Christian Kurvinen

IPv6-protokolla ja turvalliset yritysverkot (VPN)

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tietotekniikan koulutusohjelma
Insinöörityö
16.4.2012

Metropolia

Tiivistelmä

Tekijä(t) Otsikko Sivumäärä Aika	Christian Kurvinen IPv6-protokolla ja turvalliset yritysverkot (VPN) 30 sivua + 3 liitettä 16.4.2012
Tutkinto	Insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkot
Ohjaaja(t)	tietoliikenneasiantuntija Jaakko Rautanen yliopettaja Janne Salonen

Tämän työn tilaajana oli Cygate Oy. Työssä tutkittiin IPv6 (Internet-protokolla versio 6) VPN -verkkoratkaisuja. Tulevaisuudessa Internetin osoitteistus tulee siirtymään IPv6:een, jolloin Cygatella on oltava tiedossa menetelmät, joilla VPN-ratkaisut rakennetaan käytettäessä IPv6:ta. Syynä IPv6:n käyttöönottoon on edellisen IPv4 (Internet-protokolla versio 4) -osoiteavaruuden vapaiden osoitteiden väjäämätön loppuminen. Muutos vaikuttaa hitaasti kaikkiin Internetin käyttäjiin.

Työssä keskityttiin tutkimaan IPv6 VPN -toteutusta Cisco Systemsin ja Juniper Networksin laitteilla. Lisäksi otettiin huomioon vaatimukset Cygate Oy:n tarjoaman verkonvalvontapalvelun hallintayhteyksien rakentamisessa. Työ tehtiin käyttäen apuna Cygaten laboratorioympäristöä ja omia laitteistoja. Työssä hyödynnettiin julkista Internet-verkkoa, jotta voidaan simuloida tyypillistä asiakastilannetta.

Teoriaosuudessa perehdyttiin IPv6-protokollan toimintaan ja uusiin ominaisuuksiin, sekä syvennettiin tietoja IPsec:n (IP Security Architecture) teoriasta. Käytännönosuudessa selvitettiin verkkolaitteiden tukea uuden protokollan ja VPN:n kanssa kokeilemalla erilaisia asetuksia. Työn kuluessa kävi ilmi useita valmistajakohtaisia rajoituksia ja puutteita.

Lopuksi arvioitiin saadut tulokset ja pohdittiin ratkaisujen toimivuutta niin Cygaten kuin asiakkaiden kannalta. Tulosten perusteella laitteiden ohjelmistotuki IPv6:lle on vielä osin vajavainen ja eroaa valmistajien välillä jonkin verran. Cygaten vaatima tuki OSPFv3-reititysprotokollalle virtuaalisissa reitittimissä (VRF) oli vasta kehitteillä työn kirjoitushetkellä. Ennen palveluiden tuotantoon vientiä tulisi kuitenkin suorittaa laajamittausta testausta, sillä mahdollisia ohjelmistovirheitä voi vielä tulla vastaan. Jotkin ongelmat voidaan välttää valitsemalla laitteistoa saman valmistajan tuotteista.

Avainsanat	IPv6, IPv4, tunnelointi, IPsec, VPN, OSPFv3

Metropolia

Abstract

Author(s) Title Number of Pages Date	Christian Kurvinen Securing IPv6 Networks with IPsec 30 pages + 3 appendices 16 April 2012
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Jaakko Rautanen, Network Specialist Janne Salonen, Principal Lecturer

The objective of this Bachelor's Thesis was to explore the innerworks of IPv6 protocol, IPsec, and also to investigate readiness of network devices to support the new protocol. This study was carried out on assignment by Cygate Oy. Cygate needs to have plans and knowledge to address the future challenges due to the rapid exhaustion of IPv4 address space.

This study was divided into two parts. The first part focuses on theory of IPv6 protocol in addition to its new features. IPsec which stands for Internet Protocol Security is also studied briefly in the last chapter of the theory part. In the second part the work is focused on implementing IPv6 VPN based solutions with the devices of Cisco Systems and Juniper Networks. The actual work was carried out in the network lab at Cygate accompanied with the use of own devices.

A few issues were found during the testing phase and some of which affect the usability of IPv6 VPN services on customer services. The most substantial problems were related to the compatibility between devices and their respective software implementations.

The results of this study show that OSPFv3 is not yet compatible with VRF, of which both are key elements in the Cygate network monitoring system. Further testing will be needed to make sure that IPv6 is as stable as IPv4 on the current production system. This thesis will directly benefit the IPv6 project team of Cygate Oy and initiate future investigations on how to solve some of the faced issues.

Keywords	IPv6, IPv4, tunneling, IPsec, VPN, OSPFv3

Sisällys

1 Johdanto

Tässä insinöörityössä tutkitaan IPv6 VPN-yhteyksiä. IPsec-tuki on vaatimus jokaiselle IPv6-protokollaa tukevalle laitteelle [22.] Työn tilannut Cygate Oy suunnittelee, toteuttaa ja pystyttää turvallisia tietoverkkoja. Cygate Oy on osa suurempaa Cygate-konsernia, joka kattaa yhteensä n. 500 työntekijän henkilöstön. Työn kannalta olennaisinta on testata IPsecin toimintaa IPv6-ympäristössä, joka voisi olla tulevaisuudessa Cygatella tai asiakkaalla käytössä. Työ palvelee Cygaten asiantuntijoita ja asiakkaita sekä toimii yleisenä oppaana IPsec:n käyttöönottoon IPv6-ympäristössä.

