Sebastian Ruoho

Verkkoliikenteen valvonta ja analysointi

Opinnäytetyö
Kevät 2019
SeAMK Tekniikka
Tietotekniikan tutkinto-ohjelma

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Tutkinto-ohjelma: Tietotekniikan tutkinto-ohjelma

Suuntautumisvaihtoehto: Tietoverkkotekniikka

Tekijä: Sebastian Ruoho

Työn nimi: Verkkoliikenteen valvonta ja analysointi

Ohjaaja: Alpo Anttonen

Vuosi: 2019 Sivumäärä: 75

Toimivat tietoliikenneyhteydet ovat nyky-yhteiskunnassa jo melkein elinehto. On erittäin tärkeää taata kaikille häiriötön ja tasavertainen internetpalvelu. Operaattoreiden on hyvä valvoa, millaista dataa verkossa liikkuu. Näin voidaan häiriötilanteista toipua tehokkaasti. Tässä työssä tutustutaan kahteen erilaiseen vaihtoehtoon valvoa ja analysoida yrityksen asiakkaiden verkkoliikennettä. Työn tilaajana on Suupohjan Seutuverkko Oy.

Työssä käsitellään verkonvalvontaa ja analysointia operaattorin näkökulmasta ja tutustutaan Cisco Systems -yrityksen kehittämään NetFlow-protokollaan, jota verrataan sitä perinteisempään pakettianalysointiin. Ensimmäisenä tutustuttiin ntop-yrityksen ntopng-ohjelmapohjaiseen ratkaisuun ja seuraavana Extreme Networks -yrityksen ExtremeAnalytics-laiteratkaisuun. Työssä käydään läpi kummankin vaihtoehdon asennus ja tutustutaan niiden käyttöön tarkemmin. Lopussa vertaillaan kumpaakin ratkaisua yrityksen näkökulmasta ja pohditaan niiden käyttökelpoisuutta.

Avainsanat: NetFlow, verkkoliikenne, analysointi, valvonta, IPFIX, ntopng, ExtremeAnalytics

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Information Technology

Specialisation: Information Network Technology

Author/s: Sebastian Ruoho

Title of thesis: Network Traffic Monitoring and Analysis

Supervisor(s): Alpo Anttonen

Year: 2019 Number of pages:75

Well-functioning data communications are almost a lifeline in today's society. Therefore, it is very important to ensure a seamless and equal Internet service for everyone. Internet service providers should monitor the data in their network. This way interferences can be solved effectively. This thesis examined two different ways to monitor and analyze the ISP's customers' network traffic. The thesis was commissioned by Suupohjan Seutuverkko Oy.

The thesis studied network monitoring and analysis from an Internet service provider's perspective and introduced the NetFlow protocol developed by Cisco Systems, which was then compared to a more traditional packet analysis. The software-based solution, ntopng, developed by the ntop company was examined first. Next followed the hardware-based ExtremeAnalytics developed by Extreme Networks. The thesis studied the installation and usage of both these solutions. At the end, both solutions were compared from the ISP's perspective and their utility was considered.

Keywords: NetFlow, network traffic, analysis, monitoring, IPFIX, ntopng, ExtremeAnalytics

SISÄLTÖ

Kuvaluettelo

Käytetyt termit ja lyhenteet

BIOS	Basic Input-Output System, tietokoneen avautuessa ensimmäisenä käynnistyvä ohjelma, jonka tarkoitus on tarkastaa laitteet ennen varsinaisen käyttöjärjestelmän latautumista.
Cisco Systems	Verkkolaitteita, kuten reitittimiä ja kytkimiä, valmistava teknologiayritys.
DPI	Deep Packet Inspection, tietoverkossa kulkevien pakettien tutkimista ja analysointia.
Flow	Flow on sarja paketteja, jotka kulkevat lähettävän ja vastaanottavan laitteen välillä, ne jakavat samat ominaisuudet. Esimerkiksi katsottaessa TV-lähetystä palvelimelta lähtevät paketit muodostavat Flow-sarjan kulkiessaan tietokoneelle.
GTK+	GIMP Toolkit, graafinen käyttöliittymäkirjasto käyttöliittymien luontiin useille eri käyttöjärjestelmille.
GUI	Graphical User Interface, graafinen käyttöliittymä, joka tarkoittaa nähtäviin elementteihin, kuten kuviin, perustuvaa käyttöliittymää.
HTML	Hypertext Markup Language, avoimesti standardoitu kieli, jolla esimerkiksi internetsivut on kirjoitettu.
Hyper-V	Windows 10 -käyttöjärjestelmästä ominaisuutena löytyvä virtualisointialusta, jolla voidaan luoda erilaisia virtuaalisia tietokoneita eri käyttötarkoituksiin.
IETF	The Internet Engineering Task Force, organisaatio, joka vastaa internetprotokollien standardoinnista.

IP	Internet Protocol, se kuuluu TCP/IP-mallin internet-kerrokseen ja on yksi internetin perusprotokollista. Sen tehtävänä on tietoliikennepakettien toimittaminen perille verkossa.
IPv4	Internet Protocol Version 4, toistaiseksi vielä yleisimmin käytössä oleva versio IP-protokollasta. Se on tarkoitus korvata tulevaisuudessa IPv6-protokollalla.
IPv6	Internet Protocol Version 6, toistaiseksi vähän käytetty versio IP-protokollasta. Suurin etu verrattuna nykyiseen on IP-osoitteiden pidennys, joka mahdollistaa moninkertaisen määrän IP-osoitteita.
Libpcap	Library Packet Capture, pakettien kaappauksen tarkoitettu kirjasto, johon esimerkiksi ntopng- ja Wireshark-ohjelmat perustuvat.
NTP	Network Time Protocol, aikaprotokolla, jota käytetään täsmällisen ajan määrittämiseen verkkolaitteelle synkronoimalla se NTP-serverin kanssa.
Porttiskannaus	Toimenpide, jolla pyritään löytämään haavoittuvuuksia kohdelaitteesta käymällä läpi sen tietoliikenneportteja ja mahdollisia ohjelmia, jotka niitä käyttävät.
Redundanttisuus	Käsite, jolla tarkoitetaan laitetta, jossa on halutun toimenpiteen kannalta ylimääräisiä osia tai resursseja, mitkä voidaan tarpeen vaatiessa ottaa käyttöön aiheuttamatta katkosta.
SCTP	Stream Control Transmission Protocol, tietoliikenneprotokolla, jota käytetään usean datavirran kuljettamiseen kahden yhteyden muodostaneen laitteen välillä.
SNMP	Simple Network Management Protocol, tietoliikenneprotokolla, jota käytetään verkossa olevien laitteiden tilan kyselyyn.

SSDP Simple Service Discovery Protocol, tietoliikenneprotokolla, jota käytetään laitteiden ja palvelujen etsimiseen lähiverkosta.

Syslog Standardi lokitiedoille, joita laite kerää eri kategorioiden mukaan ja, jotka voidaan välittää Syslog-palvelimelle myöhempää tarkastelua varten.

TCP Transmission Control Protocol, tietoliikenneprotokolla, jolla internetiin pääsevien tietokoneiden välille luodaan luotettavia yhteyksiä.

tcpdump Yleinen komentopohjainen pakettianalysointiohjelma.

UDP User Datagram Protocol, tietoliikenneprotokolla, kuten TCP, mutta UDP ei ole “luotettava” eli se ei suorita esimerkiksi virheentarkistusta. Käytetään muun muassa live-lähetyksissä ja verkkopeleissä.

Unix Laitteistoriippumaton käyttöjärjestelmä, jota käytetään lähinnä palvelimissa ja keskuskoneissa.

UPnP Universal Plug and Play, protokollajoukko, jonka tarkoitus on auttaa lähiverkon laitteita löytämään toisensa, ja mahdollistaa esimerkiksi tiedonsiirron.

VLAN Virtual Local Area Network, virtuaalilähiverkko on tekniikka, jolla esimerkiksi fyysisesti kaukana toisistaan sijaitsevat laitteet voidaan sijoittaa samaan lähiverkkoon toistensa kanssa.

VM-Ware Hyper-V-ohjelman kaltainen virtualisointiohjelma, jonka omistaa VMware-yritys.

ZMTP ZeroMQ Message Transfer Protocol, viestinvälitysprotokolla, jota käytetään viestien välitykseen kuljetuskerroksessa.

1 JOHDANTO

1.1 Työn tausta

Lähtökohtaisesti Suupohjan Seutuverkko Oy toteutti valokuituverkon turvatakseen nopeat tietoliikenneyhteydet myös haja-asutusalueille. Perusajatuksena oli luoda verkko-operaattoreille tekninen toteutus nopeiden ja toimivien yhteyksien turvaamiseksi. Kiinteät puhelinverkot eivät enää tarjonneet riittävää kapasiteettia ja mobiiliverkkojen kehityksestä ei ollut riittävää varmuutta.

Suupohjan Seutuverkko Oy aloitti oman internetpalvelun valokuituverkkoon liittyneille asiakkaille vuonna 2017. Tarkoituksena oli sekä kasvattaa Suupohjan Seutuverkko Oy:n eli Sunetin liiketoimintaa että antaa valokuituverkon asiakkaille paikallinen ja samalla kilpailukykyinen vaihtoehto internetpalvelun tarjoajana. Internetpalvelun myynti alkoi kampanjalla, jossa etuna oli edullisen hinnan lisäksi myös mahdollisuus saada valokuituverkon käytöstä perittävä verkkomaksu ja internetpalvelumaksu yhteisellä laskulla. Asiakkaita tuntui myöskin houkuttelevan pieneen ja paikalliseen toimijaan luottaminen etäisemmän valtakunnallisen palveluntarjoajan sijaan. Internetpalvelun laajentuessa on yhä tärkeämpää tasavertaisen palvelun tuottaminen kaikille asiakkaille. Tästä syystä on erittäin tärkeää, että dataliikennettä pystytään seuraamaan mahdollisten häiriöiden, kuten erilaisten hyökkäyksien ja saastuneiden laitteiden varalta. Näistä tulisi toipua mahdollisimman nopeasti tai jopa ehkäistä niiden synty ennalta.

Eräs tällainen hyökkäys tapahtui vuoden 2018 keväällä, jolloin muutamaan verkossa olevaan laitteeseen kohdistui SSDP-protokollaa käyttävä hyökkäys, joka aiheutti katkoksia ja häiriöitä asiakkaiden palveluissa. Hyökkäyksen selvittämiseen kului aikaa ja resursseja, joten näiden tilanteiden ehkäisemiseksi ja niiden ratkaisemisen helpottamisen vuoksi päädyttiin tutkimaan asiaa tämän opinnäytetyön aiheena.

Verkon valvontaan ja monitorointiin Sunetilla on jo käytössä SNMP-protokollaa hyödyntävä Observium-ohjelmisto. Tämän ohjelmiston pääasiallinen tarkoitus on kui-

tenkin lähinnä tarkkailla verkon laitteita ja antaa tietoa esimerkiksi niiden lämpötilasta ja prosessorikuormasta. Varsinaiseen dataliikenteen analyysiin ei Observium-ohjelmisto kykenekään, joten tähän tarvitaan joku muu ratkaisu.

1.2 Työn tavoitteet

Tämän työn tavoitteena on löytää luotettava, edullinen ja tehokas tapa analysoida ja valvoa Sunetin internetpalvelun liikennettä mahdollisten häiriöiden tai ongelmien varalta. Lopputuloksena pyritään löytämään laite tai ohjelma, joka olisi helppokäyttöinen, selkeä ja luotettava. Näin mahdollisissa häiriötilanteissa saataisiin selville häiriön aiheuttaja ja turvattua datasiirron sujuvuus. Työssä tutustutaan sekä ohjelmapohjaiseen ratkaisuun että laiteratkaisuun. Erilaisia mahdollisuuksia löytyy todella useita, aina erilaisista laitteista kuten, palomuureista liikenteen kerääjiin ja ilmaisista avoimeen lähdekoodiin perustuvista ohjelmista maksullisiin ohjelmistokokonaisuuksiin.

1.3 Työn rakenne

Työ rakentuu teoriaosasta, joissa käydään läpi verkonvalvontaa operaattorin näkökulmasta, tutustutaan Netflow-protokollaan ja verrataan sitä perinteisempään pakettianalysointiin. Toisena on itse työn osuus, jossa tutkitaan kahta vaihtoehtoista ratkaisua. Laitteistopohjaiseksi ratkaisuksi valittiin Extreme Networks -yrityksen laitekokonaisuus, koska Sunetilla on jo käytössä heidän toimittamiaan laitteita. Ohjelmistopohjaisen ratkaisun tuotteeksi valikoitui avoimen lähdekoodin ntopng. Tässä työssä tutustutaan asennuksiin ja käyttöönottoon, pohditaan soveltuvuutta sekä kustannustehokkuutta.

1.4 Sunet

Sunet eli Suupohjan Seutuverkko Oy on yritys, joka rakentaa avointa tietoliikenneverkkoa Suupohjassa ja Pohjois-Satakunnassa. Yritys on perustettu vuonna 2005 ja sillä on 5 vakituista työntekijää. Sunetin omistavat toiminta-alueen kunnat eli Kauhajoki, Teuva, Karvia, Isojoki, Karijoki, Kurikka ja Siikainen. Sunetin toimintaan kuuluu valokuituverkon rakennus, liittymämyynti, ylläpito ja internetpalvelun tarjonta. Valokuituverkko on verrattavissa sähkömaailmaan, sillä verkon omistus ja ylläpito on erotettu palveluntarjoajista. Sunetin verkon alueella palveluita yksityisille tarjoaa Sunetin lisäksi Elisa Oyj, Verkko-osuuskunta Kuuskaista, JNT ja Dynamo Net. Siikaisten alueella yksityisille on tarjolla myös Telian palveluja. Yrityksille taas palveluita tarjoaa edellisten lisäksi myös Neviso ja DNA. (Sunet [Viitattu 22.2.2019].)

Sunetin runkoverkko kiertää Suupohjan ja Pohjois-Satakunnan alueella renkaanmuotoisen rungon, joka kulkee Kauhajoen, Jurvan, Teuvan, Karijoen, Isojoen, Siikaisten, Karvian ja Honkajoen kautta. Matkalla rungosta haarautuu useita kyläverkkoja. Verkon laatu on varmistettu tämän hetken laadukkaimmilla verkkokomponenteilla ja se on toteutettu yhden gigan kapasiteetilla. Rungossa on useita liityntäpisteitä mm. Isojoella, Kauhajoella, Jurvassa, Karijoella, Teuvalla, Honkajoella, Siikaisissa ja Karviassa, ja se ulottuu tällä hetkellä Seinäjoelle asti, josta toimivat yhteydet mm. Kuusiokunnille. Sunet tekee aktiivista yhteistyötä myös muiden alueellisten kuituverkkojen kanssa ja on myös osana seutuverkkoklusteria. (Sunet [Viitattu 22.2.2019].)

2 VERKONVALVONTA JA ANALYSOINTI

2.1 Yleistä

Verkkoliikenteen seuraaminen on työtä, missä valvotaan ja analysoidaan tietoverkon toimivuutta. Valvonta kertoo kuormituksesta ja analysoinnilla pyritään saamaan syvällisempää tietoa liikennöinnin laadusta. (Noction 19.10.2018.)

Asiat voivat mennä pieleen tietoverkoissa minä tahansa päivänä. On kyseessä sitten yksinkertainen vakoiluohjelma, palvelunestohyökkäys tai monimutkainen reitittimen konfiguraatio-ongelma, ratkaisua ongelmaan voi olla mahdotonta löytää heti. Parhaiten tilanteeseen voi varautua tarvittavalla osaamisella ja työkaluilla, joita tarvitaan ongelman ratkaisuun. Kaikki verkon toimivuusongelmat on ratkaistava pakettitasolla, jossa hyvin tavanomaiset ja luotettavana pidetyt protokollat ovat petollisia. Jotta ymmärretään parhaiten verkko-ongelmia, on helpointa lähteä liikkeelle pakettitasolta. Mitä enemmän voidaan vaikuttaa asioihin pakettitasolla, sitä paremmin hallitaan verkkoa ja voidaan ratkaista ongelmia. (Sanders 2011, 1.)

Verkkovalvonta on joko protokollan tai datapakettien analysointia laitteen, ohjelmiston tai niiden yhdistelmällä. Tavoitteena on suojautua haitallista liikennöintiä vastaan. Tämä työ laajentaa palomuurien, virustorjunnan, yms. ohjelmien tuomaa suojaa. (Cecil [Viitattu 17.3.2019].)

Analysoinnin avulla voidaan:

- Tuottaa yksityiskohtaista tilastoa nykyisen ja juuri tapahtuneesta liikenteestä verkossa.
- Testata haavoittuvuutta tunnetuille haitta-ohjelmille.
- Havaita epätavallisia liikennöintimääriä.
- Havaita epäilyttäviä pakettien ominaisuuksia.
- Tunnistaa pakettien lähteet ja kohteet.
- Määritellä hälytystaso tunnetuille uhille.
- Etsiä erityisiä merkkijonoja paketeista.
- Monitoroida kaistan käyttöä eri ajanjaksoina
- Luoda ohjelmallisia lisätoimintoja.

- Näyttää kaikki tilastot käyttäjäystävällisessä seurantapaneelissa. (Cecil [Viitattu 17.3.2019].)

Analysoinnilla ei ole tarkoitus korvata lähinnä loppukäyttäjille tarkoitettuja palomuureja, virustorjuntaa tai haittaohjelmia vastaan suojautumista. Analysoinnin käytöllä voidaan pienentää verkkohyökkäyksien uhkaa ja myös nopeuttaa toimia hyökkäyksen alettua. (Cecil [Viitattu 17.3.2019].)

ISO ja IEC ovat yhdessä määrittäneet verkonvalvontaa liittyviä määrityksiä standardiin ISO/IEC 7498-4. Standardi jakaa verkonvalvonnan vianhallintaan, kirjanpidon hallintaan, konfiguraation hallintaan, suorituskyvyn hallintaan ja turvallisuuden hallintaan. Vianhallinnalla pyritään ylläpitämään ja tutkimaan vikalokeja, löytämään, rajaamaan ja korjaamaan viat. Kirjanpidon hallinnassa pyritään laskuttamaan resurssien käytöstä. Konfiguraation hallinnassa tutkitaan ja kerätään dataa laitteista, ja mahdollisesti muutetaan tarpeen vaatiessa asetuksia. Suorituskyvyn hallinnassa tarkkaillaan liikennettä ja protokollia, sekä pyritään parantamaan suorituskykyä tarpeen vaatiessa. Turvallisuuden hallinnassa tiedotetaan käyttäjiä turvallisuuteen liittyvissä asioissa. (ISO/IEC 7498-4 1989.)

2.2 Operaattorin kannalta

Liikenne- ja viestintävirasto eli Traficom ohjeistaa operaattoreiden toimintaa verkkoliikenteen suhteen. Operaattoreiden on kohdeltava kaikkea verkkoliikennettä tasapuolisesti eli noudattaen internetin avoimuuden periaatteita. Operaattorilla ei ole siis oikeutta rajoittaa esimerkiksi liikennettä johonkin tiettyyn palveluun tai sovellukseen. Operaattori ei voi myöskään rajoittaa tietyn tyyppistä liikennettä. Verkon resurssien tehokkaan käytön ja internetpalvelun laadun vuoksi operaattorilla on kuitenkin oikeus ottaa käyttöön kohtuullisia liikenteenhallintamenettelyjä. Tarpeen vaatiessa operaattori voi rajoittaa internetliikennettä, jos:

- lainsäädäntö, tuomioistuin tai viranomainen tekee päätöksen asiasta
- verkko- ja päätelaitteiden tietoturva on uhattuna

- uhkana on verkon liikenteen ruuhkautuminen tai jo syntyneen ruuhkan purkaminen, jos ruuhkautuminen on poikkeuksellista tai väliaikaista. (Traficom 12.3.2019.)

Kaikkien asiakkaiden palvelujen toimivuuden ja laadun takaamiseksi on siis tärkeää kiinnittää huomiota mahdollisiin uhkiin, joita verkossa on. Operaattori voi myös tarjota verkossaan palveluita, jotka edellyttävät parempaa laatua yhteydeltä. Tämä täytyy kuitenkin tehdä niin, että kaikkia liittymiä kohdellaan tasaveroisesti eli optimointia ei voi tehdä muiden yhteyspalvelujen laadun kärsiessä. (Traficom 12.3.2019.)

Traficomin määrittämiin verkkoneutraliteettiperiaatteisiin kuuluu myös operaattorin vastuu antaa selkeät ja ymmärrettävät tiedot liittymien ominaisuuksista. Asiakkaille pitää kertoa muun muassa:

- asetusten mukaiset tiedot internetyhteyspalvelun nopeudesta
- miten mahdollinen tiedonsiirtokiintiö, nopeus ja muut tekijät vaikuttavat palveluun ja sisällönkäyttöön
- miten operaattorin käyttämät liikenteenhallintamenetelmät voivat vaikuttaa palveluun
- miten optimointia edellyttävät palvelut vaikuttavat internetpalveluun. (Traficom 12.3.2019.)

2.3 Pakettianalysointi

Pakettianalysoinnista käytetään myös termiä pakettihaistelu (sniffing) tai termiä protokolla-analyysi. Ne tarkoittavat kuitenkin prosessia, jossa kaapataan ja tulkataan tietoa samalla kun se virtaa tietoverkon läpi ja pyritään paremmin ymmärtämään, mitä verkossa tapahtuu. Pakettianalysoinnin toteuttaa tyypillisesti paketinhaistelija eli työkalu, jota käytetään kaappaamaan raakaa dataa, joka kulkee tietoverkossa. (Sanders 2011, 2.)

Pakettianalysointi voi auttaa:

- ymmärtämään verkon piirteitä
- tietämään kuka verkossa on

- määrittämään kuka tai mikä käyttää vapaana olevaa kaistaa
- löytämään verkon suurimmat käyttöhetket
- tunnistamaan mahdolliset hyökkäykset tai haitallisen toiminnan
- löytämään turvattomat ja levinneet ohjelmat. (Sanders 2011, 2.)

On olemassa monenlaisia ilmaisia ja maksullisia pakettianalysointiohjelmia. Jokainen ohjelma on suunniteltu erilaiseen tehtävään. Muutamia suosittuja pakettianalysointiohjelmia ovat tcpdump, OmniPeek ja Wireshark. tcpdump on komentopohjainen ohjelma, kun taas OmniPeek ja Wireshark hyödyntävät graafista käyttöliittymää. (Sanders 2011, 2.)

2.3.1 Npcap

Npcap on Windows-käyttöjärjestelmälle luotu pakettien kaappaukseen tarkoitettu kirjasto, joka perustuu WinPcap- ja Libpcap-kirjastoihin. WinPcap-kirjasto on Npcap-kirjaston edeltäjä, ne taas kumpikin pohjautuvat Libpcap-kirjastoon. Sen on tarkoitus olla edeltäjäänsä nopeampi ja tehokkaampi. Esimerkiksi ntopng-ohjelma Windowsille asennettuna pohjautuu Npcap-kirjastoon. (nmap [Viitattu 17.3.2019].)

2.3.2 Wireshark

Wireshark-ohjelma on tunnetuin ja eniten käytetyin verkkoprotokolla-analysaattori. Sen avulla on mahdollista hyvin tarkasti tietää, mitä tutkittavassa verkossa tapahtuu millä tahansa hetkellä. Se on saavuttanut niin merkittävän maineen, että sitä käytetään hyvin monissa eri laitoksissa, sekä opetustarkoitukseen että kriittisiin työtarkoituksiin. Wireshark-ohjelman menestys ja kehitys pohjautuu ympäri maailmaa olevien verkkoasiantuntijoiden vapaaehtoisiin panoksiin ja heidän nimiä löytyykin listattuna ohjelman verkkosivuilta. (Wireshark [Viitattu 15.2.2019].)

Wireshark-ohjelma on kaikille ilmainen ja vapaasti ladattavissa ohjelman omalta verkkosivulta. Sillä on monia erilaisia käyttötarkoituksia aina ison tietoverkon vianetsinnästä, pienen yrityksen liikenteen tutkimiseen. Wireshark-ohjelman ominaisuuksia ovat mm. datan DPI-analysointi reaaliajassa tai jo kaapatusta pcap-tiedostosta,

helppokäyttöinen graafinen käyttöliittymä ja tiedon suodattaminen komennoilla. Ohjelmalla on mahdollista mennä todella syvälle eri protokolliin ja hajottaa ne aivan pakettitasolle, kuitenkaan itse liikennettä häiritsemättä. Wireshark-ohjelmaa on mahdollista käyttää kaikilla yleisimmillä käyttöjärjestelmillä, ja sen graafinen käyttöliittymä on luotu käyttäen GTK+ widget toolkit -kirjastoa. Wireshark-ohjelma jakaa monia piirteitä tcpdump-ohjelman kanssa. Yhtenä erona on mm. se, että tcpdump-ohjelma pohjautuu komentopohjaiseen käyttöliitymään. (Technopedia [Viitattu 15.2.2019].)

