

Infoblox-ohjelmiston käyttöönotto ja todennus RGCE-ympäristössä

Tommi Aittanen

Opinnäytetyö
Maaliskuu 2015

Tietotekniikan koulutusohjelma
Tekniikan ja liikenteen ala





Tekijä(t) Aittanen, Tommi	Julkaisun laji Opinnäytetyö	Päivämäärä 02.03.2015
	Sivumäärä 66 + 11	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: (x)
Työn nimi Infoblox-ohjelmiston käyttöönotto ja todennus RGCE-ympäristössä		
Koulutusohjelma Tietotekniikan (Tietoverkkotekniikan) koulutusohjelma		
Työn ohjaaja(t) Piispanen Juha Saharinen Karo		
Toimeksiantaja(t) Jyväskylän ammattikorkeakoulu (JAMK), Jyväskylä Security Technology (JYVSECTEC) Vatanen Marko		
Tiivistelmä <p>Opinnäytetyön toimeksiantajana toimi Jyväskylän ammattikorkeakoulu (JAMK) ja sen tiloissa toimiva Jyväskylä Security Technology (JYVSECTEC). Tavoitteena oli perehtyä Infobloxin DDI-tuotteeseen (DHCP, DNS, IP Address Management) ja tutkia ohjelmalla toteutetun ympäristön toimintaa ja kykyä toimia DNS-järjestelmän turvaratkaisuna DNS-komento ja -hallintakanavia hyödyntäviä haittaohjelmia vastaan.</p> <p>Työn lähtökohtana käytettiin aiemmin RGCE-verkkoon luotua Cisco Trustsec –ympäristöä, jonka pohjalle toteutettiin Infobloxin Grid-järjestelmä. Grid-kokonaisuus rakennettiin kolmesta Infoblox-palvelimesta, joiden avulla toteutettiin työympäristön DNS-, DHCP ja IPAM-palveluiden lisäksi ympäristön tiedon kerääminen sekä raportointi.</p> <p>DNS-protokollaa hyödyntävien haittaohjelmien toiminnan estämistä tutkittiin Infobloxissa löytyvän RPZ-ominaisuuden avulla. Lisäksi Infoblox integroitiin toimimaan haittaohjelmien torjumiseen tarkoitettun FireEye-ohjelmiston kanssa toiminnan tehostamiseksi.</p> <p>Tilajalle opinnäytetyön tulos jää käyttöön esittely-ympäristönä muille opintokursseille ja muuhun opetustoimintaan.</p>		
Avainsanat (asiasanat) Infoblox, DNS, DDNS, RPZ, DHCP, FireEye		
Muut tiedot		



Author(s) Aittanen, Tommi	Type of publication Bachelor's Thesis	Date 02.03.2015
	Pages 66 + 11	Language Finnish
		Permission for web publication: (x)
Title Infoblox implementation in JYVSECTEC-environment		
Degree Programme Information Technology		
Tutor(s) Piispanen Juha Saharinen Karo		
Assigned by JAMK University of Applied Sciences (JAMK), Jyväskylä Security Technology (JYVSECTEC) Vatanen Marko		
Abstract <p>The Bachelor's thesis was assigned by JAMK University of Applied Sciences (JAMK) and Jyväskylä Security Technology (JYVSECTEC) which operates in the premises provided by JAMK. The goal of the thesis was to familiarize with and research a DDI (DNS, DHCP and IPAM) product called Infoblox. On top of the DDI features Infoblox was also utilized as a safety feature against malware that used DNS command and control channels as an attack vector.</p> <p>Infoblox Grid was built on a pre-existing Cisco Trustsec Environment within the RGCE network. The grid system consisted of three different servers that not only provided DNS, DHCP and IPAM features but was also able to discover and build reports based on the collected information.</p> <p>The protection against malware that abused DNS protocol was achieved with the help of Response Policy Zones (RPZ). To further improve the malware protection Infoblox was integrated with a FireEye implementation.</p> <p>For the customer the result of the Bachelor's thesis will be used as a demonstration environment for courses and for other educational use.</p>		
Keywords Infoblox, DNS, DDNS, RPZ, DHCP, FireEye		
Miscellaneous		

Sisältö

1	Työn lähtökohdat	6
1.1	Toimeksiantajat	6
1.2	Työn tavoitteet	6
2	Domain Name System	8
2.1	Yleistä	8
2.2	DNS:n rakenne, autoritaarisuus ja delegaatio	9
2.2.1	Rakenne	9
2.2.2	Delegaatio	10
2.3	DNS-protokolla	11
2.3.1	DNS-paketti	11
2.3.2	Vyöhykkeiden päivitys	16
2.3.3	Nimikysely	19
2.3.4	Response Policy Zone	21
2.3.5	DDNS	22
3	DHCP	24
4	Infoblox	28
4.1	Yleistä	28
4.2	Infoblox DNS	29
4.3	Infoblox IPAM	30
5	Työn toteutus	34
5.1	Toteutusympäristö	34
5.2	Infobloxin konfigurointi	37
5.2.1	Grid	37
5.2.2	Infobloxin DNS-palvelu	39
5.2.3	Infoblox DHCP-palvelu	46
5.2.4	Muut Infobloxin asetukset ja ominaisuuksien todentaminen	52

5.3 RPZ-toteutus ja tulokset	56
5.3.1 Paikallinen RPZ ja RPZ-syöte	57
5.3.2 RPZ FireEye	60
6 Pohdinta	63
Lähteet.....	65
Liitteet.....	67
Liite 1: IANAn DHCP-optiot	67
Liite 2: Toteutusympäristö	72
Liite 3: DHCP:n jaettavan IP-osoitealueen konfigurointi.....	73
Liite 4: Reporting-palvelimen asetukset	74
Liite 5: RPZ-syötepalvelimen konfigurointi	75
Liite 6: Infoblox loki "www.skycrawler.com"-osoitteen estämisestä	77

Kuviot

Kuvio 1. DNS-delegaatio	10
Kuvio 2. DNS-viestin rakenne.....	11
Kuvio 3. Nimikysely "www.iltalehti.fi"	12
Kuvio 4. Zone-tiedosto	14
Kuvio 5. Zone-tiedosto SOA RR.....	14
Kuvio 6. TSIG	18
Kuvio 7. Rekursiivinen nimikysely	20
Kuvio 8. DHCP-prosessi.....	26
Kuvio 9. Infoblox-asetusten periytyminen	29
Kuvio 10. Infobloxin ja FireEyen yhteistyö	30
Kuvio 11. Infoblox Dashboard	31
Kuvio 12. IPv4-kontit	32
Kuvio 13. IP Map.....	32
Kuvio 14. Verkon topologia.....	35

Kuvio 15. Infobloxin kirjautumissivu.....	37
Kuvio 16. Lomake itseallekirjoitetulle sertifikaatille	38
Kuvio 17. Members-välilehti	39
Kuvio 18. DNS Zones-välilehti.....	40
Kuvio 19. DNS-välilehden Add-valikko	40
Kuvio 20. Autoritaarinen vyöhykeen 1. vaihe.....	41
Kuvio 21. Autoritaarisen vyöhykkeen 2. vaihe	41
Kuvio 22. Autoritaarisen vyöhykkeen 3. vaihe	42
Kuvio 23. Mac.sectec autoritaarinen vyöhyke	42
Kuvio 24. DC.mac.sectec vyöhykkeen siirron asettaminen	43
Kuvio 25. Autoritaarinen käänteinen vyöhyke.....	44
Kuvio 26. Reporting.localdomain Host-tiedot.....	45
Kuvio 27. A-tietueen määrittämien	45
Kuvio 28. Juurininipalvelimet	46
Kuvio 29. IPv4-verkon konfigurointi vaihe 4.....	48
Kuvio 30. WLC-verkon DHCP-optio	49
Kuvio 31. Cisco ISE.....	49
Kuvio 32. Ulkoinen DDNS-vyöhyke	50
Kuvio 33. Hallinto-verkon DDNS-asetukset.....	51
Kuvio 34. DHCP, DDNS ja DNS toiminta ympäristössä	52
Kuvio 35. NTP-palvelimen asiakkaat.....	53
Kuvio 36. Infobloxin NTP-palvelun tila.....	54
Kuvio 37. Infoblox syslog.....	55
Kuvio 38. IPAM näkymä IP-osoitteesta 192.168.20.49	56
Kuvio 39. Nimikysely osoitteesta "www.iltalehti.fi"	57
Kuvio 40. Infoblox RPZ-loki	58
Kuvio 41. RPZ-syötteen nimipalvelimet.....	59
Kuvio 42. RPZ-syötteen vyöhykkeen siirto	59
Kuvio 43. Nimikysely osoitteesta "www.youtube.com"	60
Kuvio 44. FireEye hälytysten toiminnot	61
Kuvio 45. Infobloxin SysLog FireEyesta	61
Kuvio 46. DHCP-pool vaihe 1	73

Kuvio 47. DHCP-pool vaihe 2.....	73
Kuvio 48. Reporting General-välilehti	74
Kuvio 49. Reporting DNS-välilehti	75
Kuvio 50. BIND /etc/named.conf -tiedosto.....	76
Kuvio 51. BIND zone-tiedosto	76

Taulukot

Taulukko 1. Header-osion kehysrakenne	11
Taulukko 2. Question-osion kehysrakenne.....	12
Taulukko 3. Answer-, Authority- ja Additional-osion kehysrakenne	13
Taulukko 4. DHCP-kehysrakenne	25
Taulukko 5. Ympäristön IP-verkot ja VLANit.....	36
Taulukko 6. DHCP IP-verkot	47

Lyhenteet

AD	Active Directory
AXFR	Authoritative Transfer
BIND	Berkley Internet Name Domain
ccTLD	Country Code Top-Level Domain
DHCP	Dynamic Host Configuration Protocol
DIG	Domain Information Groper
DNS	Domain Name System
DDNS	Dynamic DNS
FTP	File Transfer Protocol
FQDN	Fully Qualidied Domain Name
gTLD	Global Top-Level Domain
IPAM	IP Address Management
ISC	Internet Systems Consortium
IXFR	Incremental Zone Transfer
NS	Name Server
NTP	Network Time Protocol
RGCE	Realistic Global Cyber Environment
RPZ	Response Policy Zone
RR	Resource Record
SLD	Second-Level Domain
SOA	Start of Authority
TLD	Top-Level Domain
TSIG	Transaction SIGnature
TTL	Time-To-Live
VLAN	Virtual Local Area Network

1 Työn lähtökohdat

1.1 Toimeksiantajat

Jyväskylän ammattikorkeakoulu (JAMK) on vetovoimainen ja kansainvälinen korkeakoulu. JAMK tarjoaa muun muassa korkeakoulututkintoon johtavaa koulutusta, ammatillista opettajakoulutusta, avoimia ammattikorkeakouluopintoja ja täydennyskoulutusta. Toimipisteitä JAMK:lla on Jyväskylässä ja Saarijärvellä. (Tutustu JAMKiin 2014.)

Jyväskylän ammattikorkeakoulun tiloissa toimiva JYVSECTEC (Jyväskylä Security Technology) on kyberturvallisuuden tutkimus-, koulutus- ja kehityskeskus. JYVSECTEC-projektin toiminta aloitettiin syyskuussa vuonna 2011. Rahoituksen JYVSECTEC on hankkinut Keski-Suomen Liitolta ja Euroopan aluekehitysrahastosta, ja sen rahoitus jatkuu tammikuuhun 2015 asti. (JYVSECTEC 2014.)

JYVSECTECin yhtenä tavoitteena on luoda yhteistyöverkosto yhteistyökumppaneille ja muille turvallisuusalan toimijoille sekä vahvistaa toiminnallaan yritysten tietoisuutta tietoturvasta (JYVSECTEC 2014).

JYVSECTEC ylläpitää myös RGCE (Realistic Global Cyber Environment) kyberturvallisuuden kehitysympäristöä, jonka avulla koetetaan mallintaa Internetin todellista rakennetta. Järjestelmä on eristetty omaksi ympäristöksi, joka mahdollistaa oikeiden haittaohjelmien ja haavoittuvuuksien käyttämisen testauksissa hallitusti sekä turvallisesti ilman, että toiminnasta aiheutuisi haittaa tavallisille verkoille. (JYVSECTEC-RGCE 2014.)

1.2 Työn tavoitteet

Opinnäytetyön tavoitteena oli perehtyä Infobloxin DDI (DHCP, DNS, IP Address Management) -tuotteeseen ja tutkia ohjelman tarjoamien ominaisuuksien toimintaa sekä hyödyllisyyttä testausympäristössä. Monipuolisen IP-osoit-

teiden hallinta-, DHCP- ja DNS-järjestelmien lisäksi tutkittiin Infoblox-ohjelmiston ominaisuutta toimia ympäristön DNS-järjestelmän turvaratkaisuna, joka kykenee havaitsemaan ja suojaamaan muun muassa DNS-komento- ja hallintakanavia hyödyntäviä hyökkäyksiä vastaan estämällä haitallinen liikenne verkosta. Lisäksi tutkittiin ohjelmiston DNS-palomuurin ominaisuuksia sekä FireEye implementaatiota.

Infoblox-järjestelmä liitettiin osaksi RGCE-kehitysympäristössä (Realistic Global Cyber Environment) jo valmiiseen Cisco Trustsec -verkkoympäristöön. Opinnäytetyössä ei oteta kantaa Cisco Trustsec -järjestelmän toimintaan, vaan työn pääpaino on DNS-järjestelmässä ja sen suojaamisessa Infoblox-ohjelmiston avulla. Toimeksiantajalle opinnäytetyön tulos jää käyttöön esittelyympäristönä opetuskäyttöön.

2 Domain Name System

2.1 Yleistä

Domain Name System (DNS) on järjestelmä, jonka avulla voidaan esittää esimerkiksi laitteiden tai palvelimien käyttämät IP-osoitteet, kuten "192.168.1.10", ihmisille helpommin muistettavina niminä esimerkiksi "rpz.testing.biz"-muodossa. (Aitchison 2011, luku 1.)

Internetin alkuvaiheissa IP-osoitteiden nimimuutoksia hallittiin Network Information Centerin (NIC) ylläpitämän HOST.txt-tiedoston avulla. Järjestelmän ylläpitäminen kävi kuitenkin jatkuvasti raskaammaksi, sillä HOST.txt-tiedosto jouduttiin lähettämään aina uudestaan FTP:n avulla kaikille Internetin laitteille uuden version ilmestyessä. Tämä taas kasvatti jatkuvasti tiedosta ylläpitävän osapuolen kaistanvaatimuksia. Kasvavat tarpeet ja vaatimukset johtivat useisiin eri esityksiin, joissa kuitenkin yhteisenä teemana oli rakentaa hierarkkinen nimijärjestelmä. (IETF RFC 1034 1987, 1.)

Nykypäivän DNS-järjestelmä koostuu kolmesta pääosasta: nimipalvelimista, Domain Name Space -käsitteestä ja sen resurssitietueista (Resource Records, RR). Domain Name Space on määrittely DNS-järjestelmän puumaisesta rakenteesta ja sen jokaista solmua sekä lehteä vastaavasta resurssitietueesta. Nimipalvelimet koostuvat palvelinohjelmistosta, joka säilyttää tietoa DNS-puun rakenteesta ja sen tietuista. Ne kykenevät säilyttämään informaatiota välimuistissaan mistä tahansa domainpuusta, mutta yleisesti nimipalvelimien tiedot rajoittuvat puurakenteen nimialueisiin, joihin nimipalvelimella on täysi autoritaarius nimialueelle. Resolverilla taas tarkoitetaan DNS-järjestelmän komponenttia, jonka avulla tehdään nimikyselyitä nimipalvelimille. Resolverilla täytyy alustavasti olla vähintään tieto yhdestä nimipalvelimesta, josta se kykenee etsimään haettua informaatiota nimikyselyn avulla. Jos nimipalvelimella ei ole suoraa vastausta kyselyyn, se voi antaa vastauksena referenssin esimerkiksi toiseen nimipalvelimeen, josta resolveri kykenee jatkamaan nimikyselyä. (IETF RFC 1034 1987, 5.)

2.2 DNS:n rakenne, autoritaarisuus ja delegaatio

2.2.1 Rakenne

DNS-järjestelmän rakenne koostuu hierarkkisesta tai toisin sanoen puutietorakenneyppisistä vyöhykkeistä. Järjestelmän korkeinta domain-tasoa taas kutsutaan juurivyöhykkeeksi (root zone), jonka merkinnässä käytetään ”.”-merkkiä. Juurivyöhykkeen merkki on periaatteessa aina FQDN-nimien (Fully Qualified Domain Name) esimerkiksi ”rpz.testing.biz.”-osoitteen viimeisenä merkinä, mutta sitä ei kuitenkaan käytännön syistä useimmissa tapauksissa ilmaista. (Soyinka 2012, luku 16.)

Juurivyöhyke koostuu 13 juurinimipalvelimesta, jotka on nimetty A-kirjaimesta M-kirjaimen asti. Vaikka nimellisesti juurinimipalvelimia on ainoastaan 13, koostuu yksi nimipalvelin yleensä useista kymmenistä nimipalvelimista. Esimerkiksi Internet Consortiumin (ISC) operoima F-root-palvelin koostuu yli 50 palvelimesta, jotka ovat sijoitettu ympäri maailmaa. Tämä on mahdollista hyödyntämällä jokulähetystä (anycast), joka käytännössä mahdollistaa usean palvelimen toimimisen yhden palvelimen mukaisesti. (F-root)

Juuren ensimmäiset haarat muodostavat puun toisen tason, jossa sijaitsevat TLD:t eli top-level domain-nimet. TLD:t voidaan taas jakaa edelleen tarkemmin kuvattuihin ryhmiin kuten gTLD-, ccTLD- ja muihin TLD-erikoisryhmiin. Geneeriseen TLD-ryhmään kuuluvat esimerkiksi com-, net-, org-, museum- tai biz-päätteiset domain-nimet. CcTLD-ryhmään taas kuuluvat maakoodien mukaisesti päättyvät domain-nimet esimerkiksi fi, se tai us. (Soyinka 2012, luku 16.)

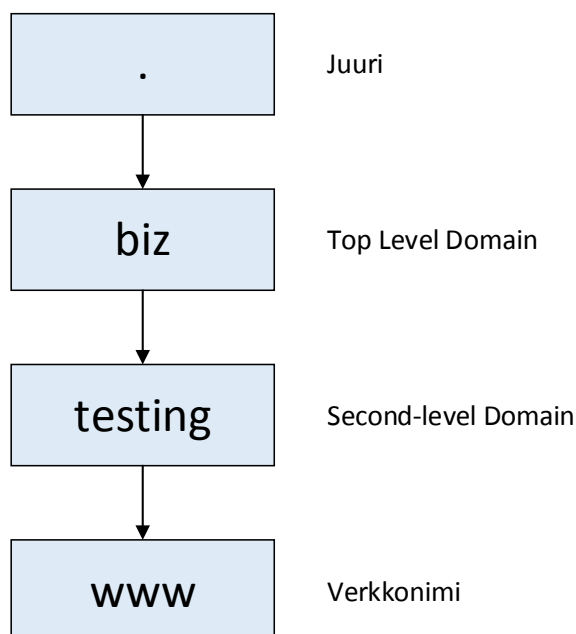
DNS-järjestelmän toista tasoa kutsutaan SLD-termillä eli Second-Level Domain names. Toisen tason osoitteita rekisteröidään yleensä organisaatioiden, järjestöjen tai yksityisten käyttöön TLD:ltä, jolloin esimerkiksi ”rpz.testing.biz” FQDN-osoitteesta ”testing”-osio olisi SLD nimenä. Kolmas ja sen jälkeiset tasot ovat vapaasti toisen SLD:n omistajan käytössä. Esimerkiksi kolmannessa

tasossa voidaan käyttää isäntäkoneiden nimiä (hostname), kuten "www" tai alidomainina seuraavalle tasolle. (Soyinka 2012, luku 16.)

2.2.2 Delegaatio

DNS:n hierarkkinen rakenne on perusta, kuinka autoritaarisuus toimii DNS-järjestelmässä. Autoritaarisuudella tarkoitetaan sitä, kuinka hierarkkisen DNS-järjestelmän solmu tai toisin sanoen autoritaarinen taho on vastuussa oman domain-nimen hallinnasta ja toiminnasta. Autoritaarinen osapuoli voi delegoida alidomainin hallitsemastaan vyöhykkeestään alemmalle DNS-hierarkiassa olevalle taholle. (Aitchison 2011, luku 1.)

Esimerkiksi FQDN "www.testing.biz.", joka koostuu kolmesta eri domain-vyöhykkeestä: Juurivyöhyke ".", gTLD "biz" ja SLD "testing". Kuviossa 1 on esitetty, kuinka autoritäärisyys on delegoitu alemmille tasolle lähtien ICANNin hallitsemasta juuritasosta, joka on delegoinut ".biz" -domainin toiselle organisaatiolle. Biz-toimialuetta hallitseva organisaatio sen sijaan on delegoinut testing-domainin oman autoritaarisen alueen alle rekisteröityvälle osapuolelle. Lopuksi "testing.biz"-domainin autoritaarisena tahona on päättänyt käyttää "www"-verkkonimeä palvelimessaan. (Aitchison 2011, luku 1.)

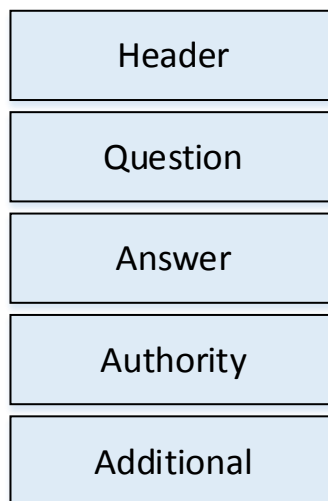


Kuvio 1. DNS-delegaatio

2.3 DNS-protokolla

2.3.1 DNS-paketti

DNS-viestien rakenne voidaan kuvata viiden eri osion avulla: Header, Question, Answer, Authority ja Additional. Kuviossa 2 on esitettyä eri osiot järjestyksessä.



Kuvio 2. DNS-viestin rakenne

Taulukon 1 Header-osio määrittää DNS-viestin oleelliset tiedot, esimerkiksi onko kyseessä kysely tai vastaus (QR), käytetyt liput, nimikyselyn ID (Query ID), kyselyn tyyppi (OPCODE) ja vastauksen tyyppi (RCODE) sekä informaation muiden osioiden tietueiden määrästä QDCOUNT-, ANCOUNT-, NSCOUNT- ja ARCOUNT -kentissä. (Aitchison 2011, luku 15.)

Taulukko 1. Header-osion kehysrakenne

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
ID															
QR	OPCODE				AA	TC	RD	RA	Z			RCODE			
QDCOUNT															
ANCOUNT															
NSCOUNT															
ARCOUNT															

Taulukossa 2 Question-osio sisältää nimikyselyn kohteen nimen, halutun resurssitietueen ja luokan QNAME-, QTYPE- ja QCLASS-kenttien avulla. Ainoastaan yksi kysely on mahdollinen yhdessä viestissä, joka on määritetty Header-osion QDCOUNT-arvossa. (Aitchison 2011, luku 15.)

Taulukko 2. Question-osion kehysrakenne

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
QNAME															
QTYPE															
QCLASS															

Esimerkiksi kuvion 3 mukaisessa nimikyselyssä osoitteesta "www.iltalehti.fi", QNAME olisi "www.iltalehti.fi", QTYPE on "A" ja QCLASS on "IN".

