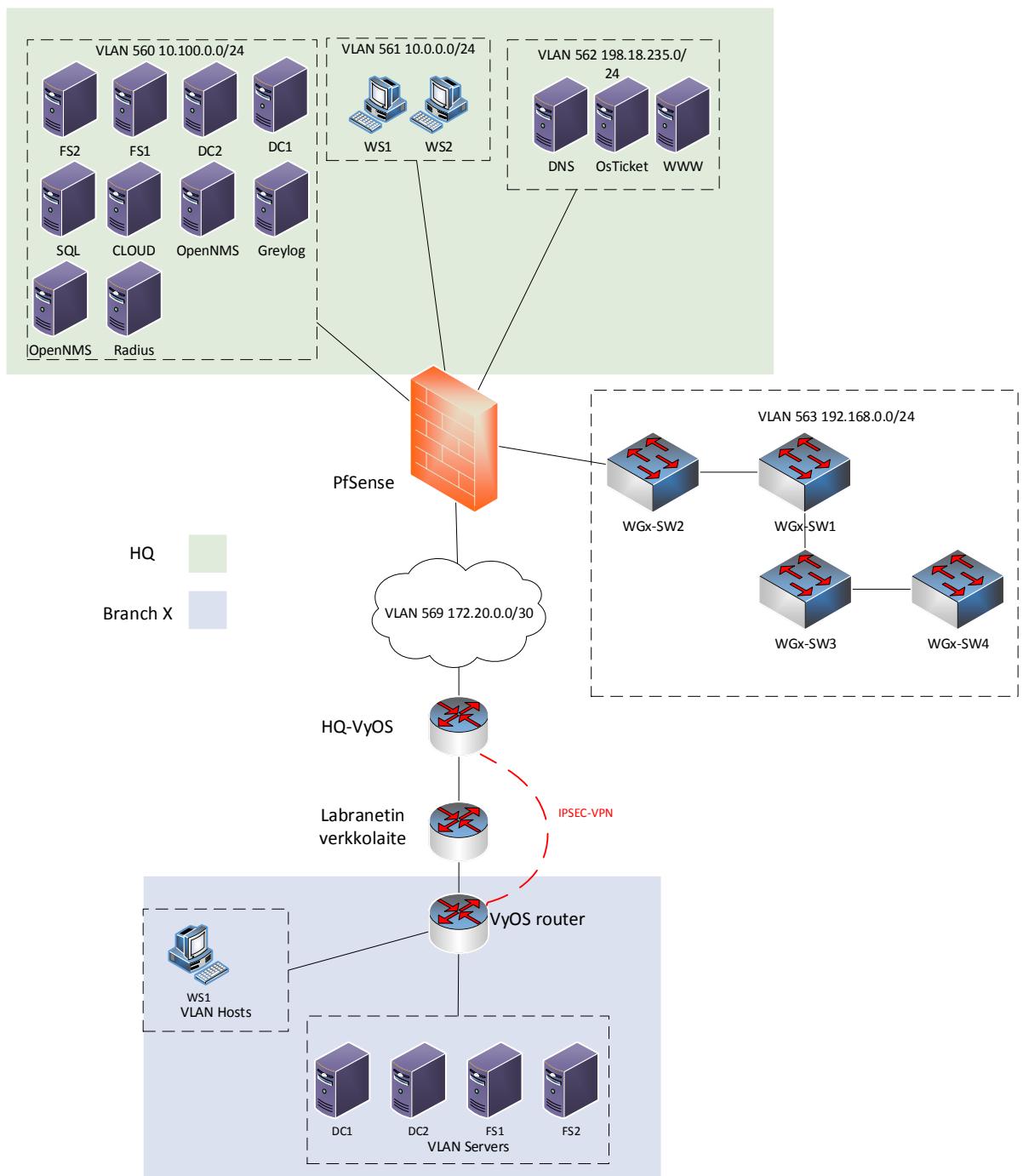
Länsi-Suomen laitelista (Domain: ls.papankki.com)			
Laiteen nimi	IP-osoite	Käyttöjärjestelmä	Palvelu(t)
R1-LS	192.168.44.227	VyOS 1.1.7	Reititys, IP Forwarding, DHCP
DC1	10.200.2.2	Windows Server 2012 R2	Ohjainpalvelin 1
DC2	10.200.2.3	Windows Server 2012 R2	Ohjainpalvelin 2
FS1	10.200.2.4	Windows Server 2012 R2	Tiedostopalvelin 1
FS2	10.200.2.5	Windows Server 2012 R2	Tiedostopalvelin 2
WS1	10.10.2.10	Windows 7 SP1	Host kone (DHCP)
WS2	10.10.2.11	Windows 7 SP1	Host kone (DHCP)
WS3	10.10.2.12	Windows 7 SP1	Host kone (DHCP)
WS(n)	10.10.2.254	Windows 7 SP1	Host kone (DHCP)

Itä-Suomen laitelista (Domain: is.papankki.com)			
Laiteen nimi	IP-osoite	Käyttöjärjestelmä	Palvelu(t)
R1-IS	192.168.44.228	VyOS 1.1.7	Reititys, IP Forwarding, DHCP
DC1	10.200.3.2	Windows Server 2012 R2	Ohjainpalvelin 1
DC2	10.200.3.3	Windows Server 2012 R2	Ohjainpalvelin 2
FS1	10.200.3.4	Windows Server 2012 R2	Tiedostopalvelin 1
FS2	10.200.3.5	Windows Server 2012 R2	Tiedostopalvelin 2
WS1	10.10.3.10	Windows 7 SP1	Host kone (DHCP)
WS2	10.10.3.11	Windows 7 SP1	Host kone (DHCP)
WS3	10.10.3.12	Windows 7 SP1	Host kone (DHCP)
WS(n)	10.10.3.254	Windows 7 SP1	Host kone (DHCP)