Itse pakettien kaappaamiseen ohjelma käyttää Unix-käyttöjärjestelmille alun perin luotua libpcap-kirjastoa, josta on johdettu Windows-käyttöjärjestelmän käyttöön soveltuva Npcap-protokolla (Harris 20.12.2018).

2.4 Mirror

Portin peilaus mirror-toiminnolla mahdollistaa porttiin saapuvan ja portista lähtevän liikenteen tarkkailun laittamalla protokolla-analysointiohjelman, kuten Wiresharkin porttiin, johon ”peilattu” tieto viedään. Tällöin peilatusta portista lähtevä tai siihen saapuva paketti ohjataan myös kohdeporttiin. Protokolla-analysointiohjelma sieppaa liikennettä vaikuttamatta alkuperäisen portin liikenteeseen. (Extreme Networks [Viitattu 15.2.2019].)

2.5 NetFlow vs pakettianalysointi

Pakettianalysoinnista puhuttaessa tarkoitetaan käytännössä liikenteen kopioimista, jotta kaikkia verkossa liikkuvia paketteja voidaan tutkia. Tällaista analysointia käytetään, kun on tarve nähdä kaikki liikenne vaikkapa kahden laitteen välillä. NetFlow-analysoinnissa taas kerätään metadataa verkon liikenteestä ja sitä tutkitaan ja analysoidaan statistisesta näkökulmasta. Kumpikaan näistä tavoista ei sulje toista pois, vaan niitä on tehokasta käyttää toistensa tukena. Jos esimerkiksi analysoidaan ison asiakasverkon liikennettä, on järkevää käyttää NetFlow-analysointia. Mutta jos verkossa havaitaan häiriötä, voidaan tällöin suorittaa liikenteestä kaappaus, jota sitten analysoitaisiin pakettianalysoinnilla. (Netfort [Viitattu 17.3.2019].)

2.6 Mikä on NetFlow?

NetFlow on Cisco-tietoliikenneyrityksen kehittämä verkkoprotokolla. Sen tarkoituksena on kerätä tietoa verkkoliikenteestä ja monitoroida sitä. Termiä NetFlow voidaan pitää jo yleisenä alan standardina, mutta kuitenkin monet muut valmistajat ovat ryhtyneet käyttämään omia vaihtoehtoisia flow-teknologioitaan. Tällaisia ovat esim. Jflow (Juniper), s-flow, (3Com/HP, Dell ja NetGear), NetStream (Huawei), Cflow (Alcatel-Lucent) ja Rflow (Ericsson). (Hale 6.9.2012.)

NetFlow-protokollasta on jo monta eri versioita, sillä se on alun perin kehitetty jo vuonna 1990. Ensimmäistä versiota ei nykyisin ole missään, sillä se on jo täysin korvattu. Versioita 2—4 ei koskaan julkaistu, vaan ne säilyivät Cisco-yrityksen sisäisessä käytössä. Yleisin versio 5 julkaistiin jo vuonna 2009 ja se tukee vain IPv4-protokollaa. Versiota 6 ei enää tueta, ja versio 7 on käytössä vain Cisco-yrityksen omilla kytkimillä. Versio 8 ei ole käytössä, vaan sen on korvannut jo versio 9. Versio 9 on kuin versio 5, mutta sitä on paranneltu mm. lisäämällä tuki jo vähitellen yleistyvälle IPv6-protokollalle. IPFIX-protokollaa kutsutaan usein myös NetFlow-protokollan kymmenenneksi versioksi, mutta se on kuitenkin vain IETF-organisaation standardoima, eikä varsinaisesti uusi versio. Nykyisin yleisimmin käytössä olevat versiot ovat versiot 5 ja 9. (Hale 6.9.2012.)

Reitittimet ja kytkimet, jotka tukevat NetFlow-protokollaa, keräävät IP-liikennestatistiikkaa kaikista rajapinnoista, joissa NetFlow-protokolla on otettu käyttöön. Myöhemmin nämä statistiikat välitetään NetFlow-luetteloina vähintään yhdelle NetFlow Collectorille, joka on tyypillisesti palvelin. Tämä tekee varsinaisen verkkoliikenteen analysoinnin. NetFlow Collector prosessoi tiedon tehdäkseen verkkoliikenteen analysoinnin ja esittääkseen tiedon käyttäjäystävällisessä muodossa. Netflow Collector voi olla joko laitteistopohjainen kerääjä tai ohjelmistopohjainen kerääjä. (Hale 6.9.2012.)

2.6.1 Flow Collector

Flow Collector on ohjelma tai laite, jonka tehtävä on vastaanottaa jonkin NetFlow-tietoa tuottavan laitteen lähettämää dataa. Flow Collector lajittelee vastaanottamansa liikennedatan myöhempää analysointia varten. (Parker 8.9.2016.)

2.6.2 IPFIX

IPFIX on lyhenne sanoista Internet Protocol Flow Information Export. Se on IETF-organisaation määrittämä standardi verkon laitteiden flow-tietojen viennistä. Se on johdettu Cisco-yrityksen patentoidusta NetFlow v9 -protokollasta. Tarkkailupisteessä kerätään flow-tietoja, jotka suodatetaan ja niistä kootaan tietopaketteja. Vientiprosessi lähettää flow-merkinnät IPFIX-viesteinä, pakattuna kerroksen 4 protokollien (SCTP, UDP tai TCP) avulla NetFlow Collector -ohjelmalle. (Noction 19.10.2018.)

IPFIX-protokollalla voidaan kerätä mitä tahansa tietoa verkkoliikenteestä kerroksilta 2—7 ja kerätty tieto viedään NetFlow Collector -ohjelmalle. IPFIX-protokollan viestin sisällä voidaan viedä kaikenlaisia erilaisia tietoja, jotka ovat joko käyttäjän määrittämiä tai muita muuttujia, kuten http-osoiteita tai esimerkiksi syslog-viestejä, SNMP-tietoja tai vaikka huoneen lämpötilan arvoja. (Noction 19.10.2018.)

3 NTOP

3.1 Yrityksestä

ntop on pieni ja innovatiivinen yritys, jonka asiakkaista suurin osa on pieniä yrityksiä, mutta myös joitain isoja yrityksiä. Yritys kehittää korkealaatuisia tietoliikenneohjelmistoja, jotka pohjautuvat avoimeen lähdekoodiin, ja joita käyttävät sekä tavalliset kuluttajat että isot teleoperaattorit. Ohjelmistot ovat usein vapaasti käytettävissä opiskelukäyttöön ja voittoa tavoittelemattomaan tarkoitukseen. Yritys pyrkii olemaan vastuullinen, käyttämään vihreää energiaa, sekä tarjoamaan asiakkailleen palveluja sellaisina kellonaikoina, kun se on heille kaikkein tehokkainta. Yritys pyrkii luomaan itse kaikki myymänsä ohjelmistot ja olemaan riippumaton muista osapuolista. ntop haluaa tarjota kaikille tuotteilleen läpinäkyvyyttä ja pyrkiä olemaan eettinen yritys bisnesmielessä ja muistamaan arvonsa. (ntop [Viitattu 8.2.2019].)

3.2 Historiaa

ntop syntyi ajatuksesta luoda yksinkertainen ja tehokas avoimen lähdekoodin verkkoliikenteen seuranta-alusta. Tavoite kehittää verkkoliikenteen seurantaa on säilynyt samana, mutta monet muut asiat ovat muuttuneet sen jälkeen, kuten analysoitava liikenne itsessään, käyttöjärjestelmät ja käyttäjät. ntop on myös kasvanut kokonaiseksi tutkimusyritykseksi. Arvojensa ja ajatusmaailmansa vuoksi ntop tekee vieläkin avoimen lähdekoodin tuotteita. Yritys haluaa luoda ohjelmistoa, joka toimii halvemmallakin laitteistolla. (ntop [Viitattu 8.2.2019].)

3.3 ntopng

ntopng tulee sanoista ntop next generation eli se on seuraavan sukupolven versio alkuperäisestä ntop-ohjelmasta. Sillä on tarkoitus monitoroida ja analysoida verkkoliikennettä. ntopng-ohjelman on tarkoitus toimia käytännössä kaikilla Unix-alustoilla, Mac OSX -käyttöjärjestelmillä ja myös Windows-käyttöjärjestelmillä ja se pohjautuu

libcap-kirjastoon. ntopng-ohjelma takaa helpon yksinkertaisen tavan tutkia ja analysoida reaaliaikaista ja historiallista liikennettä. Ohjelman pääominaisuuksia ovat mm. verkkoliikenteen järjestäminen esimerkiksi IP-osoitteen tai portin mukaan, reaaliaikaisen liikenteen tarkkailu, historiallisen liikenteen tarkkailu, eri ohjelmien käyttämien protokollien erittely, suurimpien verkon käyttäjien havainnointi ja erilaisten huomioiden ja hälytysten raportointi. (ntop [Viitattu 3.2.2019].)

3.3.1 Käyttö, vaatimukset ja versiot

ntopng-ohjelmaa voidaan käyttää minkä tahansa HTML5-kieltä tukevan internetselaimen kautta, se tukee SSL- ja HTTPS-salausta. Keskusmuistin ja prosessorin käyttö riippuu ntopng-ohjelman konfiguraatiosta ja olosuhteista, mutta modernilla koneella ei suuri verkkokaan aiheuta suurta kuormaa. ntopng-ohjelma tukee myös sFlow-, NetFlow- ja IPFIX-protokollia. Tällöin ntopng-ohjelmaa pitää käyttää yhdessä nProbe-ohjelman kanssa. Kommunikaatio ohjelmien välillä tapahtuu ZMTP-protokollan avulla, joka sallii ntopng-ohjelman keskustella nProbe-ohjelman kanssa. ntopng-ohjelma on saatavilla kolmena eri versiona: Community, Professional ja Enterprise. Community-versio on ilmainen, kun taas Professional- ja Enterprise-versiot ovat maksullisia. Maksulliset versiot tarjoavat lisäominaisuuksia verkon analysointiin. (ntop [Viitattu 3.2.2019].)

3.4 nProbe

nProbe-ohjelmaa voidaan käyttää mm. NetFlow-,sFlow- ja IPFIX-protokollien lähettämien tietojen keräämiseen ja ohjaamiseen ntopng-ohjelmalle. Tällöin nProbe-ohjelma kerää verkosta NetFlow-protokollaa tukevien kytkinten tai reitittimien lähettämiä NetFlow-virtauksia, jotka se ohjaa eteenpäin esimerkiksi ntopng-ohjelmalle liikenteen analysointia varten. nProbe-ohjelma on todella taipuisa ja sitä voidaan käyttää useissa eri moodeissa. Eri moodit mahdollistavat esimerkiksi eri Netflow-protokollien välisen muunnoksen. Ohjelma on myös suunniteltu skaalautuvaksi usean gigabitin verkkoihin. Toimiakseen kunnolla sen täytyy ”nähdä” tai kaapata haluttu

verkkoliikenne. Tämän takia verkoissa on tarpeellista joko peilata liikenne mirror-toiminnolla tai sijoittaa nProbe-ohjelma kohtaan, jonka kautta suurin osa liikenteestä kulkee. Normaalissa toimintaympäristössä nProbe kerää liikennetietoa ja lähettää sen kohti määritettyä kerääjää. Analysointiin voidaan käyttää mitä tahansa tavallista NetFlow Collector -ohjelmaa. nProbe-ohjelmaa suositellaan käytettäväksi yhdessä ntopng -ohjelman kanssa, sillä ne on optimoitu toimimaan näin. (ntop [Viitattu 15.2.2019].)

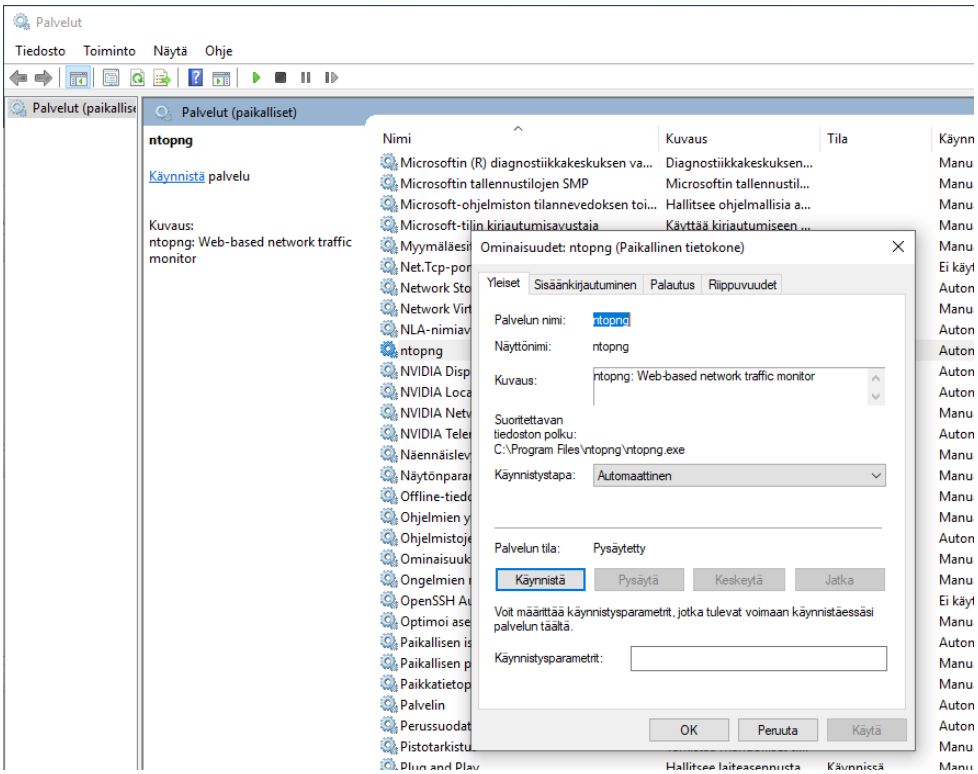
3.5 Asennus

Ennen ntopng-ohjelman asennusta liikenteen analysointia kokeiltiin Wireshark-ohjelmalla. Tässä kävi hyvin nopeasti esille, että tietokoneen resurssit eivät riittäneet liikenteen määrän hallitsemiseen. Wireshark-ohjelma myöskin kaappaa jokaisen verkossa esiintyvän paketin ja pyrkii tallentamaan sen kovalevylle, jolloin kone olisi tukkiutunut nopeasti. Wireshark-ohjelma on tällaisessa tarkoituksessa kyllä toimiva, mutta lähinnä silloin, kun toiselta ohjelmalta, kuten tässä työssä käsiteltävät ntopng-ohjelmalta tai ExtremeAnalytics-ohjelmalta, otetaan tietynlainen näyte verkkoliikenteestä pcap-tiedostona ja tuodaan se Wireshark-ohjelman tutkittavaksi. Tälloin päästään tutkimaan liikennettä pakettitasolla.

Liikenteen tuonti ntopng-ohjelmaa varten päätettiin toteuttaa luomalla mirror-portti Extremen runkoreitittimessä ja tuomalla luodusta portista liikenne suoraan tietokoneelle analysoitavaksi. Tässä ongelmaksi muodostui se, että liikenteen määrä oli niin suuri, että mirror-toimintoa ei voinut toteuttaa kaikelle liikenteelle, vaan oli tyydyttävä osaan liikenteestä. Analysointiin käytettävään tietokoneeseen olisi tarvinnut 10 Gt:n verkkokortin, että se olisi voinut ottaa kaiken liikenteen vastaan.

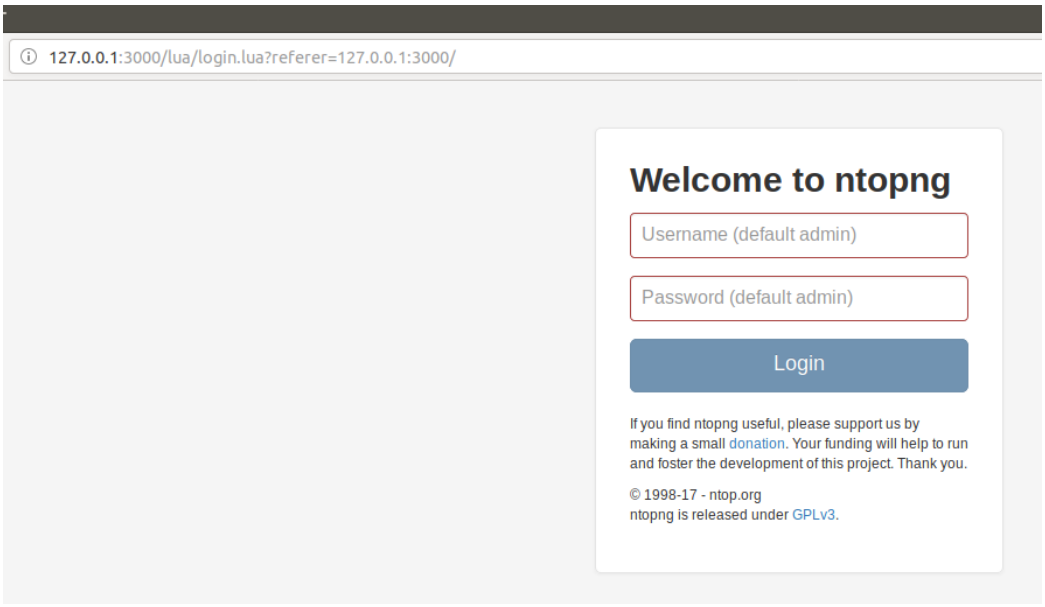
Testausta varten päädyttiin asentamaan ntopng-ohjelma suoraan tietokoneelle Windows-käyttöjärjestelmän päälle. Asennustiedosto saatiin ladattua suoraan valmistajan lataukset-sivulta. Asennus tapahtuu kuten normaali ohjelman asentaminen Windowsille, joten sitä ei ole tähän erikseen kuvattu. Asennusohjelma asentaa koneelle ntopng-ohjelman lisäksi Win10Pcap-ohjelman liikenteen kaappausta varten ja redis-

palvelimen taustalle pyöriväksi tietokannaksi. Asennuksen jälkeen tietokone täytyy käynnistää uudelleen ja tämän jälkeen ntopng-ohjelma ja redis-palvelin löytyvät Windowsin Palvelut-valikon alta.



Kuva 1. ntopng-ohjelma Palvelut-valikossa.

Ohjelmaa pääsee nyt käyttämään avaamalla selainikkunan ja kirjoittamalla haku-kenttään http://127.0.0.1:3000/. Ohjelmaan kirjaudutaan käyttäjätunnuksella admin, ja salasanana on admin, joka täytyy heti vaihtaa.



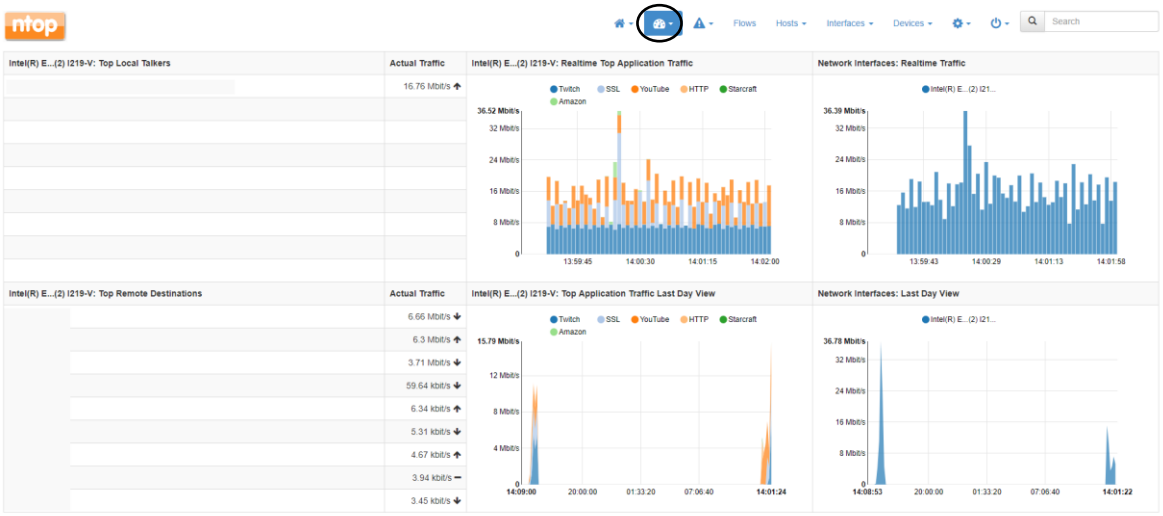
Kuva 2. ntopng-ohjelman kirjautumisnäkymä.

3.6 Käyttäminen

ntopng-ohjelmaan kirjautumisen jälkeen avautuu Dashboard-näkymä liikenteestä verkossa. Kyseessä on tosin maksullisen Professional-version näkymä, joka katoaa noin 10 minuutin kuluessa, trial-lisenssin loppuessa. Tämä hankaloittaa ohjelman testausta muutamassakin eri kohdassa, sillä kaikkia ominaisuuksia ei ehdi tai pääse testaamaan ajan lyhyyden takia. Professional-version testin loputtua kattavaa Dashboard-näkymää liikenteeseen ei käytännössä ole, joten vertailun vuoksi se on hyvä kuitenkin ottaa esille.

3.6.1 Traffic Dashboard

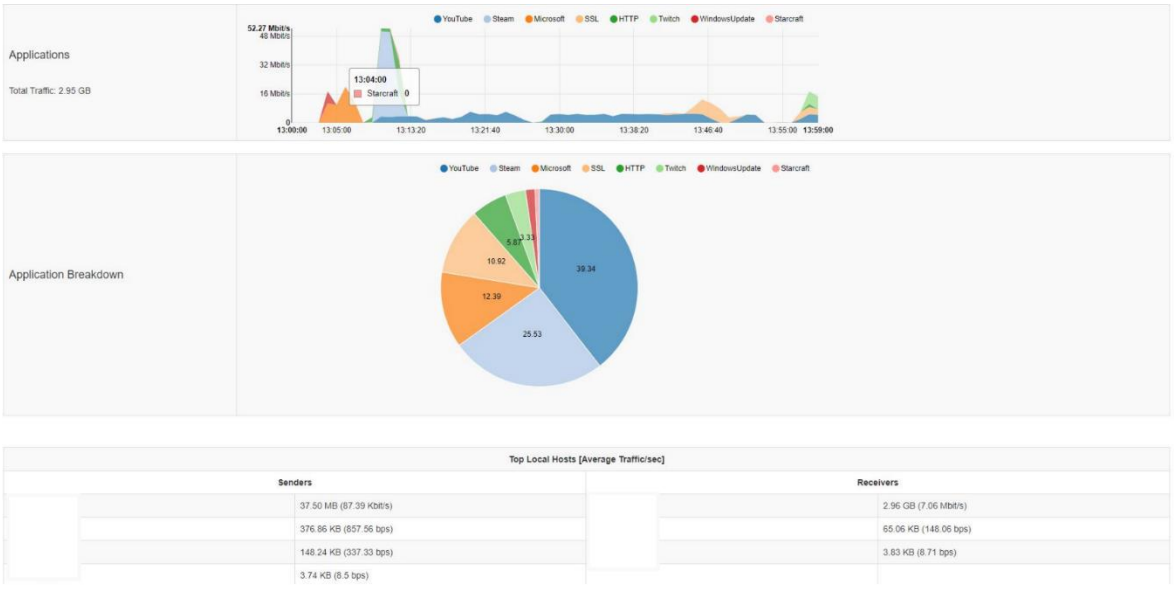
Traffic Dashboard -näkymässä näkee pylväsdiagrammina tämän ja edellisen päivän eniten käytettyjä sovelluksia, ja tämän sekä edellisen päivän liikenteen määrää tietyllä hetkellä. Näkymässä on myös tämän hetken eniten kaistaa käyttävät IP-osoitteet. Tätä näkymää ei ainakaan suoraan pääse muokkaamaan omanlaiseksi. Näkymästä saa kuitenkin hyvän kuvan verkon tämän hetkisistä sovelluksista ja käytöstä.



Kuva 3. ntopng-ohjelman Traffic Dashboard -näkymä.