Työn tavoite on pystyttää labotorioympäristöön IPv6-protokollaa käyttävä reititin, johon VPN-yhteydet päätetään, testata IPv6 IPsecin tukea eri valmistajien laitteilla ja luoda samalla uutta tietoa yhteensopivuudesta. Samalla selvitetään laitteiden tukemat siirtymämekanismit, sillä tunneloinnin avulla protokollia voidaan kuljettaa toistensa sisällä.

Työssä pyritään saamaan selville erot valmistajien välisessä IPv6 IPsec -tuessa ja toteutusten käyttökelpoisuus. IPv6:n käyttöönoton edetessä on tärkeää, että IPv4:sta tutut konseptit toimivat myös uudessa protokollassa tai muuten käyttöönotto viivästyy. Työ rajataan käsittelemään IPsecia, mutta IPv6:een liittyvää reititystä käsitellään jonkin verran. Työssä otetaan huomioon Cygate Oy:n asettamia vaatimuksia olemassa olevan IPv4-infrastruktuurin pohjalta.

2 IP-protokolla

Internetin toiminta perustuu nykyisellään IPv4-protokollaan, jonka toiminta kuvataan vuonna 1981 uusitussa RFC 791:ssa. IPv4 ja IPv6 ovat OSI-mallin verkkokerroksen protokollia, joiden tehtävänä on huolehtia verkkojen osoitteistuksesta, pakettien pilkkomisesta ja kokoamisesta. Verkkokerroksen tärkein tehtävä on ylemmän kuljetuskerroksen segmenttien siirtäminen lähteestä kohteeseen. IP-protokollalla on tieto seuraavasta protokollasta (TCP/UDP), ja se myös pilkkoo IP-paketteja pienemmiksi.

Ensimmäisen kerran IP:ta käytettiin Yhdysvaltain puolustusministeriön käynnistämässä ARPANET-projektissa. Tällöin ei kuitenkaan osattu arvella IP:n kasvavaa suosiota tulevaisuudessa, kun 32-bittinen osoiteavaruus ei enää riittäisi. Eräänlaisten erityiskäyttöön

varattujen verkkojen osuus nykyisestä osoiteavaruudesta varaa huomattavan osan IPv4:sta. Lisäksi ryhmälähetyksille on varattu oma osoitealueensa.

IANA-järjestö delegoi 3.2.2011 viimeiset osoitteet paikallisille Internet-rekistereille (RIR), jotka puolestaan jakavat niitä paikallisille operaattoreille ja yrityksille. IANAn tehtävä on hallita Internetin juurinimipalvelimia, IP-osoitteita ja AS-numeroita suuremmassa mittakaavassa [1]. Osoitteiden riittävyyttä on helpotettu osoitteenmuunnostekniikalla (NAT) ja CIDR-tekniikalla, jonka avulla entiset luokkiin perustuvat jaot pilkotaan pienempiin ja tehokkaampiin osoitelohkoihin.

Tällä hetkellä palveluntarjoajat ja yritykset ovat siirtymässä tai suunnittelevat siirtävänsä toimintoja myös IPv6:lla käytettäviksi. Laitevalmistajat ponnistelevat toteuttaakseen tuen uudelle protokollalle, ja lähitulevaisuudessa hyvä IPv6-tuki on myös myyntivaltti. Siirtymisen ja toteuttamisen tärkeyttä on korostettu järjestämällä asiaan liittyviä tapahtumia kuten World IPv6 Dayn, jolloin suurimmat sivustot ja palveluntarjoajat ottivat protokollan käyttöön vuorokaudeksi testaamista varten [2.] 8.6.2011 suoritetut testit osoittivat uuden protokollan olevan valmis suurempaankin käyttöön suosituilla sivustoilla [10.] Kasvavana suuntauksena on havaittu asiakkaiden kiinnostuksen IPv6-ominaisuuksiin kasvaneen siten, että tietyn ominaisuuden tukea tiedustellaan aiempaa enemmän. [13.]

Internetin toiminta on IPv4:n varassa, sillä kaikki päätelaitteet, palvelimet, verkkolaitteet ja järjestelmät toimivat lähtökohtaisesti vain kyseisellä protokollalla. Kotikäyttäjien kannalta tilanne ei tule muuttumaan vielä pitkään aikaan, kunnes IPv6-yhteydet tuodaan natiivisti jokaiselle käyttäjälle. Uusimmissa käyttöjärjestelmissä Windows 7:ssa, Mac OS X:ssa ja Linuxissa IPv6-tuki on valmiina.

3 IPv6-protokolla

IPv6-osoite on laajentunut 128 bittiin, ja kehysrakennetta on yksinkertaistettu. Osoitekokoa on laajennettu IPv4-osoitteiden väjäättömän loppumisen vuoksi. Uusi protokolla palauttaa Internetiin end-to-end-periaatteen, koska jokainen laite voidaan yksilöidä. IPv6:n toiminnallisuutta voidaan laajentaa erillisillä laajennetuilla kehyksillä. ICMPv6-protokolla on ICMP:n (Internet Control Message Protocol) uusi versio.