Pohjois-Suomen laitelista (Domain: ps.papankki.com)			
Laiteen nimi	IP-osoite	Käyttöjärjestelmä	Palvelu(t)
R1-PS	192.168.44.229	VyOS 1.1.7	Reititys, IP Forwarding, DHCP
DC1	10.200.4.2	Windows Server 2012 R2	Ohjainpalvelin 1
DC2	10.200.4.3	Windows Server 2012 R2	Ohjainpalvelin 2
FS1	10.200.4.4	Windows Server 2012 R2	Tiedostopalvelin 1
FS2	10.200.4.5	Windows Server 2012 R2	Tiedostopalvelin 2
WS1	10.10.4.10	Windows 7 SP1	Host kone (DHCP)
WS2	10.10.4.11	Windows 7 SP1	Host kone (DHCP)
WS3	10.10.4.12	Windows 7 SP1	Host kone (DHCP)
WS(n)	10.10.4.254	Windows 7 SP1	Host kone (DHCP)

Ahvenanmaan laitelista (Domain: ks.papankki.com)			
Laiteen nimi	IP-osoite	Käyttöjärjestelmä	Palvelu(t)
R1-AH	192.168.44.225	VyOS 1.1.7	Reititys, IP Forwarding, DHCP
DC1	10.200.5.2	Windows Server 2012 R2	Ohjainpalvelin 1
DC2	10.200.5.3	Windows Server 2012 R2	Ohjainpalvelin 2
FS1	10.200.5.4	Windows Server 2012 R2	Tiedostopalvelin 1
FS2	10.200.5.5	Windows Server 2012 R2	Tiedostopalvelin 2
WS1	10.10.5.10	Windows 7 SP1	Host kone (DHCP)
WS2	10.10.5.11	Windows 7 SP1	Host kone (DHCP)
WS3	10.10.5.12	Windows 7 SP1	Host kone (DHCP)
WS(n)	10.10.5.254	Windows 7 SP1	Host kone (DHCP)

Liite 2. Fyysinen topologia



Liite 3. Palomuurisäännöt

Verkko	Lähde	Source portti	Kohde	IP	Desti-nation portti	Kuvaus
WS	WS	53	ANY	ANY	53	DNS
	WS	5355	ANY	ANY	5355	DNS
	WS	ANY	ANY	ANY	80	HTTP
	WS	ANY	ANY	ANY	443	HTTP
	WS	67	SERVERS	10.100.0.2 10.100.0.3	67	DHCP
	WS	68	SERVERS	10.100.0.2 10.100.0.3	68	DHCP
	WS	123	SERVERS	10.100.0.2	123	NTP
	WS	ANY	SERVERS	10.100.0.2 10.100.0.3	389	LDAP
	WS	ANY	SERVERS	10.100.0.2 10.100.0.3	3268	LDAP
	WS	ANY	SERVERS	10.100.0.2 10.100.0.3	88	KERBEROS
	WS	ANY	SERVERS	10.100.0.2 10.100.0.3	135, 137, 138, 139, 445	NetBios, EPMAP, MS DS
	WS	ANY	SERVERS	10.100.0.4 10.100.0.5	135, 137, 138, 139, 445	NetBios, EPMAP, MS DS
	WS	110, 143	PUBLIC	??	110, 143	MAIL
	WS	49000 - 65535	SERVERS	10.100.0.2 10.100.0.3	49000 - 65535	DNS

Verkko	Lähde	Source portti	Kohde	IP	Desti- nation portti	Kuvaus
SERVERS	SERVERS	53	ANY	ANY	53	DNS
	SERVERS	5355	ANY	ANY	5355	DNS
	SERVERS	ANY	PUBLIC	ANY	80	HTTP
	SERVERS	ANY	PUBLIC	ANY	443	HTTP
	SERVERS	67	SERVERS	10.100.0.2 10.100.0.3	67	DHCP
	SERVERS	68	SERVERS	10.100.0.2 10.100.03	68	DHCP
	SERVERS	123	SERVERS	10.100.0.2	123	NTP
	SERVERS	ANY	SERVERS	10.100.0.2 10.100.0.3	389, 3268	LDAP
	SERVERS	ANY	Sivukont- torit	Sivukont- torit	389, 3268	LDAP
	SERVERS	110, 143	PUBLIC	??	110, 143	MAIL
	SERVERS	49000 - 65535	ANY	ANY	49000 - 65535	DNS

Verkko	Lähde	Source portti	Kohde	IP	Desti-nation portti	Kuvaus
PUBLIC	198.18.235.3	ANY	SERVERS	ANY	25, 265	WWW
	198.18.235.4	ANY	SERVERS	ANY	25, 265	TIKETTI
	PUBLIC	53	ANY	ANY	53	DNS
	PUBLIC	123	SERVERS	10.100.0.2	123	NTP
	PUBLIC	ANY	Sivukont-torit	Sivukont-torit	389, 3268	LDAP
	PUBLIC	5355	ANY	ANY	5355	DNS
	PUBLIC	49000 - 65535	ANY	ANY	49000 - 65535	DNS
	PUBLIC	ANY	SERVERS	10.100.0.2 10.100.0.3	389	LDAP
	PUBLIC	ANY	ANY	ANY	110, 143	IMAP, POP 3
	PUBLIC	ANY	SERVERS	10.100.0.2 10.100.0.3	3268	LDAP