3.6.2 Traffic Report

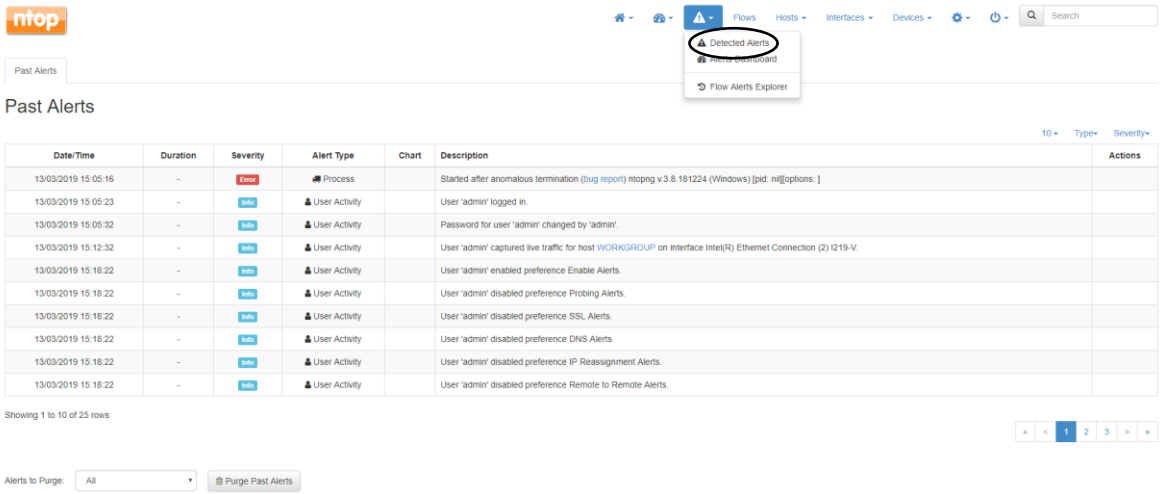
Traffic Report -ominaisuudella voidaan tehdä kattava raportti tietyn ajankohdan, vaikkapa edellisen päivän liikenteestä ja sovelluksista. Tämä raportti voidaan tulostaa PDF-tiedostona.



Kuva 4. Traffic Report -ominaisuuden piirakkadiagrammi sovelluksista.

3.6.3 Detected Alerts

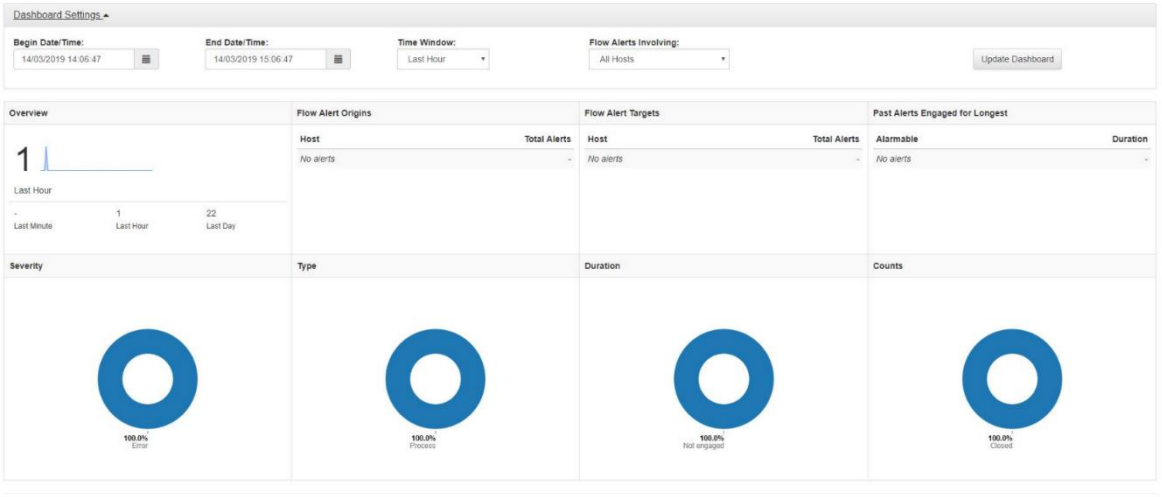
Detected Alerts -sivulta pääsee näkemään ntopng-ohjelman havaitsemia varoituksia. Ohjelma kerää huomioita eri asioista, kuten asetusten muutoksista ja luokittelee ne kategorioittain vakavuuden perusteella. Asetusten muuttaminen on vakavuudeltaan ”Info”, kun taas ohjelmavirhe on ”Error”.



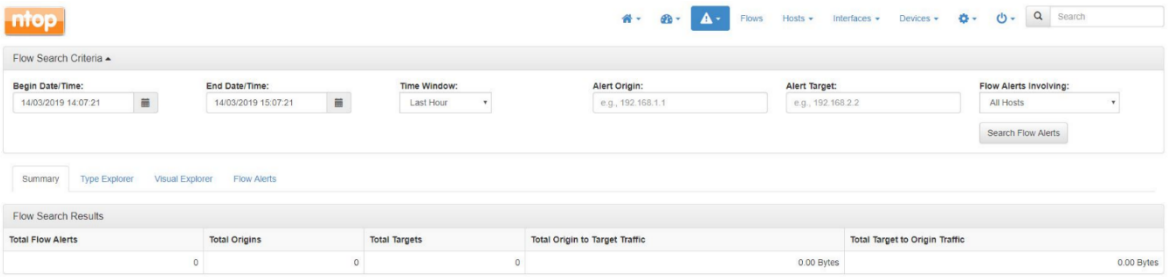
Kuva 5. Detected Alerts -näkymä.

3.6.4 Alerts Dashboard

Alerts Dashboard -sivulta pääsee tarkempaan näkymään verkossa esiintyneistä varoituksista. Sivulta näkee kätevästi esimerkiksi varoituksen kategorian, tyypin ja määrän. Varoituksia pystytään myös tutkimaan takautuvasti. Flow Alerts Explorer -toiminnolla päästään myös katsomaan tarkempia tietoja varoituksista.



Kuva 6. Alerts Dashboard -näkymä varoitusten määrästä ja tyypistä verkossa.

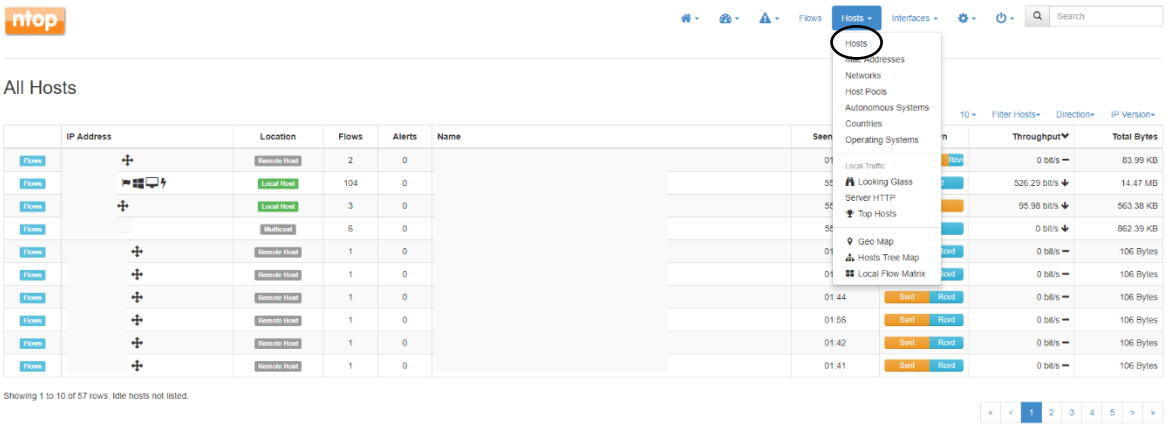


Kuva 7. Flow Alerts Explorer -toiminto varoitusten hakuun.

3.6.5 Hosts

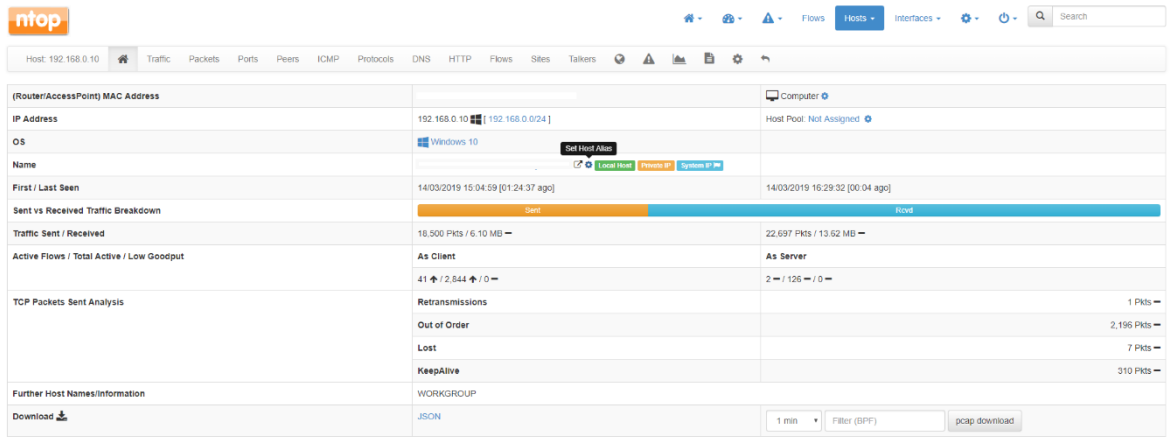
Hosts-sivun alta näkee kaikki verkossa esiintyneet IP-osoitteet ja tietoja niistä kuten Flow-määrän, varoitukset ja liikenteen. Oman verkon osoitteita voi tutkia myös MAC-osoitelistauksena, jolloin näkee tietoa kyseisen MAC-osoitteen valmistajasta

ja myöskin liikenteen määrästä. Listauksia voi tehdä myös itseluotujen Host Pool -ryhmien perusteella.



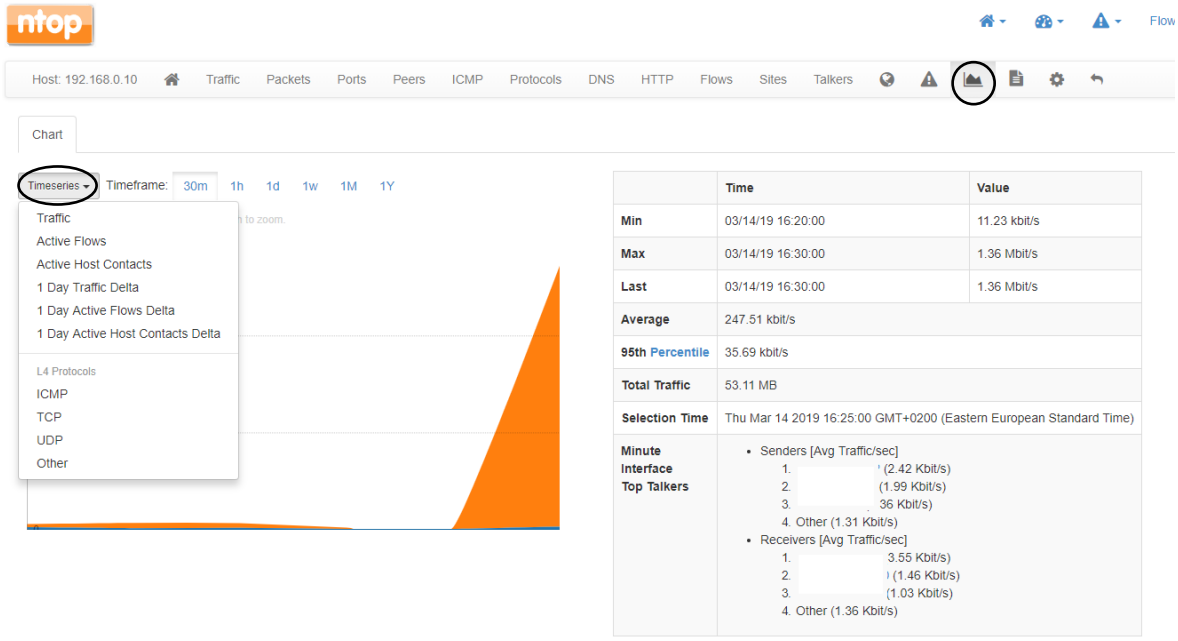
Kuva 8. Listaus verkon Host-IP-osoitteista.

Jokaista IP-osoitetta painamalla pääsee näkemään tarkempaa tietoa, kuten MAC-osoitteen ja liikennetietoa. Näkymässä voidaan myös nimetä kyseinen IP-osoite halutulla tavalla tai lisätä se omaan osoiteryhmään.

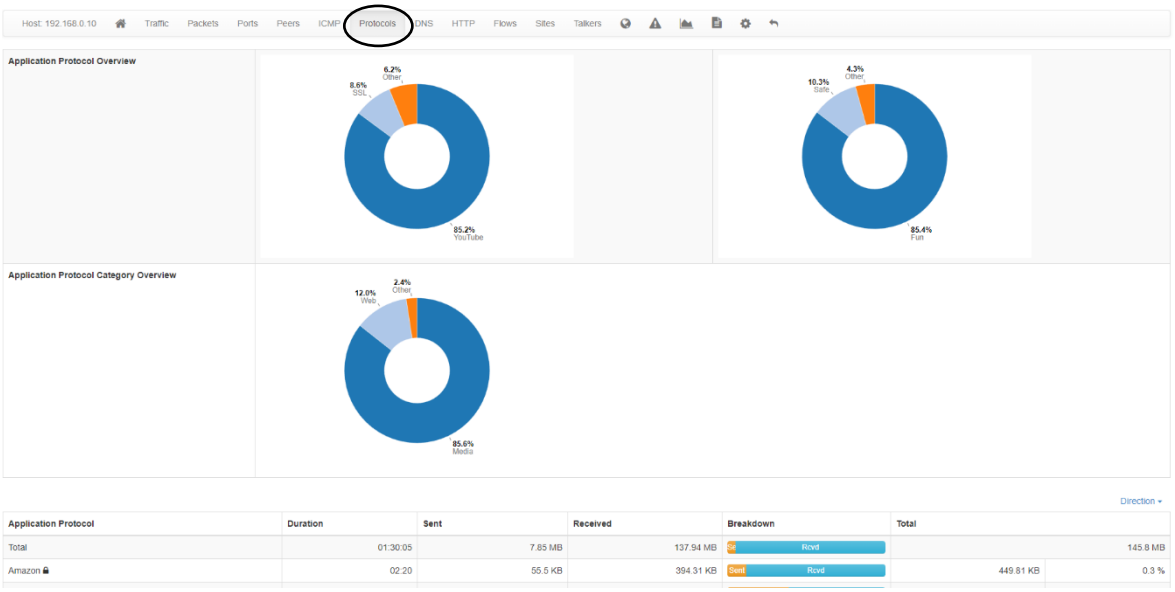


Kuva 9. IP-osoitekohtainen yleisnäkymä.

Lisäksi löytyy näkymiä liikenteelle, käytetyille protokollille ja porteille.

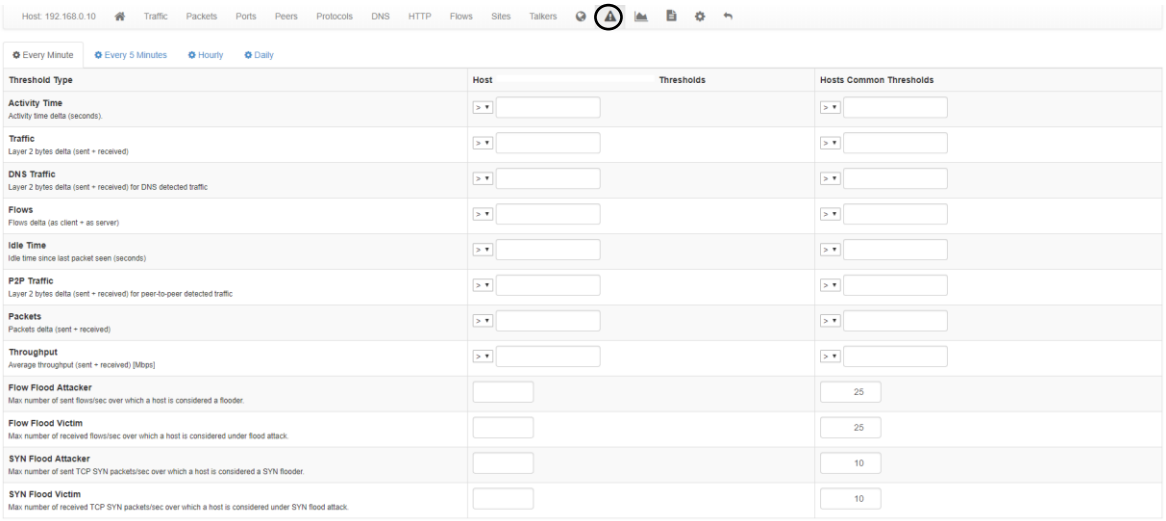


Kuva 10. Liikennenäkymä IP-osoitteelle.



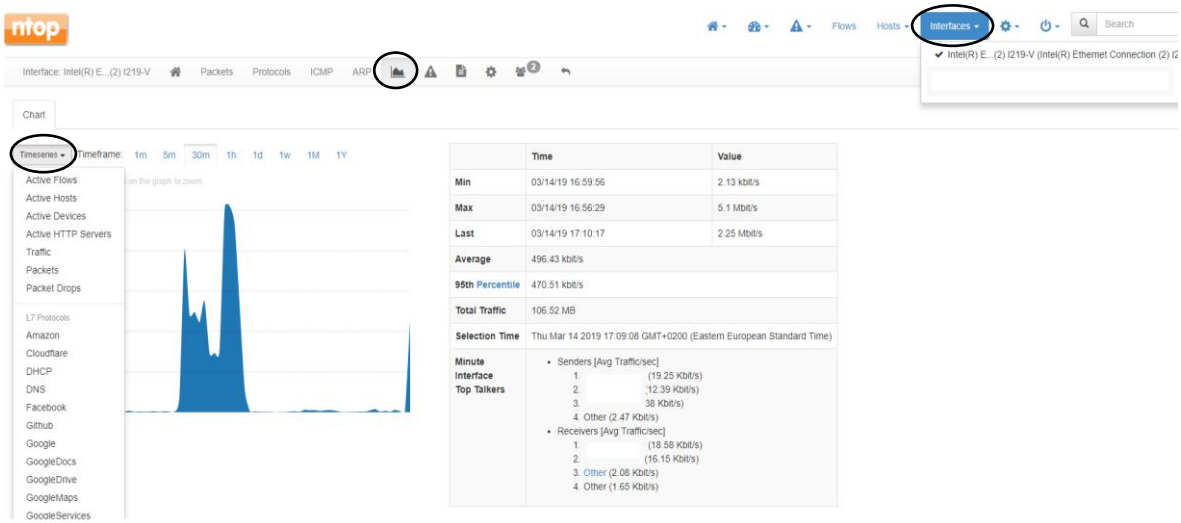
Kuva 11. Protokollanäkymä IP-osoitteelle.

Näkymästä löytyy myös Alerts-kohta, josta voidaan asettaa erilaisia raja-arvoja, jolloin syntyy varoitus kyseiselle IP-osoitteelle tai verkolle.



Kuva 12. IP-osoite tai verkkokohtainen Alarm-kohta.

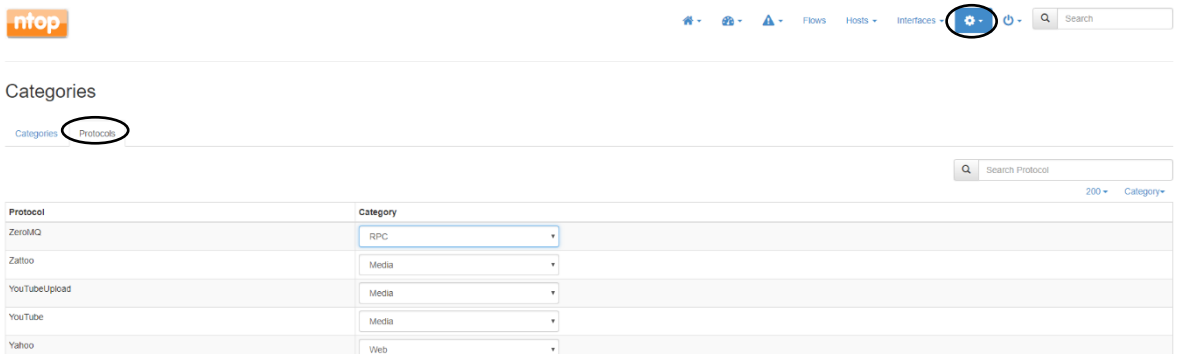
Samanlaiset näkymät löytyvät myös koko verkolle. Koko verkon liikennenäkymässä voidaan erotella vielä tarkemmin näkyvyyttä eri sovellusten perusteella.



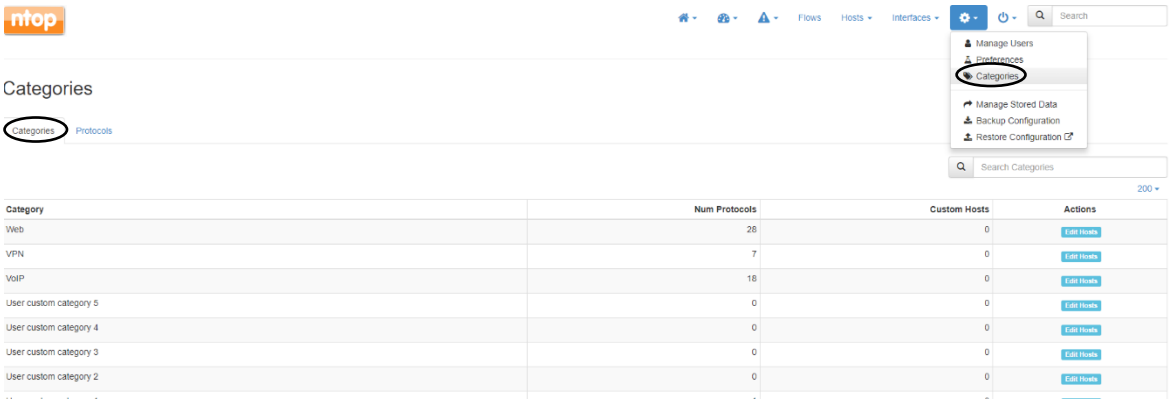
Kuva 13. Koko verkon liikenteen näkyvyys.

3.6.6 Categories

Categories-sivulta löytyvät kaikki ntopng-ohjelman tunnistamat protokollat ja sovellukset, sekä luokittelukategoriat. Protokollia ja sovelluksia on listassa 238 kappaletta ja niitä on laidasta laitaan. Jokaiseen kategoriaan voidaan myös itse lisätä IP-osoitteita. Jokaisen protokollan tai sovelluksen kategoriaa voidaan myös muokata haluttaessa ja omat kategoriat ovat myös mahdollisia.



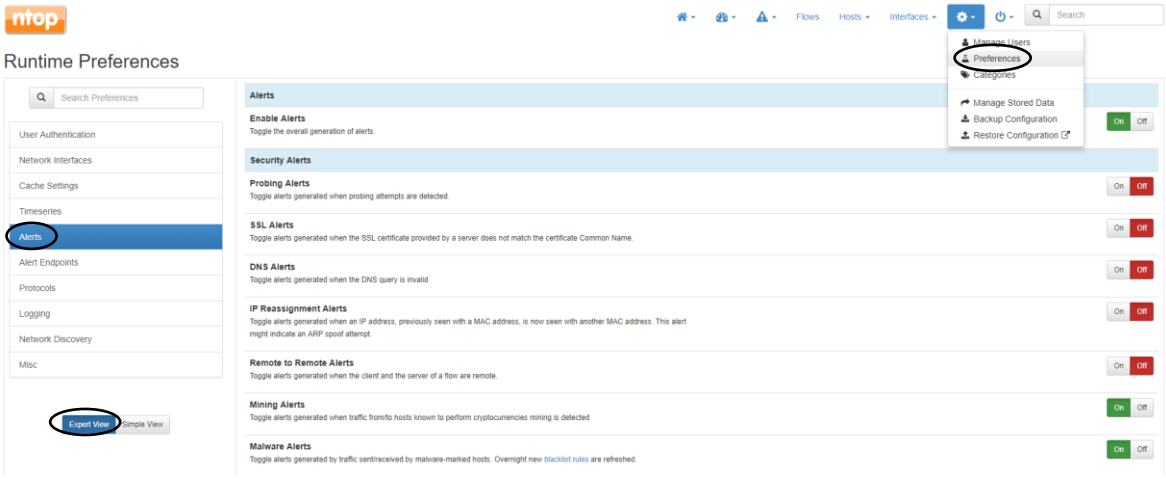
Kuva 14. ntopng-ohjelman tunnistamat protokollat ja sovellukset.