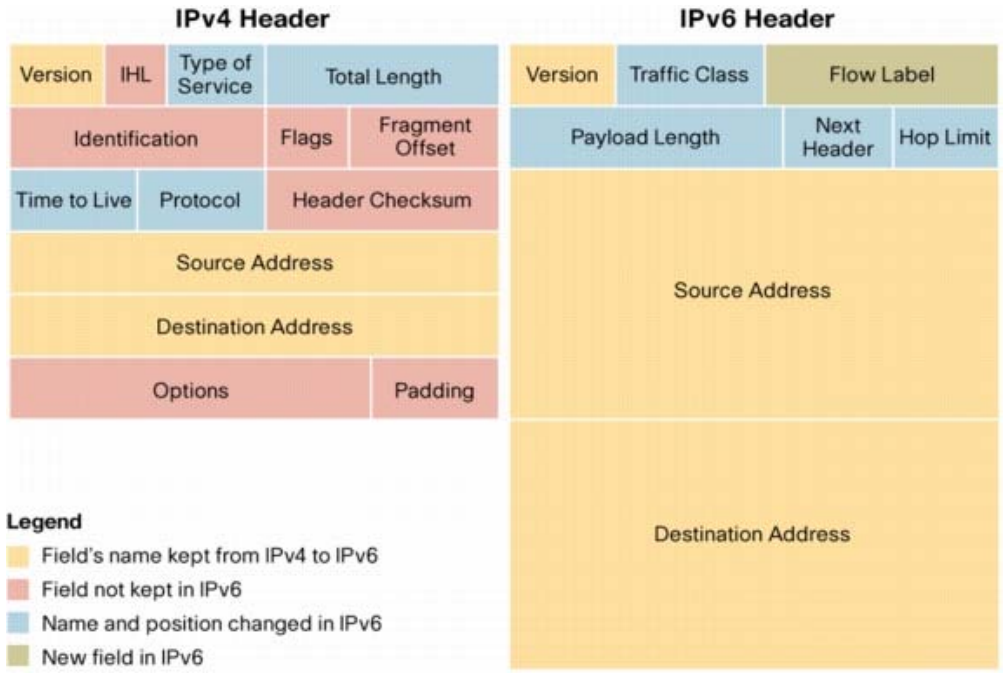
3.1 Kehysrakenne

IP-versio kuudessa kehysrakennetta on yksinkertaistettu jättämällä siitä pois IPv4:sta tutut kentät, joita ovat otsakkeen pituus, tunniste, liput, pirstaleen aloituskohta ja otsakkeen tarkistesumma. Kehys on kooltaan kiinteät 40 tavua, josta 8 tavua käytetään yleisille attribuuteille. Loput 32 tavua on jaettu lähde- ja kohdeosoitetta varten. RFC 2460 määrittelee IPv6:n kehysrakenteen. [3, s. 17.]

Kehyksen kiinteästä pituudesta johtuen kehyksen pituuden määrittelevä kenttä poistettiin. Optioiden käyttäminen IPv4:ssa kasvatti kehyksen kokoa neljän tavun välein aina 60 tavuun asti, joten pituus oli määriteltävä erikseen. IPv6:ssa optiot määritellään erillisellä jatketulla kehyksellä. [3, s. 17.]

Aikaisemmin reitittimet pilkkoivat IPv4-paketteja, mutta IPv6:ssa pirstalointi tapahtuu päätelaitteissa, joiden tehtävä on selvittää polussa käytettävissä oleva suurin siirtoyksikkö (MTU). Siirtoyksikkö sisältää mahdolliset kehykset, joten ne vievät osan käytettävissä olevasta kuormasta. Päätelaite sijoittaa pirstaloinnissa käytettävät kentät: tunnisteen, liput ja pirstaleen aloituskohdan IPv6:n jatkettuun kehykseen. Linkin MTU:n koon ylittävät paketit pudotetaan ja lähettäjälle lähtee ICMPv6-virheviesti. Standardin mukaisesti linkin pienin mahdollinen MTU on 1280 tavua. [3, s. 18.]

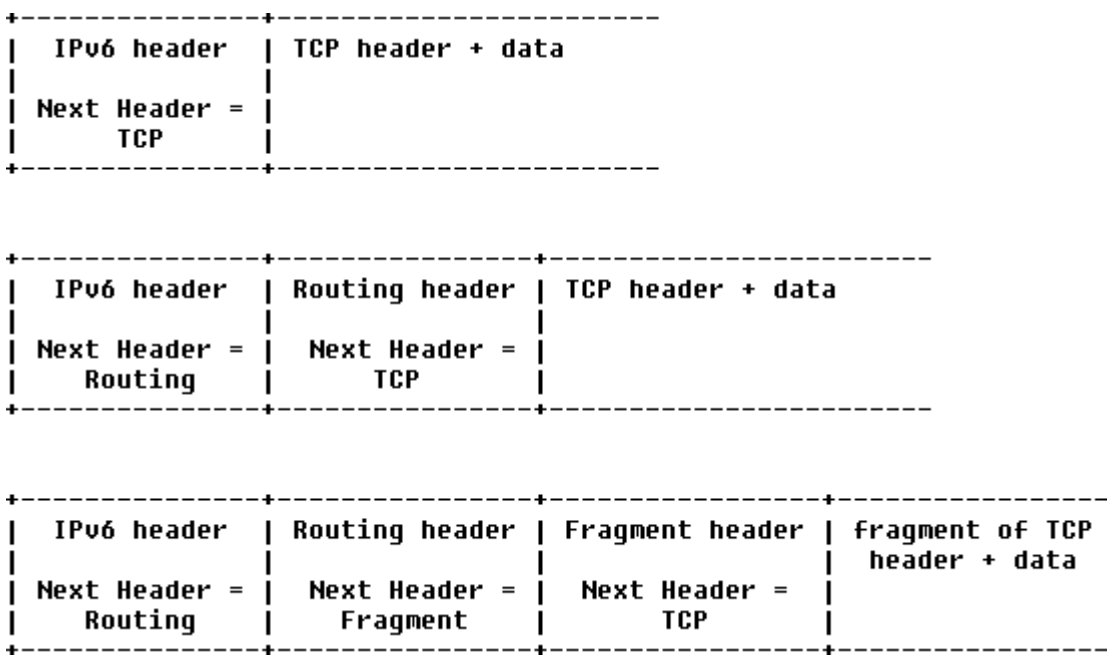
OSI-mallin neljäs kerros vastaa pakettien eheydestä, joten IPv6:ssa kolmannella kerroksella tapahtuvaa tarkistussummien tarkastamista ei enää ole. Kuvassa 1 voidaan havaita edellä mainittujen kenttien puuttuminen ja vuokehyksen lisäys kehysrakenteeseen. Vuokehyksen (flow label) tarkoitus on tarjota reaaliaikaisen tietoliikenteen siirtoon sekvensointimahdollisuuksia optioiden avulla. Vuo tunnistetaan käyttämällä kehystä ja lähdeosoitetta. [3, s. 20.]