Verkko	Lähde	Source portti	Kohde	IP	Desti-nation portti	Kuvaus
FLOATING	ANY	ANY	PUBLIC	ANY	22	SSH
	ANY	ICMP	ANY	ANY	ICMP	Ping

Verkko	Lähde	Source portti	Kohde	IP	Desti-nation portti	Kuvaus
WAN	Sivu-kontto-rit	53, 5355	ANY	ANY	53, 5355	DNS
	Sivu-kontto-rit	49000 - 65535	ANY	ANY	49000 - 65535	DNS
	Sivu-kontto-rit	53, 5355	PUBLIC	ANY	53, 5355	DNS
	Sivu-kontto-rit	49000 - 65535	PUBLIC	ANY	49000 - 65535	DNS
	Sivu-kontto-rit	123	SERVERS	10.100.0.2	123	NTP
	Sivu-kontto-rit	ANY	SERVERS	10.100.0.2 10.100.0.3	389, 3268	LDAP
	ANY	ANY	PUBLIC	198.18.235.3 198.18.235.4	443, 80	HTTP
	Sivu-kontto-rit	ANY	SERVERS	10.100.0.2 10.100.0.3	135, 137, 138, 139, 445	NetBios, EPMAP, MS DS

Liite 4. WG1-SW1

```
service password-encryption
!
hostname WG1-SW1
!
enable secret 5 $1$mERr$hU7WG5dxDH2sGRqMUJkNc.
!
no aaa new-model
ip subnet-zero
!
ip dhcp snooping vlan 560-563
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface GigabitEthernet0/1
switchport access vlan 111
switchport mode access
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet0/2
switchport trunk encapsulation dot1q
switchport trunk native vlan 111
switchport trunk allowed vlan 560-563
switchport mode trunk
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping trust
!
```

```
interface GigabitEthernet0/3
    switchport trunk encapsulation dot1q
    switchport trunk native vlan 111
    switchport trunk allowed vlan 560-563
    switchport mode trunk
    no cdp enable
    spanning-tree portfast
    spanning-tree bpduguard enable
    ip dhcp snooping trust
!

interface GigabitEthernet0/4
    switchport access vlan 111
    switchport mode access
    no cdp enable
    spanning-tree portfast
    spanning-tree bpduguard enable
!

interface GigabitEthernet0/5
    switchport access vlan 111
    switchport mode access
    shutdown
    no cdp enable
    spanning-tree portfast
    spanning-tree bpduguard enable
!

interface GigabitEthernet0/6
    switchport access vlan 561
    switchport mode access
    no cdp enable
    spanning-tree portfast
    spanning-tree bpduguard enable
    ip dhcp snooping limit rate 100
!

interface GigabitEthernet0/7
    switchport access vlan 111
    switchport mode access
```

```
shutdown
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet0/8
switchport access vlan 111
switchport mode access
shutdown
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet0/9
switchport access vlan 111
switchport mode access
shutdown
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet0/10
switchport access vlan 111
switchport mode access
shutdown
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet0/11
switchport access vlan 111
switchport mode access
shutdown
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
```

```
!
interface GigabitEthernet0/12
    switchport access vlan 111
    switchport mode access
    shutdown
    no cdp enable
    spanning-tree portfast
    spanning-tree bpduguard enable
!
interface Vlan1
    no ip address
    shutdown
!
interface Vlan561
    description Workstations
    no ip address
!
interface Vlan563
    ip address 192.168.0.3 255.255.255.0
    ip default-gateway 192.168.0.1

banner motd ^C
Unauthorized access to this device is strictly prohibited!^C
!
line con 0
    password 7 080A455D1A18544541
    logging synchronous
    login
!
line vty 0 4
    password 7 080A455D1A18544541
    login
line vty 5 15
    login
end
```