Kuva 15. ntopng-ohjelmaan luodut kategoriat.

3.6.7 Preferences

Preferences-valikosta löytyy paljon muokattavia perusasetuksia, kuten käyttäjien kirjautumisen asetuksia, flow-tietojen säilymiseen liittyviä asetuksia, varoitusten luomisen asetuksia ja lokitietojen asetuksia.



Kuva 16. Alerts-asetukset Preferences-valikossa.

4 EXTREME NETWORKS

4.1 Yrityksestä

Extreme Networks on vuonna 1996 perustettu amerikkalainen tietoliikenneverkkoratkaisuja valmistava yritys, kuten Cisco Sytems. Extreme Networks -yrityksen tuotteet ja ratkaisut on suunnattu korkean toimintavarmuuden ja suorituskyvyn haluaville asiakkaille. Yrityksen asiakaskunta koostuu lähinnä suurista organisaatioista kuten pankeista, teleyhtiöistä ja sairaaloista. Yritys pyrkii rajoja rikkovaan ajatteluun, ja yrityksellä on kolme vaatimusta laitteilleen: redundanttisuus, suorituskyky ja skaalautuvuus. (Extreme Networks [Viitattu 17.3.2019].)

4.2 Extreme Management Center

Extreme Management Center on lähinnä yrityksen sisäverkon tai datakeskusten hallintaan tehty tuote. Siihen pystytään liittämään eri tuotteita kuten ExtremeControl, ExtremeAnalytics ja ExtremeConnect, joilla voidaan verkkoliikenteen analysoinnin lisäksi hallita verkkolaitteita. Näin ollen kaikki hallintaan ja monitorointiin liittyvät työkalut saadaan kätevästi saman jaetun käyttöliittymän alle. Sen päätarkoitus on helpottaa ja vähentää hallintaan liittyviä tehtäviä, varoittaa ongelmista ja saada verkosta tehokas kokonaiskuva. (Extreme Networks [Viitattu 19.3.2019].)

4.3 ExtremeAnalytics

ExtremeAnalytics on Extreme Networks -yrityksen luoma verkkopohjainen ohjelmisto, jonka tarkoituksena on antaa käyttäjälleen kattava näkyvyys omaan verkkoonsa ja mahdollistaa sovellusten analysointi. Se kerää verkossa liikkuvaa dataa reaaliaikaisesti. Ohjelmiston tarkoitus on pyrkiä kertomaan, kuka käyttää ja mitä käyttää. Tarkan näkyvyyden kautta saadaan tietoa mahdollisista turvallisuusriskeistä ja häiriöistä. Ohjelmiston on tarkoitus olla myös helppokäyttöinen ja selkeä. Sen pääominaisuuksiin voidaan lukea visuaalisuus, muokattavuus ja näkyvyys. (Extreme Networks [Viitattu 16.3.2019].)

Näkyvyyden tehokkuus toteutetaan yli 7000 sovelluksen ja 13000 sormenjäljen muodostamalla Fingerprints-tietokannalla, jota ylläpidetään aktiivisesti ja johon pystytään myös itse lisäämään omia merkintöjä. Sovellusten tunnistaminen perustuu DPI-teknologiaan, joka pyrkii kertomaan tarkasti, mikä sovellus on kyseessä. (Extreme Networks [Viitattu 18.3.2019].)

4.4 PV-FC-180-laite

PV-FC-180-laite eli Purview Application Sensor -laite pohjautuu Extreme Networks -yrityksen kytkimiin. Siihen on jätetty vain 4 kappaletta 10G SFP+ -porttia. Laite toimii kokonaisuudessa Sensor-laitteena eli se vastaanottaa mirror-toiminnolla peilatun liikenteen kokonaisuudessa ja luo siitä NetFlow-tiedot, jotka se välittää eteenpäin. (Extreme Networks [Viitattu 17.3.2019].)

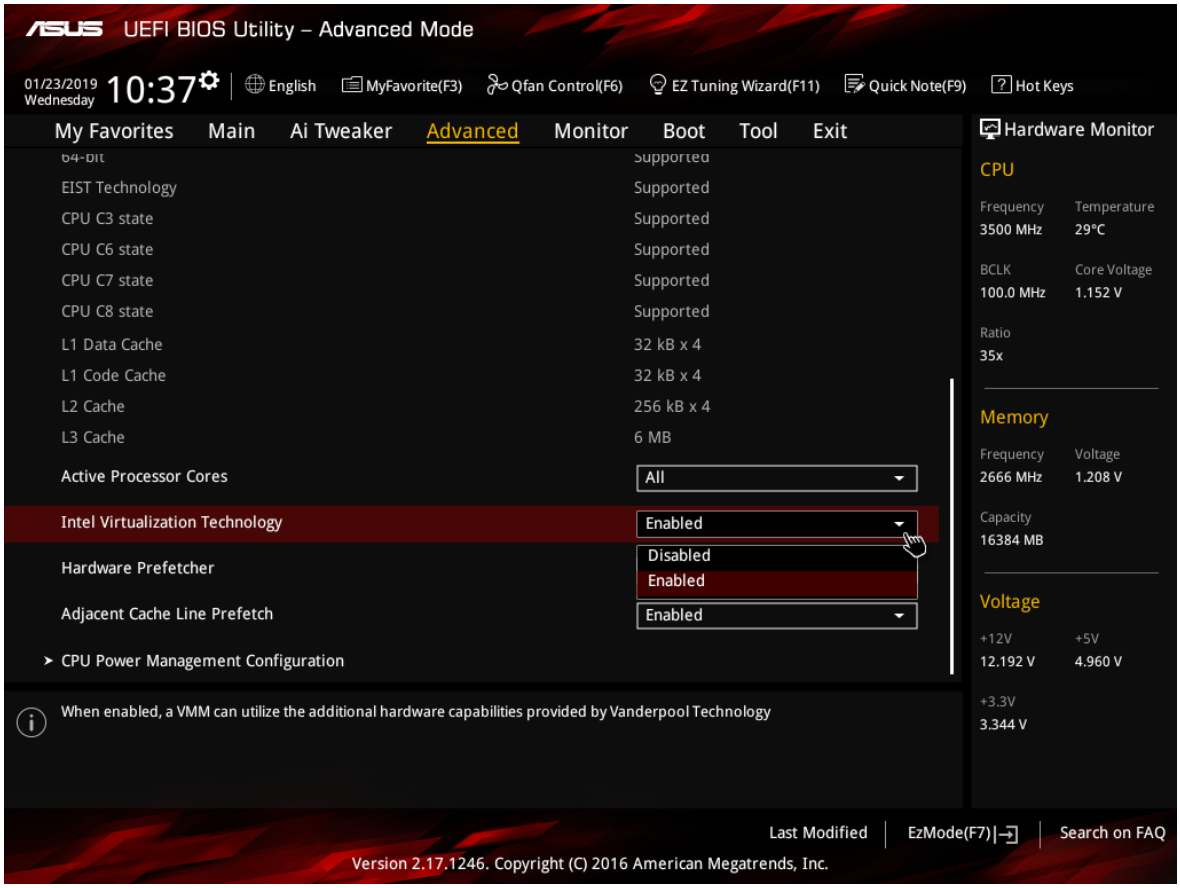
4.5 Asennus

Liikenteen keräämisen ja analysoinnin testaukseen saatiin laitevalmistajalta PV-FC-180 Flow Sensor -laite, Extreme Management Center -palvelin ja ExtremeAnalytics-palvelin. Palvelimille oli olemassa oma laitteensa, mutta testauksen helpottamisen vuoksi päädyttiin asentamaan ne virtuaaliympäristöön toimistossa ylimääräisenä olevalle koneelle. Palvelimista oli olemassa omat tiedostot Windowsin omalle Hyper-V-ohjelmalle ja VM-Ware-ohjelmalle. Testauksessa päädyttiin käyttämään Hyper-V-ohjelmaa. Koneen keskusmuistin ja prosessorin ytimien riittävyys tuli myös esille palvelimia asennettaessa, mutta kysyttäessä laitevalmistajalta ne olivat testaukseen kuitenkin riittävät. Palvelinten vaatima teho riippuukin hyvin pitkälti analysoitavan verkon FPM-arvosta eli Flows per Minute -arvosta eli käytännössä siitä, kuinka paljon verkossa on liikennettä ja minkä tyyppistä liikenne on. Tähän arvoon perustuu myös lisensointi, joka kokonaisuuteen tulee hankkia.

4.5.1 Hyper-V-asennus

Ennen Hyper-V-ominaisuuden asennusta tuli varmistaa BIOS-asetuksista, että prosessorin virtualisointiasetus on päällä.

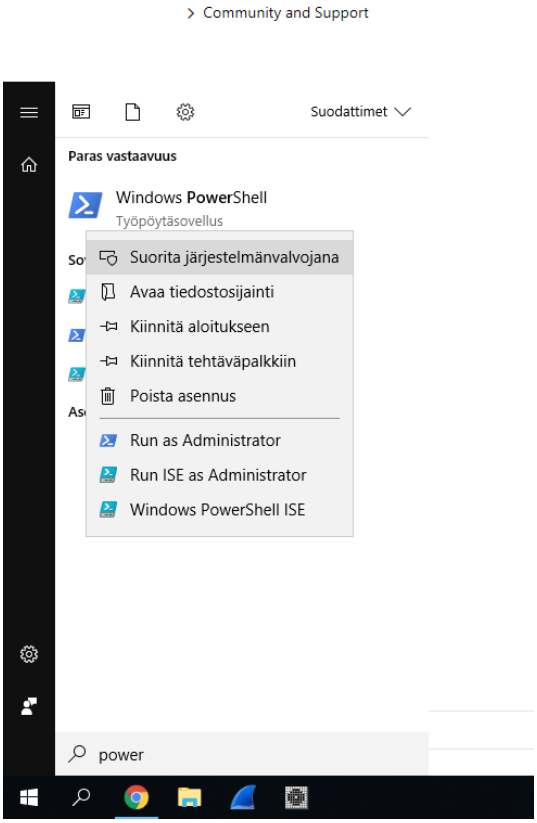
1. BIOS-asetuksiin päästään käsiksi F2- tai DEL-näppäintä painettaessa tietokoneen käynnistyessä. Asetus löytyi kyseisessä tietokoneessa Advanced-välilehden alta.



Kuva 17. Palvelinkoneen virtualisointiasetus.

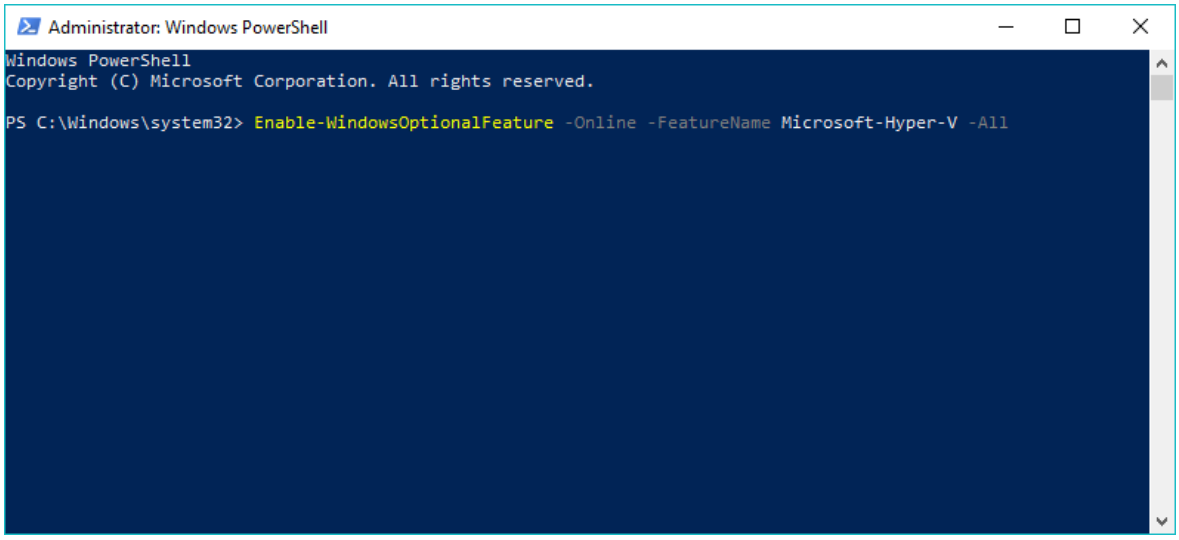
Hyper-V-ominaisuuden asennus onnistui kätevästi, sillä se löytyy kaikista Windows 10 Enterprise-, Pro- ja Education-versioista valmiina. Se täytyy vain aktivoida ja tämä onnistuu helposti Windows PowerShell -ohjelman kautta.

2. PowerShell täytyy avata järjestelmänvalvojana, että komento menee läpi.



Kuva 18. Avataan Windows PowerShell -ohjelma järjestelmänvalvojana.

3. PowerShell-ohjelmaan syötetään komento: Enable-WindowsOptional-Feature -Online -FeatureName Microsoft-Hyper-V -All



Kuva 19. Komento Hyper-V-ominaisuuden asennukseen.

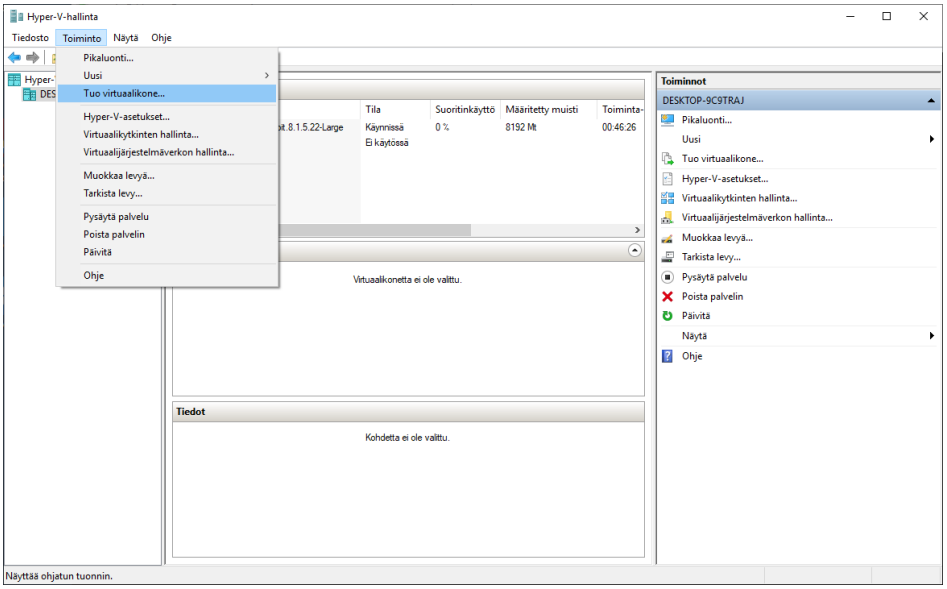
4. Asennukseen jälkeen tietokone täytyy käynnistää uudestaan.

Tämän jälkeen Hyper-V-ohjelma löytyy tietokoneelta ja virtuaalipalvelimien asennus voidaan aloittaa.

4.5.2 Extreme Management Center asennus

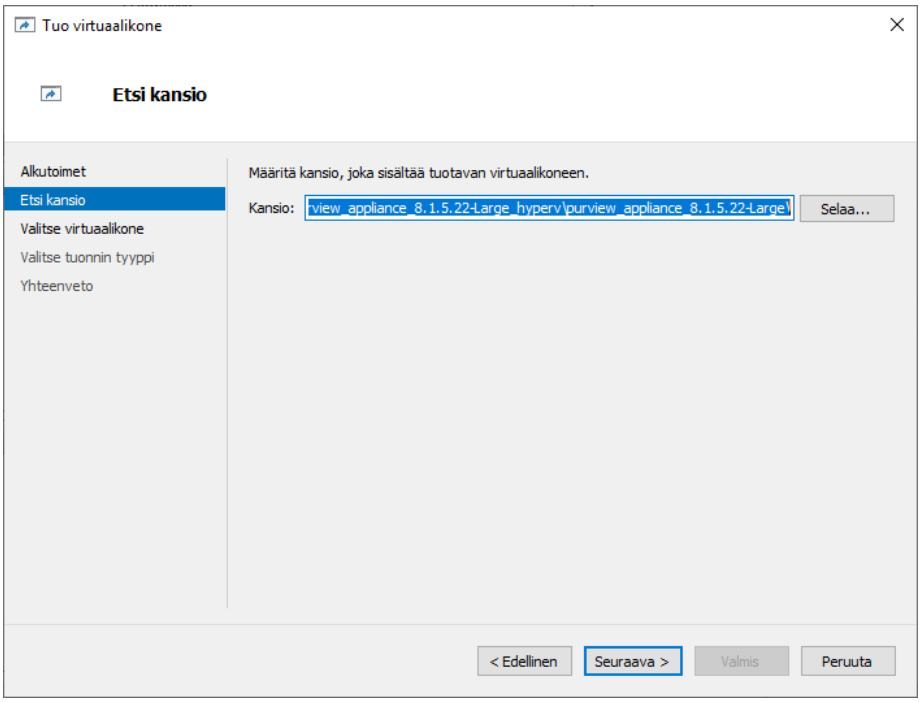
ExtremeAnalytics-palvelinta ennen tuli asentaa Extreme Management Center -palvelin, joka toimii pohjana Extreme Applications -tuotteille. Tässä tapauksessa ei ollut kuitenkaan tarvetta asentaa muita tuotteita. Virtuaalipalvelimille saatiin laitevalmistajalta valmiit tiedostot, jotka pystyttiin suoraan tuomaan Hyper-V-ohjelmalle.

1. Asennus aloitettiin avaamalla Hyper-V-hallintaohjelma ja tuomalla virtuaalipalvelin.



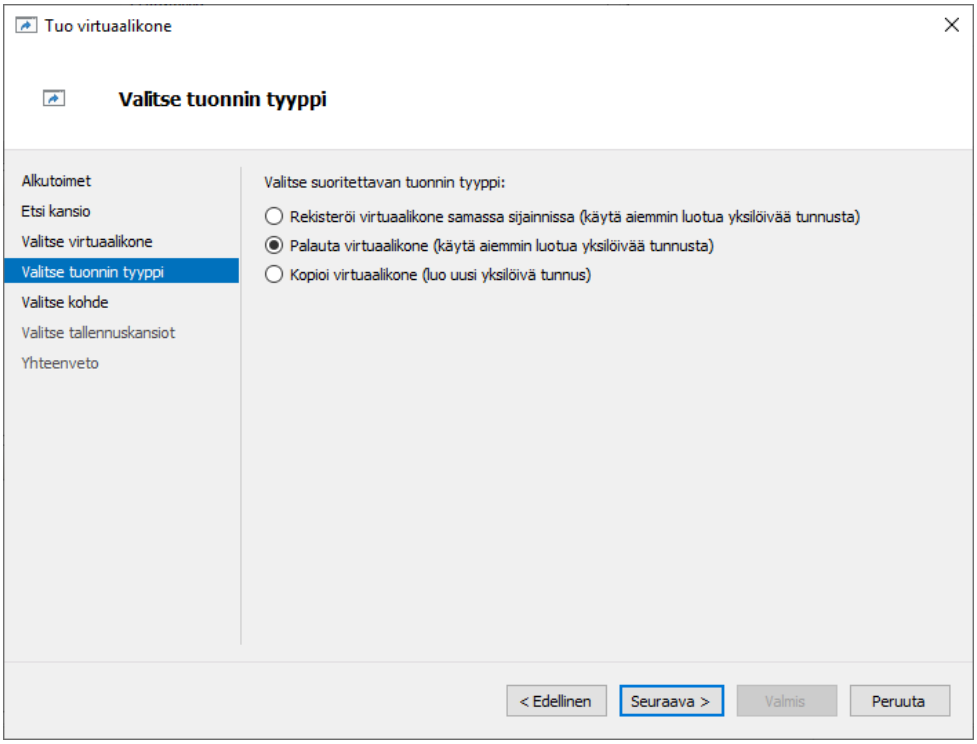
Kuva 20. Palvelimen tuonti löytyy Toiminto-valikosta

2. Alkutoimet-välilehti ohitetaan suoraan painamalla Seuraava-painiketta.
3. Etsi kansio -välilehdessä etsitään Selaa-painikkeella haluttu tiedosto tuontiin.



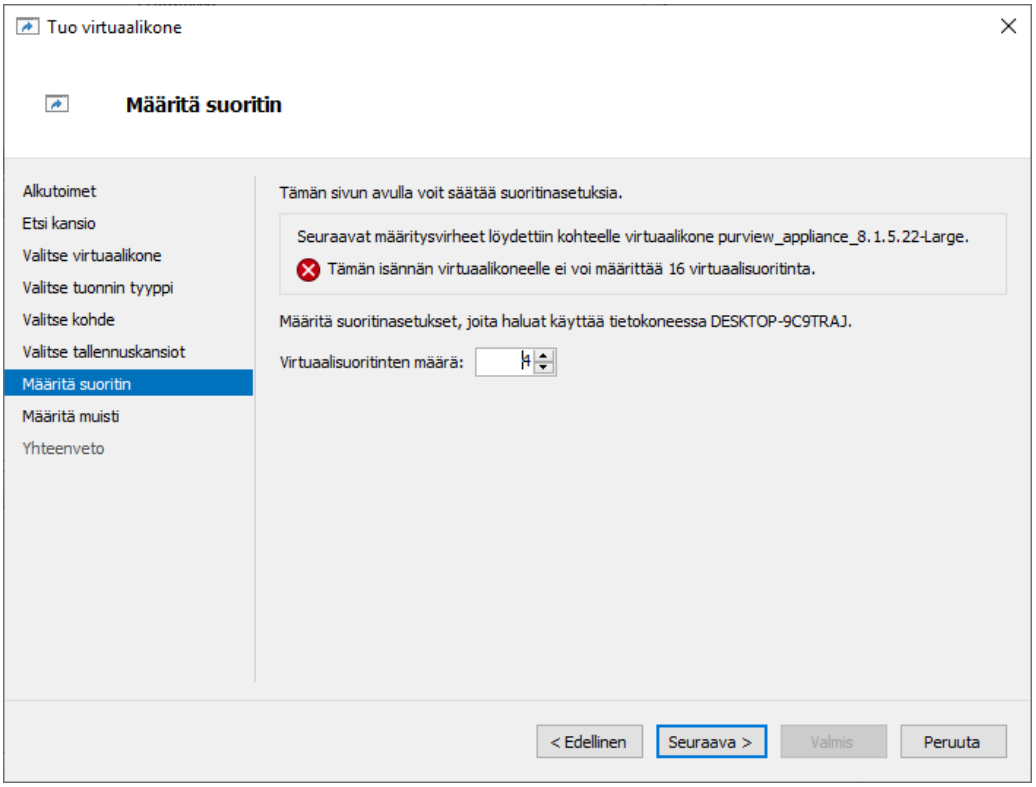
Kuva 21. Valitaan tiedosto, joka halutaan tuoda.

4. Valitse virtuaalikone -välilehdessä on virtuaalikone jo valittuna ja jatketaan Seuraava-painikkeella.
5. Valitse tuonnin tyyppi -välilehdessä valitaan virtuaalikoneen palautus.