The screenshot shows a network traffic analysis tool displaying a DNS query and response. The query (Frame 3) is a standard query for 'www.iltalehti.fi' with type A and class IN. The response (Frame 4) is a standard query response indicating 'No such name'. The expanded response details show:

- Transaction ID: 0xbb32
- Flags: 0x0100 Standard query
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries:
 - www.iltalehti.fi: type A, class IN
 - Name: www.iltalehti.fi
 - Type: A (Host address)
 - Class: IN (0x0001)

Kuvio 3. Nimikysely "www.iltalehti.fi"

Viimeiset kolme osiota Answer, Authority ja Additional jakavat taulukon 3 mukaisen kehysrakenteen. Name-kenttä sisältää vastauksena saadun osoitteen. Type määrittää kyseisen resurssitietueen tyyppin esimerkiksi SOA tai A 16 bitin kokoisessa kentässä. Class ilmaisee luokan esimerkiksi IN eli internet. TTL määrittää kyseisen resurssitietueen välimuistissa säilyttämisen enimmäisajan 32 bitin kokoisessa kentässä. RDLENGTH on 16-bittinen numero, joka määrit-

tää RDATA-kentän pituuden oktetteina. Vaihtuvan mittainen RDATA-kenttä sisältää resurssitietueelle tyypillisen datan esimerkiksi A-tietueen tapauksessa IP-osoitteen. (Aitchison 2011, luku 15.)

Taulukko 3. Answer-, Authority- ja Additional-osion kehysrakenne

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
NAME															
TYPE															
CLASS															
TTL															
RDLENGTH															
RDATA															

Zone-tiedosto on kokoelma vyöhykettä eli zonea kuvaavasta informaatiosta kuten isäntäkoneista, nimipalvelimista ja muista palveluista resurssitietueina DNS-ohjelmistoille ymmärrettävässä muodossa (Aitchison 2011, luku 2). Vyöhyke taas on osa domainia. Esimerkiksi tilanteessa, jossa domainilla on kolme eri alidomainia, tarkoittaa se sitä, että jokaista alidomainia vastaa myös oma vyöhykkeensä. Yksinkertaisimmillaan domain, jolla ei ole alidomaineja omaa ainoastaan yhden vyöhykkeen, eikä domainilla ja vyöhykkeellä ole silloin käytännössä eroja. (Soyinka 2012, luku 16.)

Direktiivit ja resurssitietueet

Kuviossa 4 on esimerkkinä yksinkertainen zone-tiedosto, jossa direktiivit alkavat "\$"-merkillä, kommentit ";"-merkillä ja viimeisenä on määritetty vyöhykkeen informaatio RR-tietueina. Standardin RFC 1035 mukaisesti zone-tiedoston määritetyt ajat ilmoitetaan sekunteina.


```

$ORIGIN testing.biz.
$TTL 10800
@      IN      SOA      ns1.testing.biz. hostmaster.testing.biz. (
                          2014042301          ; serial
                          21600              ; 6h refresh
                          3600              ; retry after 1h
                          604800           ; expire after 1 week
                          86400 )          ; TTL

;glue record and nameservers
@      IN      NS       ns1.testing.biz.
ns1.testing.biz.  IN      A       222.87.208.192
recu.testing.biz.  IN      A       222.87.208.193
client.testing.biz.  IN      A       222.87.208.195

```

Kuvio 4. Zone-tiedosto

\$TTL eli Time-To-Live määrittää ajan, kuinka kauan RR-tietueita voidaan säilyttää välimuistissa, ennen kuin ne poistetaan. Direktiiviin voidaan määrittää aika 0 sekuntista aina suurimpaan mahdolliseen arvoon 2147483647 eli 68 vuoteen. Määrittäminen nolnaan sekuntiin tarkoittaa sitä, että tietueita ei koskaan tallenneta välimuistiin. (Aitchison 2011, luku 2.)

\$ORIGIN määrittää zone-tiedoston vyöhykkeen nimen. Direktiivi on vapaaehtoinen, mutta sen käyttö on suositeltava. Määritetty \$ORIGIN-arvo lisätään RR-tietueiden perään, jotka ovat niin sanottuja ”unqualified” nimiä eli nimiä, jotka eivät pääty pisteeseen kuten esimerkiksi zone-tiedostossa oleva verkkonimi ”www”. Toisaalta kun resurssitietueen nimi loppuu pisteeseen, esimerkiksi ”www.example.com.”, määritetään sen olevan FQDN, jolloin nimeen ei lisätä \$ORIGIN-arvoa. (Aitchison 2011, luku 2.)

SOA RR (Start of Authority) määrittää vyöhykkeen ominaisuuksia ja attribuutteja. Kuviossa 5 on esitettyä kuvankaappaus SOA-resurssitietueesta.

1.	2.	3.		4.	5.	
@		IN	SOA	ns1.testing.biz.	hostmaster.testing.biz	
				2014042301	; serial	6.
				21600	; 6h refresh	7.
				3600	; retry after 1h	8.
				604800	; expire after 1 week	9.
				86400)	; Nx	10.

Kuvio 5. Zone-tiedosto SOA RR

1. @-merkki korvataan määritetyllä \$ORIGIN-direktiivin arvolla. Vyöhykkeen voi määrittää myös FQDN-muodossa esimerkiksi ”testing.biz.”.

2. **Ttl**-arvo on jätetty määrittämättä, jolloin käytetään \$TTL-direktiivissä asetettua arvoa.
3. **Class IN** tarkoittaa, että luokkana on käytetty IN eli Internet-määrittystä.
4. **Name-server** "ns1.testing.biz." määrittää vyöhykkeen ensisijaisen nimi-palvelimen.
5. **E-mail** "hostmaster.testing.biz." määrittää autoritaarisen osapuolen sähköpostiosoitteen.
6. **Serial** "2014042301" ilmaisee zone-tiedoston versionumeron. Serialin arvo voi olla 0-4294967295 väliseltä alueelta. Serial-numeron arvoa täytyy aina korottaa zone-tiedoston tietueiden muuttamisen jälkeen tai tehdyt muutokset eivät tule voimaan.
7. **Refresh**-kentän arvo "21600" määrittää toissijaisten nimipalvelimen ajan, jonka kuluttua sen täytyy tarkistaa tai päivittää ensisijaisen nimipalvelimen zone-tiedoston uusimpaan versioon.
8. **Retry**-kentän arvo "3600" määrittää aikavälin, jonka toissijaisena toimiva nimipalvelin täytyy odottaa, ennen kuin se voi yrittää zone-tiedoston päivittämistä uudestaan.
9. **Expire**-kentän arvo "604800" määrittää ajan, jonka jälkeen toissijainen nimipalvelin ei oleta ensisijaisen palvelimen olevan enää autoritaarinen vyöhykkeestä. Ajan laskuri aloitetaan aina alusta, kun zone-tiedoston tarkistaminen tai haun uudelleen yrittäminen ensisijaiselle palvelimelle suoritetaan onnistuneesti.
10. **Nx** määrittää arvon, jonka ajan nimipalvelin pitää välimuistissaan epäonnistuneiden nimikyselyiden tiedot. Näin ollen nimipalvelin vastaa samalla negatiivisella NXDOMAIN-virheellä nimikyselyihin eikä suorita nimikyselyä uudestaan, ennen kuin tieto on vanhentunut välimuistista.
(Aitchison 2011, luku 2.)

NS-resurssitietueella määritetään autoritaariset nimipalvelimet toimialueelle. Zone-tiedostossa NS-tietue voidaan esittää esimerkiksi kuvion 4 vihreällä merkityn alueen ensimmäisen tietueen mukaisesti. NS-resurssitietue koostuu kokonaisuudessaan neljästä kentästä: Nimi, TTL, luokka ja toinen nimi-kenttä.

Ensimmäiset kaksi kenttää on mahdollista jättää asettamatta, jolloin käytetään aikaisemmin määritettyjä SOA-tietueen vyöhykettä ja \$TTL-direktiivin arvoa. Tietueen luokaksi määritetään Internet-arvolla "IN" ja jälkimmäisellä nimi-kentällä määritetään autoritaarisen nimipalvelimen nimi esimerkiksi "ns1.testing.biz.". (Aitchison 2011, luku 2.)

A-resurssitietueiden avulla määritetään IPv4-osoite halutuille verkkoaseman nimille. Vastaavasti IPv6-osoitteet taas määritetään AAAA-tietueiden avulla. Tietueen ensimmäisessä nimikentässä on mahdollista käyttää joko "unqualified" tai FQDN-nimen esitysmuotoa (Aitchison 2011, luku 2.)

CNAME-tietueen avulla voidaan määrittää useita aliaksia aiemmin määritetyllä A-tietueelle. CNAME-tietueita käytetään yleensä tilanteissa, jossa samassa palvelimessa on käytössä useampi palvelu, esimerkiksi web- ja ftp-palvelu, jolloin CNAME-tietueen avulla voidaan eritellä palvelut eri nimillä vaikka molemmat käyttävät samaa IP-osoitetta. (Aitchison 2011, luku 2.)

2.3.2 Vyöhykkeiden päivitys

DNS-järjestelmässä on yksinkertaistettu useiden nimipalvelimien vyöhykkeiden ja zone-tiedostojen hallintaa. Ensisijaisen ja toissijaisen nimipalvelimen välinen vyöhykkeiden siirto (zone transfer) ja hallinta on mahdollista suorittaa hyödyntämällä AXFR-, IXFR- tai DDNS-ominaisuuksia. Vyöhykkeiden siirto kuitenkin tuo uuden uhan DNS-järjestelmälle, ellei vyöhykkeen siirtoa turvata tarvittavalla tavalla esimerkiksi hyväksymällä päivitykset ainoastaan tunnetuista lähteistä. Toissijaisen nimipalvelimen zone-tiedosto voidaan myrkyttää (poisoning) sen hyväksyessä vyöhykkeen päivityksen tuntemattomasta lähteestä. (Aitchison 2011, luku 3.)

AXFR

Authoritative Transfer eli AXFR on DNS-järjestelmän ominaisuus, jonka avulla vyöhykkeen zone-tiedoston muutokset voidaan siirtää ensisijaiselta nimipalvelimelta toissijaiselle nimipalvelimelle. AXFR:ssä kuitenkin ominaista on se, että

vyöhykkeen yksittäisten muutosten sijaan siirretään toissijaiselle nimipalvelimelle samalla kerralla kaikki zone-tiedoston resurssitietueet. (Aitchison 2011, luku 3.)

AXFR-prosessi suoritetaan aina toissijaisen nimipalvelimen aloitteesta, kun vyöhykkeen SOA-tietueessa oleva refresh-arvon aika käynyt umpeen. Tämän jälkeen toissijainen nimipalvelin lähettää ensisijaiselle nimipalvelimelle nimikyselyn vyöhykkeen SOA-tietueesta. Jos vastauksena saadun SOA-tietueen serial-versionumero on suurempi kuin toissijaisen nimipalvelimen alkuperäinen versionumero, lähettää toissijainen nimipalvelin AXFR-pyyntön uudesta vyöhykkeen versiosta. (Aitchison 2011, luku 3.)

2.3.2.1 IXFR ja Notify

IXFR (Incremental Zone Transfer) on ominaisuus, jonka avulla vyöhyke voidaan päivittää tehokkaammin lähettämällä ainoastaan vyöhykkeessä muuttuneet osat, eikä AXFR:n tapaan lähettäen koko vyöhykettä päivityksen yhteydessä. (IETF RFC 1995 1996, 1.)

IXFR toimii siten, että ensisijainen IXFR:ää tukeva nimipalvelin säilyttää muistissaan uusimman version vyöhykkeen tiedoista ja sen eroista vanhempiin versioihin nähden (IETF RFC 1995). Toiminnollisuudeltaan IXFR ei suuremmin eroa AXFR-prosessista, sillä toissijainen nimipalvelin lähettää SOA-tietueen pyynnön ensisijaiselle nimipalvelimelle refresh-ajan mukaisesti. Erona nimipalvelimet selvittävät kuitenkin ensimmäiseksi sen, onko IXFR-ominaisuus käytettävissä molemmilla nimipalvelimillä. Jos IXFR-tuki on toiminnassa molemmissa palvelimissa, lähetetään vyöhykkeen siirron yhteydessä ainoastaan muuttuneiden tietueiden tiedot. Kun toinen palvelin taas ei tue IXFR-ominaisuutta, käytetään AXFR-toimintoa oletuksena vyöhykkeen päivittämisessä. (Aitchison 2011, luku 3.)

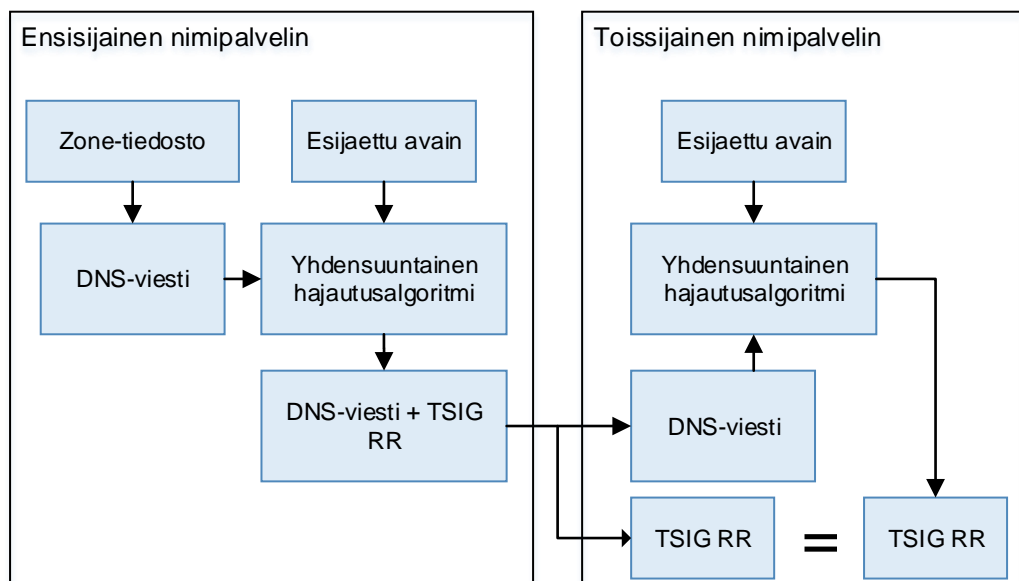
Notify on mekanismi, jonka avulla tehostetaan DNS-vyöhykkeen toimintaa nopeuttamalla vyöhykkeen päivittämistä. Se avulla ensisijainen nimipalvelin ky-

kenee ilmoittamaan vyöhykkeen tietueiden muutoksista määritetyille toissijaisille nimipalvelimille. Nimipalvelimet hyötyvät Notify-viestien lähettämisestä esimerkiksi silloin, kun SOA-tietueissa on käytössä pitkään kestävä ”refresh”-arvot palvelimien kuorman keventämiseksi ja silti halutaan pitää vyöhykkeen tiedot ajan tasalla. (IETF RFC 1996 1996, 1.)

2.3.2.2 TSIG

TSIG (Transaction Signature) on mekanismi, jonka avulla DNS-järjestelmän vyöhykkeiden siirrot voidaan todentaa käyttäen esijaettua avainta ja yhdensuuntaista avainnettua tiivistesummafunktiota. Mekanismi on määritetty RFC 2845, jossa esijaettu avain määritettiin HMAC-MD5-algoritmin avulla (Aichison 2011, luku 10.). Myöhemmin RFC 4635 laajensi TSIG:ssä käytettävien algoritmien määrää lisäämällä muun muassa GSS-TSIG-, HMAC-SHA1-, HMAC-SHA-perheen 224,256,384 ja 512 bittiset algoritmit. (IETF RFC 4635 2006, 1-2.)

Kuviossa 6 on esiteltyä TSIGin toiminta missä DNS-viestille lasketaan tarkistussumma yhdensuuntaisen avainnetun tiivistesummafunktion ja esijaetun avaimen avulla.



Kuvio 6. TSIG

Laskettu tiiviste (hash) säilytetään TSIG-resurssitietueeseen, joka lisätään DNS-paketin "Additional"-kenttään. DNS-viestin vastaanottava osapuoli tallentaa TSIG-tietueen ja poistaa sen alkuperäisestä viestistä, jonka jälkeen lasketaan uusi tiivistesumma käyttäen vastaanottajan omaa esijaettua. Lopuksi vastaanottaja vertaa viestin ohessa saatua TSIG-tietuetta sen itse laskemaan TSIG-tietueeseen. Jos tietueet täsmäävät voidaan DNS-viestin alkuperä todentaa, muuton viesti hylätään. Lisäksi vastaanotettavan viestin ollessa DNS-kysely, vastataan DNS-viestissä ilmoittaen väärästä avaimesta TSIG-ERROR arvoilla 16 (BADSIG) tai 17 (BADKEY). (IETF RFC 2845 2000, 4-5.)

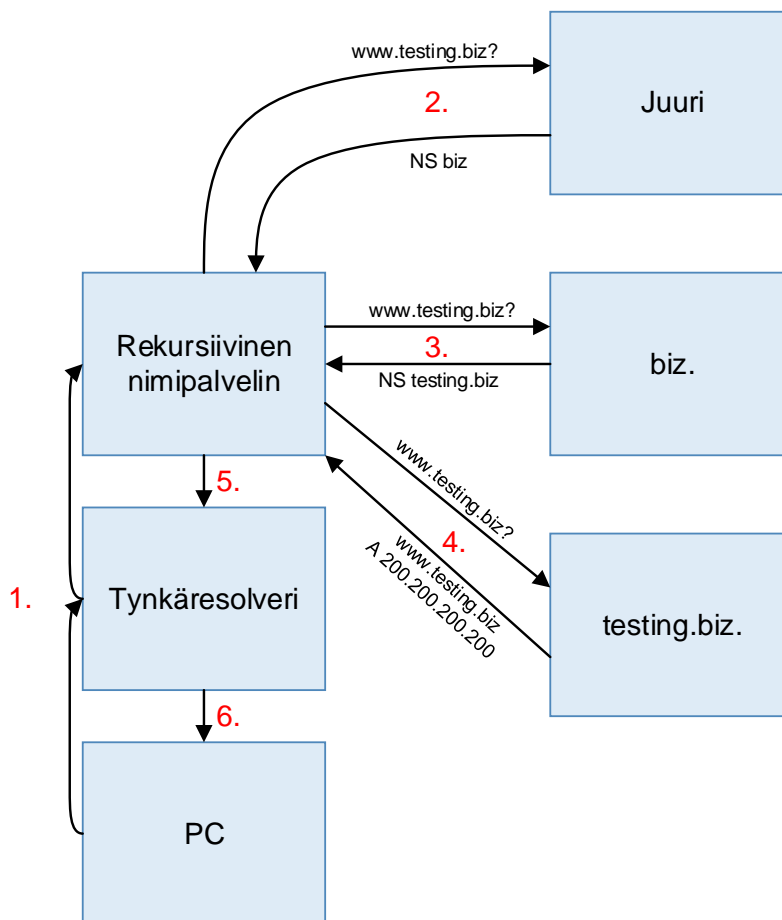
2.3.3 Nimikysely

Nimikysely on yksi DNS-järjestelmän operaatioista, jossa tarkoituksena on nimikyselyn avulla selvittää halutut resurssitietueet DNS-järjestelmästä. Nimikysely perustuu niin sanottuun kysymys-vastaus-periaatteeseen, missä asiakasohjelmisto muodostaa - yleensä tynkäresolverin (Stub resolver) avulla - nimikyselyn autoritaariselle nimipalvelimelle. Tynkäresolverit vaativat toimiakseen tukea rekursiiviselta nimipalvelimelta, sillä ne eivät kykene seuraamaan DNS-kyselyiden vastauksissa saatuja ehdotuksia (referral). Tyypillisesti PC-pohjaisissa koneissa käytetään nimikyselyitä välimuistiin tallentavia caching-only nimipalvelimia, jotka kuuluvat tynkäresolvereihin (Aitchison 2011, luku 4). Resolverilla tarkoitetaan asiakaspuolen ohjelmistoa tai nimipalvelinta, joka kykenee selvittämään DNS-informaatiota tarvittaessa. Kyselyssä DNS-järjestelmä käyttää oletuksena UDP porttia 53 kysymyksissä ja vastauksissa, mutta viestin koon ylittäessä 512 bittiä voidaan käyttää TCP-protokollan porttia 53. (Goralski 2009, luku 19.)

Erilaisia nimikyselyitä on määritetty kaksi kappaletta: rekursiivinen ja iteratiivinen nimikysely. Rekursiivisessa nimikyselyssä rekursiivinen nimipalvelin selvittää DNS-nimikyselyn kokonaisuudessaan, kunnes se saa kyselyn vastauksen tai virheilmoituksen. Vastauksen saamiseksi rekursiivinen nimipalvelin saattaa joutua tekemään useita kyselyitä autoritaarisilta nimipalvelimilta juuresta lähtien. (Aitchison 2011, luku 3.)

Iteratiivisessa nimikyselyssä DNS-viestin vastaanottava nimipalvelin ei aloita resurssitietueen selvittämistä, vaan antaa osittaisen vastauksen tai virheviestin kyselystä. Toisin sanoen se etsii ainoastaan omasta välimuististaan kysyttyä tietuetta ja sen puuttuessa nimipalvelin antaa vastauksessa ehdotuksen nimipalvelimesta, joka ehkä kykenee selvittämään nimikyselyn. (Aitchison 2011, luku 3.)

Kuviossa 7 on esiteltyä rekursiivinen nimikysely vaiheittain.



Kuvio 7. Rekursiivinen nimikysely

1. Ensimmäisessä vaiheessa PC:ltä pyritään siirtymään web-selaimella osoitteeseen "www.testing.biz", jonka sisään rakennettu tynkäresolveri (stub-resolver) etsii haettua tietuetta omasta välimuististaan. Jos tietuetta ei löydy, se lähettää DNS-kyselyn osoitteesta paikalliselle tai tunnetulle rekursiiviselle nimipalvelimelle.

2. Ennen osoitteen selvittämistä rekursiivinen nimipalvelin etsii ensin omasta välimuistista kysyttyä A-tietuetta "www.testing.biz"-osoitteesta. Jos osoitetta ei löydy, rekursiivinen nimipalvelin lähettää nimikyselyn samasta osoitteesta juuripalvelimelle. Juuripalvelin ei kykene selvittämään kysymystä rekursiivisesti, vaan vastaa viestiin iteratiivisesti antaen vastauksessa gTLD biz-vyöhykkeen nimipalvelinta vastaavan NS-tietueen.
3. Kolmannessa vaiheessa rekursiivinen nimipalvelin menettelee toisen vaiheen tavoin lähettämällä saman nimikyselyn, mutta iteratiivisessa vastauksessa saadulle biz-vyöhykkeen nimipalvelimelle. Vastauksena biz-nimipalvelin antaa iteratiivisesti "testing.biz"-vyöhykkeen nimipalvelimen NS-tietueen.
4. Neljännessä vaiheessa "testing.biz"-vyöhykkeen nimipalvelin on autoritääriäinen "www.testing.biz"-osoitteesta, jonka seurauksena se lähettää vastauksessa kysytyn palvelimen A-resurssitietueen.
5. Seuraavassa vaiheessa rekursiivinen nimipalvelin palauttaa tiedon takaisin PC:n tynkäresolverille.
6. Lopuksi tynkäresolveri lähettää nimikyselyn vastauksen PC:lle. (Goralski 2009, luku 19.)