Liite 5. WG1-SW2

```
service password-encryption
!
hostname WG1-SW2
enable secret 5 $1$mERr$hU7WG5dxDH2sGRqMUJkNc
!
ip subnet-zero
!
no ip domain-lookup
ip ssh time-out 120
ip ssh authentication-retries 3
!
spanning-tree mode rapid-pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport trunk native vlan 111
switchport trunk allowed vlan 560-563
switchport mode trunk
ip dhcp snooping trust
!
interface FastEthernet0/2
switchport access vlan 111
switchport mode access
shutdown
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/3
switchport access vlan 111
switchport mode access
shutdown
```

```
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/4
switchport access vlan 111
switchport mode access
shutdown
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/5
switchport access vlan 111
switchport mode access
shutdown
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/6
switchport access vlan 111
switchport mode access
shutdown
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/7
switchport access vlan 111
switchport mode access
shutdown
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
```

```
interface FastEthernet0/8
    no cdp enable
    ip dhcp snooping trust
!
interface FastEthernet0/9
!
interface FastEthernet0/9
    switchport access vlan 111
    switchport mode access
    shutdown
    no cdp enable
    spanning-tree portfast
    spanning-tree bpduguard enable
!
interface FastEthernet0/10
    switchport access vlan 111
    switchport mode access
    shutdown
    no cdp enable
    spanning-tree portfast
    spanning-tree bpduguard enable
!
interface FastEthernet0/11
    switchport access vlan 111
    switchport mode access
    shutdown
    no cdp enable
    spanning-tree portfast
    spanning-tree bpduguard enable
!
interface FastEthernet0/12
    switchport access vlan 111
    switchport mode access
    shutdown
    no cdp enable
    spanning-tree portfast
```

```
spanning-tree bpduguard enable
!
interface FastEthernet0/13
    switchport access vlan 111
    switchport mode access
    shutdown
    no cdp enable
    spanning-tree portfast
    spanning-tree bpduguard enable
!
interface FastEthernet0/14
    switchport access vlan 111
    switchport mode access
    shutdown
    no cdp enable
    spanning-tree portfast
    spanning-tree bpduguard enable
!
interface FastEthernet0/15
    switchport access vlan 111
    switchport mode access
    shutdown
    no cdp enable
    spanning-tree portfast
    spanning-tree bpduguard enable
!
interface FastEthernet0/16
    switchport access vlan 111
    switchport mode access
    shutdown
    no cdp enable
    spanning-tree portfast
    spanning-tree bpduguard enable
!
interface FastEthernet0/17
    switchport access vlan 111
```

```
switchport mode access
shutdown
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/18
switchport access vlan 111
switchport mode access
shutdown
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/19
switchport access vlan 111
switchport mode access
shutdown
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/20
switchport access vlan 111
switchport mode access
shutdown
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/21
switchport access vlan 561
switchport mode access
no cdp enable
spanning-tree portfast
spanning-tree bpduguard enable
```

```
ip dhcp snooping limit rate 100
!
interface FastEthernet0/22
  switchport access vlan 111
  switchport mode access
  shutdown
  no cdp enable
  spanning-tree portfast
  spanning-tree bpduguard enable
!
interface FastEthernet0/23
  switchport access vlan 111
  switchport mode access
  shutdown
  no cdp enable
  spanning-tree portfast
  spanning-tree bpduguard enable
!
!
interface FastEthernet0/24
  switchport access vlan 111
  switchport mode access
  shutdown
  no cdp enable
  spanning-tree portfast
  spanning-tree bpduguard enable
!
interface Vlan1
  no ip address
  no ip route-cache
  shutdown
!
interface Vlan563
  ip address 192.168.0.2 255.255.255.0
  no ip route-cache
  ip default-gateway 192.168.0.1
```

```

banner motd ^C
Unauthorized access to this device is strictly prohibited!^C
!
line con 0
password 7 080A455D1A18544541
logging synchronous
login
!
line vty 0 4
password 7 080A455D1A18544541
login
line vty 5 15
login
end

```

Liite 6. WG1-SW3

```

# Module stp configuration.

#
configure mstp region 000496366549
create stpd papankki
configure stpd papankki mode dot1w
configure stpd s0 delete vlan default ports all
disable stpd s0 auto-bind vlan default
enable stpd s0 auto-bind vlan Default
enable stpd Papankki
# Module vlan configuration.

#
configure vlan default delete ports all
configure vr VR-Default delete ports 1-26
configure vr VR-Default add ports 1-26
configure vlan default delete ports 1-26
create vlan "Mustareika"
configure vlan Mustareika tag 111

```

```
create vlan "Hallinta"
configure vlan Hallinta tag 563
create vlan "temp"
create vlan "Workstations"
configure vlan Workstations tag 561
disable port 3
disable port 4
disable port 5
disable port 6
disable port 7
disable port 8
disable port 9
disable port 11
disable port 12
disable port 13
disable port 14
disable port 15
disable port 16
disable port 17
disable port 18
disable port 19
disable port 20
disable port 21
disable port 22
disable port 23
disable port 24
disable port 25
disable port 26
configure vlan Mustareika add ports 3-9, 11-26 untagged
configure vlan Hallinta add ports 1-2 tagged
configure vlan Workstations add ports 1-2 tagged
configure vlan Workstations add ports 10 untagged
configure vlan Hallinta ipaddress 192.168.0.4 255.255.255.0
#
# Module ipSecurity configuration.
```

```
configure trusted-servers vlan Workstations add server 10.100.0.2
trust-for dhcp-server

configure trusted-servers vlan Workstations add server 10.100.0.3
trust-for dhcp-server

configure ip-security dhcp-snooping information option

configure ip-security dhcp-snooping information circuit-id vlan-in-
formation Mustareika vlan Mustareika

configure ip-security dhcp-snooping information circuit-id vlan-in-
formation Workstations vlan Workstations

configure ip-security dhcp-snooping information circuit-id port-in-
formation SW3-access port 10

# Module edp configuration.

disable edp ports 1
disable edp ports 2
disable edp ports 3
disable edp ports 4
disable edp ports 5
disable edp ports 6
disable edp ports 7
disable edp ports 8
disable edp ports 9
disable edp ports 10
disable edp ports 11
disable edp ports 12
disable edp ports 13
disable edp ports 14
disable edp ports 15
disable edp ports 16
disable edp ports 17
disable edp ports 18
disable edp ports 19
disable edp ports 20
disable edp ports 21
disable edp ports 22
disable edp ports 23
disable edp ports 24
disable edp ports 25
disable edp ports 26
```

```
# Module lldp configuration.  
enable lldp ports 1  
enable lldp ports 2
```