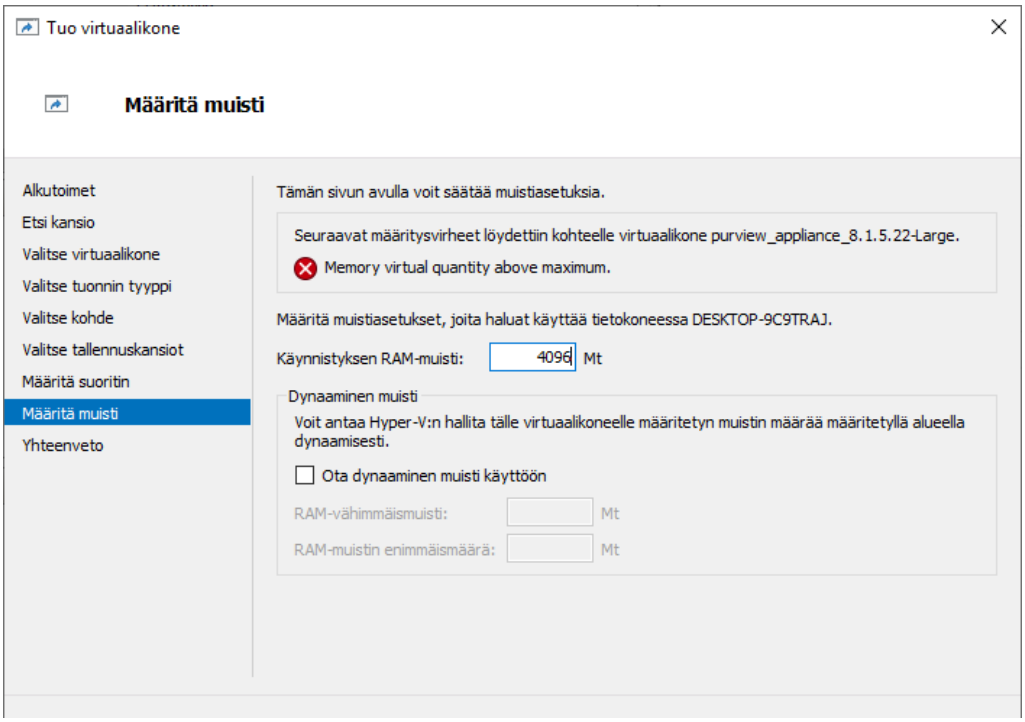
Kuva 22. Valitaan kohta "Palauta virtuaalikone"

6. Valitse virtuaalikonetiedostojen kansiot -välilehdellä mennään oletusasetuksilla eli jatketaan Seuraava-painikkeella.
7. Valitse virtuaalikiintolevyjen tallennuskansio -välilehdellä mennään myöskin oletuksella, jatketaan Seuraava-painikkeella.
8. Määritä suoritin -välilehdellä on oletuksen valittuna 16 virtuaalisuoritinta. Testikoneesta ei kuitenkaan löytynyt kuin 4 ydintä, joten asetetaan asetus siihen.



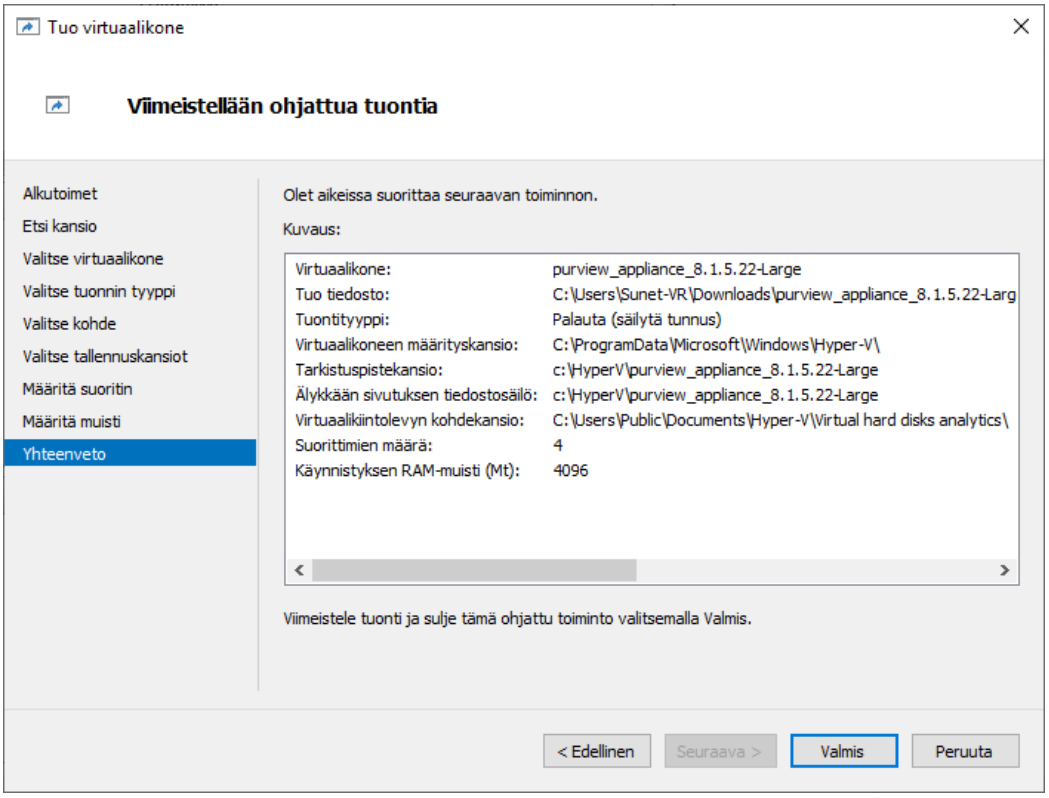
Kuva 23. Määritetään virtuaalisuoritinten määräksi 4.

9. Määritä muisti -välilehdellä on myös oletusasetus liian korkealla. Tähän vaihdetaan määräksi 4096 Mt.



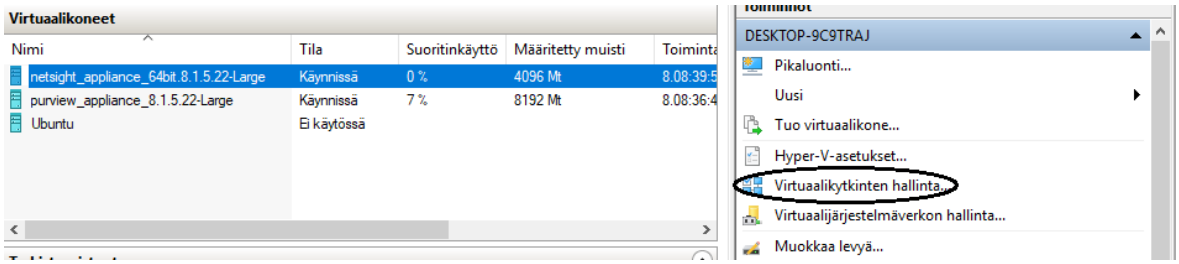
Kuva 24. Muistiksi määritetään 4096 Mt.

10. Viimeisellä välilehdellä eli Yhteenveto-välilehdellä voidaan vielä tarkistaa tehdyt määritykset. Tästä edetään Valmis-painikkeella.



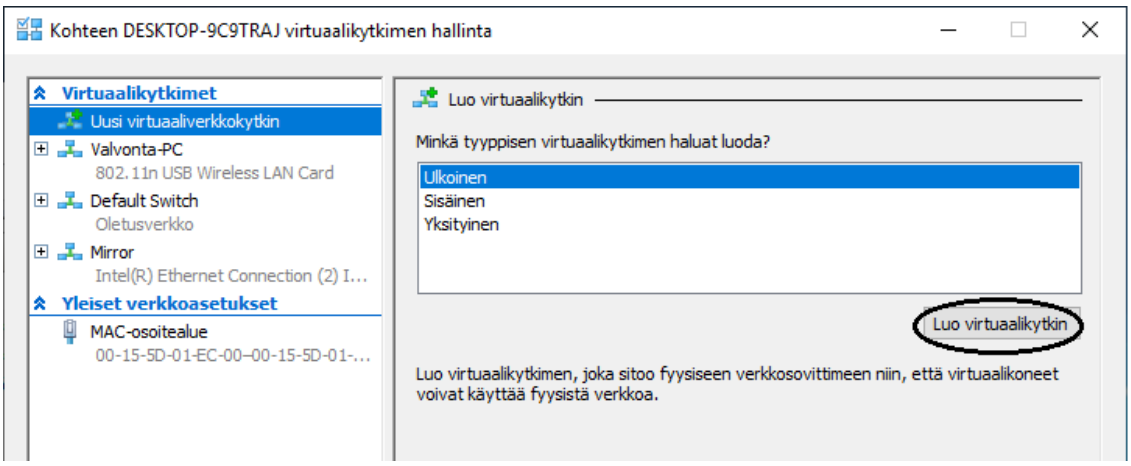
Kuva 25. Yhteenvedossa voidaan vielä tarkistaa asetukset.

11. Tämän jälkeen luotu virtuaalipalvelin avautuu Virtuaalikoneet-listaan ja on valmis käynnistettäväksi. Sille on kuitenkin vielä luotava virtuaaliverkko-kytkin, että se voi käyttää tietokoneen verkkoa. Luonti onnistuu painamalla Virtuaalikytkinten hallinta -painiketta.



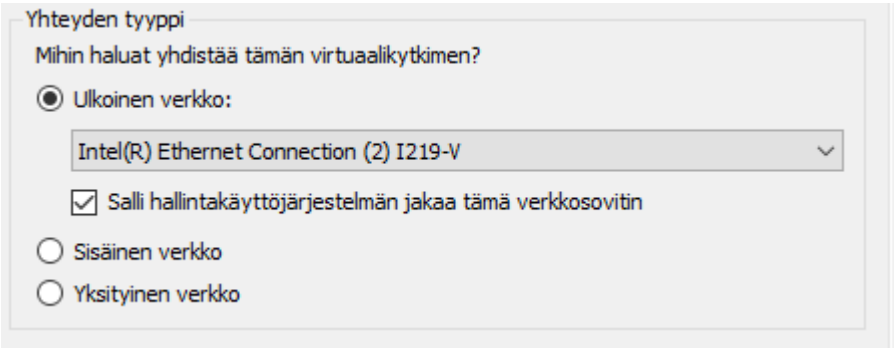
Kuva 26. Virtuaalikytkinten hallinta -painike.

12. Tyypiksi valitaan Ulkoinen ja painetaan Luo virtuaalikytkin -painiketta.



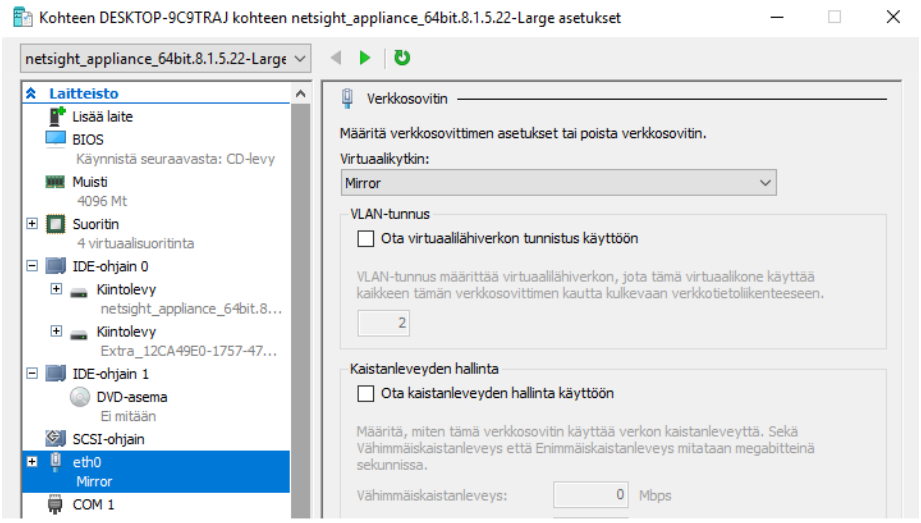
Kuva 27. Uuden virtuaaliverkkokytkimen luonti.

13. Seuraavaksi valitaan virtuaalikytkimelle oikea verkkokortti pudotusvalikosta. Virtuaalikytkin voidaan myös nimetä helpottamaan tunnistusta.



Kuva 28. Oikean verkkokortin valinta.

14. Virtuaalikytkin täytyy vielä asettaa käyttöön virtuaalipalvelimen asetuksista. Asetuksiin pääsee valitsemalla oikea virtuaalipalvelin ja painamalla hiiren oikeaa painiketta ja valitsemalla Asetukset.
15. Käyttöönotto onnistuu valitsemalla Laitteisto-listasta verkkokortin ja vaihtamalla Virtuaalikytkin-pudotusvalikkoon äskettäin luotu virtuaalikytkin.



Kuva 29. Virtuaalikytkimen valinta virtuaalipalvelimen asetuksista.

16. Seuraavaksi virtuaalipalvelin voidaan käynnistää painamalla sitä hiiren oikealla painikkeella ja valitsemalla kohta Yhdistä. Aukeavasta ikkunasta valitaan Käynnistä, jolloin virtuaalipalvelin käynnistyy. Seuraavaksi voidaan jatkaa asetusten määrittämistä itse palvelimelle.
17. Virtuaalipalvelimeen pääsee kirjautumaan käyttäjätunnuksella root ja ilman salasanaa. Salasana täytyy tämän jälkeen vaihtaa omaan.
18. Virtuaalipalvelimelle asetetaan seuraavaksi perusverkkoasetukset, kuten IP-osoite, aliverkkomaski ja oletusyhdyskäytävä. Kohdat nimipalvelimille ja NIS-palvelimelle jätettiin tyhjäksi.

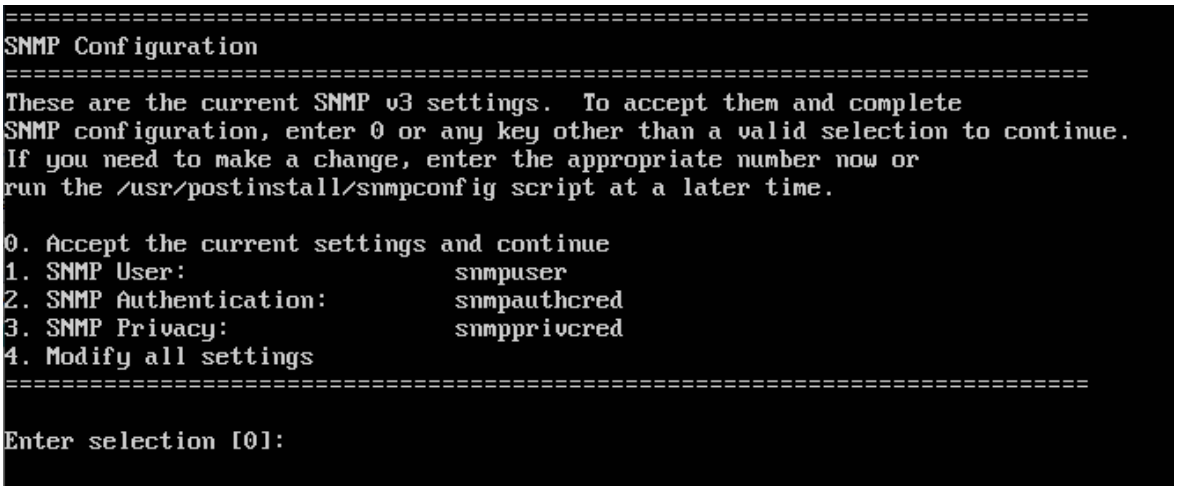
```
================================================================================
Confirm Network Settings
================================================================================
These are the settings you have entered. Enter 0 or any key other than a
valid selection to continue. If you need to make a change, enter the
appropriate number now or run the /usr/postinstall/dnetconfig script at a
later time.
================================================================================

0. Accept settings and continue
1. Hostname:            management
2. IP address:          192.168.70.11
3. Netmask:             255.255.255.0
4. Gateway:             192.168.70.1
5. Nameserver:
6. Domain name:
7. NIS Server/Domain:

Enter selection [0]:
```

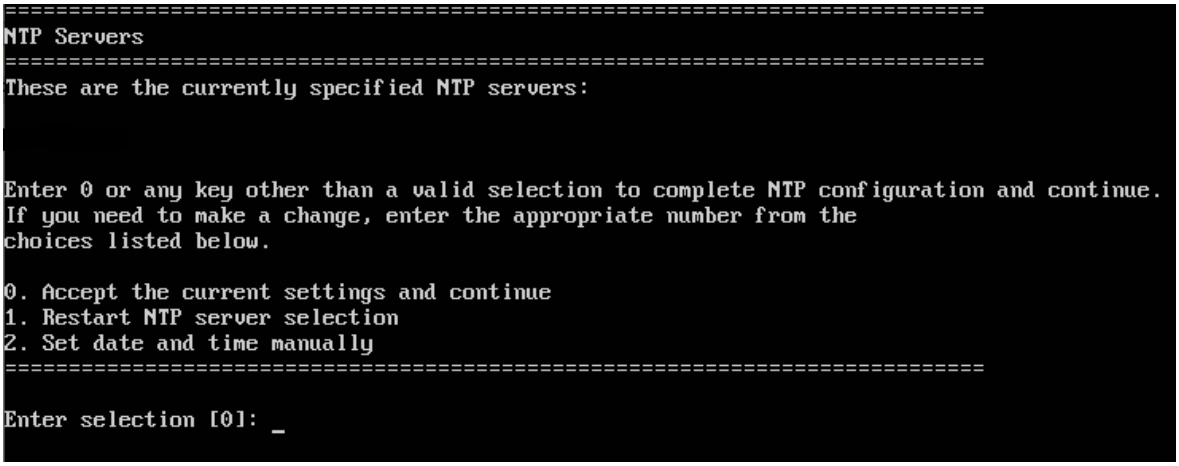
Kuva 30. Management Center -palvelimen verkkoasetukset.

19. Seuraavaksi asetetaan SNMP-asetukset, jotka jätetään oletuksiksi.



Kuva 31. Management Center -palvelimen SNMP-asetukset.

20. Tämän jälkeen voidaan asettaa NTP-palvelimen asetukset.



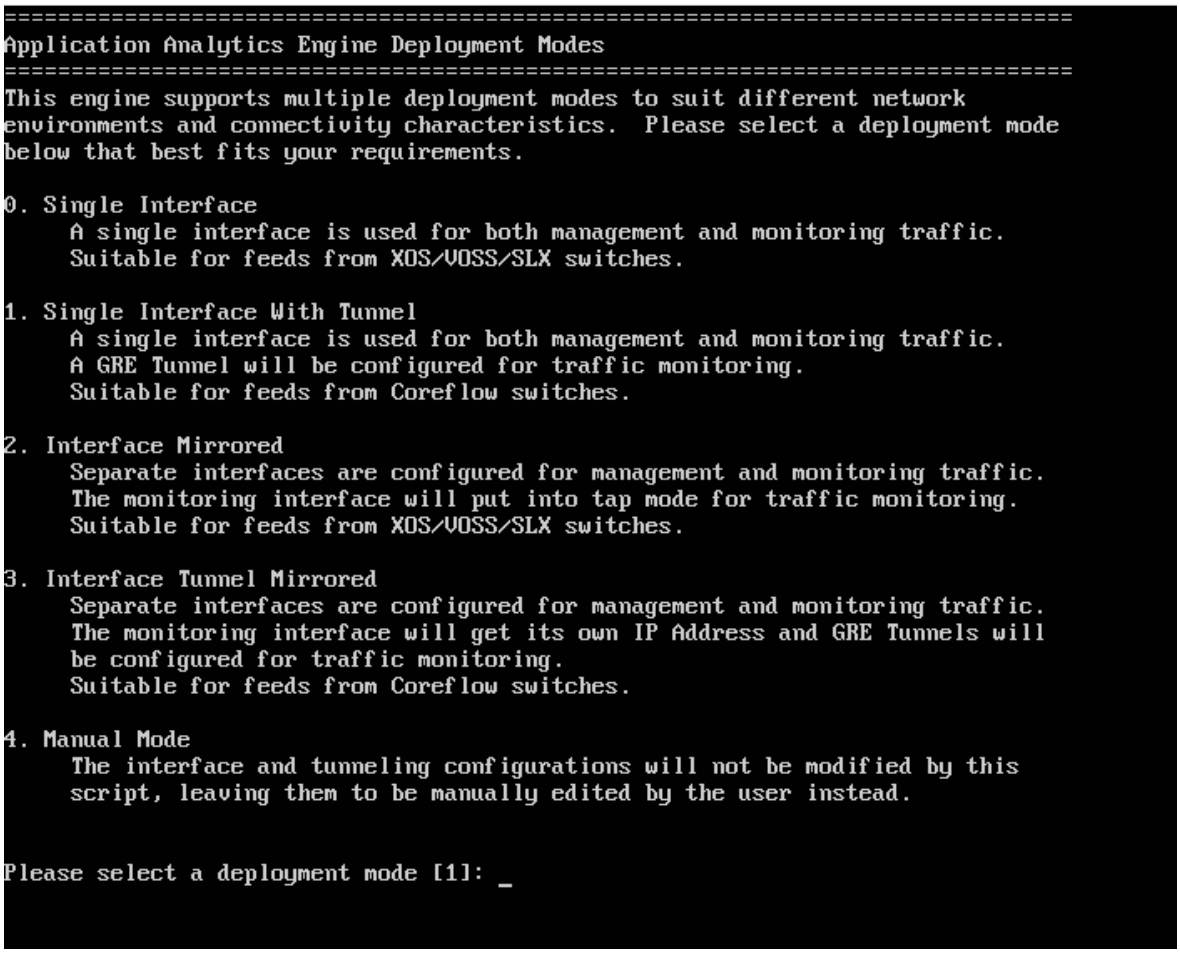
Kuva 32. Management Center -palvelimen NTP-palvelimen asetukset.

21. Lopuksi asetukset voidaan vielä tarkistaa ja aloitetaan asennus. Asennuksen jälkeen virtuaalipalvelin on käyttövalmis ja voidaan siirtyä Analytics-palvelimen asennukseen.

4.5.3 ExtremeAnalytics-asennus

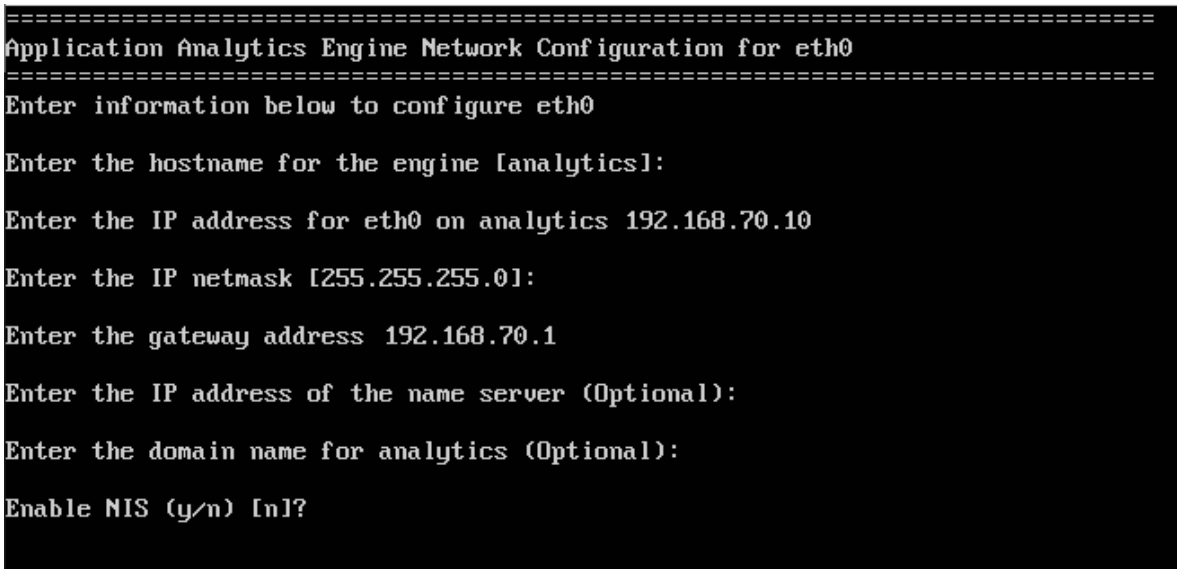
ExtremeAnalytics-palvelimen tuominen Hyper-V-ohjelmaan tapahtuu samalla tavalla, kun Extreme Management Center -palvelimen. Kun tuonti on valmis, voidaan virtuaalipalvelin käynnistää ja aloittaa asetusten tekeminen.

1. Virtuaalipalvelimen käynnistettyä siihen pääsee myös kirjautumaan käyttäjätunnuksella root ja ilman salasanaa. Salasana tulee taas vaihtaa.
2. Tämän jälkeen valitaan käyttöönottotapa palvelimelle. Tässä tapauksessa valitaan Single Interface With Tunnel -tapa, sillä se on testauksen kannalta helpoin toteuttaa.