Kuvio 1. IPv4- ja IPv6-kehyksien rakenteelliset erot. [4.]

3.2 Laajennetut kehykset

Laajennettuja kehyksiä käytetään kuvan 2 mukaisesti:



Kuvio 2. Laajennettu kehysrakenne (RFC 2460). [5.]

Tarvittaessa IPv6-pakettiin voidaan liittää useita kehyksiä, joilla voidaan vaikuttaa pirstalointiin, reititykseen ja paketin käsittelyyn sen saapuessa. RFC:ssa määritellään kuusi erilaista lisäkehystä, joiden järjestystä tulee tarkkailla, kun niitä yhdistetään peräkkäin. Laajennettu kehys liitetään pakettiin aina ennen ylemmän tason protokollaa. Kuviossa 2 viimeisellä rivillä havaitaan IPv6-kehyksen perään liitetty reitityskehys, jonka jälkeen on pirstaloitua TCP-dataa. IPv6-spesifikaation mukaisesti kaikkien liikennöivien laitteiden tulisi hyväksyä laajennettuja kehyksiä ja käsitellä niitä kykynsä mukaan.

Eräs kaikkien laitteiden prosessoitava kehys on Hop-by-Hop. Tällöin next-header-kenttä saa arvon 0 ja Hop-by-Hop-kehyksen on sijaittava välittömästi IPv6-kehyksen jälkeen [5, kpl. 4]. Hop-by-hopin mahdollistamaa jumbogram-optiota käyttämällä IPv6-paketin kokoa voi kasvattaa yli 64 kilotavun. RFC 2676 määrittelee Jumbogram-pakettien käytön ja laajennukset UDP- sekä TCP-protokollille [3, s. 26].

Reitityskehyksen avulla paketti voi kulkea ennalta määritellyn reititinpolun kautta, kunnes IPv6-kehyksen kohde saavutetaan. Kehyksessä olevan jäljellä olevien segmenttien määrän laskuria vähennetään yhdellä, kun kehys kulkee reitittimen läpi, jos laskuri saavuttaa nollan kohdetta, hylätään paketti ICMP Parameter Problem -virheilmoituksella. Reitityskehyksen optio 0 vastaa IPv4:n loose source routingia, ja voi aiheuttaa tietoturvauhan. IPv6 RFC:n mukaan kaikkien laitteiden ja reittimien tulisi käsitellä laajennettuja kehyksiä, jonka vuoksi osa laitteista saattaa päästää kehyksiä läpi. Tietoturvan vuoksi laajennetut kehykset kannattaisi estää, kun niitä ei tarvita. [11, s. 18/57.]

IPv6:ssa verkkoon dataa lähettävät päätelaitteet pirstaloivat paketteja tarpeen mukaisesti, mikä hoidetaan erillisellä pirstalekehyksellä. Kehyksessä on pilkkomattoman paketin sisältö, pirstaleen alun osoitin, M-lippu ja kyseistä palasta yksilöivä tunniste. IPv6-paketin alkuperäisen kehyksen seuraavaa kehystä osoittava kenttä saa täten arvon 44, jolloin vastaanottava laite osaa odottaa tulevia palasia. M-lippu on arvoltaan 1, kun pirstalointi jatkuu, ja vastaavasti 0, kun viimeinen osa on lähetetty. [3, s. 20.]

Tunniste toimii juoksevana numerointina jokaista ylisuurta pakettia kohden. Erityistä fragmentoinnin kieltävää Don't Fragment -lippua ei enää ole IPv6:ssa, sillä reitittimet eivät pirstaloi vaan pudottavat ylikokoiset paketit. Kaikkien osien tulisi olla perillä 60 sekunnin sisällä, tai vastaanottaja hylkää paketit ja lähettää ICMPv6-virheviestin.

Palomuureissa ja IPS-laitteissa fragmentointia voidaan lähestyä kahdelta kannalta. Yksinkertaiset palomuurit voivat välttää paljon tehoa vaativan pakettien kokoamisen. Joissain tapauksessa tunnelointi saattaa vaikeutua paketin käsittelyn vuoksi. Selvänä etuna pakettien kasaamisessa on koko paketin tarkastelu, joka on pakollista deep packet inspection -menetelmää käyttävissä palomuureissa ja IPS-laitteissa. [12, s. 15-19.]

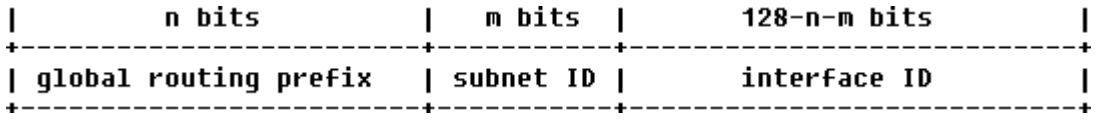
IPsec on huomioitu IPv6:n suunnitteluvaiheessa, joten autentikaatiokehys (AH) ja salatun paketin (ESP) kehys ovat osa laajennettuja kehyksiä. AH ja ESP sijaitsevat siis ylemmän kerroksen kehyksiä, joita ovat esimerkiksi TCP ja UDP.