2.3.4 Response Policy Zone

Response Policy Zone (RPZ) on ISC:n (Internet Systems Consortium) kehittämä mekanismi DNS-järjestelmälle, joka mahdollistaa DNS-kyselyjen vastausten muokkaamisen reaaliajassa asetettujen käytäntöjen (policy) avulla. Sen avulla voidaan manipuloida kyselyn vastauksessa annettua informaatiota, kuten esimerkiksi pakottamalla nimikyselyn epäonnistuminen NXDOMAIN-virheellä tai ohjaamalla kysely toiseen osoitteeseen aliaksen avulla. (Schryver & Vixie 2011, 1.)

Käytännössä RPZ:ssa käytetyt säännöt ovat pakattu zone-tiedostoon, jotta se pystytään jakamaan RPZ-listojen tuottajilta asiakkaille DNS-järjestelmän vyö-

hykkeiden siirtoon tarkoitetuilla IXFR- ja AXFR-ominaisuuksien avulla. Suurempia eroja RPZ:n zone-tiedostossa ei kuitenkaan ole verrattuna tavalliseen vyöhykkeeseen. Molemmissa täytyy vähintään olla yksi SOA- ja yksi NS-resurssitietue. RPZ-vyöhykkeitä jakavat nimipalvelimet eli RPZ-syötteen ei myöskään tarvitse vyöhykkeen delegointia ylemmän tason vyöhykkeeltä, sillä nimipalvelimien ei tarvitse vastata nimikyselyihin, vaan ainoastaan jakaa RPZ-vyöhykkeen tiedostoa asiakkailleen. RPZ-syötteen asiakasnimipalvelimet täytyy lisätä syötteen konfiguraatitiedostoon toissijaisiksi nimipalvelimiksi, jotta vyöhyke voidaan siirtää asiakkaalle. On myös suositeltavaa, että ensisijainen nimipalvelin hyödyntää IXFR-mekanismia ja Notify-viestejä RPZ-vyöhykkeen päivittämisen nopeuttamiseksi. (Vixie, Schryver 2011, 1.)

RPZ:n zone-tiedostossa käytänteiden resurssitietueen voidaan määrittää neljällä eri toiminnolla:

- NXDOMAIN-toiminnolla pakotetaan nimikyselyn vastauksena NXDOMAIN-virheviesti (Non-existent domain) CNAME-resurssitietueella, jonka kohde on juurivyöhyke (.).
- NODATA-toiminnolla pakotetaan nimikyselyn vastauksena NODATA-virheviestin CNAME-resurssitietueella, jonka kohde on vyöhyke (*).
- PASSTHRU-toiminnolla voidaan varmistaa, että muut RPZ-syötteen toiminnot eivät muokkaa määritettyä resurssitietuetta.
- Local Data -toiminnon avulla voidaan luoda keinotekoisia DNS-vastauksia. Esimerkiksi kyselyn vastaus voidaan uudelleenohjata toiseen osoitteeseen CNAME-tietueen avulla.

(Vixie, Schryver. 2011, 2.)

2.3.5 DDNS

DDNS (Dynamic DNS) on menetelmä, jonka avulla DNS-järjestelmän vyöhykkeitä on mahdollista päivittää toisesta ulkoisesta lähteestä. Menetelmä on määritetty IETF RFC 2136 standardissa. DDNS-standardi määrittää kuitenkin

muutamia vaatimuksia ja rajoituksia vyöhykkeen päivittämiselle, sillä DDNS:n avulla voidaan ainoastaan muokata, poistaa tai lisätä uusia resurssitietueita vain olemassa oleviin toimialueisiin tai vyöhykkeisiin. (Aitchison 2011, luku 3.)

3 DHCP

DHCP (Dynamic Host Configuration) on verkkoprotokolla, jonka avulla jaetaan verkkoasetukset dynaamisesti asiakaslaitteille. Protokolla toimii asiakas-palvelin-mallin mukaisesti, jossa DHCP-palvelimena toimiva laite vastaa asiakaslaitteen DHCP-viesteihin verkon asetuksilla ja muilla parametreilla TCP/IP-verkon ylitse. (IETF RFC 2131 1997, 1.)

DHCP-protokolla tarjoaa kaksi palvelua. Se muun muassa tarjoaa käyttäjäkohtaisesti pysyvän tiedon tallennuspaikan verkkoasetuksille. DHCP-palvelin kykenee siten jakamaan tarvittaessa samat verkkoasetukset samalle verkon laitteelle uniikin tunnisteeseen, kuten isäntänimen avulla. Toisena palveluna DHCP kykenee jakamaan IP-osoitteita dynaamisesti asiakkailleen pysyvästi tai väliaikaisesti. DHCP-palvelimen asiakaslaitteilleen jaetut osoitteet ovat niin sanotusti ”vuokralla” (lease). Palvelin varmistaa, että osoitteita ei jaeta uudelleen vuokran aikana. Kun asiakaslaitteen osoitteen vuokrauksen aika päättyy se vapauttaa osoitteen takaisin DHCP-palvelimelle. Asiakaslaiteen on mahdollista pidentää vuokra-aikaa uusilla DHCP-pyynnöillä. DHCP-viesteissä palvelimen ja asiakkaan välillä käytetään UDP-protokollaa, jossa asiakkaalta palvelimelle lähetetyissä viesteissä käytetään porttia 67 ja palvelimelta asiakkaalle taas porttia 68. (IETF RFC 2131 1997, 1-2.)

DHCP-protokollassa verkon ja valmistajakohtaiset asetukset sekä muut parametrit jaetaan DHCP-viestin optio-kentän avulla. DHCP-viestissä optio-kenttä on joko muuttuva tai kiinteäkokoinen, joka alkaa option määrittelevällä leimalla. Muuttuva mittaisiksi määritetään optiot, joiden leiman numero on suurempi kuin 255. Optio-kentän pituus määritetään taas leiman jälkeisessä okteetissa. DHCP-protokollan kehysrakenne on taulukossa 4. (IETF RFC 2132 1997, 3.)

Taulukko 4. DHCP-kehysrakenne

32 bit			
1 B	1B	1B	1B
OPCODE	Hardware Type	Length of Hardware Address	Hop Counter
Transaction ID			
Second Elapsed Since Sent First Request Message		Flag Field	
Client IP Address			
Client IP Address			
IP Address of Server			
Relay Route IP Address			
Client Hardware Address			
Server Host Name			
File Name			
Options			

Liitteessä 1 on IANA:n (Internet Assigned Numbers Authority) hallitsema lista 0-255 DHCP-optioista ja niiden pituuksista.

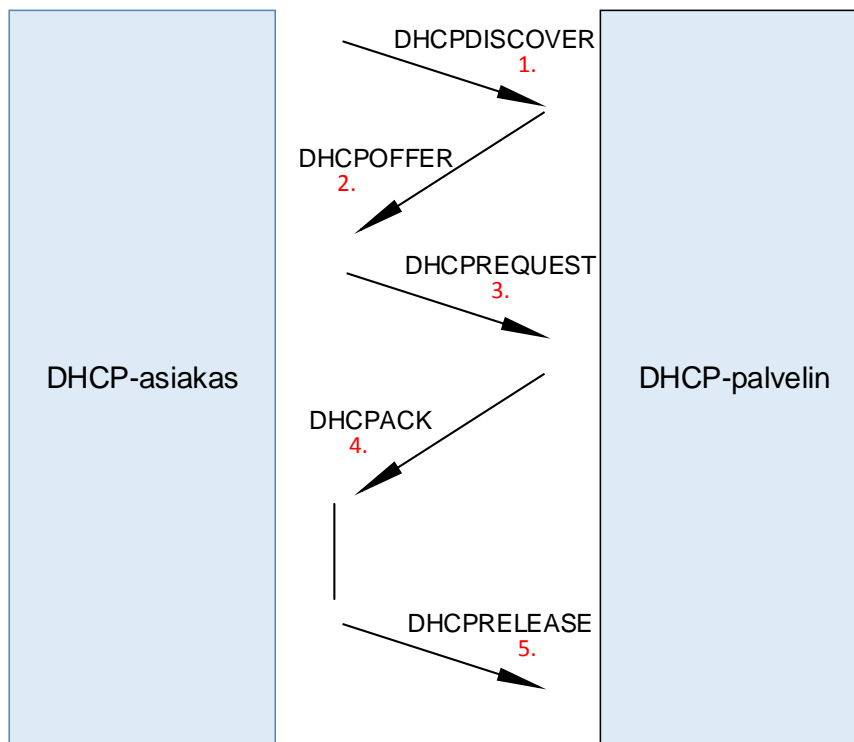
DHCP-operaatiossa käytetään kahdeksaa erilaista viestiä:

- **DHCPDISCOVER**-viestillä asiakaslaite etsii DHCP-palvelinta yleislähetksen (broadcast) avulla.
- **DHCPOFFER**-viestillä DHCP-palvelin lähettää asiakaslaitteelle tarjouksena DHCP-parametreja sisältävän asetuspaketin.
- **DHCREQUEST**-viestillä asiakaslaite voi pyytää tarjottua DHCPOFFER-pakettia halutulta DHCP-palvelimelta. Asiakaslaite pystyy myös pidentämään IP-osoitteen vuokrausta DHCP-palvelimelta.
- **DHCPDECLINE**-viestillä asiakaslaite pystyy hylkäämään tarjotun DHCPOFFER-paketin.
- **DHCPACK** eli Acknowledge-sanomalla DHCP-palvelin voi hyväksyä asiakkaan DHCPREQUEST-pyyntöä.
- **DHCPNAK**-sanomalla DHCP-palvelin voi taas kieltäytyä asiakkaan DHCPREQUEST-pyyntöstä.

- **DHCPRELEASE**-viestillä asiakaslaite voi vapauttaa jo DHCP:llä saadun IP-osoitteensa takaisin palvelimelle.
- **DHCPINFORM**-viesti lähetetään DHCP-palvelimelle, kun asiakaslaitteella on asetettu IP-osoite, mutta palvelimelta halutaan pyytää vielä muut verkon parametrit.

(Goralski 2009, luku 18.)

Kuviossa 8 on esitettyä asiakaslaitteen ja palvelimen välinen DHCP-prosessin kulku vaiheittain.



Kuvio 8. DHCP-prosessi

1. Ensimmäisessä vaiheessa DHCP-asiakaslaite lähettää IP-osoitteella 255.255.255.255 eli yleislähetyksellä DHCPDISCOVER-sanoman kaikille lähiverkonlaitteille. Asiakaslaitteen on mahdollista ehdottaa DHCPDISCOVER-viestiin haluttuja parametreja.
2. Kaikki sanoman vastaanottaneet DHCP-palvelimet voivat vastata DHCPOFFER-viestillä, jossa on sisällytettynä käyttämättä oleva IP-osoite.

3. Jos asiakaslaite on vastaanottanut useampia DHCPOFFER-paketteja, voi asiakaslaite valita haluamansa tarjouksen DHCPDISCOVER-viestissä ehdotettujen parametrien perusteella. Valinnan jälkeen asiakaslaite lähettää yleislähetyksellä DHCPREQUEST-sanoman, jossa on määritetty DHCP-viestin optiokentän "server identifier"-parametrin avulla sen DHCP-palvelimen IP-osoite, jonka DHCPOFFER-paketti pyydetään.
4. DHCP-palvelin voi hylätä DHCPREQUEST-pyyntöä DHCPNAK-sanomalla tai hyväksyä se lähettämällä DHCPACK-viesti DHCP-parametreilla. Jos asiakaslaite huomaa IP-osoitteen olevan jo käytössä se voi hylätä ja aloittaa DHCP-prosessi alusta DHCPDECLINE-viestillä.
5. Viimeisessä vaiheessa asiakaslaite vapauttaa IP-osoitteen varauksensa lähettämällä DHCPRELEASE-sanoman DHCP-palvelimelle.

(RFC 2131 1997, 12-16.)

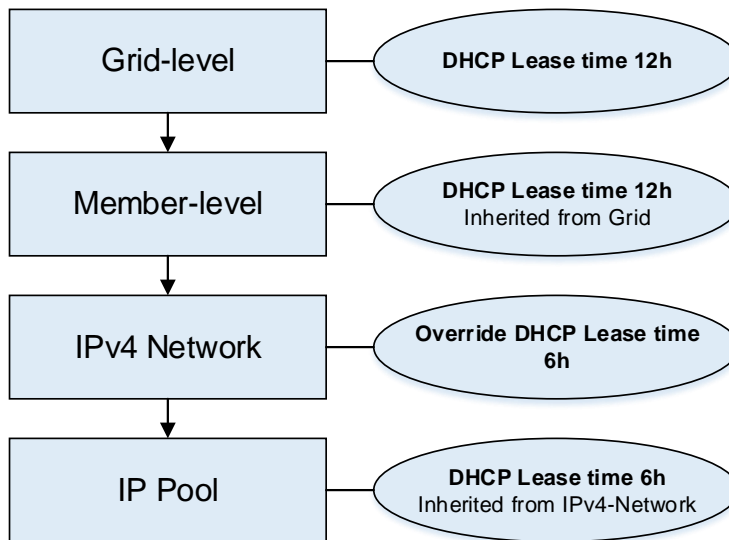
4 Infoblox

4.1 Yleistä

Infoblox on kaupallinen DDI-tuote eli tuote, joka tarjoaa DNS-, DHCP- ja IPAM- palveluja (IP Address Management). Infoblox-ohjelmiston tärkein ominaisuus on DDI ja muiden Infobloxiin liitettyjen palveluiden, kuten NTP tai FTP, hallitseminen keskitetysti Infobloxin Grid-järjestelmän avulla. Palveluiden hallinnan keskittämisen lisäksi Infobloxin on siten helppo synkronisoida informaatiota laitteiden välillä ja päivittää Grid-järjestelmä saumattomasti. (Trinzic DDI overview 2014.)

Gridiksi kutsutaan ryhmää, joka koostuu yhdestä tai useammasta Infobloxin NIOS-käyttöjärjestelmän fyysisestä tai virtualisoidusta vNIOS-laitteesta. NIOS-laitteet jakavat osan omasta tietokannastaan, mikä mahdollistaa laitteiden hallinnan ja konfiguroinnin keskitetysti Grid Masteriksi kutsutulta laitteelta. Muita Gridiin liitettyjä laitteita kutsutaan Grid Member -nimellä. (Infoblox NIOS Administrator Guide 2014.)

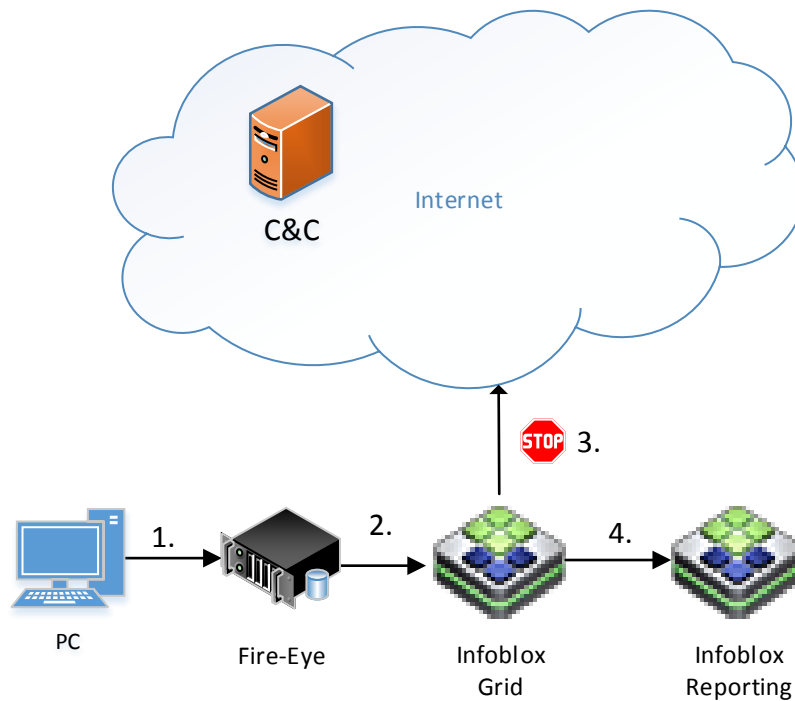
Infobloxissa on tärkeä ottaa huomioon, kuinka konfiguroinnin asetukset voidaan jakaa monitasoisen hierarkian avulla. Oletuksena korkeamman tason asetukset periytyvät suoraan alemmille tasoille. Esimerkiksi hierarkian korkeimman Grid-tason asetukset periytyvät kaikille Gridin Member-tason laitteille ja niistä taas seuraaville tasoille. Kaikilla alemmilla tasoilla voidaan kuitenkin yliajaa perityt asetukset tarvittaessa. Kuviossa 9 on esimerkki DHCP-asetusten periytymisestä Infobloxissa. (Infoblox NIOS Administrator Guide 2014.)



Kuvio 9. Infoblox-asetusten periytyminen

4.2 Infoblox DNS

Infobloxin NIOS-käyttöjärjestelmässä on käytössä BIND-ohjelmistoon pohjautuva DNS-järjestelmä. Graafista käyttöliittymän lisäksi Infobloxin DNS-ohjelmisto tarjoaa DNS-perustoimintojen lisäksi esimerkiksi DNSSEC-, DDNS- ja RPZ-toimintoja (Infoblox NIOS Administrator Guide). Erikoisuutena Infobloxin RPZ-ominaisuutta voidaan tehostaa integroimalla se FireEye-laitteeseen. FireEye on haittaohjelmien havaitsemiseen tarkoitettu järjestelmä. Yhdessä Infoblox ja FireEye muodostaa yhdistelmän, joka kykenee parhaimmillaan havaitsemaan haittaohjelmia FireEyellä, estämään tai häiritsemään niiden toimintaa automatisoidulla RPZ-vyöhykkeellä ja lopuksi paikantamaan saastunut kone verkosta Infobloxin avulla. Kuviossa 10 on esimerkki FireEyen ja Infobloxin yhteistyöstä vaiheittain. (Infoblox DNS Firewall - FireEye Adapter 2013.)



Kuvio 10. Infobloxin ja FireEyen yhteistyö

1. Ensimmäisessä vaiheessa sisäverkossa oleva saastunut laite pyrkii ottamaan yhteyttä esimerkiksi haittaohjelman C&C-palvelimeen.
2. Verkon liikennettä seuraava FireEye huomaa haittaohjelman toiminnan, joka aiheuttaa hälytyksen Infobloxin DNS-palomuurille. Hälytyksessä ilmoitetaan estettävä IP-osoite ja siihen liittyvä verkkotunnus.
3. Infoblox taas luo automaattisesti nimikyselyn estävän RPZ-säännön omaan järjestelmäänsä, jolloin haittaohjelman nimikyselyyn jätetään vastaamatta.
4. Infoblox selvittää saastuneen laitteen sen IP-osoitteen, DHCP-tietojen ja laitteen sormenjäljen avulla, ja luo lisäksi raportin tapahtumasta.

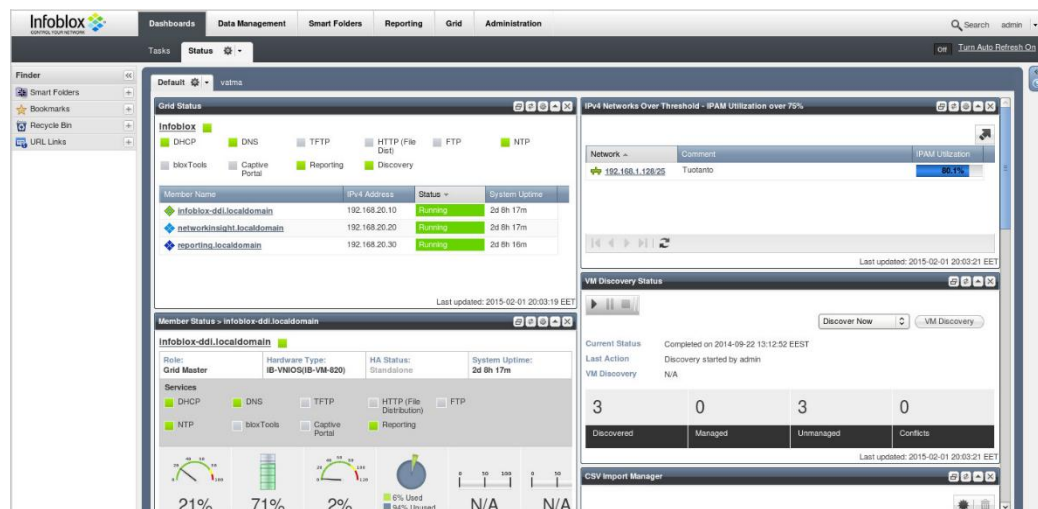
(Infoblox DNS Firewall - FireEye Adapter 2013.)

4.3 Infoblox IPAM

Jatkuvasti kasvavat IP-verkot, virtualisoidut sekä kannettavat laitteet luovat jatkuvasti enemmän paineita ja monimutkaisuutta IP-verkon hallintaan, jolloin

tarve IP-osoitteiden keskitetylle hallinnalle on kasvanut. IPAM eli IP-osoitteiden hallinta on käsite, jolla tarkoitetaan yksityisten IP-osoitteiden allokointia, suunnittelua, hallintaa, raportointia ja niiden seuranta IP-osoiteavaruudessa. Automatisoitu IP-osoitteiden hallinta voi parhaimmillaan nopeuttaa ja yksinkertaistaa IP-osoitteiden käsittelyä ja siten alentaa kustannuksia sekä konfiguroinnissa tapahtuvien virheiden määrää. (Infoblox IP Address Management 2013.)

Infobloxin tarjoaa IPAM-palvelun muiden DDI-palveluiden ohessa. IPAM on Infobloxin tapauksessa sisäänrakennettu DNS- ja DHCP-palveluihin, minkä seurauksena erillisiä laitteita tai sovelluksia ei tarvita sen käyttöönottamiseksi. Infobloxin muiden palveluiden hallinnan tavoin IPAM-ominaisuuksia hallitaan web-käyttöliittymän avulla. Kuviossa 11 on esitelty Infobloxin halintanäkymä, joka sisältää tiivistelmän verkon tilasta. (Infoblox IP Address Management 2013.)



Kuvio 11. Infoblox Dashboard

Infobloxissa IP-verkot esitetään kuvion 12 mukaisissa konteissa. Konttien avulla voidaan nopeasti huomata halutun verkon IP-osoitteiden käyttöaste.

Network	Comment	IPAM Utilization	Discover Now
192.168.1.0/25	Myynti	72.2%	
192.168.1.128/25	Tuotanto	80.1%	
192.168.4.0/24	Vierailijat	35.8%	
192.168.6.0/24	Hallinto	35.8%	
192.168.7.0/24	Wlan-yrityksenl...	4.3%	
192.168.20.0/24	LAN1	41.3%	
192.168.100.0/24	mgmt-vlan100	4.3%	
192.168.110.0/24	Infoblox Manag...	1.5%	
192.168.255.0/24	wlc	4.3%	

Kuvio 12. IPv4-kontit

Konttien sisältö on tarkemmin esiteltynä Kuvion 13 IP Map -paneelissa, jossa jokainen solu kuvaa IP-osoitetta. Solun väri sen sijaan kuvaa osoitteen tilaa esimerkiksi onko IP-osoite käytössä, kuuluuko osoite DHCP-osoitealueeseen ja niin edelleen.