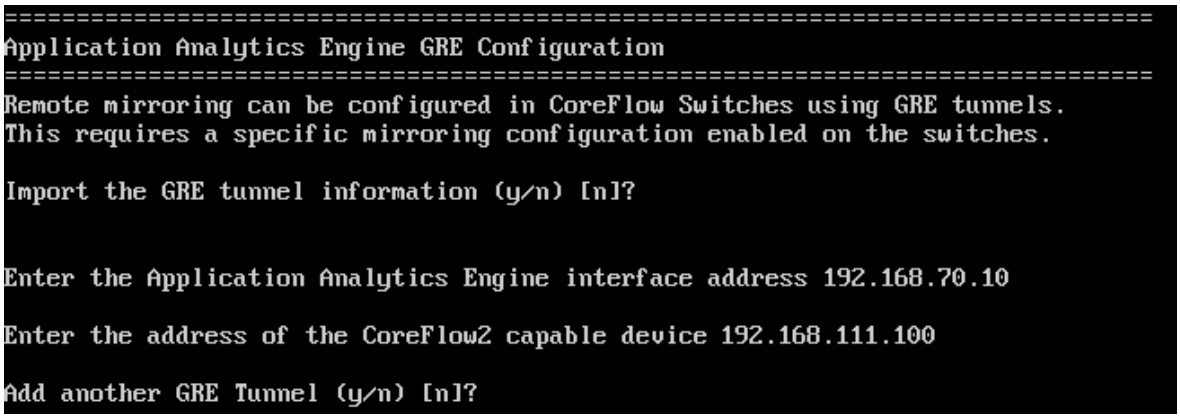
Kuva 33. Analytics-palvelimen käyttöönottoasetus.

3. Seuraavaksi palvelimelle asetetaan taas perusverkkoasetukset.



Kuva 34. Analytics-palvelimen verkkoasetukset.

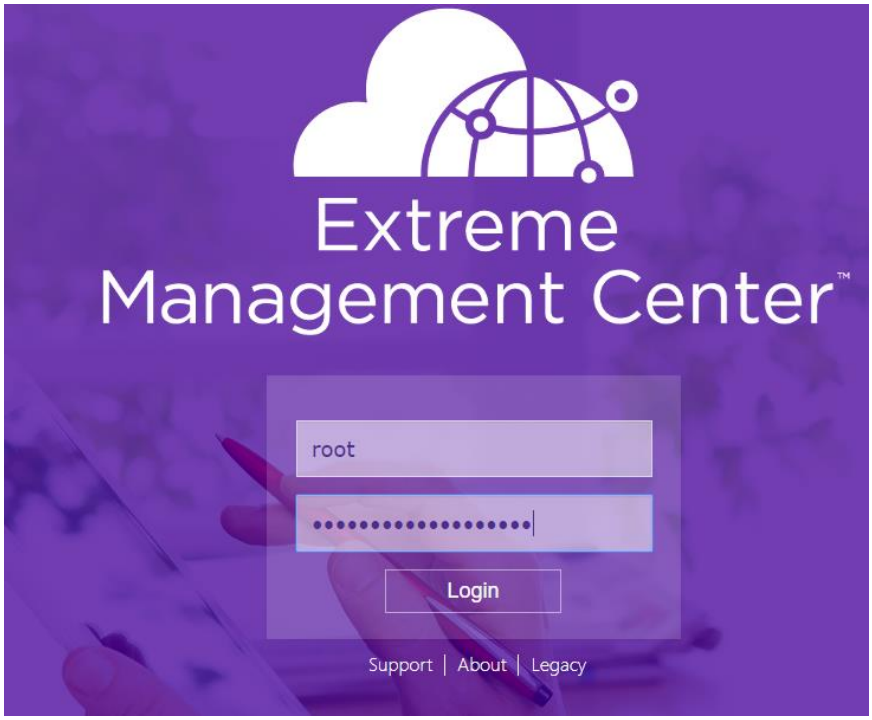
4. Seuraavaksi määritetään GRE-tunnelin asetukset. Tunnelin alkupisteeksi laitetaan Flow Collector -laite ja loppupisteeksi Analytics-palvelin. Näin mirror-toiminnolla liikenteestä luodut Flow-tiedot saadaan ohjattua GRE-tunnelia pitkin analysoitavaksi.



Kuva 35. Analytics-palvelimen GRE-tunnelin asetukset.

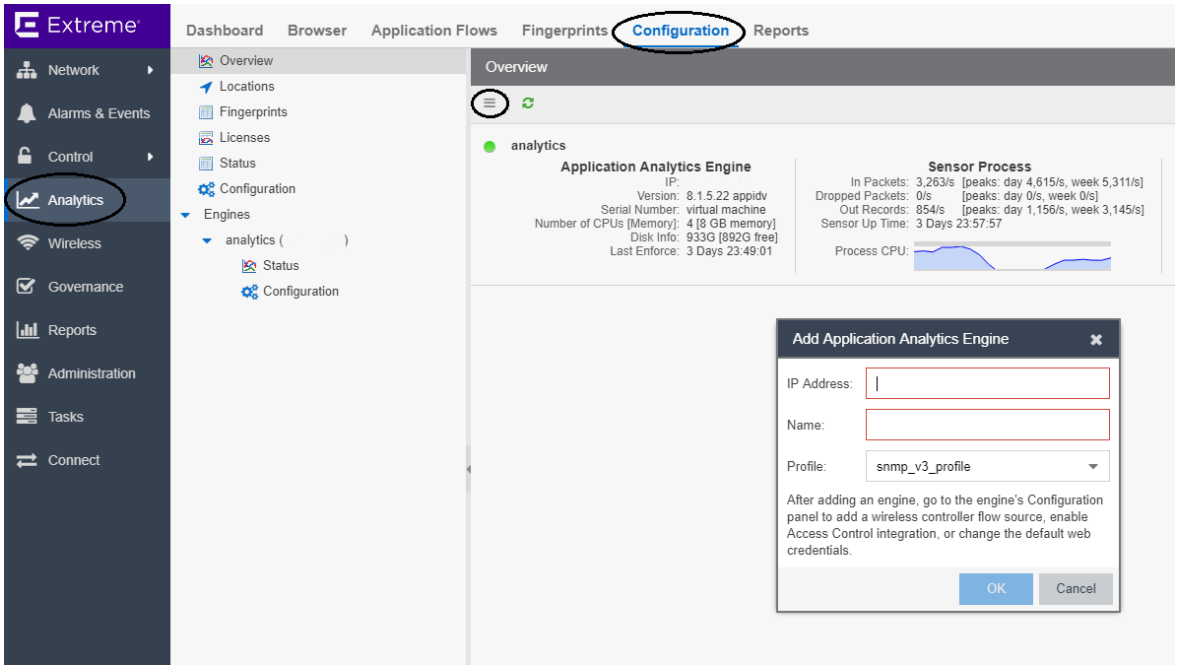
5. Lopuksi palvelimelle määritetään SNMP- ja NTP-asetukset, kuten Management Center -palvelimessakin. Tämän jälkeen asennus käynnistyy ja Analytics-palvelin on käyttövalmis.

6. Nyt kun kumpikin palvelin on asennettuna, voidaan Analytics-palvelin liittää Management Center -palvelimeen. Tämä onnistuu avaamalla Client-koneella selainikkuna ja kirjoittamalla hakukenttään **http://<palvelimen_ip>:8080/**. Tässä ”palvelimen_ip” on Management Center -palvelimelle itse asettettu IP-osoite.
7. Kirjautumaan pääsee käyttäjätunnuksella root ja salasana on itse asetettu. Ensimmäisellä kirjautumisella palvelin pyytää lisenssiavainta, joka on tässä tapauksessa saatu suoraan laitevalmistajalta.



Kuva 36. Kirjautuminen Management Center -palvelimelle.

8. Analytics-palvelimen lisäys tehdään valitsemalla vasemmasta reunasta kohta Analytics ja yläreunasta kohta Configuration. Tämän jälkeen painetaan pudotusvalikko-kuvaketta ja valitaan Add Engine. Tähän syötetään Analytics-palvelimelle asetettu IP-osoite ja nimi. Nyt palvelimet on yhdistetty.

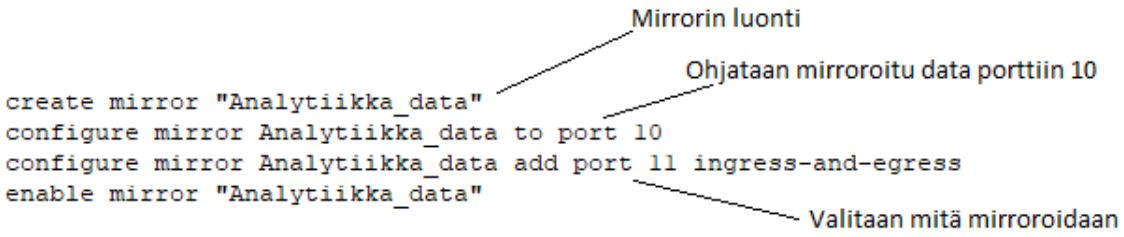


Kuva 37. Analytics-palvelimen lisäys Management Center -palvelimeen.

4.5.4 PV-FC-180-asennus

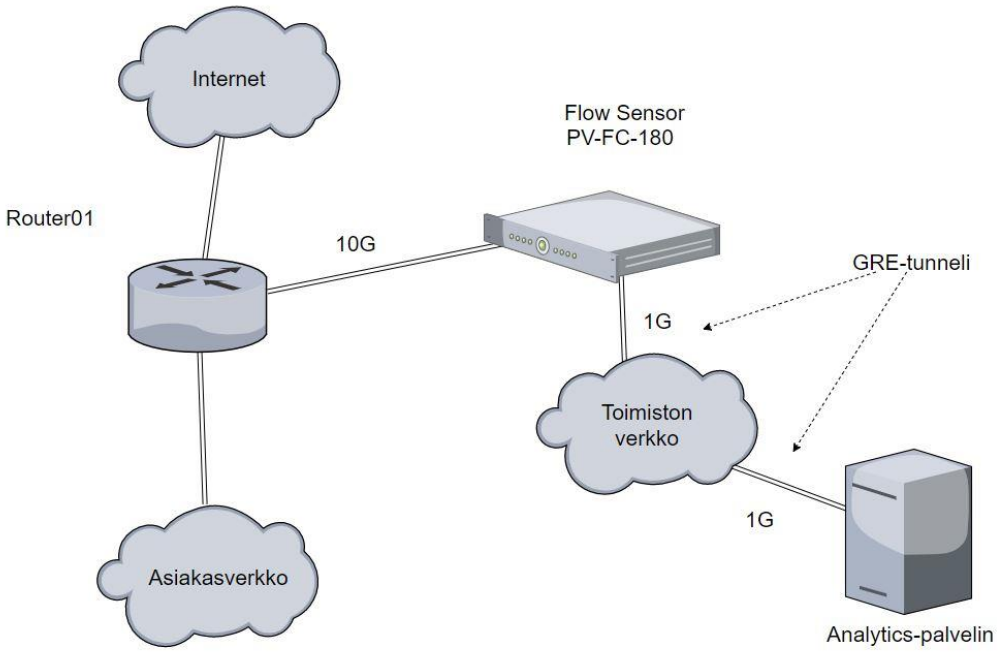
Kuva 38. Extreme Networks -valmistajan PV-FC-180-laite.

PV-FC-180-laite sijoitettiin Sunetin laitetilaan runkoreitittimen läheisyyteen. Runko-reitittimessä, joka on myöskin Extreme Networks -valmistajan, luotiin peilaus mirror-toiminnolla portista, josta Sunetin asiakasliikenne lähtee verkosta maailmalle päin.



Kuva 39. Mirror-portin konfiguraatio reitittimessä.

Näin Flow Sensor -laitteelle saatiin luotua ”kopio” kaikesta Sunetin omasta asiakasliikenteestä. Tämä reitittimen portti yhdistettiin Flow Sensor -laitteelle 10G:n linkillä liikenteen suuren määrän takia. Flow Sensor -laitteelta yhteys palvelimille on luotu 1G:n linkillä ja se on toteutettu käyttäen GRE-tunnelia, jolloin hallinta ja liikenteen tuonti palvelimelle tapahtuu samaa kautta. GRE-tunneli tulee kuitua pitkin suoraan Sunetin toimistolle, jossa se kulkee Zyxel-kytkimen kautta palvelinkoneelle.



Kuva 40. Flow Sensor -laitteen ja Analytics-palvelimen kytkentäkaavio.

Laitteen konfigurointi muistuttaa läheisesti Cisco-valmistajan laitteita. Konfigurointiin saatiin laitevalmistajalta tukea ja ohjeet. Laitteen konsolikaapeli oli hukkunut matkalla, joten se täytyi tehdä uudestaan. Flow Sensor -laitteen konfigurointi toteutettiin oheisilla komennoilla.

1. Laitteeseen pääsi kirjautumaan käyttäjäntunnuksella: admin ja salasanana ei mitään. Aluksi laite tyhjättiin vanhoista konfiguraatioista komennolla clear config. Tämän jälkeen laite käynnistyy uudestaan.
2. Tyhjäyksen jälkeen laitteeseen päästiin syöttämään uutta konfiguraatiota, joka aloitettiin poistamalla oletus VLAN 1 kaikista porteista, luomalla uusi VLAN 100 ja asettamalla luotu VLAN 100 porttiin 1.

```
# vlan
clear vlan egress 1 *.*.*
set vlan create 100
set port vlan tg.1.1 100
```

Kuva 41. VLAN 100 luonti ja asetus porttiin 1.

3. Seuraavaksi luotu VLAN asetetaan defaultiksi.

```
# ip interface
set ip interface vlan.0.100 default
```

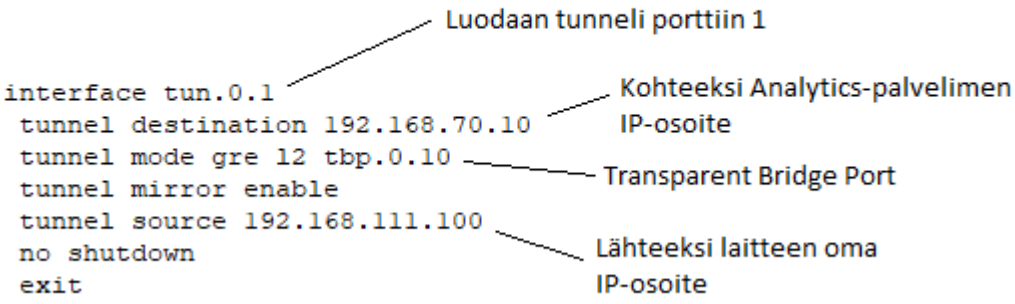
Kuva 42. Asetus defaultiksi.

4. Laitteelle määritetään IP-osoite ja oletusreitti. Komento ip forwarding on tärkeä, että liikenne pääsee ulos määritetystä portista.

```
configure terminal
!
 interface vlan.0.100
  ip address 192.168.111.100 255.255.255.0
  ip forwarding
  no shutdown
  exit
!
 # Static routes configured on routed interfaces
 ip route 0.0.0.0/0 192.168.70.1 interface vlan.0.100 1
```

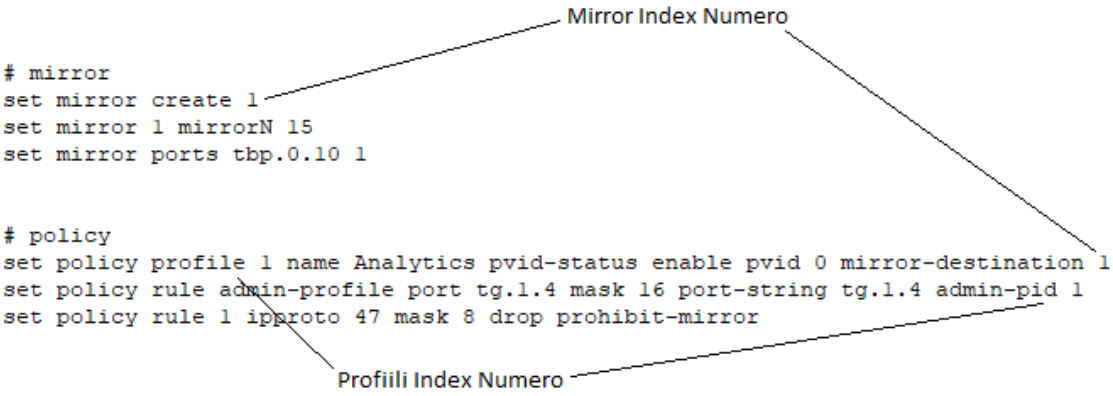
Kuva 43. Asetetaan IP-osoite ja oletusreitti.

5. Seuraavaksi luodaan GRE-tunneli, jota pitkin analysoitava liikenne kulkee palvelimelle. Tunnelille täytyy määrittää lähteeksi Flow Sensor ja kohteeksi Analytics-palvelin. Tässä tapauksessa voidaan käyttää transparent bridge port -asetusta, sillä käytössä on Application Analytics Sensor -laite.



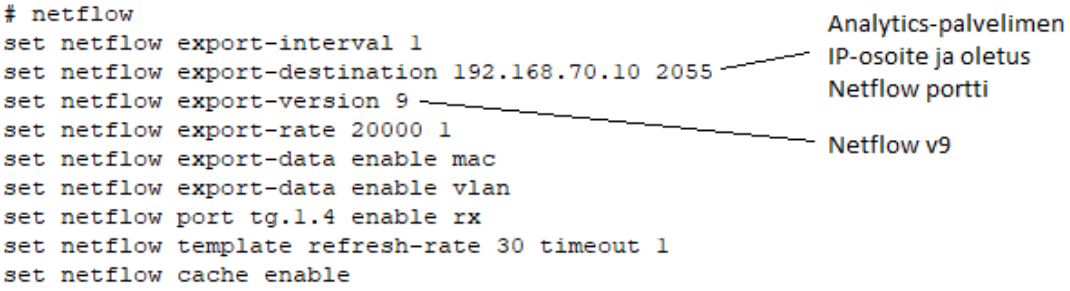
Kuva 44. GRE-tunnelin luonti.

6. Seuraavaksi määritetään, että reitittimeltä tulevista Flow-virtauksista otetaan ensimmäiset 15 pakettia ja ohjataan ne portin 1 kautta analysoitavaksi. Luoduissa säännöissä määritetään, että Flow-liikenteen ei tarvitse kulkea laitteen läpi ja varmistetaan, että laitteen sisällä kulkeva liikenne ei monistu. Tärkeä myös huomioida, että index-numerot täsmäävät.



Kuva 45. Luodaan mirror ja säännöt.

7. Netflow-protokolla konfiguroidaan laitteelle siten, että jokaisesta flow-virtauksesta, jonka reititin laitteelle lähettää, luodaan merkintä. Näistä Netflow-merkinnöistä otetaan 15 ensimmäistä pakettia ja ohjataan ne kohti Analytics-palvelinta.




```
# netflow
set netflow export-interval 1
set netflow export-destination 192.168.70.10 2055
set netflow export-version 9
set netflow export-rate 20000 1
set netflow export-data enable mac
set netflow export-data enable vlan
set netflow port tg.1.4 enable rx
set netflow template refresh-rate 30 timeout 1
set netflow cache enable
```

Kuva 46. Laitteen Netflow-protokollan konfiguraatio.

8. Laitteelta poistetaan vielä turhia kytkinprotokollia käytöstä ja asetetaan vielä jumbo frame -tuki päälle porttiin, josta liikenne kulkee Analytics-palvelimelle.

```
# cdp
set cdp state disable tg.1.1-4
!

# ciscodp
set ciscodp port status disable tg.1.1-4


# gvrp
set gvrp disable
!

# lacp
set lacp disable

# spantree
set spantree stpmode none
set spantree portadmin tg.1.1 disable
set spantree portadmin tg.1.2 disable
set spantree portadmin tg.1.3 disable
set spantree portadmin tg.1.4 disable

# port
set port jumbo enable tg.1.1
```

Kuva 47. Turhien protokollien poisto ja jumbo frame -asetus.

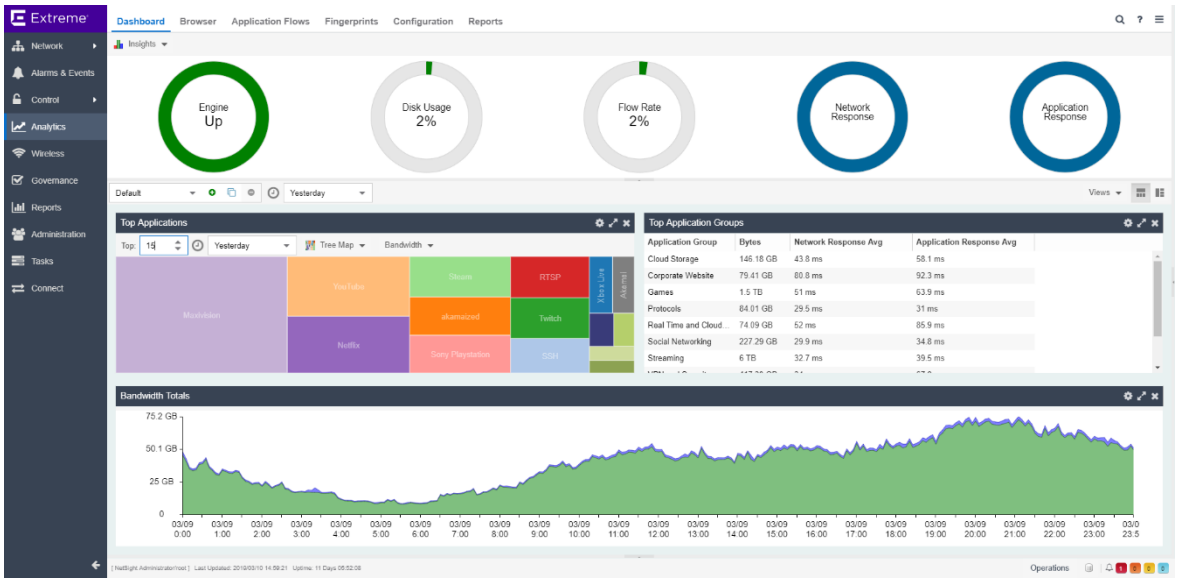
9. Tässä vaiheessa voidaan tarkistaa ping-komennolla, kuinka yhteydet palvelimien ja Flow Sensor -laitteen välillä toimivat.

4.6 Käyttö

Kun kaikki asennukset saatiin suoritettua, itse liikennettä pääsi analysoimaan avaamalla Extreme Management Centerin -palvelimen selaimesta ja avaamalla Analytics-näkymän sivupalkista. Extreme Management Center -palvelimeen on mahdollisuus liittää muitakin Extreme Networksin tuotteita, kuten Extreme Control -palvelin, jolla hallitaan Extremen laitteita. Tähän työhön oleellinen on kuitenkin vain Analytics-näkymä, sillä tässä näkymässä on liikenteen analysointiin liittyvä tieto.

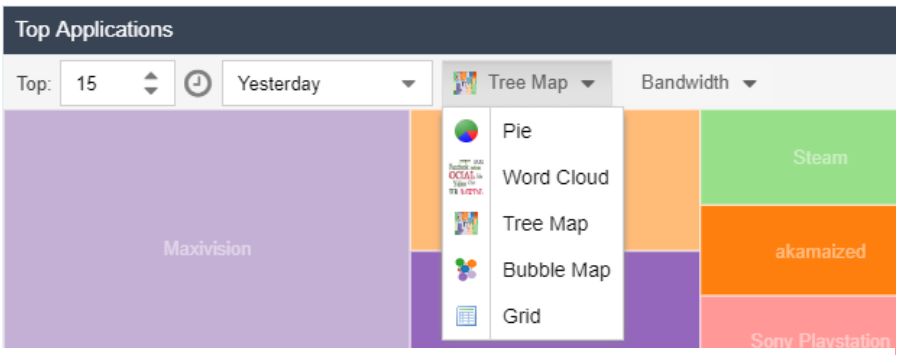
4.6.1 Dashboard

Ensimmäisenä aukeava Dashboard-välilehti kokoaa kattavan kokoelman tietoa verkossa kulkevasta liikenteestä. Oletuksena käytössä oleva Insights-sivu antaa tietoa Flow Collector -laitteen tilasta, verkon Flow-määrästä, verkon sovelluksista, verkkoa eniten kuormittavista sovellusryhmistä ja verkon liikenteen määrästä per minuutti.



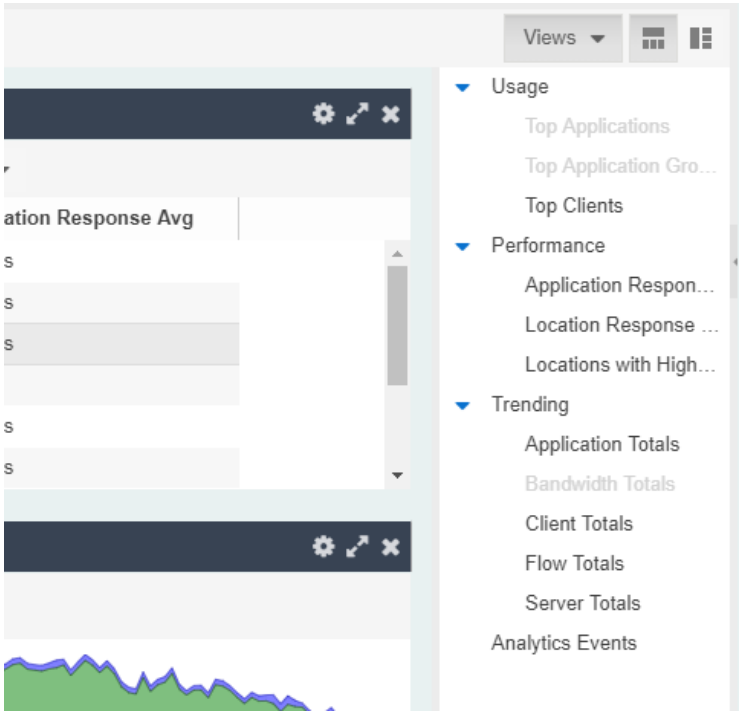
Kuva 48. Dashboard Insights -profiilin näkymä.