3.3 Osoitejärjestelmä

IPv6:ssa osoite on pituudeltaan 128 bittiä, joten se riittää kattamaan jokaisen mahdollisen verkkoon kytkettävissä olevan laitteen. Osoitteet voidaan jakaa kolmeen ryhmään: unicastiin, multicastiin ja anycastiin. IP-protokollan versiosta 4 tunnettu yleislähetys ei ole enää käytössä, mutta tunnetaan link-local-tyyppisenä multicastina. Osoite voi olla tyypiltään globaali, ei-globaali tai linkkiosoite (link-local). Linkkiosoitteet ovat osa uuden protokollan toimintaa, joten sellainen tulee olla jokaisella liikennöivällä laitteella. [3, s. 36–37.]

Osoitteet esitetään heksadesimaalijärjestelmällä niiden pituuden vuoksi. Esitystapa on säilynyt periaatteeltaan IPv4:n mukaisena muodossa *osoite/prefiksin pituus*. IPv6-verkoissa prefiksin pituus rajaa verkon ja hostin käytettävissä olevat osoitteet. Osoite on jaettu kahdeksaan 16 bitin pituiseen lohkoon [3, s. 36.]

IPv6-osoite voi olla muodoltaan kuten 2001:db8:18a::216:cbff:fe9f:da45/64. Esimerkin osoite sijaitsee aliverkossa 2001:db8:18a:0000::/64 ja hostin tunniste on 216:cbff:fe9f:da45. Kaksoispiste vastaa osoitteessa olevia useita nollia, joten niitä ei tarvitse kirjoittaa erikseen. Vastaavasti 0db8 voidaan lyhentää muotoon db8 eli etunollilla ei ole merkitystä. Kuva 3 havainnollistaa osoitteen rakennetta.



Kuvio 3. IPv6-osoitteen rakenne (RFC 3587) [6.]

3.4 ICMPv6-protokolla

Tärkeänä osana IPv6-protokollaa on ICMPv6, joka kontrolloi pakettien välittämistä hostien ja reitittimien välillä. Se tarjoaa lisäksi tietoa pakettien siirrossa tapahtuvista ongelmista ja on ICMP-protokollan tavoin diagnostisen funktion. ICMPv6 seuraa mm. naapurien linkkiosoitteita, reitittimiä, naapurien saavutettavuutta ja muuttuneita linkkitason osoitteita. Nämä toiminnot olivat aikaisemmin ARPin tehtäviä. [3, s. 60.]

ICMP:n lähettämät viestit on jaettu kahteen luokkaan; virheet ja informatiiviset viestit. Virheviestien tyyppikoodit alkavat nollasta ja loppuvat lukuun 127. Erilaisia virheviestejä ovat [7.]

- Destination Unreachable (message type 1)
- Packet Too Big (message type 2)
- Time Exceeded (message type 3)
- Parameter Problem (message type 4).

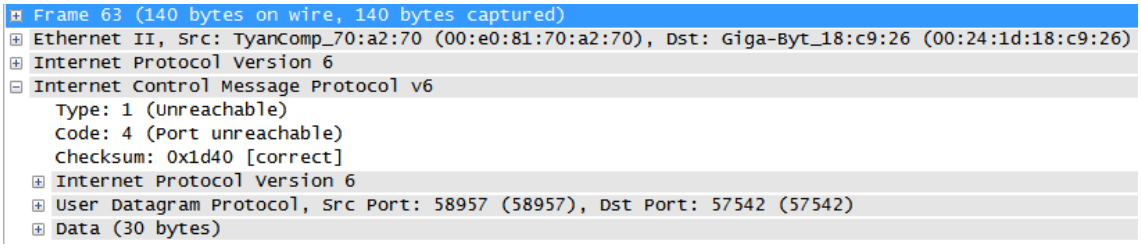
Informatiivisia ja verkon diagnostiikan kannalta tärkeitä viestejä ovat [7.]

- Echo Request (message type 128)
- Echo Reply (message type 129).

Yleisin Destination Unreachable -viesti lähetetään, kun IPv6-paketti ei tavoita kohdeosoitettaan. Syynä voi olla puuttuva reitti kohteeseen (koodi 0), liikenteen suodatus (koodi 1), osoite tavoittamattomissa linkistä johtuen (koodi 3) tai portti tavoittamattomissa (koodi 4). Virheviesti sisältää tyypin, joka tässä tapauksessa on 1 sekä koodi-, tarkistesumma- ja datakentän. Datakenttä sisältää kohteeseen lähetetyn paketin kehyksen ja datan, joka mahtuu ICMPv6-viestin sisälle [3, s. 64-65].

Virheviesti Parameter Problem kertoo lähettäjälle, että paketti on sisältänyt virheellisen kehyksen tai laajennetussa kehyksessä on virheitä. Viestin sisältämä koodi 0 ilmaisee syyksi kehyksen olevan virheellinen, 1 vastaavasti tunnistamattoman laajennetun kehyksen tyyppikoodin, ja viimeisenä 2 tunnistamattoman IPv6 option. Virheviestissä on osoitinkenttä, joka ilmoittaa alkuperäisessä paketissa tavun tarkkuudella tapahtuneen

virheen sijainnin. ICMPv6-viesti sisältää maksimissaan 1280 tavua alkuperäisestä viestistä eli IPv6:n minimi tiedonsiirtoyksikön (MTU) verran [3, s. 68].