IPAM Home
192.168.20.0/24 IPv4 Network [Go to DHCP View](#)

IP Map List

Go to Go

192.168.20.0 - 192.168.20.255

192.168.20.10

Type: A Record, PTR Record MAC Address: Name: infoblox-ddi.localdomain

Comment: Auto-created by Add Zone Name: infoblox-ddi.localdomain

Toggle Basic View

- Unused
- Conflict
- Used
- Pending
- Unmanaged
- Fixed Address / Reservation
- DNS Object
- Host Not In DNS/DHCP
- Device
- Active Lease
- Selected IP Address
- DHCP Range
- DHCP Exclusion Range
- Reserved Range

Kuvio 13. IP Map

Infoblox tarjoaa lisäksi mekanismin aktiivisten laitteiden etsimiseen Network Discovery -työkalun avulla. Network Discoveryn avulla voidaan kerätä infor-

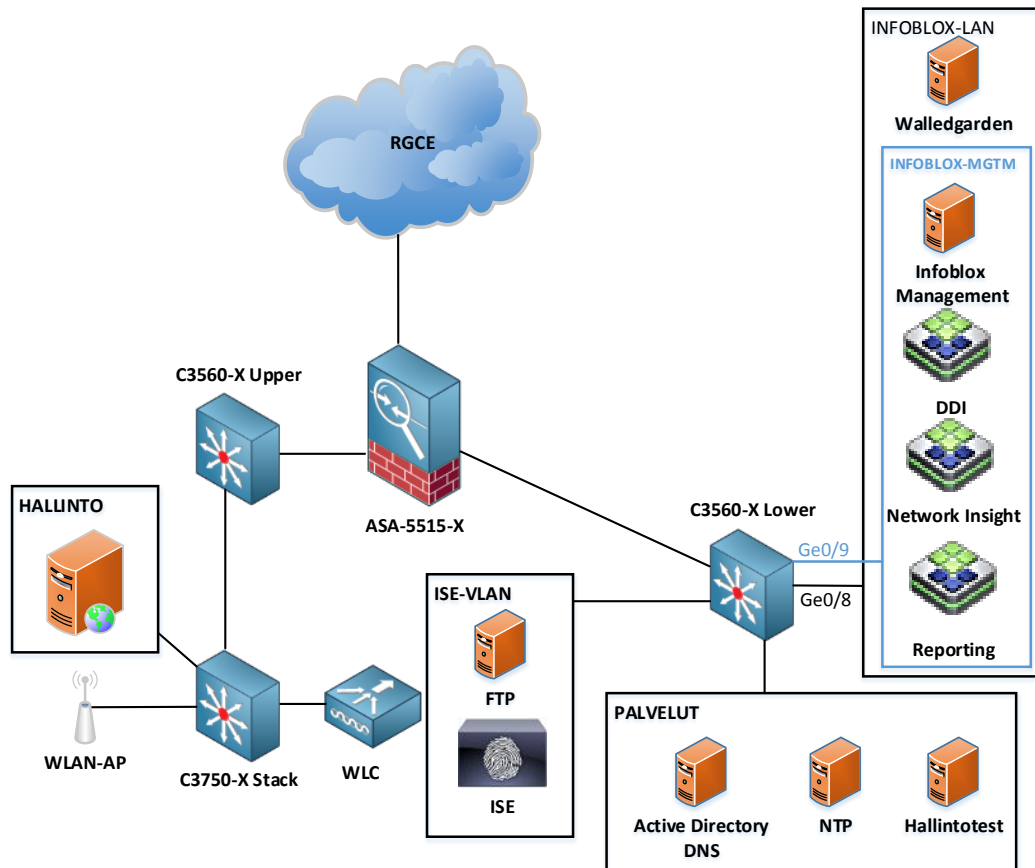
maatiota, kuten laitteiden MAC-osoitteita tai käytettyjä käyttöjärjestelmiä kaikista halutun verkon tuntemattomista ja tunnetuista laitteista. Tunnistamiseen Network Discovery käyttää ylläpitäjän määrittämää tapaa, kuten ICMP-protokollaa, NetBios tai TCP SYN-viestejä. Käytetty tapa määrittää sen mitä laitteista voidaan selvittää. Esimerkiksi pelkällä ICMP-viestillä voidaan ainoastaan selvittää laitteen aktiivisuus ja IP-osoite, kun taas TCP-viestillä Network Discovery voi selvittää IP ja MAC-osoitteen lisäksi käyttöjärjestelmän sen perusteella, miten kyselyn kohde vastaa avoimiin ja suljettuihin portteihin. (Info-blox NIOS Administrator Guide 2014.)

5 Työn toteutus

5.1 Toteutusympäristö

Opinnäytetyön toteutusympäristönä käytettiin JYVSECTEC RGCE-ympäristöön aiemmin suunniteltua Cisco Trustsec –ympäristöä. Ympäristöä käytettiin aikaisemmin Joni Honkasen (2014) opinnäytetyössä ”Cisco Trustsec käyttöönotto JYVSECTEC-ympäristössä”, joten haasteena oli konfiguroida Infoblox-järjestelmä osaksi ympäristöä vaikuttamatta suuremmin jo olemassa olevan järjestelmän toimintaan.

Muutokset alkuperäiseen topologiaan olivat suhteellisen pieniä. Infbloxin INFOBLOX-LAN- ja INFOBLOX-MGMT-VLANeja varten luotiin verkot Cisco C3560-X Lower –kytkimen portteihin Ge0/8 ja Ge0/9. Kuviossa 14 on esitettyä verkon topologia ja sen eri palvelut sekä komponentit. Liitteessä 2 on kuvio verkon koko topologiasta, kytkinten porteista ja palvelimien IP-osoitteista.



Kuvio 14. Verkon topologia

Kuviosta huomioitavaa on se, että Infobloxin kolme komponenttia DDI, Network Insight ja Reporting sekä lisäksi Infobloxin web-käyttöliittymän hallintaan käytetty kone Infoblox Management on liitetty molempiin INFOBLOX-LAN- ja INFOBLOX-MGMT -verkkoihin. Infoblox käyttää INFOBLOX-MGMT -verkkoa Grid-järjestelmän laitteiden hallintaliikenteelle, kun taas INFOBLOX-LAN verkkoa hyödynnetään kaikkeen muuhun liikennöintiin. Taulukossa 5 on taas lueteltu ympäristön kaikki eri verkot ja niiden VLANit.

Taulukko 5. Ympäristön IP-verkot ja VLANit

VLAN	Nimi	Osoiteavaruus	Prefix
10	MYYN TI	192.168.1.0	/25
30	VIERAILIJA	192.168.4.0	/24
40	PALVELUT	192.168.3.0	/24
70	WLAN-TYONTEKIJAT	192.168.7.0	/24
100	HALLINTO	192.168.6.0	/24
150	INFOBLOX-LAN	192.168.20.0	/24
160	INFOBLOX-MGMT	192.168.110.0	/24
255	WLC	192.168.255.0	/24
1000	ISE-WLAN	192.168.100.0	/24
3513	MGMT	192.168.5.0	/25
3514	MGMT 2	192.168.5.128	/24

Ympäristöön lisättiin lisäksi CentOS-käyttöjärjestelmällä toimivia virtuaalikoneita RPZ-testausta varten. Esimerkiksi Walledgarden lisättiin INFOBLOX-LAN-verkkoon ja Hallintotest PALVELUT-verkkoon. Myöhemmin toimeksiantajan johdolla lisättiin FireEye-implemентаatio ja tarvittut virtuaalikoneet sen testaamista varten.

Ympäristön kytkimiin porttikohtaisten VLAN-tietojen lisäksi muutettiin ainoastaan aikaisemmat DHCP-liikennettä ohjaavat DHCP Relay ja helper-address – asetukset Ciscon ASA-5515-X, C3750X-Stack ja WLC-laitteilta komendoilla:

ASA-5515-X

```
interface gi 0/1.40
  no dhcprelay server 192.1168.3.3
```

```
interface gi 0/1.150
  dhcprelay server 192.168.20.10
interface gi 0/1.160
  dhcprelay information trusted
```

```
no dhcprelay server 192.168.3.3
dhcprelay server 192.168.20.10 infoblox-lan
```

WLC

```
config interface dhcp management 192.168.20.10
save config
```

```

C3750X-Stack
interface vlan 255
  no ip helper-address 192.168.3.3
  ip helper-address 192.168.20.10

```

5.2 Infobloxin konfigurointi

5.2.1 Grid

DDI-, Network Insight- ja Reporting-palvelimet olivat valmiiksi asennettuja virtuaalikoneille toimeksiantajan toimesta pohjautuen Infobloxin vNIO-alustaan. Palvelimissa oli aluksi määritetty lisenssien lisäksi LAN1- ja MGMT-rajapintojen IP-osoitteet sekä hallintaan käytetyt tunnukset. Lisäksi DDI-palvelin oli asetettu Grid-masteriksi "Infoblox"-nimiselle Grid-ryhmälle. Kaikkien Infoblox-palvelimien konfigurointi suoritettiin web-käyttöliittymän yli ottaen yhteyttä laitteen MGMT-rajapinnan osoitteeseen, joka avasi kuvion 15 mukaisen kirjautumissivuston.



Kuvio 15. Infobloxin kirjautumissivu

Kirjautumisen ohessa DDI-palvelin muistuttaa jokaisella kirjautumiskerralla virheellisestä sertifikaatista. Tämä johtuu siitä, että oletuksena Infobloxissa on käytössä sen oma sertifikaatti. Valitus poistettiin luomalla uusi itseallekirjoitettu sertifikaatti kaikille Membereille. Uusi sertifikaatti luotiin valitsemalla Grid → Grid Manager → Toolbar → Certificates → HTTPS Cert → Generate Self-

signed Certificate –optio, joka avaa kuvion 16 mukaisen lomakkeen DDI-palvelimen sertifiointiin määrittämiseen.

The image shows a Windows-style dialog box titled "Generate Self-signed Certificate". It contains the following fields and values:

- Key Size*: 2048
- Days Valid*: 730
- Common Name (e.g. FQDN)*: infoblox-ddi.localdomain
- Organization (e.g. Company): JAMK
- Organizational Unit (e.g. Department): JYVSECTEC
- Locality: JKL
- State or Province: KESKI-SUOMI
- Country Code (2-letter code): FI
- Admin Email Address: admin@infoblox.localdomain
- Comment: (empty)

Buttons: Cancel, OK

Kuvio 16. Lomake itseallekirjoitetulle sertifiointille

Sertifiointien jälkeen Network Insight –palvelin ja Reporting-palvelin asetettiin osaksi Infoblox Gridiä Membereinä. Infobloxissa on kaksi samantyyppistä tapaa liittää Membereitä Gridiin. Ensimmäiseksi halutulle Memberille kirjautettiin esimerkiksi Reporting-laitteelle MGMT-rajapinnan osoitteella 192.168.110.30, jonka jälkeen käytettiin Grid Manager –välilehden työkalupalkista löytyvällä Join Grid –optiolla. Optio avaa lyhyen valikon, jossa määritetään seuraavat arvot:

- **Virtual IP of Grid Master** - Grid Masterin LAN1 rajapinnan osoite eli 192.168.20.10
- **Grid Name** – Grid instanssin nimi eli Infoblox
- **Grid Shared Secret** – eli Infoblox Gridin salasana

Lomakkeen täyttämisen ja hyväksymisen jälkeen palvelin uudelleen käynnistettiin Grid –välilehden alle ilmestyneestä Restart –nappulasta. Onnistuneen liittämisen jälkeen palvelimen hallintaosoitteeseen ei voida enää ottaa yhteyttä, vaan hallinta tapahtuu aina Grid Masterilta. Masterilla uudet Memberit voidaan todentaa Grid Managerin Members-välilehdeeltä löytyvistä uusista Gridin laitteista kuvion 17 mukaisesti.

		Name	HA	Status	IPv4 Address	Management IPv4 Address
		infoblox-ddi.localdomain	No	Running	192.168.20.10	192.168.110.10
		networkinsight.localdomain	No	Running	192.168.20.20	192.168.110.20
		reporting.localdomain	No	Running	192.168.20.30	192.168.110.30

Kuvio 17. Members-välilehti

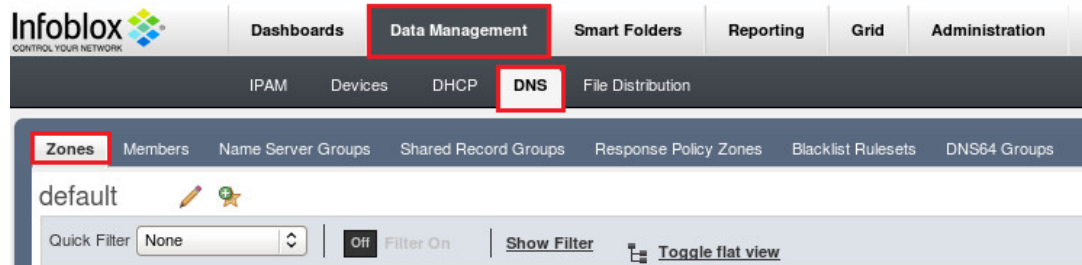
Tuntemattomasta syystä Reporting-palvelimen lisääminen ei onnistunut ensimmäisellä kerralla, vaan virtuaalipalvelin jouduttiin asentamaan uudestaan hallintayhteyden menetettyä palvelimelle lopullisesti. Asennuksen yhteydessä laite lisättiin suoraan Infoblox Gridiin ”set network”-konsolikomennolla määrittäen lisäksi liittymiseen tarvittavat parametrit. Lisääminen konsolikomennolla ei periaatteessa eronnut tavallisesta tavasta muutoin kuin käyttöliittymältään.

5.2.2 Infobloxin DNS-palvelu

Toteutusympäristössä oli ennen Infobloxin asennusta käytössä Windows 2008 R2 –käyttöjärjestelmällä toimiva Domain Controller, joka tarjosi DNS-, DHCP- ja Active Directory –palveluja. DC:n DNS-palvelun vyöhyke mac.sectec oli kytkettynä AD:n toimintaan, joten se päätettiin säilyttää toimintakykyisenä suurempien ongelmien välttämiseksi. Infobloxille tämä tarkoitti myös sitä, että sille asennettiin kaksi autoritaarisista vyöhykettä. Infoblox asetettiin toimimaan localdomain autoritaarisen vyöhykkeen ensisijaisena nimipalvelimena ja toissijaisena nimipalvelimena mac.sectec-vyöhykkeelle.

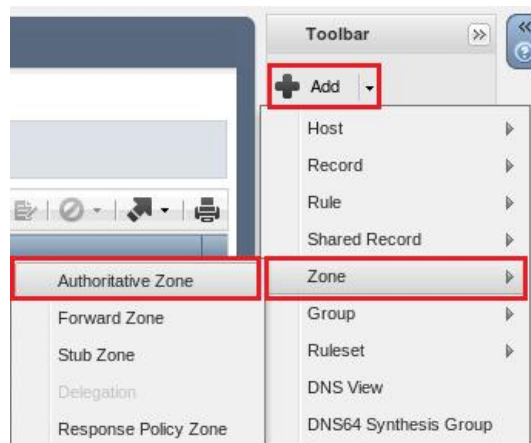
Localdomain- ja mac.sectec-vyöhykkeet

Infobloxin DNS-palvelu konfiguroitiin aloitettiin lisäämällä localdomain-vyöhyke siirtymällä kuvion 18 mukaisesti Data Management → DNS → Zones-välilehdelle.



Kuvio 18. DNS Zones-välilehti

Välilehdeä valitaan sen työkalupalkista Add-valikon alta löytyvä Zone → Authoritative zone kuvion 19 mukaisesti.



Kuvio 19. DNS-välilehden Add-valikko

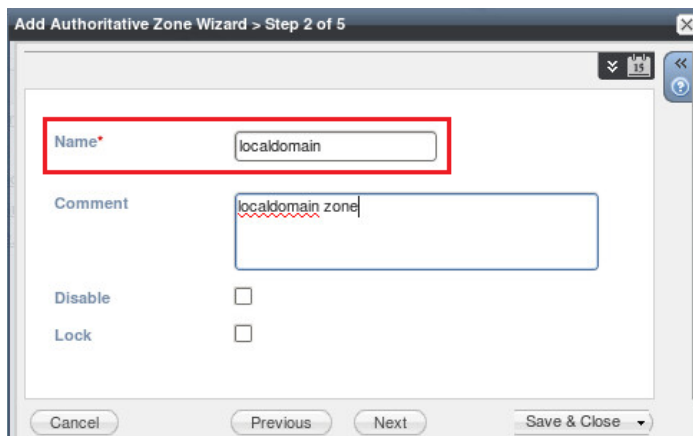
Kuten suurimmassa osassa muissakin Infobloxin konfiguroinneissa Authoritative Zone –valinta avaa monivaiheisen asennusavustajan, jossa määritetään arvot graafisessa käyttöympäristössä erilaisten lomakkeiden ja valintojen avulla. Seuraavassa kuvasarjassa käsitellään usein Infobloxin konfiguroinnissa tapahtuvaa monivaiheista asennusprosessia.

Ensimmäisessä vaiheessa kuvion 20 mukaisesti valitaan ensimmäisen vaihtoehto autoritaarisen vyöhykkeen lisäämiseksi.



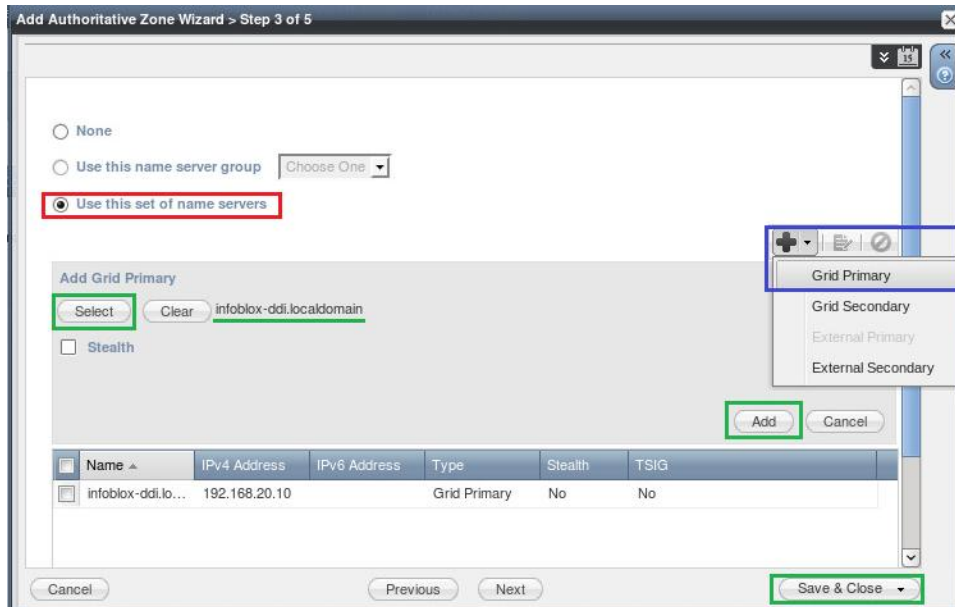
Kuvio 20. Autoritaarinen vyöhykeen 1. vaihe

Kuvion 21 toisessa vaiheessa määritetään vyöhykkeen nimi Name-kentässä. Juurivyöhykettä kuvaava viimeinen piste jätetään merkitsemästä nimeen. Vaihtoehtoisesti vyöhykkeelle voi antaa Comment-kenttään kuvauksen vyöhykkeestä.



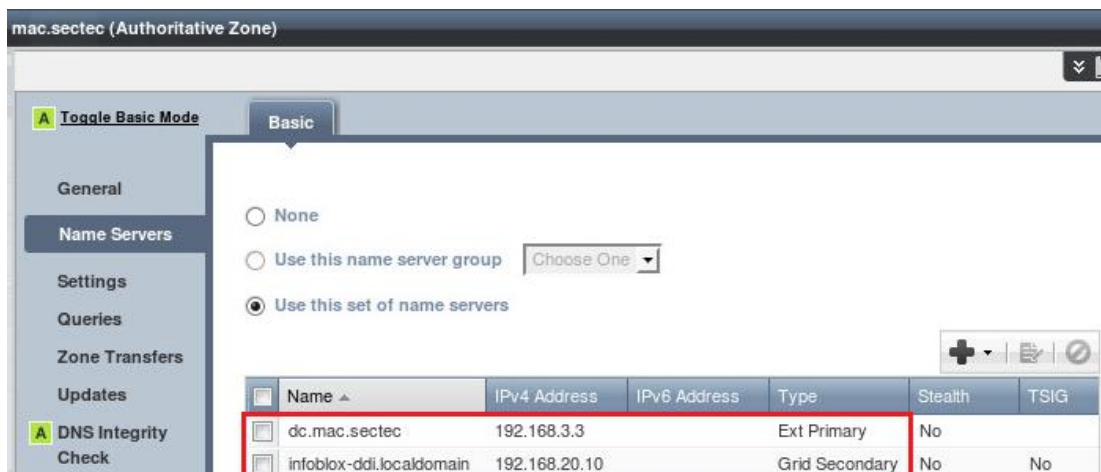
Kuvio 21. Autoritaarisen vyöhykkeen 2. vaihe

Kolmannessa vaiheessa määritetään vyöhykkeen ensisijainen nimipalvelin. Siirtämällä ensin valinta "Use this set of name servers" kohtaan, jonka jälkeen voidaan kuvion 22 sinisellä merkitystä Add-valikosta määrittää nimipalvelimen tyyppi. Grid Primary –valinnalla tarkoitetaan sitä, että nimipalvelimena on tarkoitus käyttää Gridiin liitettyä palvelinta ensisijaisena nimipalvelimena. Nimipalvelin valitaan automaattisesti painamalla vihreällä merkittyä Select-nappulaa, joka ehdottaa infoblox-ddi.localdomain–palvelimen nimipalvelimeksi. Ehdotettu palvelin täytyy vielä vahvistaa lisäämällä se Add-nappulalla. Koska asennuksen viimeisiä vaiheita ei vaadittu, tallennettiin muutokset Save & Close –nappulalla.