Insights-sivu on täysin muokattavissa käyttäjän tai yrityksen tarpeiden mukaan. Muokkausta voidaan tehdä esimerkiksi, kuinka kaukaa historiasta tietoa haetaan, kuinka monta sovellusta tai protokollaa näkymässä näytetään tai millaisessa muodossa tietoa havainnollistetaan.



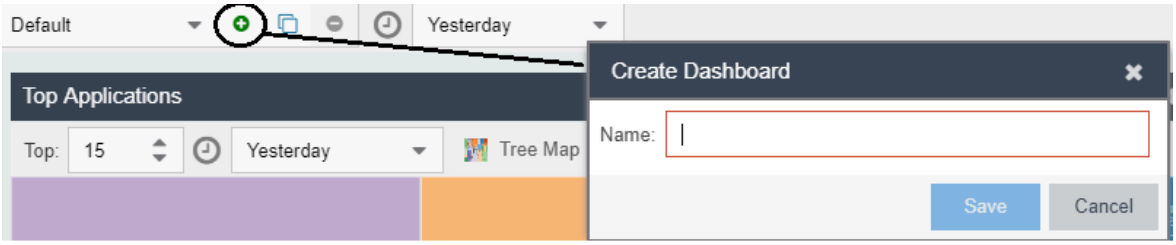
Kuva 49. Eri vaihtoehtoja tiedon näyttämiselle.

Vaihtoehtoja löytyy monia ja käytännössä kaikki sivulla oleva on jossain määrin muokattavissa. Sivulla näkyvät kentät voidaan myös vaihtaa muihin vaihtoehtoihin.



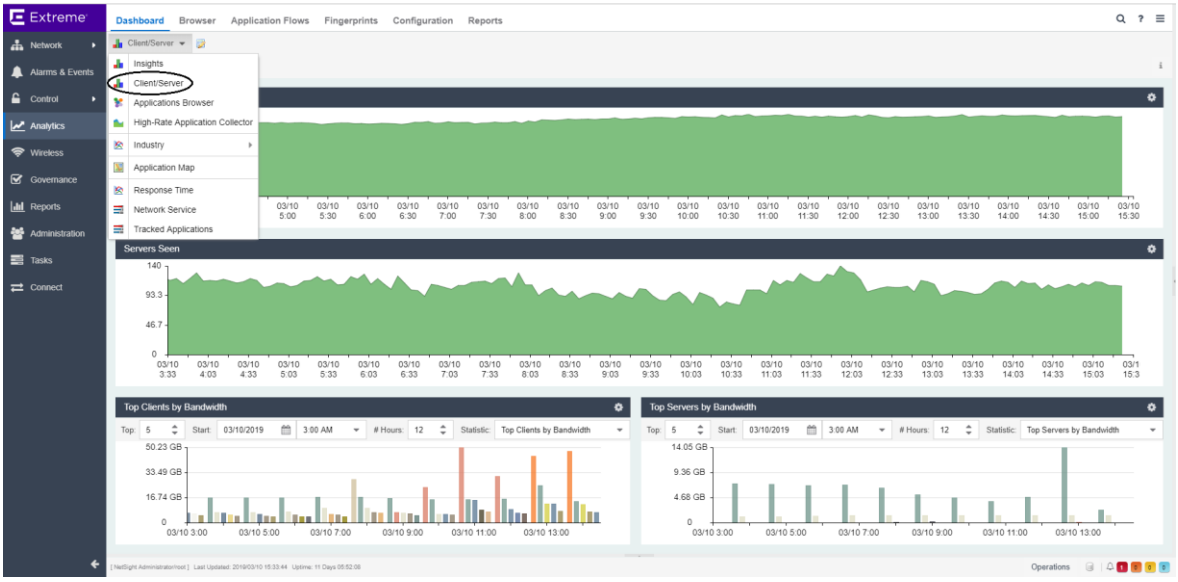
Kuva 50. Sivun kenttien vaihtaminen muihin.

Sivulle voidaan myös luoda omia Dashboardeja yksityiskohtaisia tarkoituksia varten.



Kuva 51. Oman Dashboardin luonti.

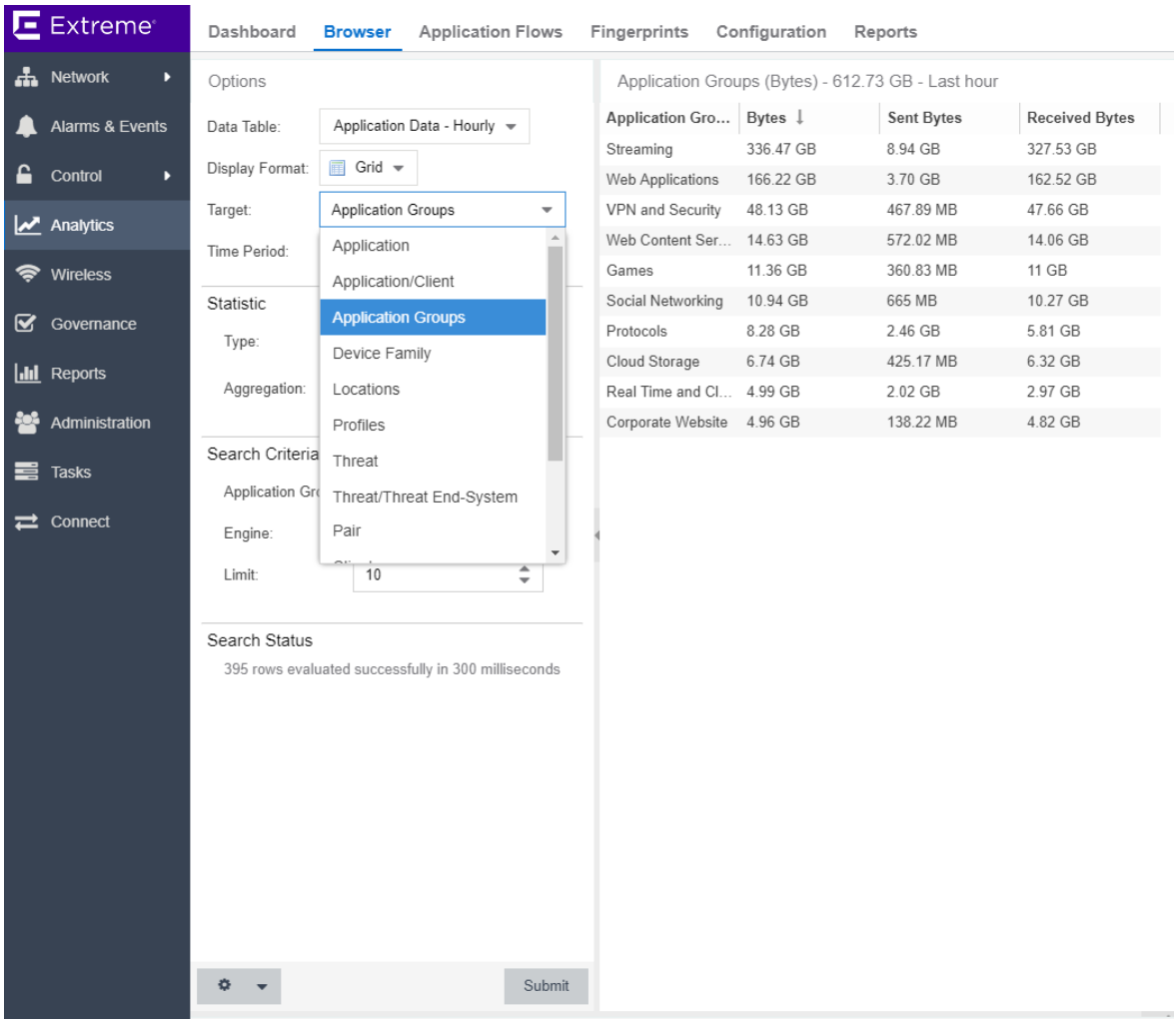
Insights-sivun lisäksi löytyy myös muita vaihtoehtoisia sivuja, jotka antavat yleiskuvaa verkon liikenteestä. Esimerkiksi Client/Server-sivulta löytyy tietoa verkossa keskustelevien laitteiden määrästä ja suurimmista kaistan käyttäjistä tietyllä aikajaksolla.



Kuva 52. Client/Server-sivun näkymä.

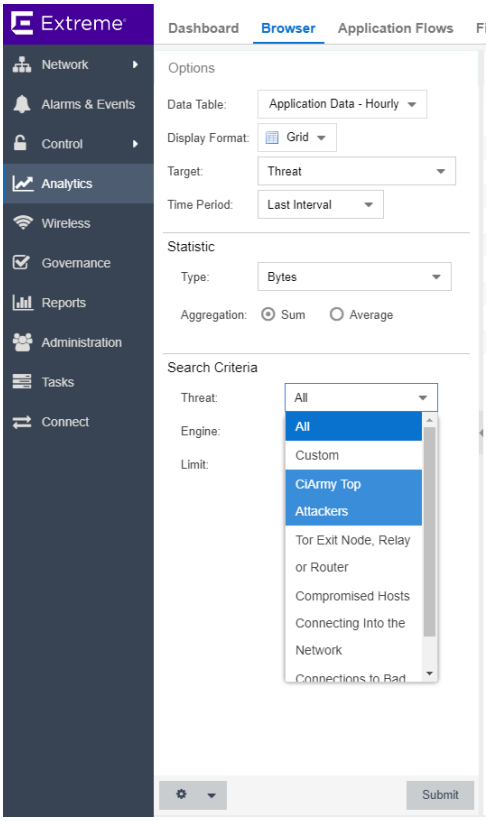
4.6.2 Browser

Browser-välilehdeltä voidaan hakea haluttujen kriteerien perusteella tietoa verkon liikenteestä. Hakuja voi tehdä esimerkiksi verkossa eniten käytetyistä sovelluksista tai suurimmista verkon käyttäjistä tietyllä ajanjaksolla. Tiedot voidaan tallentaa .csv-tiedostoksi Excel-ohjelmalle ja niistä voidaan tehdä raportteja Report Designer -toiminnolla. Raportteja voidaan sitten lähettää sähköpostilla tiettyinä aikoina haluttuihin osoitteisiin.



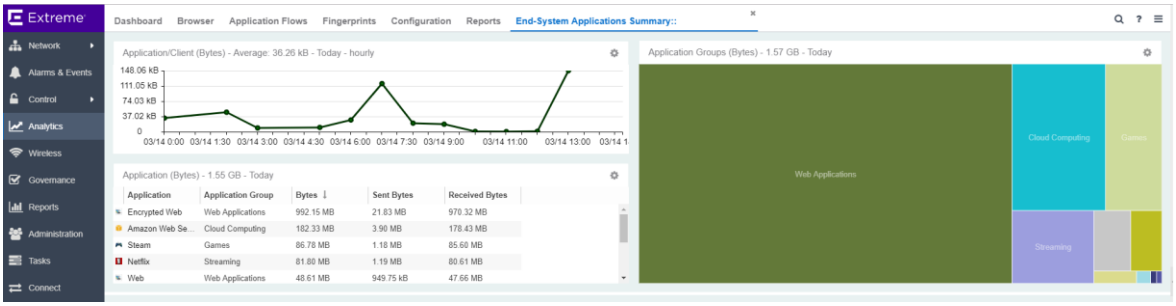
Kuva 53. Browser-välilehden valintamahdollisuuksia.

Hakuvaihtoehdoista löytyy myös Threat-kohta, joka kertoo verkossa havaituista uhista. Tämä on kätevä tapa paikantaa uhkia helposti verkosta, sillä usein paikannuksen tehokkuus on ratkaiseva tekijä haittojen ehkäisyssä. Threat-kohdan alta löytyy muutamia kategorioita, kuten ”Connections to Bad Hosts” ja ”Compromised Hosts Connecting Into Network”.



Kuva 54. Uhkien hakeminen Browser-välilehdellä.

Hakuja voidaan tehdä myös IP-osoitteen, portin, sovelluksen tai protokollan perusteella. Tällöin haun kohteesta riippuen saadaan tietoa esimerkiksi tietyn IP-osoitteen

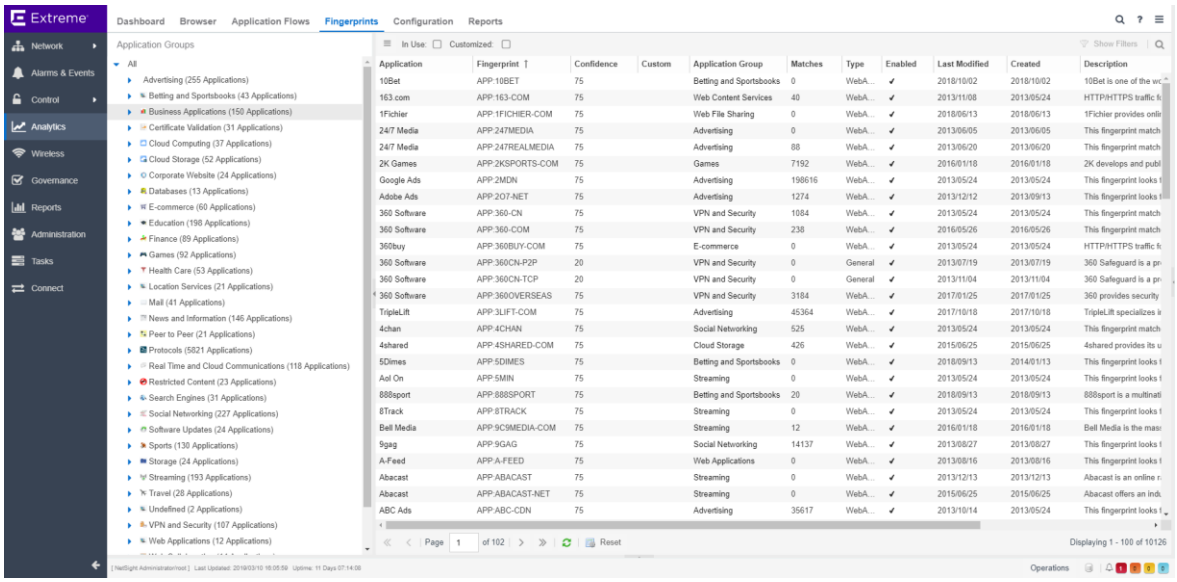


Kuva 55. Tietyn IP-osoitteen perusteella tehty haku.

käyttämistä sovelluksista, protokollista ja liikenteestä tai vaikkapa mitkä IP-osoitteet käyttävät tiettyä protokollaa.

4.6.3 Fingerprints

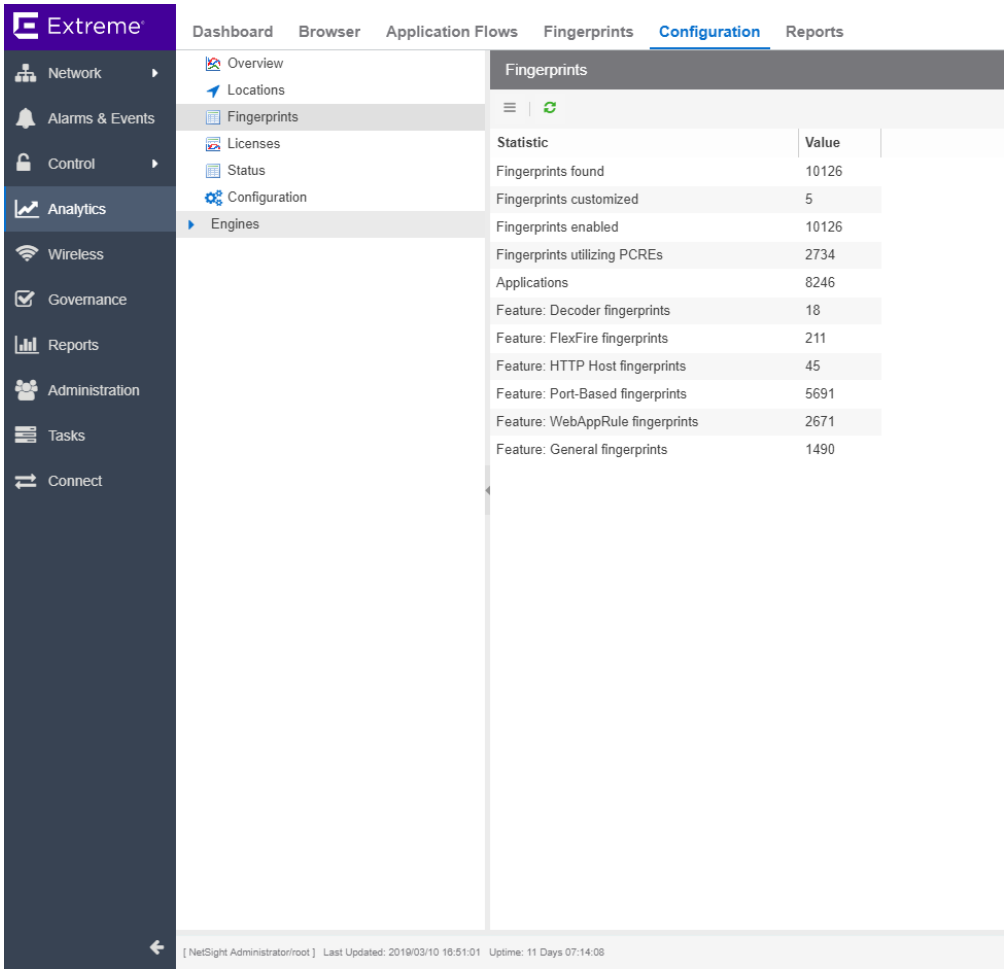
Fingerprints-välilehdellä on Exterme Networksin oma tietokanta eri verkkoprotokollista ja sovelluksista, joiden avulla Analytics-palvelin kykenee tunnistamaan ison osan verkon liikenteestä. Tietokanta on laaja ja se kattaa useita eri kategorioita ja sovelluksia. Tietokanta on kätevä varsinkin haitallisen liikenteen erottamiseen normaalista käytöstä. Koska tietokanta on laaja ja siihen saa päivityksiä tietyin väliajoin, se kykenee hyvällä tarkkuudella siirtämään analysoinnin pois normaalista ei-haitallisesta liikenteestä ja siirtämään keskittymisen liikenteeseen, jota se ei tunnista. Fingerprints-tietokantaan pystytään myös lisäämään omia lisäyksiä esimerkiksi liikennöivän IP-osoitteen tai käytetyn portin perusteella. Tämä on erittäin hyödyllistä tilanteessa, jossa verkossa alkaa esiintyä omituinen IP-osoite, jota halutaan tarkkailla. Myöskin ei-haitallisia lisäyksiä voidaan tehdä tietokantaan oman tarkkailun helpottamiseksi.



Kuva 56. Fingerprints-välilehden tietokanta.

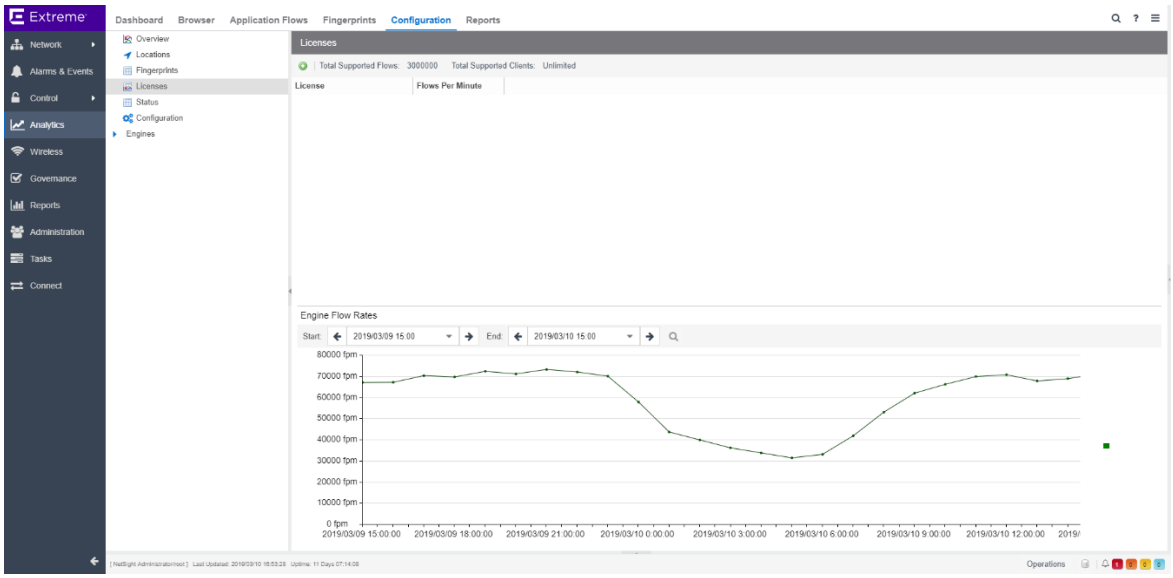
4.6.4 Configuration

Configuration-välilehdeltä löytyy Analytics-palvelimen ja PV-FC-180-laitteen asetusten lisäksi paljon tietoa Flow-liikenteen määrästä. Välilehdeltä löytyvästä Locations-kohdasta voidaan myös nimetä oman verkon IP-osoiteavaruudet analysoinnin helpottamista varten. Fingerprints-kohdasta löytyy statistiikkaa luoduista omista Fingerprinteistä sekä jo olemassa olevista.



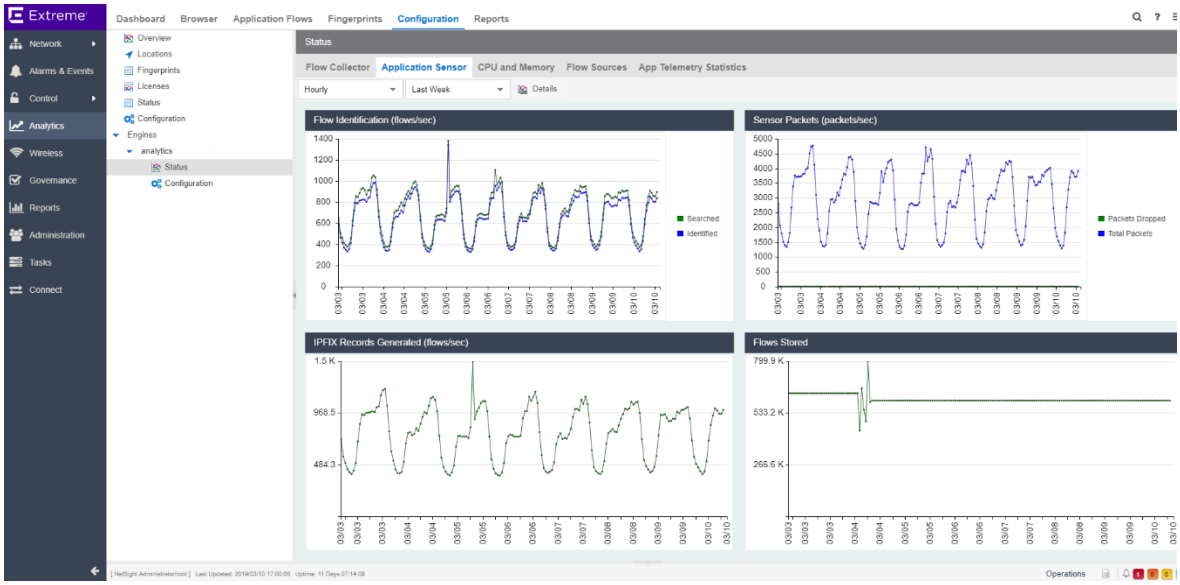
Kuva 57. Fingerprints-kohdan statistiikkaa.