Kuvio 4. Esimerkki ICMPv6 Destination Unreachable viestistä, jossa koodikenttä on 4. Tällöin kyseessä on ollut jonkin kohteen portin tavoittamattomuus, ja tässä tapauksessa UDP-portin 57542. Virheviestiin on siis sisällytetty alkuperäinen kehys datan kanssa.

3.4.1 Neighbor Discovery (ND)

ND eli naapurien selvitys on IPv4:n osoitteenselvitysprotokollaa (ARP) vastaava menetelmä, mutta on kuitenkin paranneltu monin tavoin. ND yhdistää ICMP:n reitittimen etsinnän ja uudelleenohjauksen, sekä verkon jäsenien osoitteiden selvittämisen. Uusittu menetelmä tarjoaa myös tavoittamattomien jäsenten tunnistuksen (Neighbor Unreachability Detection = NUD) ja päällekkäisten IP-osoitteiden tunnistamisen (Duplicate IP address detection = DAD). Naapureiden selvittämistä tarvitaan verkkoliitännän osoitteen automaattisessa konfiguroinnissa, prefiksien ja reittien määrittämisessä, DAD-menetelmässä, vaihtoehtoisten reititinten etsinnässä ja naapurien tavoitettavuuden selvityksessä. ND toimii ICMPv6:n informatiivisten ja virheviestien avulla. [3, s. 73-74.]

3.4.2 Reititinkyselyt (RS) ja mainostukset (RA)

Reitittimet lähettävät tasaisin väliajoin RA-viestejä multicast-osoitteeseen FF02::1, jota kaikki verkon jäsenet kuuntelevat. Verkon laite voi lähettää tarvitessaan RS-kyselyn osoitteeseen FF02::2, jota reitittimet seuraavat. Tällöin verkossa oleva reititin voi lähettää juuri kyseiselle laitteelle tietoa käytettävästä prefiksistä ja muista asetuksista.

RA-viestin kehyksessä oleva M-bitti kertoo viestin saajalle, että verkossa tulee käyttää tilallista konfiguraatiota (stateful configuration), joka IPv6:n tapauksessa on DHCPv6. Kaikissa laitteissa ei kuitenkaan aina ole DHCPv6-clienttia, mikä tarkoittaa laitteen toi-

mimista automaattisesti konfiguroidulla IPv6-osoitteella. O-bitin ollessa 1 laite hakee muut asetukset, kuten DNS:n, käyttämällä tilallista konfigurointia. H-bitti liittyy mobiiliin IPv6-verkkoon, mihin ei perehdytä tässä työssä. Loput viisi optiobittiä on varattu tulevaisuutta varten. [3, s. 76-77.]

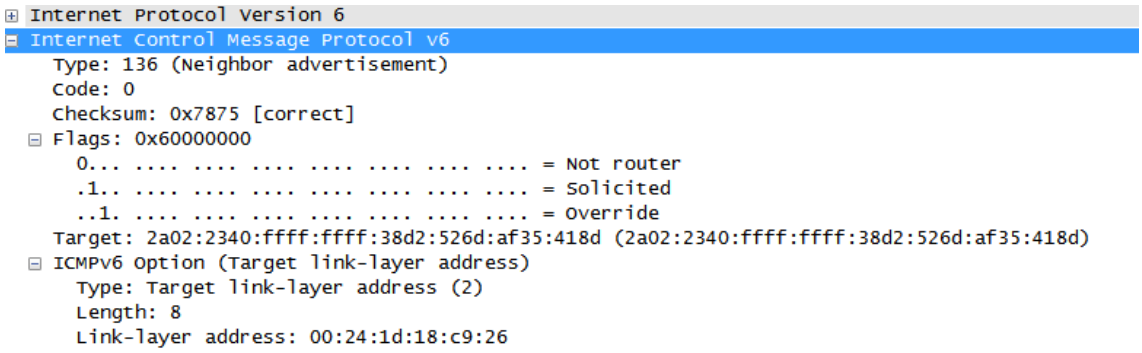
Viestissä kulkee tieto reitittimen elinajasta, jonka tulisi poiketa nollasta, kun reitittimen halutaan olevan aliverkon oletusreititin. Elinaika ilmoitetaan sekunneissa ja maksimikesto on 18,2 tuntia. RA-viestin optiot mahdollistavat myös tarkempien reittien mainostamisen loppukäyttäjälle, mikä voi olla hyödyllistä, kun halutaan parempi reititys vain tietylle verkolle. [3, s. 77.]

Lopuksi RA-viestin optiokenttä voi sisältää tiedon linkkikerroksen lähdeosoitteesta, MTU:n koosta ja käytettävästä prefiksistä.

3.4.3 Naapurikyselyt ja naapurimainostukset

Naapurin kysely ja naapurin mainostus viestien tarkoitus on toimia ARP-protokollan tavoin ja yhdistää IP6-osoite laitteen linkkikerroksen MAC-osoitteeseen. Sen lisäksi NS- ja NA-viesteillä selvitetään naapurin saatavuutta. Vastaavasti ARP:ssa kohteen MAC-osoitetta ei välttämättä saada selville. Tällöin naapuri todetaan kuolleeksi ja liikennöinti siihen estyy. [3, s. 77-78.]