Kuvio 22. Autoritaarisen vyöhykkeen 3. vaihe

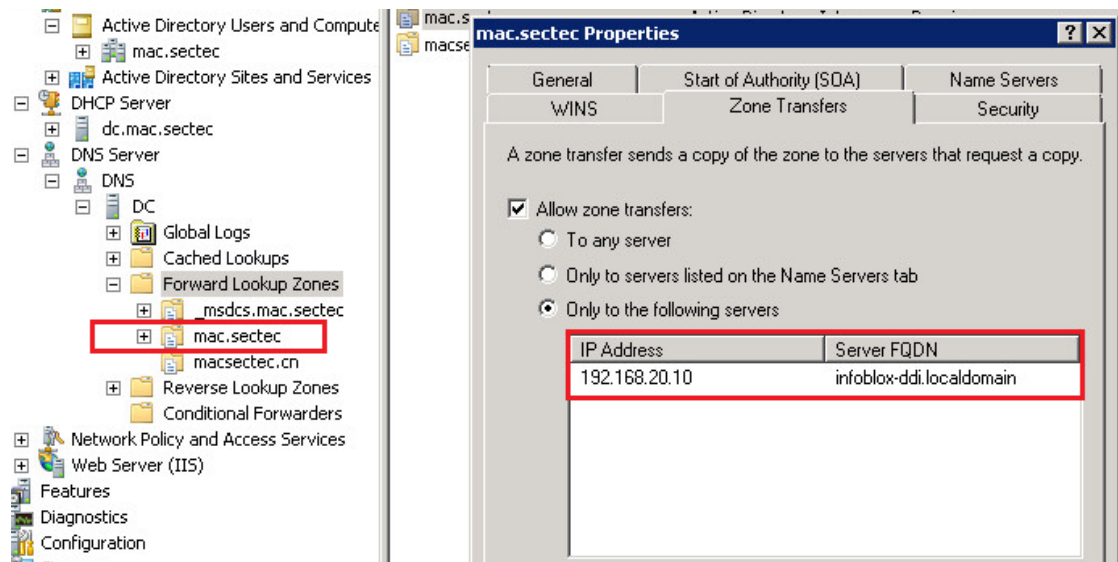
Mac.sectec-vyöhyke konfiguroitiin localdomainin tapaan kolmatta vaihetta lukuun ottamatta lähes samalla tavalla. Koska tarkoituksena oli asettaa Infobloxin nimipalvelin vyöhykkeen toissijaiseksi, kolmannessa vaiheessa määritettiin käyttämään kuvion 23 mukaisesti ulkopuolista ensisijaista nimipalvelinta (Ext Primary) eli dc.mac.sectec-palvelinta ja toissijaisena Gridin infoblox-ddi.localdomain-palvelinta (Grid Secondary).



Kuvio 23. Mac.sectec autoritaarinen vyöhyke

Jotta ensisijainen dc.mac.sectec jakaisi vyöhykkeen toissijaiselle Infobloxin palvelimelle, täytyi DNS-palvelun mac.sectec-vyöhykkeen asetuksista asettaa

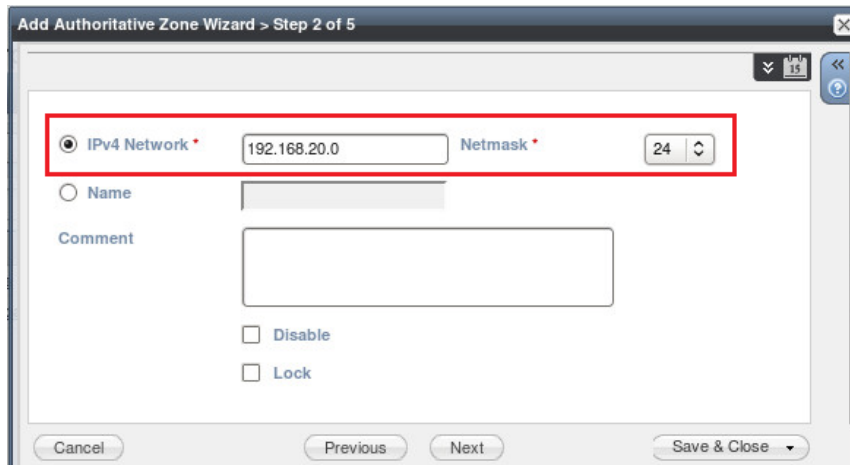
vyöhykkeiden siirto ainoastaan osoitteeseen 192.168.20.10 kuvion 24 mukaisesti. Infoblox sen sijaan hyväksyy automaattisesti ensisijaiseksi määritetyn nimipalvelimen tarjoaman vyöhykkeen, joten muita konfiguraatioita ei tarvitse tehdä.



Kuvio 24. DC.mac.sectec vyöhykkeen siirron asettaminen

Käänteinen nimikysely

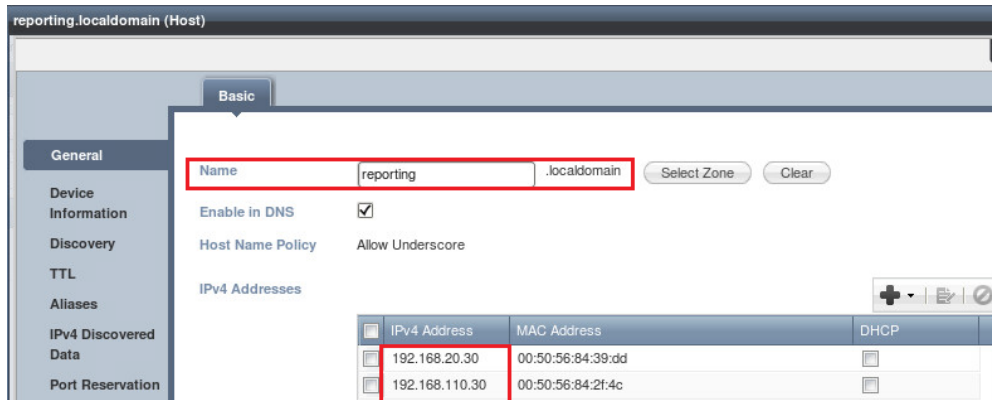
Käänteinen nimikysely eli nimikysely missä selvitetään päinvastaisesti IP-osoitteen avulla isäntäkoneen nimi, mahdollistettiin Infobloxissa luomalla sille uusi autoritääriin IPv4 reverse-mapping -vyöhyke. Vyöhyke luodaan autoritaarisen vyöhykkeen tavoin samalla asennusavustajalla, mutta ensimmäisessä vaiheessa valitaan ”Add an authoritative IPv4 reverser-mapping zone”-optio. Toisessa vaiheessa määritetään vyöhykkeen nimen sijasta IPv4-osoitealue kuvion 25 mukaisesti.



Kuvio 25. Autoritaarinen käänteinen vyöhyke

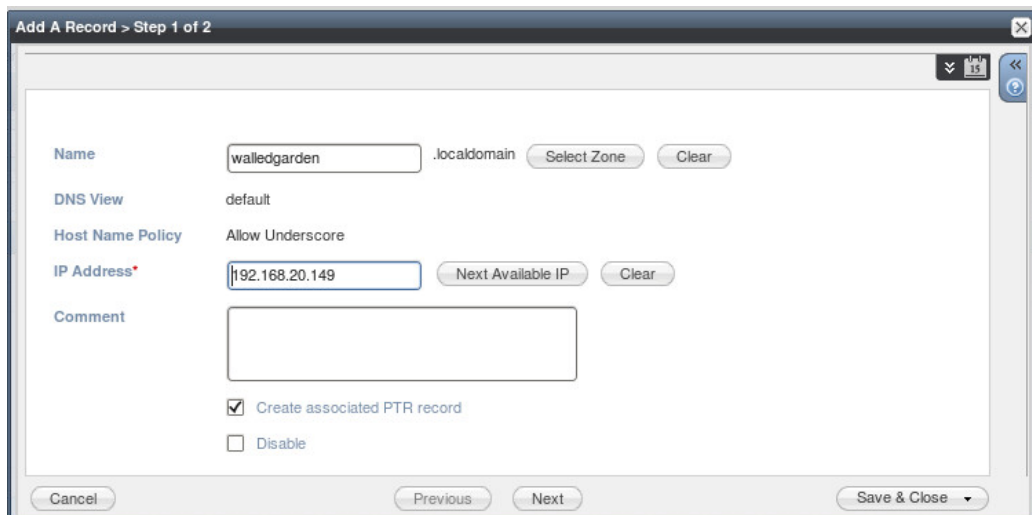
Kolmannessa vaiheessa määritetään autoritaarisen vyöhykkeen mukaisesti käytetyt nimipalvelimet. 192.168.20.0/24 käänteisen vyöhykkeen nimipalvelimena käytettiin Gridin infoblox-ddi.localdomain-palvelinta. Lisäksi lisättiin 192.168.110.0/24 -verkolle käänteinen vyöhyke.

Localdomain-vyöhykkeeseen lisättiin myös Infobloxin Reporting-, Network Insight- ja Infoblox-ddi-palvelimien tietueet työkalupalkin Add → Host → Host -optiolla. Add Host:n avulla voidaan määrittää DNS-, DHCP- ja IPAM-dataa helposti yhdelle laitteelle samasta asennusavustajasta. Palvelimien tietojen konfiguroinnissa käytettiin ainoastaan ensimmäistä vaihetta, jossa määritettiin palvelimien isäntäkoneen nimi ja siihen liittyvät IP-osoitteet. Kuviossa 26 on esimerkiksi avattuna reporting.localdomain-palvelimen tietue localdomain-vyöhykkeestä. Koska palvelimella oli kaksi rajapintaa, sen molemmat IP-osoitteet määritettiin konfigurointivaiheessa.



Kuvio 26. Reporting.localdomain Host-tiedot

Yksittäisiä tavallisia tietueita esimerkiksi A-tietueita lisättiin työkalupalkin Add → Record → A-record-optiolla. Kuviossa 27 on esimerkiksi määritetty walledgarden.localdomain-palvelimen tietue, jossa on yksinkertaisesti määritetty sen nimi ja IP-osoite. Lisäksi Infobloxissa on mahdollisuus luoda automaattisesti PTR-tietueet käänteistä nimikyselyä varten, jos IP-osoitteita vastaavat vyöhykkeet ovat asetettu ennen tietueiden asettamista.

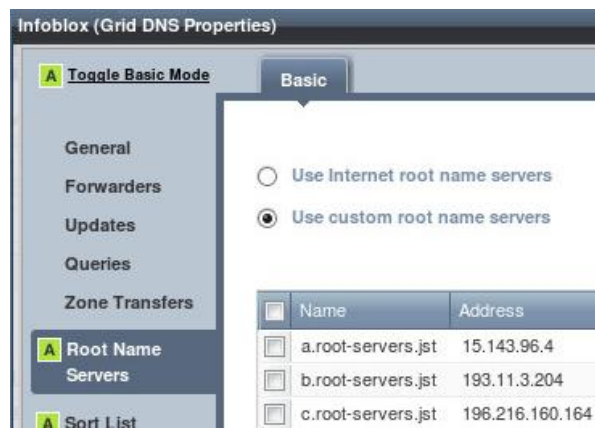


Kuvio 27. A-tietueen määrittämien

Muut DNS-palvelun asetukset

Jotta Infoblox kykenisi selvittämään nimikyselyitä muista, kuin sisäisestä verkosta, täytyi DNS-palvelulle määrittää Grid-tasolla RGCE-verkon juuriniimpalvelimien IP-osoitteet. Oletuksena Infoblox käyttää julkisen internetin juuriniimpalvelimien osoitteita, joten ne täytyi muuttaa Data Management → DNS →

Toolbar → Grid DNS Properties valikon Root Name Servers –sivulta kuvion 28 mukaisesti.



Kuvio 28. Juurinimipalvelimet

Lopuksi Grid-tasolla määritettiin Infobloxin DNS-palvelu hyväksymään ja suorittamaan rekursiivisia nimikyselyitä. Ominaisuus otettiin käyttöön valitsemalla ”Allow recursion”–optio sekä käyttämällä ”Allow recursion queries from” arvolla ”none”, jolloin Infoblox hyväksyy kaikki nimikyselyt lähettäjistä riippumatta.

5.2.3 Infoblox DHCP-palvelu

DHCP-palvelu otettiin käyttöön infoblox-ddi.localdomain–palvelimella. Kuten DNS-palvelun tapauksessa, DHCP-palvelua haluttiin suorittaa Infobloxin avulla eikä Domain Controllerilla, koska silloin voidaan todella hyödyntää Infobloxin tarjoamia raporttipohjia, statistiikkoja ja muita IPAM-ominaisuuksia.

IPv4 verkot

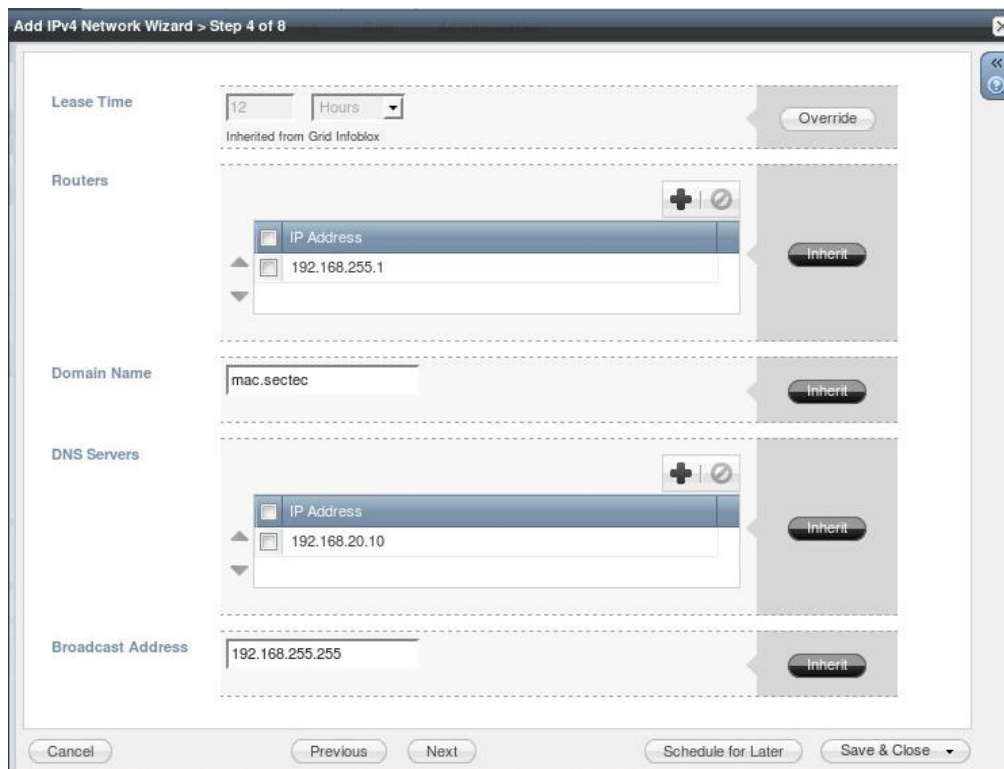
Ensimmäiseksi lisättiin edelliseltä DC.mac.sectec DHCP-palvelimelta löytyvät IP-verkot ja jaettavat IP-osoitealueet sekä Infobloxin Management- ja LAN1-verkot. Taulukossa 6 on listattuna lisätyt verkot, niiden nimet, jaettavat osoitealueet (address pool) ja reitittimen sekä yleislähetysten (broadcast) osoitteet. Kaikille IP-verkoille määritettiin lisäksi DNS-palvelimeksi infoblox-ddi.localdo-

main-palvelin IP-osoitteella 192.168.20.10. Lisäksi kaikille paitsi LAN1- ja Infoblox Management –verkoille määritettiin DNS-vyöhykkeeksi mac.sectec. Kahdelle ensimmäiseksi mainitulle asetettiin käyttämään localdomain-vyöhykettä.

Taulukko 6. DHCP IP-verkot

Nimi	Verkko	Address Pool	Reititin	Broadcast
Myynti	192.168.1.0/25	10-100	192.168.1.1	192.168.1.127
Tuotanto	192.168.1.128/25	140-240	192.168.1.129	192.168.1.129
Vierailijat	192.168.4.0/24	10-100	192.168.4.1	192.168.4.255
Hallinto	192.168.6.0/24	10-100	192.168.6.1	192.168.6.255
Wlan-yrityksenlaitteet	192.168.7.0/24	10-20	192.168.7.1	192.168.7.255
mgmt-vlan100	192.168.100.0/24	20-30	192.168.100.1	192.168.100.255
wlc	192.168.255.0/24	20-30	192.168.255.1	192.168.255.255
LAN1	192.168.20.0/24	50-150	192.168.20.1	192.168.20.255
Infoblox Management	192.168.110.0/24	-	192.168.110.1	192.168.110.255

Verkkojen lisäys tehtiin Data Management → DHCP → Networks –välilehden työkalupalkin Add → Network → IPv4-optiosta, joka avaa 8 osaisen asennus-avustajan. Kolmessa ensimmäisessä vaiheessa määritetään ainoastaan IPv4-verkon osoite, aliverkonpeite ja DHCP-palvelua tarjoava Infobloxin laite. Kuvion 29 neljännessä vaiheessa käytettiin WLC-verkkoa IP-osoitteella ja aliverkonpeitteellä 192.168.255.0/24 sekä Grid Masteria DHCP-palvelua tarjoavana laitteena. Optiot asennettiin neljännessä vaiheessa siten, että kaikissa verkoissa asetettiin DHCP jakamaan oman verkkonsa reitittimen osoitetta oletusyhdykäytävänä taulukon 6 mukaisilla arvoilla. DHCP:n avulla pyrittiin myös ohjaamaan DNS-liikenne Grid Master –palvelimelle käyttämällä DNS-palvelimen IP-osoitetta 192.168.20.10 kaikissa DHCP-viesteissä.

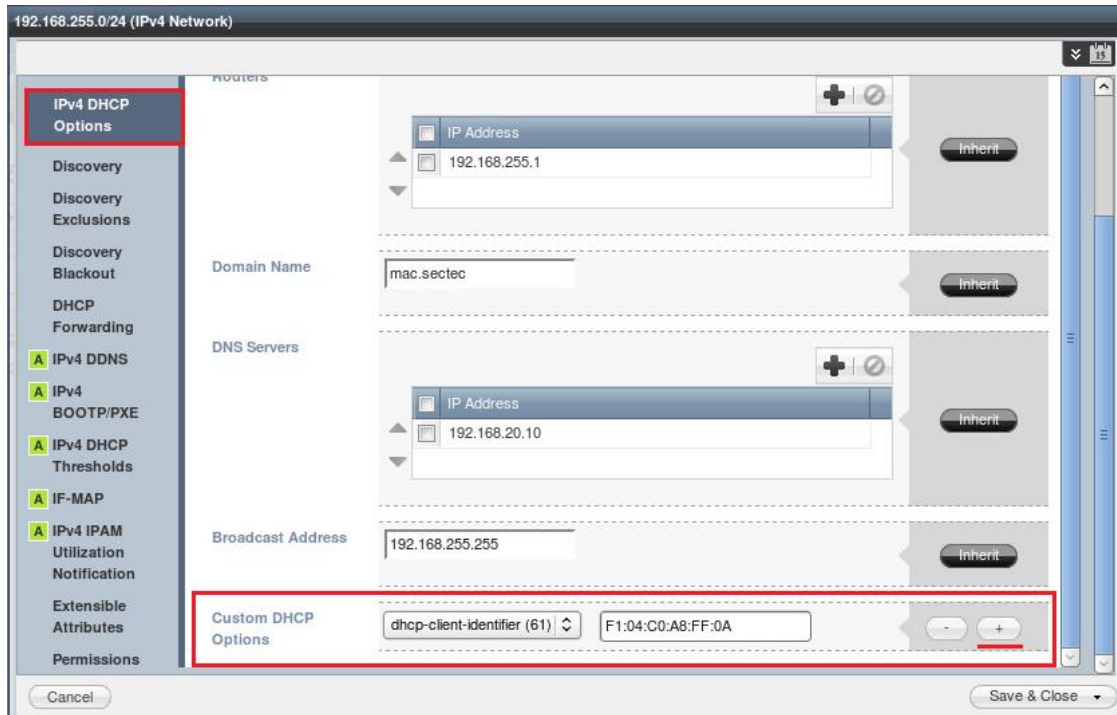


Kuvio 29. IPv4-verkon konfigurointi vaihe 4

DHCP-palvelua varten lisättiin vielä jokaiselle asetetulle verkolle taulukossa 6 määritetyt IP-osoitealueet. Liitteessä 3 on esimerkki kuinka Infobloxin LAN1-verkkoon konfiguroitiin jaettava IP-osoitealue. Kaikki muut IP-verkot konfiguroitiin sama kaavan mukaisesti.

WLC-optiot

Dc.mac.sectec-palvelimella oli lisäksi määritetty muista DHCP-pooleista poiketen WLC-verkolle DHCP-optioihin valmistajakohtaisia asetuksia. Jotta edelliset Cisco ISE-palvelut saataisiin toimimaan uuden DHCP-palvelun kanssa, täytyi WLC-laitetta varten lisätä manuaalisesti Domain Controllerin mukaisesti samat option arvot. Toisin kun Window 2008 R2 -palvelimella, Infobloxissa DHCP-option dhcp-client-identifier (61) IP-osoitteen arvo 192.168.255.10 täytyi määrittää heksadesimaalina, missä IP-osoitteen edessä käytettiin F1:04 arvoa kuvaamassa yhtä WLC-laitetta. Arvo lisättiin valitsemalla WLC-verkko ja lisäämällä DHCP Options -välilehteen DHCP-optio 61 kuvion 30 mukaisesti arvolla F1:04:C0:A8:FF:0A.



Kuvio 30. WLC-verkon DHCP-optio

Koska Infoblox oli ympäristössä ainoa käytettävä DHCP-palvelin, annettiin sille edellisen DHCP-palvelimen tavoin Cisco ISE:stä SGT-leima (Security Group Tag) liittämällä se jo ISE:ssä olevaan SG_PALVELIMET-ryhmään. Lisäys tapahtui ISE:n hallintapaneelista Policy → Policy Elements → Results → Security Group Access → Security Group Mappings -välilehdeltä "Add"-toiminnolla, jossa määritettiin SGT-ryhmän lisäksi Infoblox palvelimen IP-osoite 192.168.20.10 kuvion 31 mukaisesti.



Kuvio 31. Cisco ISE

DDNS-asetukset

Infobloxissa hyödynnettiin DDNS-ominaisuutta molemmissa localdomain- ja mac.sectec-vyöhykkeissä. Sen avulla pystyttiin DHCP-prosessin suorittamisen jälkeen muun muassa automaattisesti johtaa laitteille verkkoaseman nimi DHCP:llä annetusta IP-osoitteesta esimerkiksi muotoa ”*dhcp-192-168-6-98.mac.sectec*”, ellei nimeä ollut kyselyn ohessa määritetty. Toimintoa varten täytyi Domain Controller säätää hyväksymään DNS Update –viestit.

DDNS-ominaisuuden konfigurointi aloitettiin muokkaamalla localdomain-vyöhykkeen DNS-asetuksia Data Management → DNS → localdomain → Edit → Updates-sivulta, jossa määritettiin ”Allow updates from”-kenttässä ”Set of ACEs”-valinta. Valinnan avulla määritetään Infobloxille osoite, josta Update-viestejä voidaan hyväksyä. Oletuksena Infoblox ei hyväksy DDNS-toimintoa, joten sille täytyi määrittää palvelimen oma IP-osoite 192.168.20.10 ominaisuuden käyttöönottamiseksi.