Liite 7. WG1-SW4

```
hostname "WG1-SW4"  
trunk 1 trk1 trunk  
ip default-gateway 192.168.0.1  
interface 1 10  
    dhcp-snooping trust  
    exit address  
interface 3  
    disable  
    exit  
interface 4  
    disable  
    exit  
interface 5  
    disable  
    exit  
interface 7  
    disable  
    exit  
interface 8  
    disable  
    exit  
interface 9  
    disable  
    exit  
interface 10  
    dhcp-snooping max-bindings 100  
    exit  
interface 11  
    disable
```

```
exit
interface 12
disable
exit
interface 13
disable
exit
interface 14
disable
exit
interface 15
disable
exit
interface 16
disable
exit
interface 17
disable
exit
interface 18
disable
exit
interface 19
disable
exit
interface 20
disable
exit
interface 21
disable
exit
interface 22
disable
exit
interface 23
disable
```

```
exit
interface 24
disable
exit
snmp-server community "public" unrestricted
lldp admin-status 2-24 disable
no cdp enable 1-24
vlan 1
  name "DEFAULT_VLAN"
  no untagged 2-24
  untagged 25-28
  tagged 1
  ip address dhcp-bootp
  exit
vlan 111
  name "Mustareika"
  untagged 3-9,11-24
  no ip address
  exit
vlan 561
  name "Workstations"
  untagged 10
  tagged 1
  no ip address
  exit
vlan 563
  name "Hallinta"
  tagged 1
  ip address 192.168.0.5 255.255.255.0
  exit
spanning-tree 2 bpdu-protection
spanning-tree bpdu-protection-timeout 65535
  dhcp-snooping max-bindings 100
```

Liite 8. 802.1X konfiguraatio SW2

```
enable
configure terminal
aaa new-model
aaa authentication dot1x default group radius
dot1x system-auth-control
identify profile default
interface FastEthernet0/8
access-session port-control auto
dot1x pae authenticator
end

enable
conf t
radius-server vsa send authentication
interface FastEthernet0/8
access-session host-mode single-host FastEthernet0/8
end

enable
conf t
snmp-server enable traps dot1x no-guest-vlan
end
```