Laite lähettää verkon all nodes -osoitteeseen FF02::1 määräajoin NS-viestin, jolla se selvittää, onko kyseinen IP6-osoite jo käytössä verkossa. Toisen verkon jäsenen tulisi vastata suoraan kyselyn lähettäneelle, kun tämä tiedustelee, onko laite elossa. Tässä tapauksessa lähettäjä asettaa NA-viestin S-bitin päälle (solicited), joka ilmaisee pyydettyä naapurin mainostusta. [3, s. 79.]



Kuvio 5. Neighbor advertisement -viesti käytännössä. Liput kertovat, että vastaanottajaa on pyydetty lähettämään unicast-kuittaus. Override-lippu pakottaa vastaanottajan päivittämään naapuritaulukkoaan kyseiselle osoitteelle. Link-layerin MAC-osoite yhdistetään silloin paketissa näkyvään kohdeosoitteeseen.

4 Tietoliikenteen salaaminen (IPsec)

IPsecia (IP Security Architecture) käytetään suojaamaan salaamatonta liikennettä julkisen verkon ylitse yhdistämään vaikka kahta eri toimipistettä. Tällöin liikenne tunneloidaan, salataan ja sille lasketaan tarkistussumma, jonka avulla koskemattomuus voidaan tarkistaa. IPsec-tuki on osa IPv6-toteutusta, minkä avulla sovellukset voivat salata liikenteen neuvottelemalla salauksen päästä päähän.

4.1 Turvallisuusassosioaatiot (Security Associations / SA)

IPsecin avulla liikennöivät laitteet muodostavat ns. SA-sopimuksia, joilla yhteys varmennetaan. Käytössä on kolme parametria: avain, salaus- tai autentikointimenetelmä ja muut yhteyteen liittyvät parametrit kuten avaimen elinaika. Ensimmäisessä vaiheessa neuvotellaan yksi kaksisuuntainen SA. Toisessa vaiheessa neuvotellaan yksi SA kuhunkin suuntaan, jolloin niitä käytännössä on vähintään kaksi kappaletta. [8.]

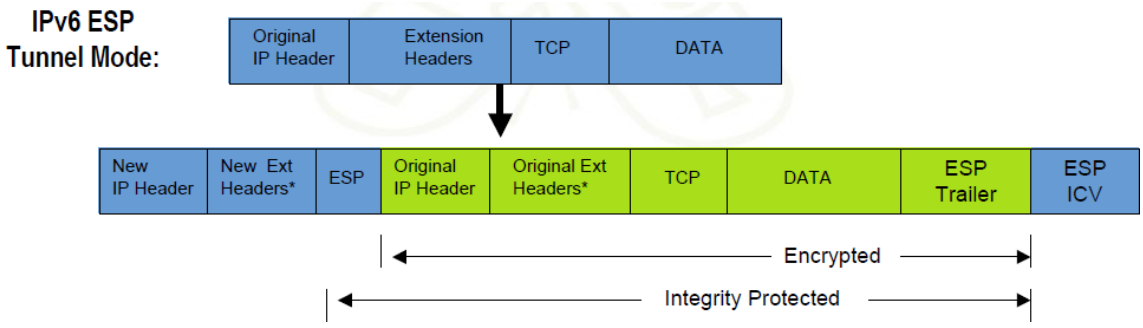
IPsec:ssa on kaksi erilaista tapaa siirtää tietoa. Transport-tilassa sovellukset neuvottelevat keskenään SA:n IP-paketin hyötykuormalle, mutta kehyksiä ei salata. Ulkopuolinen näkee liikenteestä vain lähteen ja kohteen, mutta ei esimerkiksi käytössä olevaa palvelua tai viestien sisältöä. Tunnelitilassa reitittimet tai palomuurit salaavat koko IP-paketin kehyksineen. Yritysverkoissa tämän tyyppinen tietoliikenteen tietoturvallisuus on kaikkein yleisintä. [3, s. 104.]

4.2 Avaintenhallinta

SA-viestit tulee suojata, mitä varten IPsec:ssa on tietoturvan varmistava IKE-protokolla (Internet Key Exchange). IKE-versio yhden yleisin protokolla avainten siirtämiseen on ISAKMP, joka kattaa SA-viestien ja avaimien hallinnan.

Ensimmäisessä vaiheessa vastapäät neuvottelevat IKE SA:n, joiden avulla parametrit neuvotellaan, avaimet vaihdetaan ja tunnistaminen sekä autentikointi tapahtuu. IKE SA suojaa toisessa vaiheessa tapahtuvaa Diffie-Hellman-vaihtoa. Ensimmäisen vaiheen SA muodostetaan tunnistamalla neuvottelevat IP-osoitteet sekä esijaetut avaimet.