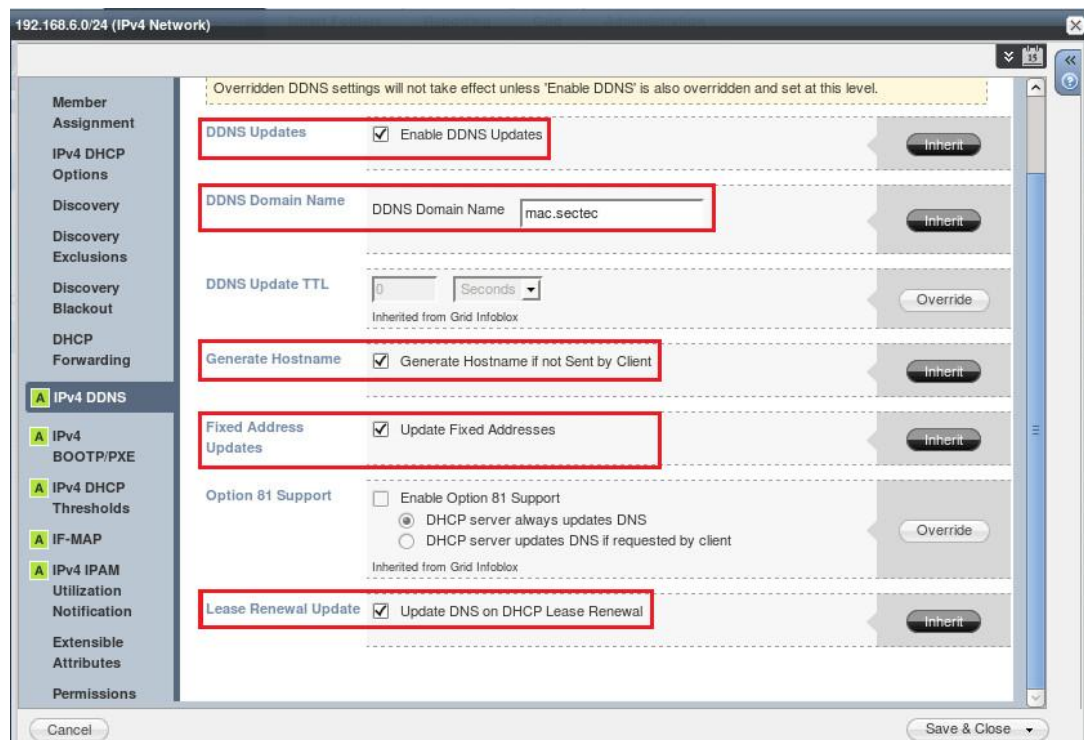
Mac.sectec-vyöhykettä varten täytyi määrittää Data Management → DHCP-välilehden työkalupalkista ”Configure DDNS”-optio. Koska mac.sectec-vyöhykkeen ensisijainen nimipalvelin ei ole Infoblox-laitteessa, täytyi ulkoinen DDNS-vyöhyke määrittää osoittamaan kohti dc.mac.sectec-palvelinta. DDNS-päivityksiä varten yritettiin suojata TSIG-avaimella, mutta avaimien käyttöönotossa oli ongelmia Windows palvelimen kanssa. Kuviossa 32 on DDNS-asetukset.



Kuvio 32. Ulkoinen DDNS-vyöhyke

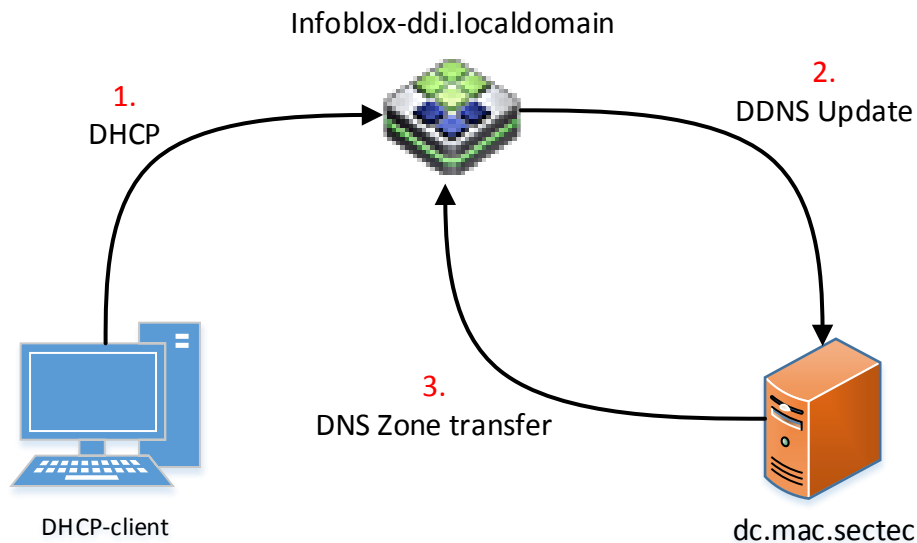
DDNS-ominaisuus täytyi vielä määrittää asetukset Gridin verkkotasolla erikseen jokaiselle IPv4-verkolle. Kuviossa 33 on esiteltyä Hallinto-verkon DDNS-asetukset, jossa on yliajettu Gridiltä perityt asetukset missä:

- **DDNS Update** –kenttä ottaa käyttöön DDNS-ominaisuuden
- **DDNS Domain Name** määrittää Update-viesteissä käytetyn vyöhykkeen
- **Generate Hostname** ottaa käyttöön automaattisen verkkoaseman nimen muodostamisen, jos sitä ei ole kyselyssä määritetty.
- **Fixed Address Updates** –kenttä säilyttää DHCP:llä jaetut osoitteet, jotka ovat määritetty pysyviksi riippumatta siitä onko asiakaslaitteen osoitteen vuokra-aika päättynyt.
- **Lease Renewal Update** –kenttä päivittää DNS-palvelimen aina uudella Update-viestillä vuokran uusimisen ohessa.



Kuvio 33. Hallinto-verkon DDNS-asetukset

Konfiguroinnin jälkeen Infobloxin ja Domain Controllerin välinen DNS-, DHCP ja DDNS-liikenne toimii kuvion 34 mukaisesti.



Kuvio 34. DHCP, DDNS ja DNS toiminta ympäristössä

1. Ensimmäisessä vaiheessa DHCP-asiakkaana toimiva laite aloittaa tavallisen DHCP-prosessin Infobloxin DHCP-palvelimen kanssa DHCPDISCOVER-viestillä.
2. Onnistuneen DHCP-prosessin jälkeen Infoblox lähettää DDNS Update-viestin dc.mac.sectec-palvelimelle mac.sectec-vyöhykkeen päivittämiseksi, joka sisältää uuden DHCP-asiakkaan verkkoaseman nimen ja IP-osoitteen.
3. Mac.sectec-vyöhykkeen ensisijaisena nimipalvelimena Domain Controller lähettää päivitetyn vyöhykkeen takaisin toissijaiselle Infoblox-palvelimelle.

5.2.4 Muut Infobloxin asetukset ja ominaisuuksien todentaminen

NTP

Infobloxissa otettiin myös käyttöön ajan synkronoimista varten tarkoitettu NTP-palvelu. Infobloxin Grid Master synkronoitiin NTP-palvelimeen, joka oli asennettu CentOS-käyttöjärjestelmällä Palvelut-verkon IP-osoitteeseen 192.168.3.2. Koska palvelin oli jo käytössä alkuperäisessä ympäristössä, Infobloxin lisääminen palveluun oli yksinkertaista. NTP-palvelimen `"/etc/ntp.conf"`-

asetustiedostoon lisättiin Infobloxin käyttämät verkot riveillä, jotka sallivat NTP-protokollan käytön asetetuista IPv4-verkoista.

```
restrict 192.168.110.0 mask 255.255.255.0 nomodify notrap
restrict 192.168.20.0 mask 255.255.255.0 nomodify notrap
```

Infoblox-palvelimella NTP otettiin käyttöön Grid → Grid Manager → Members –välilehden työkalupalkista löytyvästä NTP → NTP Grid Config –optiosta, jossa asetettiin Grid synkronisoimaan aika ulkoisesta NTP-palvelimesta valitsemalla ”Synchronize the Grid with these External NTP Servers” –optio ja määrittämällä sen IP-osoite. Kaikista Gridin laitteista otettiin seuraavaksi NTP käyttöön Member-tasolla NTP → NTP Member Config –option avulla. Lisäksi Infobloxin Network Insight- ja Reporting-palvelimet asetettiin päivittämään NTP-aika ainoastaan Grid Masterilta ”Synchronize this Member only with the Grid Master” –valinnalla. NTP:n toiminta todennettiin aluksi kirjautumalla NTP-palvelimelle ja suorittamalla komento ”*ntpd -c monlist*”, joka ilmoittaa kaikki NTP-asiakaslaitteet kuvion 35 mukaisesti, kuten Infobloxin Grid Masterin.

```
[root@client2 ~]# ntpdc -c monlist
remote address          port local address      count m ver  rstr avgint  lstint
=====
80.74.192.2             123 192.168.3.2           6 4 4   1d0    57    21
192.168.3.1            65535 192.168.3.2           1 3 3   180    179   179
192.168.20.10          123 192.168.3.2           1 3 4   180    241   241
```

Kuvio 35. NTP-palvelimen asiakkaat

Infobloxin sisällä onnistunut NTP-toiminta voidaan huomata Grid Managerin Services–välilehdeltä, jossa NTP-palvelun tila on merkitty kuvion 36 mukaisesti.

Name	Service Status	IPv4 Address	Comment
infoblox-ddi.localdomain	NTP Service is working	192.168.20.10	
networkinsight.localdomain	NTP Service is working	192.168.20.20	
reporting.localdomain	NTP Service is working	192.168.20.30	

Kuvio 36. Infobloxin NTP-palvelun tila

Reporting-palvelin

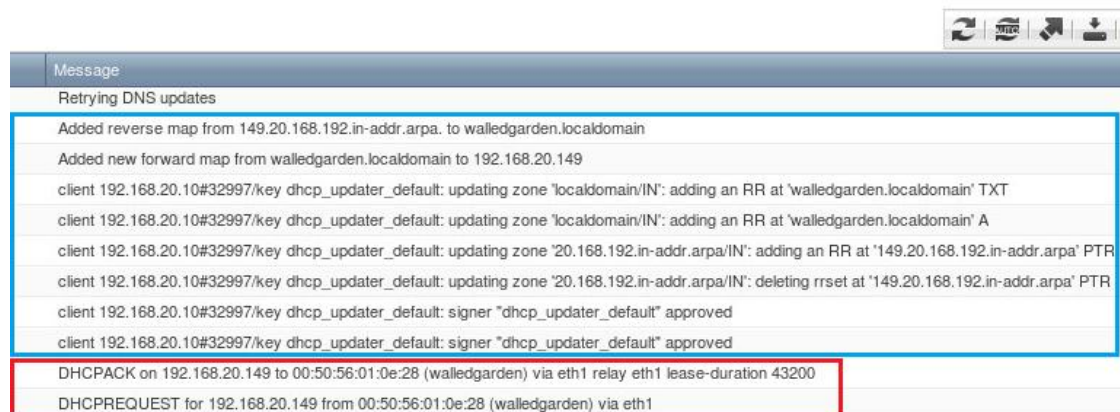
Infobloxin reporting.localdomain-palvelin on, joka ei kykene mihinkään muuhun, kuin datan keräämiseen, sen arkistointiin ja raporttien luomiseen muista Infoblox-laitteista. Tarkoituksena oli alun perin luoda omia raporttipohjia, jossa kerättyä dataa olisi purettu halutulla tavalla. Esimerkiksi sellainen raportti, jossa olisi voitu selvittää eniten DNS-kyselyissä TXT-tietueita lähettänyt laite. Infobloxissa raporttipohjat olivat kuitenkin esimääritettyjä, joiden muokkaaminen oli halutulla tavalla mahdotonta. Raporttien saadaan kuitenkin kattava kuva verkossa tapahtuvasta DHCP-, DNS-, RPZ- ja DDI-toiminnoista sekä varoituksista.

Reporting-palvelimen käyttöönotto tapahtui Reporting-välilehden työkalupalkista Grid Reporting Properties -optiolla. Avautuneesta valikosta General-sivulta otettiin käyttöön datan indeksointi liitteen 4 kuvion 48 mukaisesti, joka käskee muut Infoblox-palvelimet lähettämään dataa Reporting.localdomain-palvelimelle. Muut asetukset säilytettiin oletusarvoissa. DNS-välilehdeltä palvelulle otettiin käyttöön localdomain- ja mac.sectec-vyöhykkeiden nimikyselyiden ja tietueiden monitorointi lisäämällä vyöhykkeet liitteessä olevan kuvion 49 mukaisesti.

DHCP-, DNS ja DDNS-palveluiden testaus walledgarden-laitteen avulla

DHCP-, DNS, ja DDNS-palveluita testattiin walledgarden.localdomain-koneen avulla. Kone asetettiin hakemaan DHCP:llä IP-osoitetta Infoblox-palvelimelta käyttäen esimääritettyä verkkoaseman nimeä määrittämällä se palvelimen ”/etc/syconfig/network-scripts/ifcfg-eth0”-tiedostoon rivillä ”DHCP_HOST-NAME=walledgarden”. Infoblox-palvelin taas pitäisi lisätä DDNS:n avulla uusi DHCP-asiakas omaan localdomain zone-tiedostoonsa ja samalla automaattisesti luoda käänteistä nimikyselyä varten PTR-tietue.

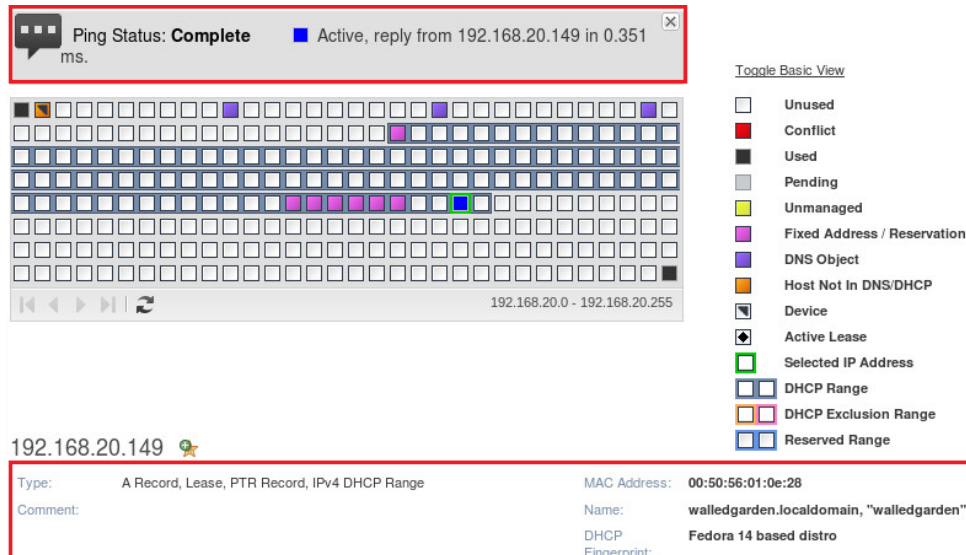
Kuviossa 37 on kuvankaappaus Infobloxin lokeista, jossa alemmassa kehyksessä DHCP-prosessissa pyydetään DHCPREQUEST-viestillä osoitetta 192.168.20.149 ja lisäksi ilmoitetaan verkkoaseman nimi walledgarden. Pyyntöön Infoblox vastaa DHCPACK-viestillä. Ylemmässä kehyksessä DHCP-palvelu suorittaa DDNS-viestejä Infobloxin sisällä, jossa lisätään alhaalta ylöspäin luettuna ensiksi PTR-tietueet käänteiselle vyöhykkeelle 20.168.192.in-addr.arpa ja myöhemmin taas A- ja TXT-tietueet localdomain-vyöhykkeelle. Lokin kaksi viimeistä viestiä ovat DNS-palvelulta, jossa ilmoitetaan tietueiden lisäyksestä.



Kuvio 37. Infoblox syslog

IPAM-käyttöliittymästä voidaan tarkemmin tutkia 192.168.20.149 IP-osoitteella olevaa laitetta. Laitteen aktiivisuus tarkistettiin IPAM:n Ping-ohjelmalla, kuten

kuviossa 38. Lisäksi Infoblox antaa lisää informaatiota IP-osoitteen takana olevasta laitteesta esimerkiksi sen MAC-osoitteen, verkkoaseman nimen, DHCP-sormenjäljen ja tyypissä kaikki IP-osoitteeseen liittyvät tiedot Infobloxissa.



Kuvio 38. IPAM näkymä IP-osoitteesta 192.168.20.49

5.3 RPZ-toteutus ja tulokset

Infobloxissa DNS-protokollaa hyödyntävien haittaohjelmien estäminen perustuu RPZ-vyöhykkeisiin, jossa tarkoituksena on estää niiden toiminta manipuloimalla DNS-kyselyssä annettuja vastauksia. Ohjelmassa on kolme tapaa toteuttaa RPZ-vyöhykkeitä, joko paikallisesti määritetyillä, RPZ-syöttestä saaduilla tai FireEyen varoituksista generoiduilla säännöillä. Paikallisilla ja RPZ-syötteiden säännöillä tutkittiin tarkemmin kuinka DNS-liikennettä manipuloitiin RPZ:n avulla. FireEyen avulla toteutetussa RPZ-vyöhykkeessä taas tutkittiin Infobloxin kykyä torjua JYVSECTECin DNS-protokollaa hyödyntävien haittaohjelmien toimintaa.

RPZ:n toiminnan edellytyksenä täytyy Infobloxin kyetä vastaamaan rekursiivisiin nimikyselyihin. Lisäksi RPZ:n dokumentoinnin ja seurannan mahdollistamiseksi täytyi RPZ:n lokitus ottaa käyttöön erikseen Grid-tasolla "Grid DNS Properties"-valikon Loggins-välilehdeltä.

5.3.1 Paikallinen RPZ ja RPZ-syöte

Infobloxiin konfigurointiin paikallinen RPZ-vyöhyke Data Management → DNS → Response Policy Zone –välilehdestä työkalupalkin Add → Zone → Response Policy Zone –toiminnolla. RPZ-vyöhykkeen luominen ei eroa rakenteeltaan suuremmin tavallisen vyöhykkeen lisäämisestä, sillä vyöhykkeelle määritetään nimen "local" lisäksi RPZ-toiminnosta vastaava nimipalvelin infoblox-ddi.localdomain.

Paikalliseen RPZ-vyöhykkeeseen lisättiin testausta varten RPZ-sääntö, joka muuttaa nimikyselyn vastausta NXDOMAIN-virheeksi, kun kyselyn kohteena käytettiin RGCE:n verkosta löytyvää "www.iltalehti.fi"-osoitetta. Sääntö asetettiin vyöhykkeen Add → Block (No Such Domain) Rule → Block Domain Name -valinnalla. Avautuneeseen valikkoon määritettiin ainoastaan osoite "www.iltalehti.fi", jonka jälkeen nimikysely osoitteeseen pitäisi epäonnistua NXDOMAIN-viestillä. RPZ-sääntöä testattiin hallintotest.mac.sectec -palvelimelta (192.168.6.12) dig-komennolla "dig www.iltalehti.fi", jonka kuvion 39 olevan tulosteesta huomataan, kuinka DNS-kyselyn vastauksena on annettu statuskentässä RPZ-säännön mukaisesti NXDOMAIN-virheviesti.

```
[root@hallintotest ~]# dig www.iltalehti.fi
; <<> DiG 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 <<> www.iltalehti.fi
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 53001
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.iltalehti.fi.          IN      A

;; Query time: 3 msec
;; SERVER: 192.168.20.10#53(192.168.20.10)
;; WHEN: Sun Mar  1 19:23:38 2015
;; MSG SIZE  rcvd: 34
```

Kuvio 39. Nimikysely osoitteesta "www.iltalehti.fi"

Kuviossa 40 on kuvankaappaus Infobloxin lokeista, jossa nähdään miten Infoblox merkitsee ja käsittelee RPZ-tapahtumia. RPZ-merkinnän jälkeen voidaan huomata Infobloxin lähettämä muokattu nimikysely, jossa vastauksena on NXDOMAIN.

```

Message
01-Mar-2015 19:26:13.253 client 192.168.6.12#34133: UDP: query: www.iltalehti.fi IN A response: NXDOMAIN +
CEF:0|Infoblox|NIOS|6.12.1-259847|RPZ-QNAME|NXDOMAIN|4|app=DNS dst=192.168.20.10 src=192.168.6.12 spt=34133
view=_default qtype=A msg="rpz QNAME NXDOMAIN rewrite www.iltalehti.fi [A] via www.iltalehti.fi.local"
client 192.168.6.12#34133 (www.iltalehti.fi): query: www.iltalehti.fi IN A + (192.168.20.10)

```

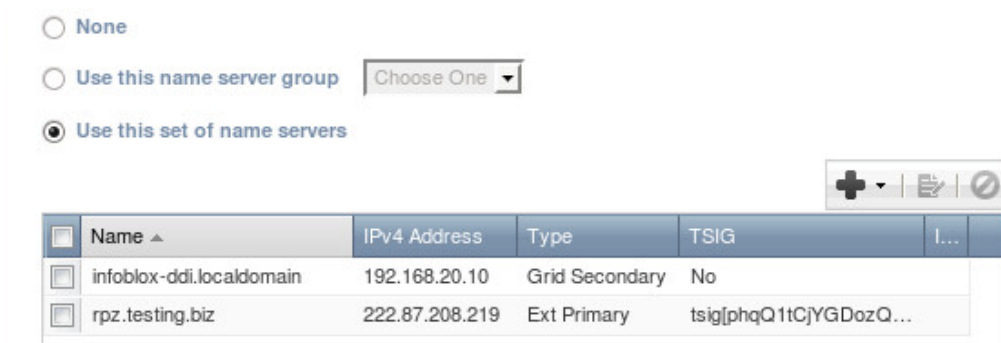
Kuvio 40. Infoblox RPZ-loki

Lokitietoja luetaan seuraavasti:

- **RPZ-QNAME | NXDOMAIN** määrittää säännössä käytetyn politiikan
- **dst=192.168.20.10** nimikyselyn vastaanottaneen IP-osoitteen
- **src=192.168.6.12** Nimikyselyn lähettäjän IP-osoitteen
- **qtype=A** määrittää tietueen tyyppin
- **msg** –viestin sisällöstä voidaan tulkita mitä nimikyselylle tehdään ja minkä RPZ-vyöhykkeen mukaisesti se käsiteltiin esimerkiksi ”via www.iltalehti.fi.local” tarkoittaa, että käytettiin local-vyöhykkeen sääntöjä.

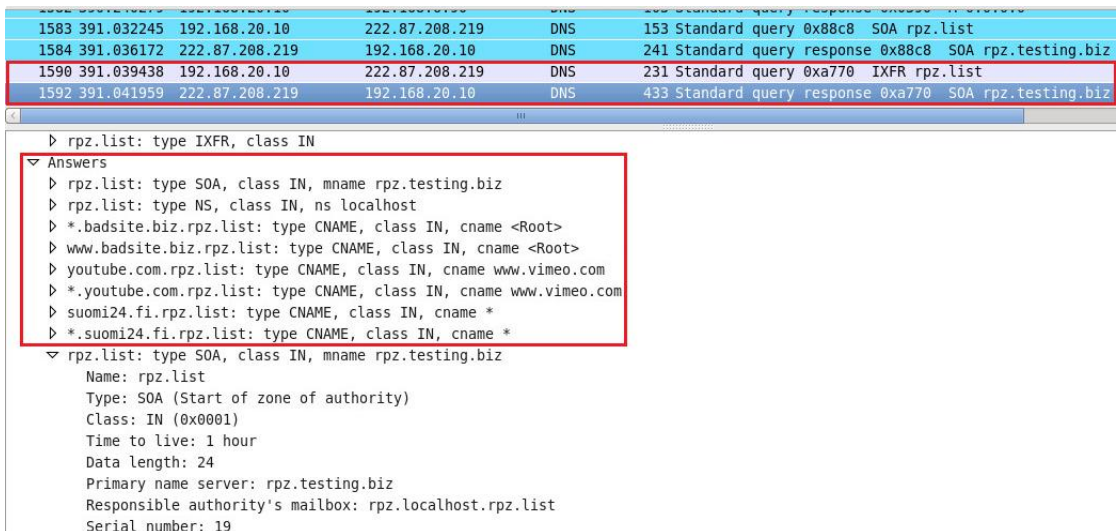
Koska ympäristö oli liitettynä JYVSECTEC:n RGCE-verkkoon, opinnäyte-työssä ei voitu tutkia tai käyttää Infobloxin ylläpitämää RPZ-syötettä. RPZ-syötteen toimintaa Infoblox-järjestelmän kanssa oli kuitenkin mahdollista tutkia asentamalla RGCE-verkkoon oma RPZ-vyöhykettä jakava palvelu. Käytännössä RPZ-syöte vastaa tavallista nimipalvelinta, joka jakaa sääntöjä sisältävän zone-tiedoston IXFR:n tai AXFR:n avulla. Liitteessä 5 on kuvattu syötepalvelimen asetukset.