Licenses-kohdasta pääsee katsomaan Flow-liikenteen määrää minuuttitasolla verkossa. Tämän tarkkailu on eritoten lisensointia varten tärkeää, sillä kokonaisuuteen tarvitsee lisenssin määrän perusteella. Myös joissain tilanteissa käyrästä voinee havaita piikkejä Flow-liikenteessä, jolloin voisi päätellä kyseessä olevan mahdollisen häiriön verkossa.



Kuva 58. FPM-arvo verkossa tietyllä aikavälillä.

Engines-kohdan alta pääsee näkemään Analytics-palvelimeen ja Flow Sensor -laitteeseen liittyviä kuvaajia. Täältä voi seurata muun muassa kummankin prosessorin ja muistin kuormaa, sekä liikenteen, pakettien ja Flow-tietojen tunnistamisen määrää.



Kuva 59. Analytics-palvelimen ja Flow Sensor -laitteen kuvaajia.

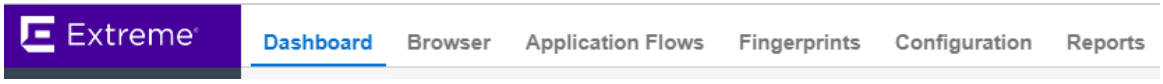
5 YHTEENVETO

5.1 Hinta

Hinnaltaan ExtremeAnalytics-kokonaisuus ja ntopng-ohjelma ovat aivan ääripäistä. Vaikka ntopng-ohjelmasta oli testauksessa käytössä vain ilmaisversio, on vertailun järkevyyden vuoksi tehty suurin osa tarkasteluista hyödyntäen ntopng-ohjelman Trial-lisenssiä. ntopng-ohjelman kalleimman version ja ExtremeAnalytics-kokonaisuuden hintaero on siltikin todella suuri. Kuitenkin pelkästään ilmaisversiolla ntopng-ohjelmasta pääsee yllättävänkin lähelle ExtremeAnalytics-kokonaisuutta.

5.2 Käytettävyys

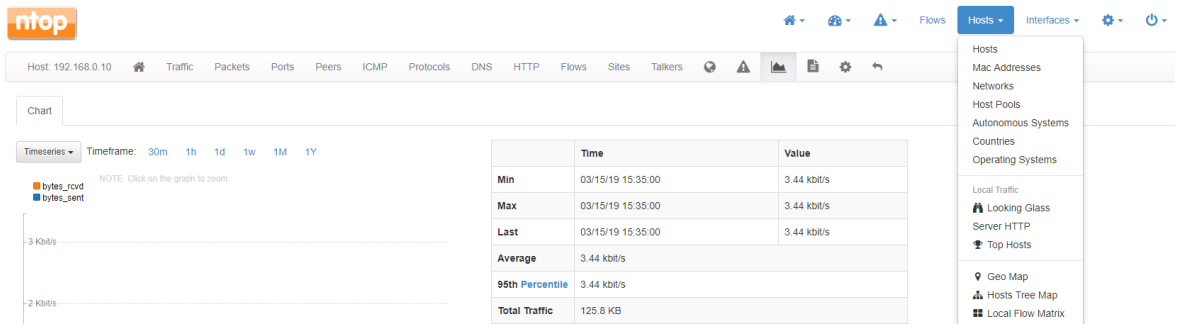
Käytettävyydeltään ExtremeAnalytics-palvelin on parempi kuin ntopng-ohjelma. Palvelimeen kirjauduttaessa saa nopeasti käsityksen, mitä minkäkin välilehden alta löytyy. Välilehtiä ei myöskään ole liikaa, jolloin ulkoasu säilyy selkeänä.



Kuva 60. ExtremeAnalytics-palvelimen välilehdet.

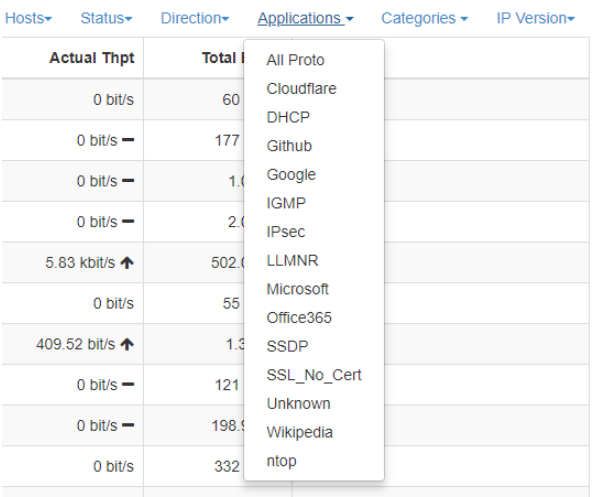
Lähes kaikkia näkymiä voidaan myös jossain määrin muokata, mikä tekee niistä käteviä käyttää. Hakutoiminto on myös parempi kuin ntopng-ohjelmassa, sillä siitä voi hakea melkeinpä millä tahansa hakusanalla, kuten protokollalla, sovelluksen nimellä, portin numerolla, IP-osoitteella tai jopa yhdistelemällä näitä. ExtremeAnalytics-palvelimen sivut tuntuvat välillä aukeavan hitaasti ja joskus palvelin tuntuu jäävän jopa jumiin. Tämä kuitenkin taitaa johtua tietokoneesta, jolla palvelin pyörii, sillä sen resurssit eivät ole optimaaliset tähän käyttöön. Tietokoneella pyörii ExtremeAnalytics-palvelimen kanssa kuitenkin myös Extreme Management Center -palvelin, joka toimii pohjana muille palvelimille, ja tämä vie oman osansa tietokoneen resursseista.

ntopng-ohjelman käyttäminen vaatii enemmän totuttelua kuin ExtremeAnalytics-palvelimen. Tämä ei välttämättä kuitenkaan ole ongelma, jos ohjelma on muuten tehokas käyttää. ntopng-ohjelmasta tulee myöskin olo, että siinä olisi enemmän tietoa verkon liikenteestä. Ohjelmasta löytyy enemmän erilaisia sivuja ja näkymiä liikenteestä, ja hetken totuttelun jälkeen ohjelmaa on yhtä sulava käyttää kun ExtremeAnalytics-palvelinta. Muokattavuus on ntopng-ohjelmassa toteutettu enemmänkin niin, että kaikki löytyy erilaisina välilehtinä valintojen sijaan. Tämäkään ei ole välttämättä huono asia, mutta tekee kokemattomalle käyttäjälle näkymistä sekavia.



Kuva 61. ntopng-ohjelman välilehtiä ja valikkoja.

Hakukenttä on ntopng-ohjelmassa selkeästi huonompi, sillä siitä ei voi hakea kuin IP-osoitteella ja omalla nimellä, joka jollekin IP-osoitteelle on annettu. Ohjelmassa täytyy siis usein etsiä luokittelemalla ja järjestelemällä listoja esimerkiksi liikenteen tai protokollan mukaan.



Kuva 62. Järjestäminen sovellusten mukaan ntopng-ohjelmassa.

5.3 Näkyvyys

Heti ExtremeAnalytics-palvelimen ensimmäisessä Dashboard-näkymässä on kattava näkymä verkon liikenteeseen ja liikenteen määrään. Tämä näkymä on vielä helposti muokattavissa käyttäjän mukaan, ja omia Dashboard-näkymiäkin voi tehdä. Näkymässä pystyy myös valitsemaan haluamansa aikajakson, jolloin kokematonkin käyttäjä pystyy helposti vertaamaan liikenteen määrää tai sovellusten jakaumaa aikaisempaan ja tekemään havaintoja. ExtremeAnalytics-palvelimen tarjoama näkyvyys liikenteeseen on myöskin tarkempaa kuin ntopng-ohjelmassa. Palvelimelta löytyy todella kattava Fingerprints-tietokanta, johon on mahdollista myös omien tietojen lisäys. ntopng-ohjelmassa on mahdollista myöskin tietojen lisäys eri kategorioihin IP-osoitteiden perusteella, mutta toiminto on ExtremeAnalytics-palvelimessa kuitenkin helpompi ja tehokkaampi. ntopng-ohjelma saattaa tunnistaa liikenteen Streaming-kategoriaan, kun taas ExtremeAnalytics-palvelin tunnistaa, onko sovellus Netflix vai Twitch. Tarkemmasta näkyvyydestä ei välttämättä kuitenkaan ole hyötyä alkuperäisessä käyttötarkoituksessa eli häiriöliikenteen paikantamisessa, johon tätä työtä on lähdetty tekemään.

ntopng-ohjelmassa samanlaisen verkkoliikenteen näkyvyyden saamiseksi pelkästään ensimmäinen Traffic Dashboard -näkymä ei riitä. Tätä näkymää ei pystytä suoraan muokkaamaankaan, jolloin on tyydyttävä siihen, mitä siinä näkyy oletuksena. Myöskään näkymän aikajaksoon ei pystytä vaikuttamaan, joten siinä näkyy aina tämän hetkinen ja edellisen päivän liikenne. Samanlaisen näkyvyyden ntopng-ohjelmalla kyllä saa, mutta käyttäjä joutuu tutkimaan liikennettä useammalta sivulta, kuten esimerkiksi Traffic Report -sivulta. Tilanteessa, jossa verkossa esiintyisi häiriöliikennettä, on tärkeää, että sen paikantaminen olisi nopeaa ja tehokasta. ntopng-ohjelmassa voisi näin ollen esiintyä tilanteita, jossa häiriön paikannus ei olisi aivan yhtä tehokasta kuin ExtremeAnalytics-palvelimen kautta. Tällaisessa tapauksessa täytyy kuitenkin olettaa, että häiriön aiheuttaja näkyy suoraan esimerkiksi liikennekäyrässä tai sovellusdiagrammissa, mikä ei välttämättä pidä paikkaansa.

5.4 Varoitukset

ExtremeAnalytics-palvelimessa Browser-sivun Threat-haku on helpoin tapa löytää palvelimen itse tunnistamia uhkia. Palvelin on toistaiseksi luokitellut muutaman eri uhan ja lähinnä se tukeutuu kahteen eri tietokantaan: DShield ja CiArmy, jotka ovat keränneet haitallisia IP-osoitteita. Palvelin ilmoittaa Threat-listauksessa, jos tietokantojen haitallisilta IP-osoitteilta on havaittu liikennettä analysoitavan verkon suuntaan, kuinka paljon liikennettä on ollut, ja mitkä IP-osoitteet ovat olleet kyseessä. Näitä IP-osoitteita tarkastellessa pystyy toteamaan, että niitä käytetään lähinnä porttiskannaukseen. Muita palvelimen toistaiseksi luokittelemia uhkia ovat ”Tor Exit Node, Relay or Router”, ”Connections to Bad Hosts” ja ”Compromised Hosts Connecting Into the Network”. Näissä muissa kategorioissa ainakin BitTorrent-liikenne näkyi uhkana. Uhille ei ole tarjolla luokittelua vaarallisuuden perusteella.

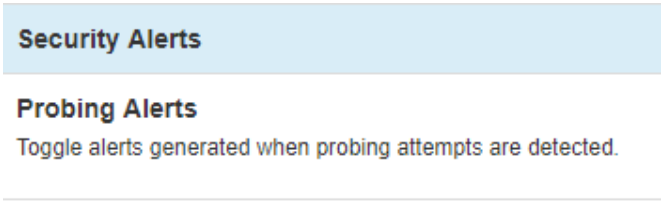
Threat (Bytes) - 12.38 kB - Last hour

Threat	Bytes ↓	Sent Bytes	Received Bytes
Tor Exit Node, Relay or Router	10.83 kB	6.65 kB	4.18 kB
CiArmy Top Attackers	1.35 kB	0	1.35 kB
Connections to Bad Hosts	204 bytes	204 bytes	0

Kuva 63. Threat-listaus verkosta.

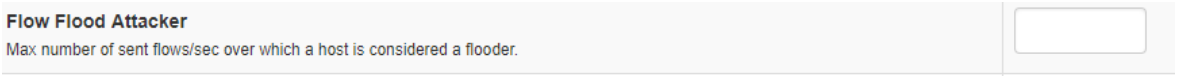
Toinen tehokas tapa analysoida liikennettä haittaliikenteen varalta on käyttää ExtremeAnalytics-palvelimen tehokasta hakua. Tällöin voidaan tehdä hakuja esimerkiksi Sunetia aikaisemmin vaivanneella SSDP-protokollalla, jolloin voidaan heti havainnoida, näkyykö protokollaa verkossa. Tämä keino kuitenkin edellyttää, että tiedetään etukäteen oikeita hakusanoja, kuten protokollia tai portteja, joita pitää silmällä.

ntopng-ohjelmassa varoituksille löytyy omat sivunsa ja Preferences-valikosta pystyy niitä tarkemmin muokkaamaan. Esimerkiksi voidaan määrittää, syntyykö porttiskannauksista varoitus.



Kuva 64. ntopng-ohjelman Probing Alerts -kohta.

Jokaiselle omalle IP-osoitteelle tai verkolle pystyy myös itse määrittämään rajoja, milloin varoitus syntyy tai ei synny



Kuva 65. Flow Flood Attacker -varoitus.

ntopng-ohjelman varoitukset on listattu selkeämmin, sillä jokaiselle varoitukselle on oma vakavuusluokkansa, jonka perusteella pystyy päättelemään, onko kyseessä ongelma. Ohjelman Alerts Dashboard- ja Flow Alerts Explorer -sivut ovat myöskin etu, jota ExtremeAnalytics-palvelimesta ei löydy. Sivuilta pääsee heti näkemään, kuinka vakavasta varoituksesta on kyse, ja mikä sen on aiheuttanut. Ylipäätään varoitukset vaikuttavat ntopng-ohjelmassa olevan paremmin tehty ja häiriötilanteessa helpommin paikannettavissa. Tehokas hakutoiminto ntopng-ohjelmasta kuitenkin puuttuu, jolloin samanlaista häiriöliikenteen etsintää ohjelmassa on vaikea toteuttaa. ntopng-ohjelmassa täytyy siis lähinnä turvautua siihen, että mahdolliset häiriöt ilmestyvät varoituksiin ja ne saadaan sitä kautta huomattua. Varmuudella asiaa on kuitenkin vaikea todeta, sillä häiriötilanne pitäisi saada päälle, että asian voisi todeta käytännössä. Lähtöedellytykset tuntuvat kuitenkin olevan ntopng-ohjelman puolella.

5.5 Raportit

ExtremeAnalytics-palvelimessa pystytään muokkaamaan ja luomaan omia raportteja sen perusteella, mitä halutaan ilmoittaa. Raportti voidaan esimerkiksi tehdä edellisviikon liikenteestä ja sovelluksista, tai pelkästään uhista ja lähettää se joka viikon maanantaina kello 08.00 kaikille työntekijöille. ntopng-ohjelmassa tämä ei onnistu, vaan ohjelmasta löytyy ainoastaan Traffic Report -näkymä, jossa on halutun aikajakson tietoja kattavasti. Tätä ei kuitenkaan saa automaattisesti sähköpostiin, vaan se pystytään ottamaan pdf-tiedostona.

5.6 Pohdintaa

Opinnäytetyön tarkoituksena oli löytää tehokas ja toimiva ratkaisu verkkoliikenteen analysointiin ja saada hyvä näkyvyys liikenteen sisällöstä. Tässä vaiheessa ensimmäisenä kokeiltiin ntopng-ohjelmaa, sillä se oli ilmainen ja myöskin helppo ensimmäinen askel kohti ratkaisua. Liikenteen tuonti ntopng-ohjelmalle toteutettiin helpoimmalla tavalla eli mirror-toiminnolla peilaamalla suoraan koneelle. Tällä toteutuksella saatiin jo käsitys, mikä on mahdollista, jos liikenteen analysointiin käytetään kalliimpia ratkaisuja. Työn edetessä alkoi selvitä, kuinka toteutus olisi kaikista järkevintä tehdä ja mitä se vaatisi. Extreme Networks -yritykseltä saatu laite- ja palvelinkokonaisuus avarsi tätä näkymää enemmän ja syntyi käsitys siitä, mitä tulisi tehdä.

Järkevin toteutustapa olisi siis vastaava, kun ExtremeAnalytics-kokonaisuudessa rakennettiin eli liikenteen peilaus mirror-toiminnolla jollekin Sensor-laitteelle, joka Netflow-protokollaa hyödyntäen muuntaa liikenteen jonkin Netflow Collector-ohjelman analysoitavaksi. Tämä johtopäätös voidaan tehdä sen takia, että verkon liikenteen määrä on tällä hetkellä niin suurta, että vastaanottavan laitteen pitää se pystyä ottamaan vastaan. Laitteen täytyy tukea yli 1 Gbit/s liikennettä ja sen tulisi myös pystyä hallitsemaan tuo määrä. Näin suuret liikennemäärät ovat teoriassa mahdollista viedä suoraan tietokoneelle, mutta se vaatisi 10 Gbit/s verkkokortin ja todennäköisesti myös lisää tehoa tietokoneelta. Tietokoneen vaatimat tehot on vaikea päätellä etukäteen. Toinen vaihtoehto olisi rajoittaa analysoitavan liikenteen määrää,

joka ei tässä tapauksessa kuitenkaan ole järkevää, koska analysoinnin kannalta on tärkeää nähdä kaikki liikenne.

Sensor-laitteen tulee olla yhteensopiva käytetyn Netflow Collector -ohjelman kanssa ja tarpeeksi tehokas käsittelemään liikenteen. ExtremeAnalytics-kokonaisuus olisi tähän toimiva kokonaisuus ja siihen saataisiin hyvä tuki, sillä Sunet on aikaisemmin hankkinut Extreme Networks -yritykseltä verkkokytkimiä. Toisaalta kokonaisuus on mielestäni hintava suhteessa siihen hyötyyn mitä siitä saa. Loppujen lopuksi on vaikea päästä lopputulokseen, onko kokonaisuus hintansa arvoinen, koska siitä saatavan hyödyn toteaminen on vaikeaa ilman verkossa esiintyvää häiriötä. Tällä hetkellä kokonaisuuden hyöty pystytään ainoastaan toteamaan kattavalla näkyvyydellä liikenteeseen.

ntopng-ohjelman kautta saataisiin joissain osa-alueissa lähes vastaava hyöty, ja joissain osa-alueissa, kuten varoitusnäkymissä, se on jopa lähtökohtaisesti parempi kuin ExtremeAnalytics-kokonaisuus. Toisaalta taas hakutoiminnoissa ntopng-ohjelma jää pahasti jälkeen. Ei ole vaikea kuvitella tilannetta, missä häiriötilanne on päällä, mutta ohjelma ei suoraan anna minkäänlaisia suoria varoituksia. Tällaisessa tilanteessa tehokas hakutoiminto on varmasti eduksi, kunhan vaan tietää mitä hakee. Kuitenkaan on vaikea sanoa varmuudella, kumpi on parempi ja kumpi huonompi, sillä ohjelmia ei testattu täsmälleen samalla toteutuksella, eikä samaan aikaan. Jälkikäteen ajateltuna ntopng-ohjelma olisi ollut hyvä asentaa yhdessä nProbe-ohjelman kanssa ja Linux-pohjaiselle virtuaalipalvelimelle, sillä Windows-käyttöjärjestelmälle asennettuna ohjelman toimivuudessa oli jonkin verran ongelmia. Ohjelma saattoi hukata liikennetietoja tai kaatua yllättäen. Sensor-laitetta hyödyntäen ja yhdessä nProbe-ohjelman kanssa toimien ntopng-ohjelmasta voisi saada muodostettua samankaltaisen kokonaisuuden kuin ExtremeAnalytics-kokonaisuus. Tätä on kuitenkaan hankala todeta, sillä nProbe-ohjelmaan täytyisi saada testilisenssi. Ohjelmasta löytyy ilmaisversio, jota voisi kokeilla yhdessä ntopng-ohjelman kanssa, mutta nProbe-ohjelmaan erikseen myytävät plugin-paketit jäisivät silloin testaamatta kokonaan.

LÄHTEET

Cecil, A. Ei päiväystä. A Summary of Network Traffic Monitoring and Analysis Techniques. [Verkkodokumentti]. [Viitattu 17.3.2019]. Saatavissa: https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring.pdf

Extreme Networks. Ei päiväystä. What is Port Mirroring? [www-sivu]. Extreme Networks. [Viitattu 15.2.2019]. Saatavissa: https://gtacknowledge.extremenetworks.com/articles/Q_A/What-is-Port-Mirroring

Extreme Networks. Ei päiväystä. ExtremeAnalytics – sovellusten analysointiin ja optimointiin. [www-sivu]. Extreme Networks. [Viitattu 16.3.2019]. Saatavissa: https://www.extremenetworks.fi/extremeanalytics/

Extreme Networks. Ei päiväystä. Extreme Networks yrityksenä. [www-sivu]. Extreme Networks. [Viitattu 17.3.2019]. Saatavissa: https://www.extremenetworks.fi/extreme-networks/

Extreme Networks. Ei päiväystä. ExtremeAnalytics. [Verkkodokumentti]. Extreme Networks. [Viitattu 18.3.2019]. Saatavissa: https://www.extremenetworks.com/product/extremeanalytics/

Extreme Networks. Ei päiväystä. Extreme Management Center. [Verkkodokumentti]. Extreme Networks. [Viitattu 19.3.2019]. Saatavissa: https://www.extremenetworks.com/product/extreme-management-center/

Hale, B. 6.9.2012. NetfFlow V9 Datagram Knowledge Series: Part 1 – NetFlow Overview. [Verkkodokumentti]. Thwack – The Community of SolarWinds. [Viitattu 10.2.2019]. Saatavissa: https://thwack.solarwinds.com/community/solarwinds-community/geek-speak/blog/2012/09/06/netflow-v9-datagram-knowledge-series-part-1--netflow-overview

Harris, G. 20.12.2018. Packet capture library (libpcap). [www-sivu]. Wireshark. [Viitattu 17.3.2019]. Saatavissa: https://wiki.wireshark.org/libpcap

ISO/IEC 7498-4. 1989. Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4 : Management Framework. [Verkkodokumentti]. International Standard Organisation. [Viitattu 17.3.2019]. Saatavissa: http://standards.iso.org/ittf/PubliclyAvailableStandards/s014258_ISO_IEC_7498-4_1989%28E%29.zip

Netfort. Ei päiväystä. Flow Analysis Versus Packet Analysis. What Should You Choose? [Verkkodokumentti.] Netfort. [Viitattu 17.3.2019]. Saatavissa: https://www.netfort.com/wp-content/uploads/PDF/WhitePapers/NetFlow-Vs-Packet-Analysis-What-Should-You-Choose.pdf

Nmap. Ei päiväystä. Npcap. [www-sivu]. nmap. [Viitattu 17.3.2019]. Saatavissa: https://nmap.org/npcap/

Noction. 19.10.2018. NetFlow vs. sFlow vs. IPFIX vs. NetStream. Network traffic monitoring explained. [www-sivu]. Noction – Network Intelligence. [Viitattu 10.2.2019]. Saatavissa: https://www.noction.com/blog/netflow-sflow-ipfix-netstream-network-traffic-monitoring-explained

ntop. Ei päiväystä. ntopng. [www-sivu]. ntop. [Viitattu 3.2.2019]. Saatavissa: https://www.ntop.org/products/traffic-analysis/ntop/

ntop. Ei päiväystä. About Us. [www-sivu]. ntop. [Viitattu 8.2.2019]. Saatavissa: https://www.ntop.org/about/about-us-2/

ntop. Ei päiväystä. nProbe. [www-sivu]. ntop. [Viitattu 15.2.2019]. Saatavissa: https://www.ntop.org/products/netflow/nprobe/

Parker, J. 8.9.2016. What is Netflow? [www-sivu]. PC & Network Downloads. [Viitattu 17.3.2019]. Saatavissa: https://www.pcwdld.com/what-is-netflow

Sanders, C. 2011. Practical Packet Analysis. 2 painos. San Francisco: No Starch Press Incorporation.

Sunet. Ei päiväystä. Mikä Sunet?. [www-sivu]. Suupohjan Seutuverkko Oy. [Viitattu 22.2.2019]. Saatavissa: https://sunet.fi/yritysesittely/

Technopedia. Ei päiväystä. Wireshark. [www-sivu]. Technopedia. [Viitattu 15.2.2019]. Saatavissa: https://www.techopedia.com/definition/25325/wireshark

Traficom. 12.3.2019. Internetin avoimuus eli verkkoneutraliteetti. [www-sivu]. Traficom. [Viitattu 17.3.2019]. Saatavissa: https://www.traficom.fi/fi/viestinta/viestinta-verkot/internetin-avoimuus-eli-verkkoneutraliteetti

Wireshark. Ei päiväystä. About Wireshark. [www-sivu]. Wireshark. [Viitattu 15.2.2019]. Saatavissa: https://www.wireshark.org/about.html#authors

LIITTEET