Liite 9. HQ VyOS konfiguraatio

```
set interfaces ethernet eth0 address '192.168.17.16/24'
set interfaces ethernet eth0 description 'OUTSIDE'
set interfaces ethernet eth0 duplex 'auto'
set interfaces ethernet eth0 hw-id '00:0c:29:a1:1e:84'
set interfaces ethernet eth0 smp_affinity 'auto'
set interfaces ethernet eth0 speed 'auto'
set interfaces ethernet eth1 address '172.20.0.1/24'
set interfaces ethernet eth1 description 'INSIDE'
set interfaces ethernet eth1 duplex 'auto'
set interfaces ethernet eth1 hw-id '00:0c:29:a1:1e:8e'
set interfaces ethernet eth1 smp_affinity 'auto'
set interfaces ethernet eth1 speed 'auto'
set interfaces loopback lo address '1.1.1.1/32'
set interfaces tunnel tun0 address '172.16.5.1/30'
set interfaces tunnel tun0 description 'tunnel-to-ps'
set interfaces tunnel tun0 encapsulation 'gre'
set interfaces tunnel tun0 ip ospf dead-interval '40'
set interfaces tunnel tun0 ip ospf hello-interval '10'
set interfaces tunnel tun0 ip ospf network 'broadcast'
set interfaces tunnel tun0 ip ospf priority '1'
set interfaces tunnel tun0 ip ospf retransmit-interval '5'
set interfaces tunnel tun0 ip ospf transmit-delay '1'
set interfaces tunnel tun0 local-ip '192.168.17.16'
set interfaces tunnel tun0 mtu '1400'
set interfaces tunnel tun0 multicast 'enable'
set interfaces tunnel tun0 policy route 'policy1'
set interfaces tunnel tun0 remote-ip '192.168.44.229'
set interfaces tunnel tun1 address '172.16.1.1/30'
set interfaces tunnel tun1 description 'Tunnel-to-KS'
set interfaces tunnel tun1 encapsulation 'gre'
set interfaces tunnel tun1 ip ospf dead-interval '40'
set interfaces tunnel tun1 ip ospf hello-interval '10'
```

```
set interfaces tunnel tun1 ip ospf network 'broadcast'
set interfaces tunnel tun1 ip ospf priority '1'
set interfaces tunnel tun1 ip ospf retransmit-interval '5'
set interfaces tunnel tun1 ip ospf transmit-delay '1'
set interfaces tunnel tun1 local-ip '192.168.17.16'
set interfaces tunnel tun1 mtu '1400'
set interfaces tunnel tun1 multicast 'enable'
set interfaces tunnel tun1 policy route 'policy1'
set interfaces tunnel tun1 remote-ip '192.168.44.226'
set interfaces tunnel tun3 address '172.16.2.1/30'
set interfaces tunnel tun3 description 'Tunnel-to-Is'
set interfaces tunnel tun3 encapsulation 'gre'
set interfaces tunnel tun3 ip ospf dead-interval '40'
set interfaces tunnel tun3 ip ospf hello-interval '10'
set interfaces tunnel tun3 ip ospf network 'broadcast'
set interfaces tunnel tun3 ip ospf priority '1'
set interfaces tunnel tun3 ip ospf retransmit-interval '5'
set interfaces tunnel tun3 ip ospf transmit-delay '1'
set interfaces tunnel tun3 local-ip '192.168.17.16'
set interfaces tunnel tun3 mtu '1400'
set interfaces tunnel tun3 multicast 'enable'
set interfaces tunnel tun3 policy route 'policy1'
set interfaces tunnel tun3 remote-ip '192.168.44.227'
set interfaces tunnel tun4 address '172.16.3.1/30'
set interfaces tunnel tun4 description 'Tunnel-to-IS'
set interfaces tunnel tun4 encapsulation 'gre'
set interfaces tunnel tun4 ip ospf dead-interval '40'
set interfaces tunnel tun4 ip ospf hello-interval '10'
set interfaces tunnel tun4 ip ospf network 'broadcast'
set interfaces tunnel tun4 ip ospf priority '1'
set interfaces tunnel tun4 ip ospf retransmit-interval '5'
set interfaces tunnel tun4 ip ospf transmit-delay '1'
set interfaces tunnel tun4 local-ip '192.168.17.16'
set interfaces tunnel tun4 mtu '1400'
```

```
set interfaces tunnel tun4 multicast 'enable'
set interfaces tunnel tun4 policy route 'policy1'
set interfaces tunnel tun4 remote-ip '192.168.44.228'
set interfaces tunnel tun5 address '172.16.4.1/30'
set interfaces tunnel tun5 description 'Tunnel-to-AH'
set interfaces tunnel tun5 encapsulation 'gre'
set interfaces tunnel tun5 ip ospf dead-interval '40'
set interfaces tunnel tun5 ip ospf hello-interval '10'
set interfaces tunnel tun5 ip ospf network 'broadcast'
set interfaces tunnel tun5 ip ospf priority '1'
set interfaces tunnel tun5 ip ospf retransmit-interval '5'
set interfaces tunnel tun5 ip ospf transmit-delay '1'
set interfaces tunnel tun5 local-ip '192.168.17.16'
set interfaces tunnel tun5 mtu '1400'
set interfaces tunnel tun5 multicast 'enable'
set interfaces tunnel tun5 policy route 'policy1'
set interfaces tunnel tun5 remote-ip '192.168.44.225'
set nat source rule 10 description 'NAT-to-SRV'
set nat source rule 10 outbound-interface 'eth0'
set nat source rule 10 source address '10.100.0.0/24'
set nat source rule 10 translation address 'masquerade'
set nat source rule 20 description 'NAT-to-WS'
set nat source rule 20 outbound-interface 'eth0'
set nat source rule 20 source address '10.0.0.0/24'
set nat source rule 20 translation address 'masquerade'
set nat source rule 30 description 'NAT-to-DMZ'
set nat source rule 30 outbound-interface 'eth0'
set nat source rule 30 source address '192.18.235.0/24'
set nat source rule 30 translation address 'masquerade'
set policy route policy1 rule 1 protocol 'tcp'
set policy route policy1 rule 1 set tcp-mss '1360'
set policy route policy1 rule 1 tcp flags 'SYN'
set policy route-map CONNECT rule 10 action 'permit'
set policy route-map CONNECT rule 10 match interface 'lo'
```

```
set protocols bgp 65250 neighbor 192.168.17.11 remote-as '65000'
set protocols bgp 65250 neighbor 192.168.17.11 update-source '192.168.17.16'
set protocols bgp 65250 neighbor 192.168.17.12 remote-as '65050'
set protocols bgp 65250 neighbor 192.168.17.12 update-source '192.168.17.16'
set protocols bgp 65250 neighbor 192.168.17.13 remote-as '65100'
set protocols bgp 65250 neighbor 192.168.17.13 update-source '192.168.17.16'
set protocols bgp 65250 neighbor 192.168.17.14 remote-as '65150'
set protocols bgp 65250 neighbor 192.168.17.14 update-source '192.168.17.16'