Infobloxissa RPZ-syötteelle konfiguroitiin uusi RPZ-vyöhyke. Paikallisen vyöhykkeen sijaan valittiin kuitenkin ensimmäisessä vaiheessa ”Add Response Policy Zone Feed”-optio. Kuviossa 41 on kuvankaappaus kolmannesta vaiheesta, jossa määritettiin vyöhykkeen nimipalvelimet. Toissijaiseksi nimipalvelimeksi täytyi valita vyöhykkeen vastaanottava palvelin eli tässä tapauksessa Gridin infoblox-ddi.localdomain, kun taas ensisijaiseksi määritettiin rpz.testing.biz –nimipalvelin. Koska vyöhykkeen päivitys tulee ulkoverkosta, suojattiin siirto TSIG-avaimella.



Kuvio 41. RPZ-syötteen nimipalvelimet

Vyöhykkeen siirto todennettiin kaappaamalla Wireshark-ohjelmalla liikennettä Infobloxin portista. Kuviossa 42 huomataan ylemmässä merkinnässä miten Infoblox pyytää oletuksena rpz.list-vyöhykettä IXFR:n avulla, mutta rpz.testing.biz taas vastaa ilmoittamalla kaikki zone-tiedoston tietueet alemmassa vastauskentässä.



Kuvio 42. RPZ-syötteen vyöhykkeen siirto

Rpz.list syötteen toiminta varmistettiin tekemällä nimikysely dig-ohjelmalla ”www.youtube.com”-osoitteeseen, jonka vastaus vaihdettiin osoittamaan CNAME-tietueen avulla ”www.vimeo.com”-osoitteeseen mistä suoritetaan tavallinen nimikysely kuvion 43 mukaisesti.

```
[root@hallintotest ~]# dig www.youtube.com
; <<> DiG 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 <<> www.youtube.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 44799
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.youtube.com.                IN      A

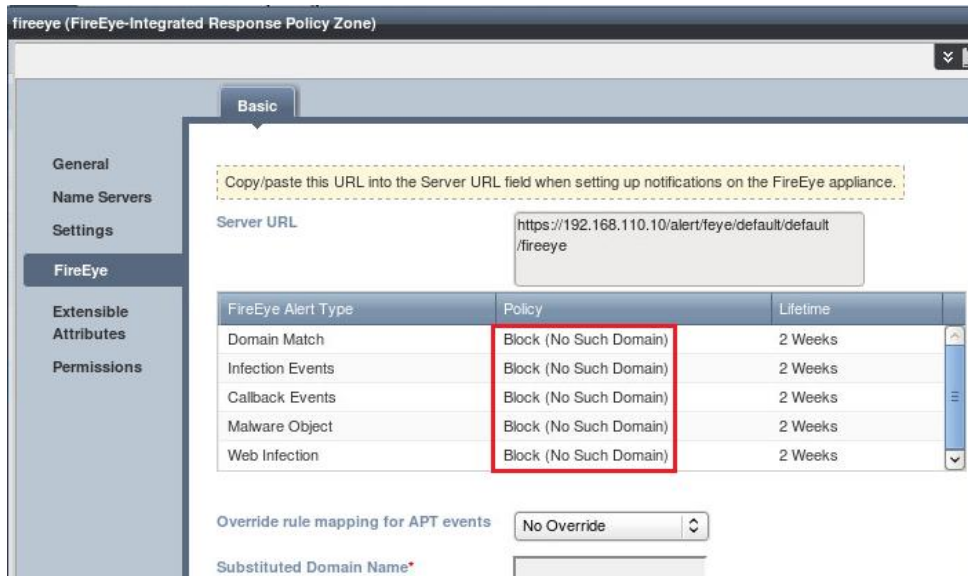
;; ANSWER SECTION:
www.youtube.com.                3600    IN      CNAME   www.vimeo.com.
www.vimeo.com.                  75002   IN      A       144.243.214.39

;; Query time: 8 msec
;; SERVER: 192.168.20.10#53(192.168.20.10)
;; WHEN: Sun Mar 1 22:31:46 2015
;; MSG SIZE rcvd: 73
```

Kuvio 43. Nimikysely osoitteesta ”www.youtube.com”

5.3.2 RPZ FireEye

FireEye RPZ toteutusta varten täytyi ensimmäiseksi lisätä uusi RPZ-vyöhyke, jotta Infoblox määrittäisi automaattisesti vyöhykkeen ulkopuoliseen hallintaan tarkoitetun FireEye-ryhmän. RPZ-vyöhyke konfiguroitiin muiden vyöhykkeiden tavoin samalla avustusohjelmalla, jossa asetettiin ensimmäisessä vaiheessa ”Add FireEye-integrated Response Policy Zone” valinta ja toisessa vyöhykkeen nimeksi määritettiin ”fireeye”. Kuvion 44 kolmannessa vaiheessa fireeye-vyöhykkeelle määritettiin FireEyen aiheuttamille hälytyksille suoritettavat toiminnot. Oletuksena kaikissa hälytystyypeissä oli käytössä Passthru-sääntö, joka ainoastaan lokittaisi tapahtumat. Block-säännöllä asetettiin Infoblox estämään DNS-liikennettä hälytyksen tyypistä riippumatta. URL-kenttään Infoblox generoi automaattisesti FireEye-laitteessa käytettävän RPZ-vyöhykkeen osoitteen.



Kuvio 44. FireEye hälytysten toiminnot

Vyöhykkeen konfiguroinnin jälkeen Infobloxiin lisättiin FireEye-laitteelle ylläpitäjän tunnukset FireEye-ryhmään, jota laite käyttää vyöhykkeen automaattiseen päivittämiseen. Itse FireEye-laite asetettiin toimenantajan toimesta kuuntelemaan ympäristöstä ulospäin suuntautuvaa liikennettä.

Infobloxin ja FireEyen yhteistyötä haittaohjelmien torjumista vastaan tutkittiin liittämällä työympäristön Hallinto-verkkoon 192.168.6.0/24 toimeksiantajan haittaohjelmilla saastuttamia virtuaalikoneita. Virtuaalikoneiden haittaohjelmat käyttivät muun muassa hyväkseen DNS-protokollaa esimerkiksi yhteyden muodostamiseen niiden C&C-palvelimelle.

Kuviossa 45 on kuvankaappaus Infobloxin SysLog:sta, jossa tapahtuu FireEyen aiheuttama hälytys.

Server	Message	
named[30186]	12-Nov-2014 10:12:23.779 client 192.168.6.90#53352: UDP: query: 34105.beacon.skycrawler.com IN A response: NOERROR + 34105.beacon.skycrawler.com. 1 IN A 0.0.0.0;	
named[30186]	client 192.168.6.90#53352 (34105.beacon.skycrawler.com): query: 34105.beacon.skycrawler.com IN A + (192.168.20.10)	3
named[30186]	12-Nov-2014 10:12:13.774 client 192.168.6.90#55561: UDP: query: 34105.beacon.skycrawler.com IN A response: NOERROR + 34105.beacon.skycrawler.com. 1 IN A 0.0.0.0;	
named[30186]	client 192.168.6.90#55561 (34105.beacon.skycrawler.com): query: 34105.beacon.skycrawler.com IN A + (192.168.20.10)	
named[30186]	zone fireeye/IN: ZRQ applied transaction 117 with SOA serial 21. Zone version is now 20.	2
named[30186]	zone fireeye/IN: ZRQ applied ADD for " : 28800 IN SOA infoblox-ddi.localdomain. please_set_email.absolutely.nowhere. 21 180 3600 2419200 900 (ro).	
named[30186]	zone fireeye/IN: ZRQ applied ADD for 'www.skycrawler.com': 28800 IN CNAME . (none).	
named[30186]	zone fireeye/IN: ZRQ applying transaction 117.	
httpd[]	fireeye-rpt: 868,malware-callback,crit,FireEye-NX,www.skycrawler.com.fireeye,Block (No Such Domain)	1
httpd[]	FireEye: Create an RPZ rule for 'www.skycrawler.com' with 'Block (No Such Domain)' rule in RPZ zone 'fireeye'	

Kuvio 45. Infobloxin SysLog FireEyesta

Lokin sisältö voidaan jakaa kolmeen osaan seuraavasti:

Ensimmäisessä kohdassa FireEye-laite tekee hälytyksen haittaohjelman Call-back-tyyppisestä tapahtumasta, jossa kohteen osoitteena on "www.skycrawler.com". FireEye lähettää pyynnön fireeye-vyöhykkeeseen säännöstä, jossa lisätään "Block (No Such Domain)"-toiminnolla estetään nimikyselyt hälytyksen osoitteeseen.

Toisessa vaiheessa nimipalvelin (named) päivittää fireeye-vyöhykkeen lisäämällä uuden RPZ-säännön ja päivittämällä lopuksi vyöhykkeen serial-arvoa 21:een.

Kolmannessa merkityssä alueessa kuitenkin huomataan puute Infobloxin ja FireEyen toiminnassa. Riippumatta onnistuneesta "www.skycrawler.com"-säännön lisäyksestä huolimatta huomataan, että Infoblox ei välitä muista "skycrawler.com"-vyöhykkeen osoitteista. Tämä johtaa siihen, että haittaohjelman toimintaa ei saatu häirittyä tai estettyä tarpeeksi tehokkaasti, vaan sen toiminta jatkui Infobloxista ja FireEyesta huolimatta. Sääntö "www.skycrawler.com"-osoitteeseen toimi kuitenkin odotetulla tavalla muokkaamalla nimikyselyn vastaus asiakaspalvelimelle NXDOMAIN-virheeksi liitteen 6 mukaisesti. Infobloxissa ei ollut mahdollisuutta muokata automaattista säännön asettamista koskemaan kaikkia vyöhykkeen osoitteita, vaan ainoa vaihtoehto olisi ollut määrittää sääntö osoitteella "*.skycrawler.com" manuaalisti RPZ-vyöhykkeelle.

6 Pohdinta

Opinnäytetyön tavoitteena oli toteuttaa Infobloxin tarjoamat DDI-ominaisuudet osana jo olemassa olevaan ympäristöön. Infobloxin avulla oli tarkoitus laajentaa koko ympäristön tietoturvaominaisuuksia lisäämällä siihen uuden suoja-kerroksen muun muassa DNS-protokollaa hyödyntäviä haittaohjelmia vastaan. Pohjana käytetty Ciscon Trustsec-ympäristö helpotti Infoblox järjestelmän käyttöönottoa, mutta toi myös uusia haasteita, kun DDI-palveluita täytyi siirtää Infobloxin palvelimelle kuitenkin säilyttäen alkuperäisen toiminnollisuuden.

DNS- ja DHCP-palveluiden toteuttaminen Infoblox-palvelimella onnistui suhteellisen pienellä vaivalla. Alussa palveluiden konfigurointiin liittyvät ongelmat johtuivat suurimmalta osalta graafisen käyttöliittymän tavasta ilmaista konfiguraatioita usealla eri tasolla tai useiden eri välilehtien takana. Asetusten periytyvyyden ymmärrettyä konfigurointi muuttui huomattavasti helpommaksi.

DHCP-palvelun ja IP-verkkojen asetusten jälkeen verkosta sai Infobloxin IPAM-järjestelmästä yleisen kuvan laitteiden IP-osoitteista ja muista koneisiin liittyvistä tiedoista. Verkkojen tutkimiseen ja laitteiden tietojen keräämiseen tarkoitettu Network Discovery –palvelu ei toiminut täysin halutulla tavalla sillä esimerkiksi SNMP:n hyödyntäminen olisi vaatinut muutoksia Cisco kytkinten asetukseen, jotka olisivat voineet hajottaa ISE:n vaatiman toiminnollisuuden.

Opinnäytetyössä keskeisimpänä aiheena oli DNS-protokollaa hyödyntävien haittaohjelmien torjuminen Infobloxin avulla. Toteutuksen aikana kuitenkin huomattiin, kuinka Infoblox-ohjelma ei oletuksena kykene havaitsemaan DNS-väärinkäytöksiä, vaan luottaa ainoastaan ulkoiselta RPZ-syötepalveluilta saatuihin vyöhykkeisiin. FireEyen liittäminen ympäristöön parantaa Infobloxin valmiutta estää haittaohjelmia, mutta ainoastaan osittain kuten testauksessa huomattiin. Estämisen epäonnistumisesta huolimatta Infoblox ilmoittaa kaikista RPZ-tapahtumista tehokkaasti lokeihin ja RPZ-raportteihin, joka mahdollistaa

saastuneiden laitteiden paikantamisen helpolla tavalla. Infobloxin kyky haittaohjelmien torjumiseen perustuu siis täysin RPZ-syötteen ja FireEyen toteutukseen ja tehokkuuteen.

Kokonaisuutena Infoblox on monipuolinen vaihtoehto keskitetyksi DDI-palveluita tarjoavaksi järjestelmäksi, jonka avulla voidaan ainakin parantaa DNS-järjestelmän turvallisuutta RPZ-ominaisuudella.

Lähteet

Aitchison, R. 2011. Pro DNS and BIND 10. Yhdysvallat: Apress.

BOOTP Vendor Extensions and DHCP Options. 2015. DHCP Options-kentän arvot IANAn sivustolla. Viitattu 9.3.2015. <http://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml>.

F-Root. N.d. Tietoa F-Root -palvelimesta Internet Systems Consortium:n sivustolla. Viitattu 10.2.2015. <https://www.isc.org>, Network F-Root.

Goralski, W. 2009. The Illustrated Network: How TCP/IP Works in a Modern Network. Yhdysvallat: Morgan Kaufmann Publishers.

Honkanen. J. 2014. Cisco TrustSec käyttöönotto JYVSECTEC-ympäristössä. Opinnäytetyö. Jyväskylän ammattikorkeakoulu, tietotekniikan koulutusohjelma, Viitattu 9.3.2015. <http://urn.fi/URN:NBN:fi:amk-2014090413742>.

IETF RFC 1034. 1987. Internet Engineering Task Forcen määrittämä standardi. Viitattu 10.2.2015. <https://www.ietf.org/rfc/rfc1034.txt>.

IETF RFC 1995. 1996. Internet Engineering Task Forcen määrittämä standardi. Viitattu 10.2.2015. <https://www.ietf.org/rfc/rfc1095.txt>.

IETF RFC 1996. 1996. Internet Engineering Task Forcen määrittämä standardi. Viitattu 10.2.2015. <https://www.ietf.org/rfc/rfc1996.txt>.

IETF RFC 2131. 1997. Internet Engineering Task Forcen määrittämä standardi. Viitattu 10.2.2015. <https://www.ietf.org/rfc/rfc2131.txt>.

IETF RFC 2132. 1997. Internet Engineering Task Forcen määrittämä standardi. Viitattu 10.2.2015. <https://www.ietf.org/rfc/rfc2132.txt>.

Infoblox DNS Firewall – FireEye Adapter. 2013. Infobloxin esittely FireEye integraatiosta. Viitattu 10.2.2015. https://www.infoblox.com/sites/infobloxcom/files/resources/infoblox-datasheet-dns-firewall-fireeye-adapter_0_0.pdf.

Infoblox NIOS Administrator Guide. 2014. Infoblox-ohjelmiston ohjekirja. Viitattu 10.2.2015. http://dloads.infoblox.com/direct/appliance//NIOS/NIOS_AdminGuide_6.10.pdf.

JYVSECTEC. 2014. JYVSECTEC:n esittely sivusto. Viitattu 20.12.2014. <http://jyvsectec.fi/>, JYVSECTEC.

JYVSECTEC-RGCE. 2014. RGCE:n kuvaus Jyvsectec:n sivustolla. Viitattu 20.12.2014. <http://jyvsectec.fi/>, RGCE.

Soyinka, W. 2012. Linux Administration: A Beginner's Guide, Sixth Edition. Yhdysvallat: McGraw-Hill/Osborne.

Schryver, V. & Vixie, P. 2011. DNS Response Policy Zones (DNS RPZ, Format 3). Viitattu 10.2.2015. <https://deephought.isc.org/getAttach/22/AA-00512/rpz.pdf>.

Trinzic DDI overview. N.d. 2014. Infoblox:n DDI esittely. Viitattu 10.2.2015. https://www.infoblox.com/sites/infobloxcom/files/resources/infoblox-datasheet-trinzic-ddi-overview_0.pdf.

Tutustu JAMKiin. 2014. JAMK:n sivusto. Viitattu 1.10.2015. <http://www.jamk.fi/fi/Tietoa-JAMKista/Tutustu-JAMKiin/>.

Liitteet

Liite 1: IANAn DHCP-optiot

0	Pad	0	None	[RFC2132]
1	Subnet Mask	4	Subnet Mask Value	[RFC2132]
2	Time Offset	4	Time Offset in Seconds from UTC (note: deprecated by 100 and 101)	[RFC2132]
3	Router	N	N/4 Router addresses	[RFC2132]
4	Time Server	N	N/4 Timeserver addresses	[RFC2132]
5	Name Server	N	N/4 IEN-116 Server addresses	[RFC2132]
6	Domain Server	N	N/4 DNS Server addresses	[RFC2132]
7	Log Server	N	N/4 Logging Server addresses	[RFC2132]
8	Quotes Server	N	N/4 Quotes Server addresses	[RFC2132]
9	LPR Server	N	N/4 Printer Server addresses	[RFC2132]
10	Impress Server	N	N/4 Impress Server addresses	[RFC2132]
11	RLP Server	N	N/4 RLP Server addresses	[RFC2132]
12	Hostname	N	Hostname string	[RFC2132]
13	Boot File Size	2	Size of boot file in 512 byte chunks	[RFC2132]
14	Merit Dump File	N	Client to dump and name the file to dump it to	[RFC2132]
15	Domain Name	N	The DNS domain name of the client	[RFC2132]
16	Swap Server	N	Swap Server address	[RFC2132]
17	Root Path	N	Path name for root disk	[RFC2132]
18	Extension File	N	Path name for more BOOTP info	[RFC2132]
19	Forward On/Off	1	Enable/Disable IP Forwarding	[RFC2132]
20	SrcRte On/Off	1	Enable/Disable Source Routing	[RFC2132]
21	Policy Filter	N	Routing Policy Filters	[RFC2132]
22	Max DG Assembly	2	Max Datagram Reassembly Size	[RFC2132]
23	Default IP TTL	1	Default IP Time to Live	[RFC2132]
24	MTU Timeout	4	Path MTU Aging Timeout	[RFC2132]
25	MTU Plateau	N	Path MTU Plateau Table	[RFC2132]
26	MTU Interface	2	Interface MTU Size	[RFC2132]
27	MTU Subnet	1	All Subnets are Local	[RFC2132]
28	Broadcast Address	4	Broadcast Address	[RFC2132]
29	Mask Discovery	1	Perform Mask Discovery	[RFC2132]
30	Mask Supplier	1	Provide Mask to Others	[RFC2132]
31	Router Discovery	1	Perform Router Discovery	[RFC2132]
32	Router Request	4	Router Solicitation Address	[RFC2132]
33	Static Route	N	Static Routing Table	[RFC2132]
34	Trailers	1	Trailer Encapsulation	[RFC2132]
35	ARP Timeout	4	ARP Cache Timeout	[RFC2132]
36	Ethernet	1	Ethernet Encapsulation	[RFC2132]
37	Default TCP TTL	1	Default TCP Time to Live	[RFC2132]
38	Keepalive Time	4	TCP Keepalive Interval	[RFC2132]

39	Keepalive Data	1	TCP Keepalive Garbage	[RFC2132]
40	NIS Domain	N	NIS Domain Name	[RFC2132]
41	NIS Servers	N	NIS Server Addresses	[RFC2132]
42	NTP Servers	N	NTP Server Addresses	[RFC2132]
43	Vendor Specific	N	Vendor Specific Information	[RFC2132]
44	NETBIOS Name Srv	N	NETBIOS Name Servers	[RFC2132]
45	NETBIOS Dist Srv	N	NETBIOS Datagram Distribution	[RFC2132]
46	NETBIOS Node Type	1	NETBIOS Node Type	[RFC2132]
47	NETBIOS Scope	N	NETBIOS Scope	[RFC2132]
48	X Window Font	N	X Window Font Server	[RFC2132]
49	X Window Manager	N	X Window Display Manager	[RFC2132]
50	Address Request	4	Requested IP Address	[RFC2132]
51	Address Time	4	IP Address Lease Time	[RFC2132]
52	Overload	1	Overload "sname" or "file"	[RFC2132]
53	DHCP Msg Type	1	DHCP Message Type	[RFC2132]
54	DHCP Server Id	4	DHCP Server Identification	[RFC2132]
55	Parameter List	N	Parameter Request List	[RFC2132]
56	DHCP Message	N	DHCP Error Message	[RFC2132]
57	DHCP Max Msg Size	2	DHCP Maximum Message Size	[RFC2132]
58	Renewal Time	4	DHCP Renewal (T1) Time	[RFC2132]
59	Rebinding Time	4	DHCP Rebinding (T2) Time	[RFC2132]
60	Class Id	N	Class Identifier	[RFC2132]
61	Client Id	N	Client Identifier	[RFC2132]
62	NetWare/IP Domain	N	NetWare/IP Domain Name	[RFC2242]
63	NetWare/IP Option	N	NetWare/IP sub Options	[RFC2242]
64	NIS-Domain-Name	N	NIS+ v3 Client Domain Name	[RFC2132]
65	NIS-Server-Addr	N	NIS+ v3 Server Addresses	[RFC2132]
66	Server-Name	N	TFTP Server Name	[RFC2132]
67	Bootfile-Name	N	Boot File Name	[RFC2132]
68	Home-Agent-Addr	N	Home Agent Addresses	[RFC2132]
69	SMTP-Server	N	Simple Mail Server Addresses	[RFC2132]
70	POP3-Server	N	Post Office Server Addresses	[RFC2132]
71	NNTP-Server	N	Network News Server Addresses	[RFC2132]
72	WWW-Server	N	WWW Server Addresses	[RFC2132]
73	Finger-Server	N	Finger Server Addresses	[RFC2132]
74	IRC-Server	N	Chat Server Addresses	[RFC2132]
75	StreetTalk-Server	N	StreetTalk Server Addresses	[RFC2132]
76	STDA-Server	N	ST Directory Assist. Addresses	[RFC2132]
77	User-Class	N	User Class Information	[RFC3004]
78	Directory Agent	N	directory agent information	[RFC2610]
79	Service Scope	N	service location agent scope	[RFC2610]
80	Rapid Commit	0	Rapid Commit	[RFC4039]
81	Client FQDN	N	Fully Qualified Domain Name	[RFC4702]
82	Relay Agent Information	N	Relay Agent Information	[RFC3046]
83	iSNS	N	Internet Storage Name Service	[RFC4174]
84	REMOVED/Unassigned			[RFC3679]
85	NDS Servers	N	Novell Directory Services	[RFC2241]
86	NDS Tree Name	N	Novell Directory Services	[RFC2241]