set protocols bgp 65250 neighbor 192.168.17.15 remote-as '65200'
set protocols bgp 65250 neighbor 192.168.17.15 update-source '192.168.17.16'
set protocols bgp 65250 neighbor 192.168.17.17 remote-as '65300'
set protocols bgp 65250 neighbor 192.168.17.17 update-source '192.168.17.16'
set protocols bgp 65250 neighbor 207.11.134.2 remote-as '65350'
set protocols bgp 65250 neighbor 207.11.134.2 update-source '192.168.17.16'
set protocols bgp 65250 network '192.0.2.0/24'
set protocols bgp 65250 parameters router-id '192.168.17.16'
set protocols ospf area 0.0.0.0 authentication 'md5'
set protocols ospf area 0.0.0.0 network '10.0.0.0/24'
set protocols ospf area 0.0.0.0 network '10.100.0.0/24'
set protocols ospf area 0.0.0.0 network '172.16.5.0/30'
set protocols ospf area 0.0.0.0 network '172.16.1.0/30'
set protocols ospf area 0.0.0.0 network '172.16.2.0/30'
set protocols ospf area 0.0.0.0 network '172.16.3.0/30'
set protocols ospf area 0.0.0.0 network '172.16.4.0/30'
set protocols ospf area 0.0.0.0 network '172.16.0.0/30'
set protocols ospf default-information originate 'always'
set protocols ospf default-information originate metric '10'
set protocols ospf default-information originate metric-type '2'
set protocols ospf 'log-adjacency-changes'
set protocols ospf parameters abr-type 'cisco'
set protocols ospf parameters router-id '1.1.1.1'
set protocols ospf passive-interface 'default'
set protocols ospf passive-interface-exclude 'eth0'
set protocols ospf passive-interface-exclude 'tun0'
```

```
set protocols ospf passive-interface-exclude 'tun1'
set protocols ospf passive-interface-exclude 'tun3'
set protocols ospf passive-interface-exclude 'tun4'
set protocols ospf passive-interface-exclude 'tun5'
set protocols ospf redistribute connected metric-type '2'
set protocols ospf redistribute connected route-map 'CONNECT'
set protocols static route 10.0.0.0/24 next-hop '172.20.0.2'
set protocols static route 10.10.1.0/24 next-hop '172.16.1.2'
set protocols static route 10.10.2.0/24 next-hop '172.16.2.2'
set protocols static route 10.10.3.0/24 next-hop '172.16.3.2'
set protocols static route 10.10.4.0/24 next-hop '172.16.5.2'
set protocols static route 10.10.5.0/24 next-hop '172.16.4.2'
set protocols static route 10.100.0.0/24 next-hop '172.20.0.2'
set protocols static route 10.200.1.0/24 next-hop '172.16.1.2'
set protocols static route 10.200.2.0/24 next-hop '172.16.2.1'
set protocols static route 10.200.3.0/24 next-hop '172.16.3.2'
set protocols static route 10.200.4.0/24 next-hop '172.16.5.2'
set protocols static route 10.200.5.0/24 next-hop '172.16.4.2'
set protocols static route 192.168.44.0/24 next-hop 192.168.17.1 distance '1'
set protocols static route 198.18.235.0/24 next-hop '172.20.0.2'
set service dns forwarding cache-size '0'
set service dns forwarding listen-on 'eth1'
set service dns forwarding name-server '10.100.0.2'
set service dns forwarding name-server '8.8.4.4'
set service snmp community opennms authorization 'rw'
set service snmp community opennms client '10.100.0.9'
set service ssh 'allow-root'
set service ssh port '22'
set system config-management commit-revisions '20'
set system console device ttys0 speed '9600'
set system host-name 'R1-HQ'
set system login radius-server 10.100.0.2 port '1812'
set system login radius-server 10.100.0.2 secret 'Kissa123'
set system login radius-server 10.100.0.2 timeout '2'
```

```

set system login user kaijakuitu authentication encrypted-password '$6$aV-
pkeFFjLHsx$Bfp4B1cuFsRHUzLVklzxT305IxOmyur-
qWiLK/BFJgRcPEBd0I7Pf2k9R3WjZYb3y5exFaoINUml5BeHi2YEof0'

set system login user kaijakuitu authentication plaintext-password ""

set system login user kaijakuitu level 'admin'

set system login user kallekytkin authentication encrypted-password '$6$NVnX7DjQ$2tvZZtxg-
JaaiBu62De3mL65qUgp8u3UgYwAeYztUFaw6F1yjFHEOTUvNECQ61RQstd8VLjzduI0UE8g/DLh0/'

set system login user kallekytkin authentication plaintext-password ""

set system login user kallekytkin level 'admin'

set system login user kirvakonffi authentication encrypted-password '$6$mGQKHH6v3s7MI6$0nXYS-
jihGwKBFQ9OJ0cQUA51OxrdBZnQJltGewy3.l7EqbnHFl2kWQ0.UKXxfW7WSNVj7E6zBJmiUiRb3j0'

set system login user kirvakonffi authentication plaintext-password ""

set system login user kirvakonffi level 'admin'

set system login user patepalvelin authentication encrypted-password
'$6$J3NE29tzvLuCh$kpna4YYn1wDkyvDnmclmM6N4JrXvhNjKEoa93D62wY/hBbhoNbJc3UnE3idFTxlvF
TAcsND7vv7.tGaPrbixk1'

set system login user patepalvelin authentication plaintext-password ""

set system login user patepalvelin level 'admin'

set system login user pekkaautonen authentication encrypted-password
'$6$vjDr6mtQVf$akESdGyvdXVwXltX0SN5W0bG4O/2zPAJaw7TJg6hFa1f/uXKoKAKbD7K9NydzqCvwoy
94BqFmstr.JffAGY1d.'

set system login user pekkaautonen authentication plaintext-password ""

set system login user pekkaautonen level 'admin'

set system login user ristoreititin authentication encrypted-password
'$6$sDrQU00/B$7T/XVXFVWYMhDW8ZI-
vtaLQnzMu6EtUy.H4b.NmstRPUEnJ1Nc963hzWcQ65vTL3UJJXwXkfc7R95zE0gBIGPm1'

set system login user ristoreititin authentication plaintext-password ""

set system login user ristoreititin level 'admin'

set system login user vyos authentication encrypted-password
'$1$c7PG7ubp$FrDnWCZqtWL0IN8T5Nn3D1'

set system login user vyos authentication plaintext-password ""

set system login user vyos level 'admin'

set system ntp server '192.168.17.2'

set system package auto-sync '1'

set system package repository community components 'main'

set system package repository community distribution 'helium'

set system package repository community password ""

set system package repository community url 'http://packages.vyos.net/vyos'

set system package repository community username ""