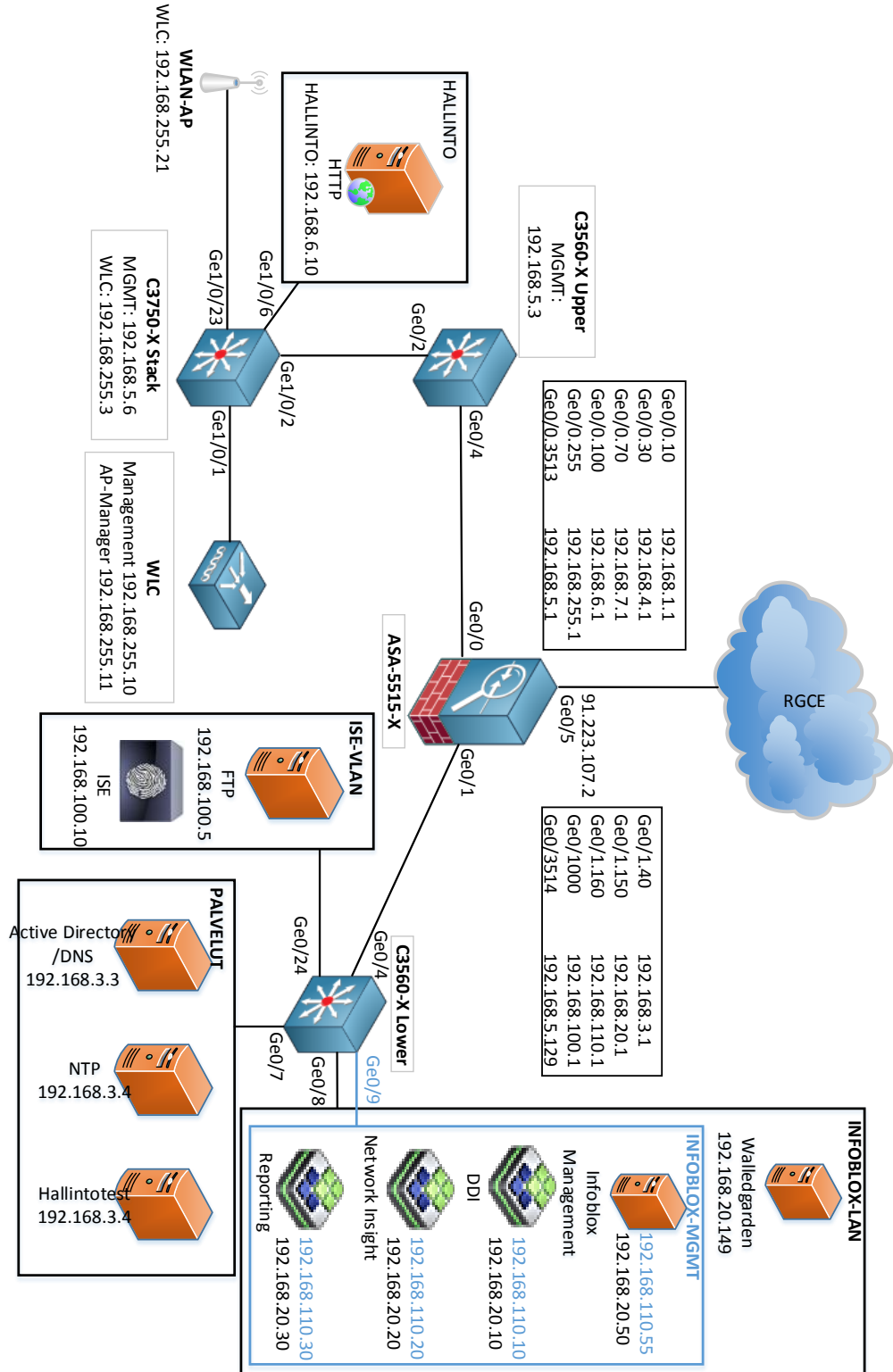
87	NDS Context	N	Novell Directory Services	[RFC2241]
88	BCMCS Controller Domain Name list			[RFC4280]
89	BCMCS Controller IPv4 address option			[RFC4280]
90	Authentication	N	Authentication	[RFC3118]
91	client-last-transaction-time option			[RFC4388]
92	associated-ip option			[RFC4388]
93	Client System	N	Client System Architecture	[RFC4578]
94	Client NDI	N	Client Network Device Interface	[RFC4578]
95	LDAP	N	Lightweight Directory Access Protocol	[RFC3679]
96	REMOVED/Unassigned			[RFC3679]
97	UUID/GUID	N	UUID/GUID-based Client Identifier	[RFC4578]
98	User-Auth	N	Open Group's User Authentication	[RFC2485]
99	GEOCONF_CIVIC			[RFC4776]
100	PCode	N	IEEE 1003.1 TZ String	[RFC4833]
101	TCode	N	Reference to the TZ Database	[RFC4833]
102-107	REMOVED/Unassigned			[RFC3679]
108	REMOVED/Unassigned			[RFC3679]
109	Unassigned			[RFC3679]
110	REMOVED/Unassigned			[RFC3679]
111	Unassigned			[RFC3679]
112	Netinfo Address	N	NetInfo Parent Server Address	[RFC3679]
113	Netinfo Tag	N	NetInfo Parent Server Tag	[RFC3679]
114	URL	N	URL	[RFC3679]
115	REMOVED/Unassigned			[RFC3679]
116	Auto-Config	N	DHCP Auto-Configuration	[RFC2563]
117	Name Service Search	N	Name Service Search	[RFC2937]
118	Subnet Selection Option	4	Subnet Selection Option	[RFC3011]
119	Domain Search	N	DNS domain search list	[RFC3397]
120	SIP Servers DHCP Option	N	SIP Servers DHCP Option	[RFC3361]
121	Classless Static Route Option	N	Classless Static Route Option	[RFC3442]
122	CCC	N	CableLabs Client Configuration	[RFC3495]
123	GeoConf Option	16	GeoConf Option	[RFC6225]
124	V-I Vendor Class		Vendor-Identifying Vendor Class	[RFC3925]
125	V-I Vendor-Specific Information		Vendor-Identifying Vendor-Specific Information	[RFC3925]
126	Removed/Unassigned			[RFC3679]
127	Removed/Unassigned			[RFC3679]
128	PXE - undefined (vendor specific)			[RFC4578]
128	Etherboot signature. 6 bytes: E4:45:74:68:00:00			
128	DOCSIS "full security" server IP address			

128	TFTP Server IP address (for IP Phone software load)		
129	PXE - undefined (vendor specific)		[RFC4578]
129	Kernel options. Variable length string		
129	Call Server IP address		
130	PXE - undefined (vendor specific)		[RFC4578]
130	Ethernet interface. Variable length string.		
130	Discrimination string (to identify vendor)		
131	PXE - undefined (vendor specific)		[RFC4578]
131	Remote statistics server IP address		
132	PXE - undefined (vendor specific)		[RFC4578]
132	IEEE 802.1Q VLAN ID		
133	PXE - undefined (vendor specific)		[RFC4578]
133	IEEE 802.1D/p Layer 2 Priority		
134	PXE - undefined (vendor specific)		[RFC4578]
134	Diffserv Code Point (DSCP) for VoIP signalling and media streams		
135	PXE - undefined (vendor specific)		[RFC4578]
135	HTTP Proxy for phone-specific applications		
136	OPTION_PANA_AGENT		[RFC5192]
137	OPTION_V4_LOST		[RFC5223]
138	OPTION_CAPWAP_AC_V4	N	CAPWAP Access Controller addresses [RFC5417]
139	OPTION-IPv4_Address-MoS	N	a series of suboptions [RFC5678]
140	OPTION-IPv4_FQDN-MoS	N	a series of suboptions [RFC5678]
141	SIP UA Configuration Service Domains	N	List of domain names to search for SIP User Agent Configuration [RFC6011]
142	OPTION-IPv4_Address-ANDSF	N	ANDSF IPv4 Address Option for DHCPv4 [RFC6153]
143	Unassigned		
144	GeoLoc	16	Geospatial Location with Uncertainty [RFC6225]
145	FORCERENUE_NONCE_CAPABLE	1	Forcerenue Nonce Capable [RFC6704]
146	RDNSS Selection	N	Information for selecting RDNSS [RFC6731]
147-149	Unassigned		[RFC3942]
150	TFTP server address		[RFC5859]
150	Etherboot		
150	GRUB configuration path name		

151	status-code	N+1	Status code and optional N byte text message describing status.	[RFC6926]
152	base-time	4	Absolute time (seconds since Jan 1, 1970) message was sent.	[RFC6926]
153	start-time-of-state	4	Number of seconds in the past when client entered current state.	[RFC6926]
154	query-start-time	4	Absolute time (seconds since Jan 1, 1970) for beginning of query.	[RFC6926]
155	query-end-time	4	Absolute time (seconds since Jan 1, 1970) for end of query.	[RFC6926]
156	dhcp-state	1	State of IP address.	[RFC6926]
157	data-source	1	Indicates information came from local or remote server.	[RFC6926]
158	OPTION_V4_PCP_SERVER	Variable; the minimum length is 5.	Includes one or multiple lists of PCP server IP addresses; each list is treated as a separate PCP server.	[RFC7291]
159-174	Unassigned			[RFC3942]
175	Etherboot (Tentatively Assigned - 2005-06-23)			
176	IP Telephone (Tentatively Assigned - 2005-06-23)			
177	Etherboot (Tentatively Assigned - 2005-06-23)			
177	PacketCable and CableHome (replaced by 122)			
178-207	Unassigned			[RFC3942]
208	PXELINUX Magic	4	magic string = F1:00:74:7E	[RFC5071] [Deprecated]
209	Configuration File	N	Configuration file	[RFC5071]
210	Path Prefix	N	Path Prefix Option	[RFC5071]
211	Reboot Time	4	Reboot Time	[RFC5071]
212	OPTION_6RD	18 + N	OPTION_6RD with N/4 6rd BR addresses	[RFC5969]
213	OPTION_V4_ACCESS_DOMAIN	N	Access Network Domain Name	[RFC5986]
214-219	Unassigned			
220	Subnet Allocation Option	N	Subnet Allocation Option	[RFC6656]
221	Virtual Subnet Selection (VSS) Option			[RFC6607]
222-223	Unassigned			[RFC3942]
224-254	Reserved (Private Use)			
255	End	0	None	[RFC2132]

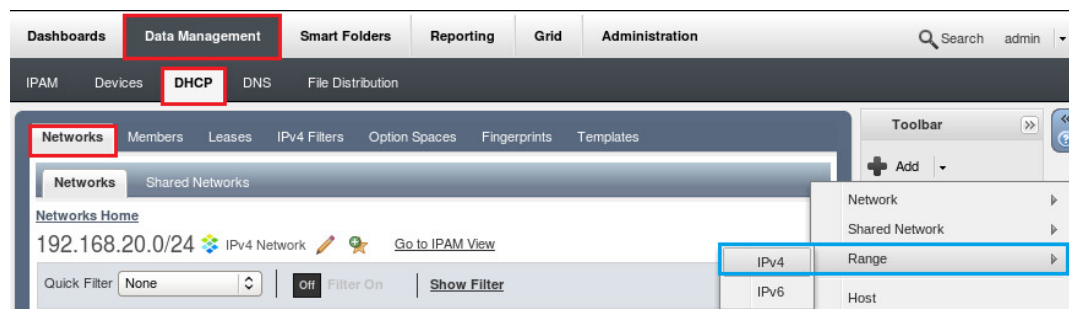
(BOOTP Vendor Extensions and DHCP Options 2015.)

Liite 2: Toteutusympäristö



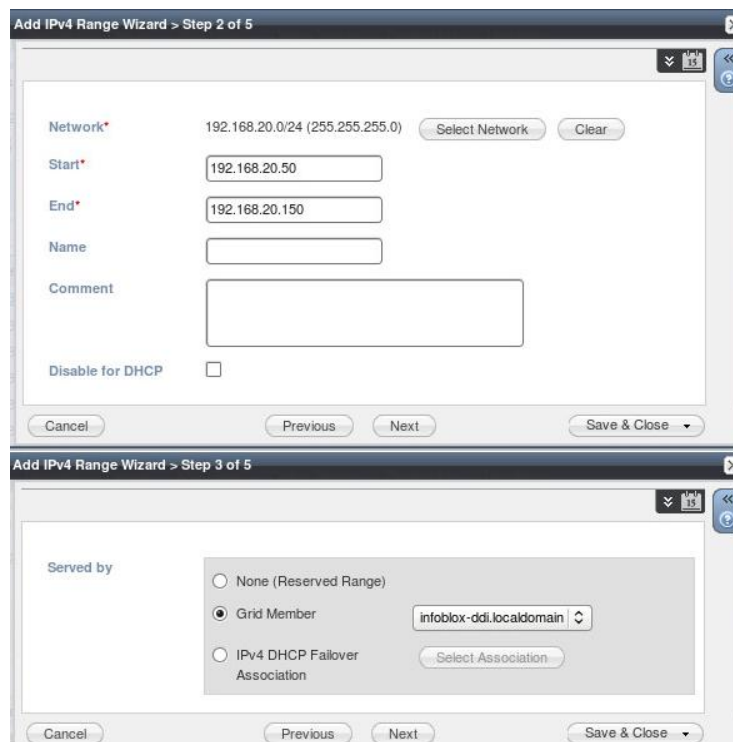
Liite 3: DHCP:n jaettavan IP-osoitealueen konfigurointi

LAN1-verkoon 192.168.20.0/24 määritettiin IP-osoitealue, josta jaetaan IP-osoitteita DHCP-asiakaslaitteille väliltä 192.168.20.50 – 192.168.20.150. Konfigurointi aloitettiin siirtymällä Data Management → DHCP → Networks –välilehteen, josta valittiin kuvion 46 mukaisesti työkalupalkista Add → Range → IPv4 –optio.



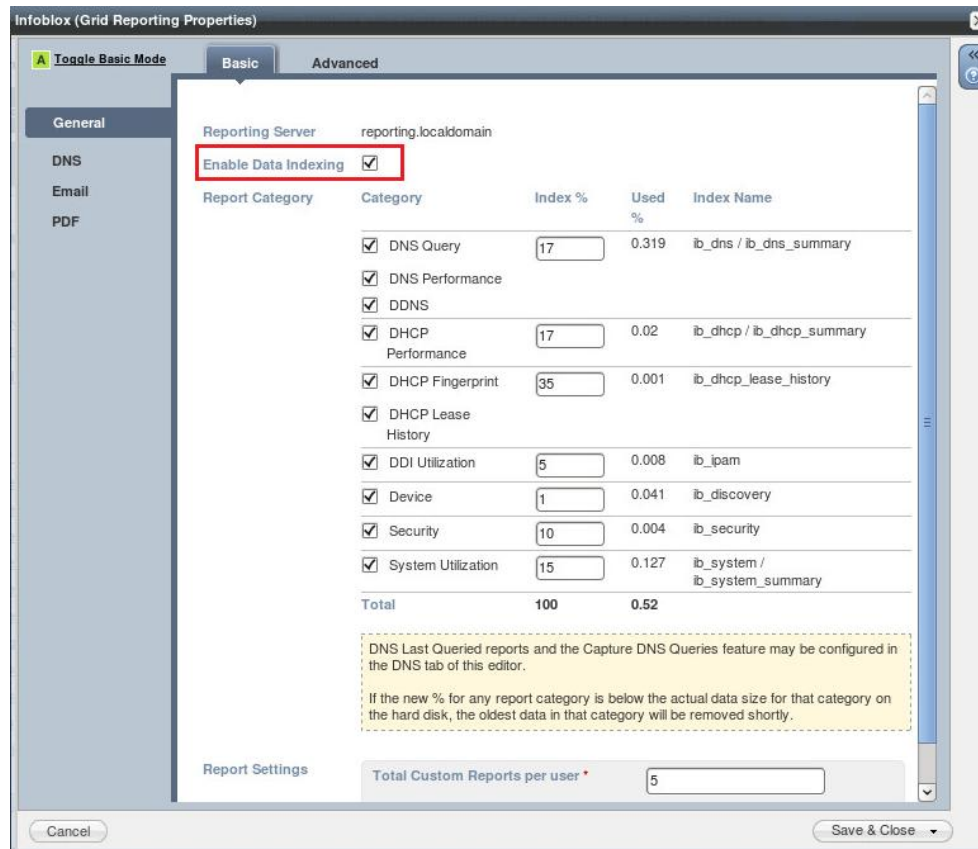
Kuvio 46. DHCP-pool vaihe 1

Kuviossa 47 on konfiguroinnin toinen ja kolmas vaihe, jossa määritetään osoitealueen lisäksi DHCP-palvelua tarjoava eli infoblox-ddi.localdomain –palvelin.

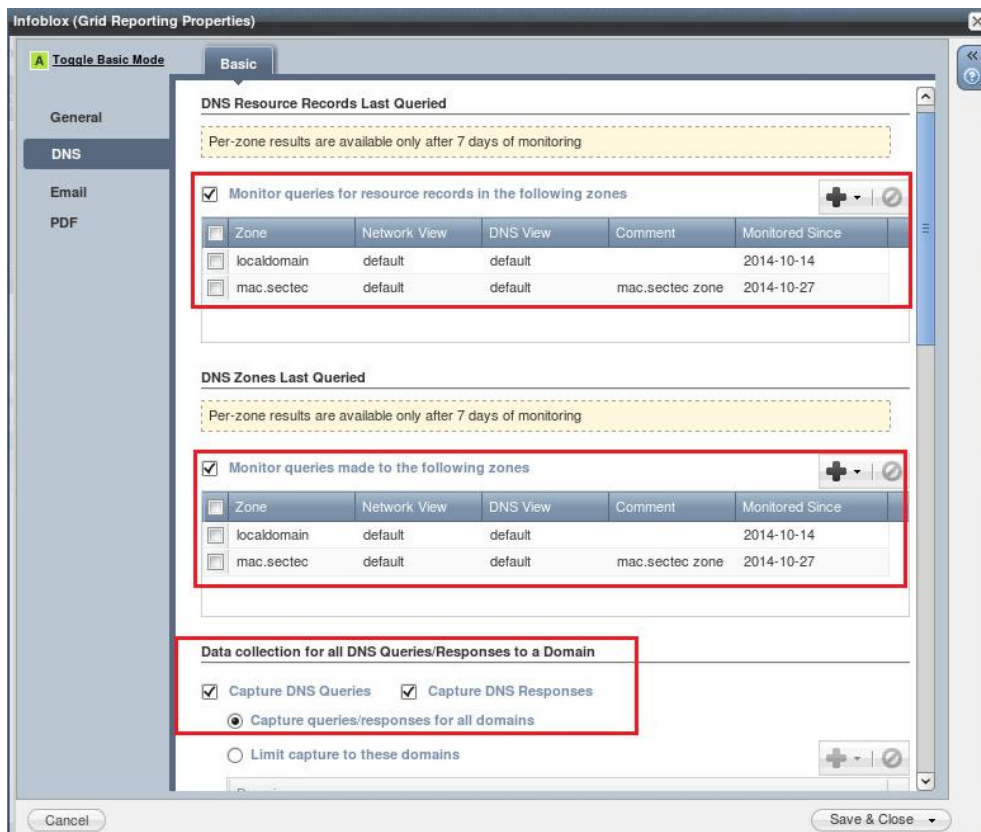


Kuvio 47. DHCP-pool vaihe 2

Liite 4: Reporting-palvelimen asetukset



Kuvio 48. Reporting General-välilehti



Kuvio 49. Reporting DNS-välilehti

Liite 5: RPZ-syötepalvelimen konfigurointi

Syötepalvelin rpz.testing.biz toteutettiin asentamalla CentOS 6.5 –palvelimelle DNS-palvelu BIND 9.8.2 –ohjelmistolla komennolla:

```
yum install bind
```

Käytännössä syötepalvelin on asetettu RPZ-säännöt sisältävän alueen ensisijaiseksi nimipalvelimeksi, joka jakaa kopion vyöhykkeestä asetetuille toissijaisille nimipalvelimille. Vyöhykettä ja toissijaisen nimipalvelimen määrittämisen lisäksi BIND:n asetukset säilyivät lähes oletusasetuksilla.

Kuviossa 50 on BIND:n "/etc/named.conf"-tiedosto, jossa on määritetty vyöhykkeen siirrossa HMAC-MD5 -avain ja sallittu kyselyiden suorittamisen Cisco ASA:n portin osoitteesta 91.223.107.2, kun käytössä on tsig-avaimella allekirjoitettu kysely.

```

key "tsig" {
    algorithm HMAC-MD5;
    secret "phqQ1tCjY6DozQ+Ht339Fnae/kVCN2j5baG64V8hYI2K2x9C/S5vdRqqtH/X4nIza5ymvFK5k1n6xr4Lutj/CA==";
};
server 91.223.107.2 {
    keys { tsig; };
};

zone "rpz.list" IN {
    type master;
    file "/var/named/rpz.list";
    allow-query { 91.223.107.2; };
    allow-transfer { key tsig; };
};

```

Kuvio 50. BIND /etc/named.conf -tiedosto

Kuviossa 51 on määritetty jaettava rpz.list-vyöhyke.

```

$TTL 3600
@      SOA      rpz.testing.biz. rpz.localhost (
        24      ; serial
        1800    ; 30min refresh 1800
        900     ; retry after 15min 900
        604800 ; expire after 1 week 604800
        3600 ) ; TTL 1h
      NS       localhost.

; NXDOMAIN policy records
www.badsite.biz CNAME .
*.badsite.biz  CNAME .

; No data policy records
suomi24.fi     CNAME *.
*.suomi24.fi  CNAME *.

; redirect policy records
youtube.com    CNAME www.vimeo.com.
*.youtube.com CNAME www.vimeo.com.

```

Kuvio 51. BIND zone-tiedosto

Liite 6: Infoblox loki ”www.skycrawler.com”-osoitteen estämisestä

The screenshot displays the Infoblox management interface. At the top, navigation tabs include IPAM, Devices, DHCP, DNS, and File Distribution. The 'DNS' tab is selected, showing a list of zones. The 'fireeye' zone is highlighted, and the 'Response Policy Zones' sub-tab is active. It shows a policy named 'Block Domain Name (No Such Domain)' assigned to the zone. Below this, the 'Syslog' section provides a detailed log entry for a DNS query.

Timestamp	Facility	Level	Server	Message
2014-11-12 11:31:57 EET	daemon	INFO	named:30186j	CEF-0 infoblox NOS 6.11.2-249613 RPZ-ONAME NXDOMAIN 4 app-DNS ds1-192.168.20.10 src=192.168.6.12 spt=40289 view=_default qtype=A msg="_rpz ONAME NXDOMAIN remote www.skycrawler.com [A] via www.skycrawler.com:fireeye"