```

```
set system syslog global facility all level 'notice'
set system syslog global facility protocols level 'debug'
set system time-zone 'Europe/Helsinki'
set vpn ipsec esp-group hq compression 'disable'
set vpn ipsec esp-group hq lifetime '86400'
set vpn ipsec esp-group hq mode 'tunnel'
set vpn ipsec esp-group hq pfs 'enable'
set vpn ipsec esp-group hq proposal 1 encryption 'aes128'
set vpn ipsec esp-group hq proposal 1 hash 'md5'
set vpn ipsec ike-group hq ikev2-reauth 'no'
set vpn ipsec ike-group hq key-exchange 'ikev1'
set vpn ipsec ike-group hq lifetime '86400'
set vpn ipsec ike-group hq proposal 1 dh-group '14'
set vpn ipsec ike-group hq proposal 1 encryption 'aes256'
set vpn ipsec ike-group hq proposal 1 hash 'md5'
set vpn ipsec ipsec-interfaces interface 'eth0'
set vpn ipsec site-to-site peer 192.168.44.225 authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer 192.168.44.225 authentication pre-shared-secret 'kissa123'
set vpn ipsec site-to-site peer 192.168.44.225 connection-type 'initiate'
set vpn ipsec site-to-site peer 192.168.44.225 ike-group 'hq'
set vpn ipsec site-to-site peer 192.168.44.225 ikev2-reauth 'inherit'
set vpn ipsec site-to-site peer 192.168.44.225 local-address '192.168.17.16'
set vpn ipsec site-to-site peer 192.168.44.225 tunnel 5 allow-nat-networks 'disable'
set vpn ipsec site-to-site peer 192.168.44.225 tunnel 5 allow-public-networks 'disable'
set vpn ipsec site-to-site peer 192.168.44.225 tunnel 5 esp-group 'hq'
set vpn ipsec site-to-site peer 192.168.44.225 tunnel 5 protocol 'gre'
set vpn ipsec site-to-site peer 192.168.44.226 authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer 192.168.44.226 authentication pre-shared-secret 'kissa123'
set vpn ipsec site-to-site peer 192.168.44.226 connection-type 'initiate'
set vpn ipsec site-to-site peer 192.168.44.226 ike-group 'hq'
set vpn ipsec site-to-site peer 192.168.44.226 ikev2-reauth 'inherit'
set vpn ipsec site-to-site peer 192.168.44.226 local-address '192.168.17.16'
set vpn ipsec site-to-site peer 192.168.44.226 tunnel 1 allow-nat-networks 'disable'
set vpn ipsec site-to-site peer 192.168.44.226 tunnel 1 allow-public-networks 'disable'
```

```
set vpn ipsec site-to-site peer 192.168.44.226 tunnel 1 esp-group 'hq'
set vpn ipsec site-to-site peer 192.168.44.226 tunnel 1 protocol 'gre'
set vpn ipsec site-to-site peer 192.168.44.227 authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer 192.168.44.227 authentication pre-shared-secret 'kissa123'
set vpn ipsec site-to-site peer 192.168.44.227 connection-type 'initiate'
set vpn ipsec site-to-site peer 192.168.44.227 ike-group 'hq'
set vpn ipsec site-to-site peer 192.168.44.227 ikev2-reauth 'inherit'
set vpn ipsec site-to-site peer 192.168.44.227 local-address '192.168.17.16'
set vpn ipsec site-to-site peer 192.168.44.227 tunnel 3 allow-nat-networks 'disable'
set vpn ipsec site-to-site peer 192.168.44.227 tunnel 3 allow-public-networks 'disable'
set vpn ipsec site-to-site peer 192.168.44.227 tunnel 3 esp-group 'hq'
set vpn ipsec site-to-site peer 192.168.44.227 tunnel 3 protocol 'gre'
set vpn ipsec site-to-site peer 192.168.44.228 authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer 192.168.44.228 authentication pre-shared-secret 'kissa123'
set vpn ipsec site-to-site peer 192.168.44.228 connection-type 'initiate'
set vpn ipsec site-to-site peer 192.168.44.228 ike-group 'hq'
set vpn ipsec site-to-site peer 192.168.44.228 ikev2-reauth 'inherit'
set vpn ipsec site-to-site peer 192.168.44.228 local-address '192.168.17.16'
set vpn ipsec site-to-site peer 192.168.44.228 tunnel 4 allow-nat-networks 'disable'
set vpn ipsec site-to-site peer 192.168.44.228 tunnel 4 allow-public-networks 'disable'
set vpn ipsec site-to-site peer 192.168.44.228 tunnel 4 esp-group 'hq'
set vpn ipsec site-to-site peer 192.168.44.228 tunnel 4 protocol 'gre'
set vpn ipsec site-to-site peer 192.168.44.229 authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer 192.168.44.229 authentication pre-shared-secret 'kissa123'
set vpn ipsec site-to-site peer 192.168.44.229 connection-type 'initiate'
set vpn ipsec site-to-site peer 192.168.44.229 ike-group 'hq'
set vpn ipsec site-to-site peer 192.168.44.229 ikev2-reauth 'inherit'
set vpn ipsec site-to-site peer 192.168.44.229 local-address '192.168.17.16'
set vpn ipsec site-to-site peer 192.168.44.229 tunnel 0 allow-nat-networks 'disable'
set vpn ipsec site-to-site peer 192.168.44.229 tunnel 0 allow-public-networks 'disable'
set vpn ipsec site-to-site peer 192.168.44.229 tunnel 0 esp-group 'hq'
set vpn ipsec site-to-site peer 192.168.44.229 tunnel 0 protocol 'gre'
set vpn pptp remote-access authentication mode 'radius'
set vpn pptp remote-access authentication radius-server 10.100.0.2 key 'Kissa123'
```

```
set vpn pptp remote-access client-ip-pool start '10.0.0.1'  
set vpn pptp remote-access client-ip-pool stop '10.0.0.254'
```

Liite 10. Spidernettiin laajennus topologia