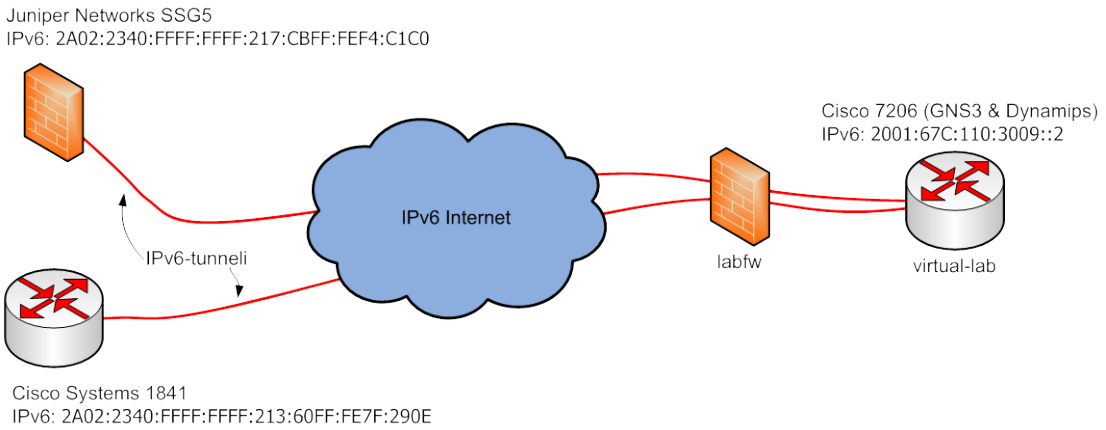
Toisen vaiheen tarvitsemat SA:t saadaan salaamalla ja autentikoimalla viestit ensimmäisen vaiheen IKE SA:lla. ESP ja AH käyttävät toisessa vaiheessa neuvoteltuja SA:ta, joten niitä on vähintään kaksi tai ESP+AH yhdistelmässä neljä. Liikenteen välittäminen VPN:n ylitse voidaan aloittaa, kun toisen vaiheen IPsec SA:t on neuvoteltu. IPsec sallii myös vain liikenteen koskemattomuuden tarkistamisen (AH), mutta yleensä koko viesti salataan käyttämällä ESP:ta. [3, s. 105.]



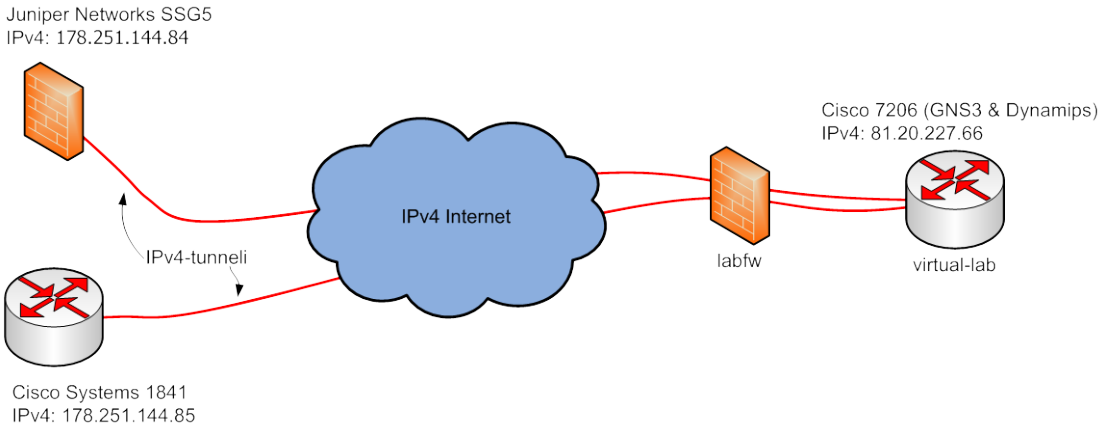
Kuvio 6. IPv4- ja IPv6-kehykset liikenteen kulkiessa tunneloidussa IPsec:ssa, ESP on laajennettu kehys. [9.]

5 IPsec-yhteyksien konfigurointi

IPsecin toimintaa testataan IPv4- ja IPv6-protokollilla käyttämällä vastapäänä Ciscon ja Juniperin laitteita. Erityistä huomiota kiinnitetään siihen, kykeneekö laite tunneloimaan IPv4-liikenteen IPv6 IPsec-tunnelin ylitse, IPv6-liikenteen IPv4 IPsecin kautta ja viimeisenä pelkän IPv6 IPsecin toimivuus. VPN-tunneleiden päätepisteeksi valittiin Cygaten virtuaalilaboratoriossa oleva GNS3-alustan päällä ajossa oleva Ciscon 7200-sarjan reititin. Virtuaalilaboratorio mahdollistaa reitittimelle menevän linkin seuraamisen Wireshark nimisellä pakettienkaappausohjelmalla ilman muun verkon konfigurointia.



Kuvio 7. IPv6 VPN -verkon yleiskuva. Tunneleiden sisällä kuljetetaan salattuja IPv4- tai IPv6-paketteja.



Kuvio 8. IPv4 VPN -verkon yleiskuva. Tunneleiden sisällä kuljetetaan salattuja IPv4- tai IPv6-paketteja.

5.1 Cisco - Cisco – VPN -yhteydet

Testilaitteina käytettiin virtuaalilaboratorion Cisco VXR7206 -reititintä, jonka ohjelmistoversiona oli uusin *(C7200-ADVENTERPRISEK9-M), Version 15.1(4)M3, RELEASE SOFTWARE (fc1)*. Vastapäänä käytettiin fyysistä Cisco 1841 -reititintä, jossa vastaavasti IOS *(C1841-ADVENTERPRISEK9-M), Version 15.1(4)M3, RELEASE SOFTWARE (fc1)*.

IPv6:sta ja reititystä varten laitteisiin tulee tehdä muutamia asetuksia, joilla IPv6 otetaan käyttöön. Ciscon reitittimet eivät tarvitse erityisiä lisenssejä tai lisäosia, jotta IPv6-protokollaa voidaan käyttää. Suositeltavaa on kuitenkin päivittää IOS uusimpaan, jotta mahdolliset ohjelmistovirheet eivät aiheuta ongelmia.

```
ipv6 unicast-routing
ipv6 cef

interface GigabitEthernet0/0
 ip address 81.20.227.66 255.255.255.248
 ipv6 address 2001:67C:110:3009::2/64

ipv6 route ::/0 2001:67C:110:3009::1
```

Liitännän alla olevista asetuksista on leikattu pois nopeuteen vaikuttavat konfiguraatiot, joilla ei labraympäristön reitittimen emuloinnin vuoksi ole merkitystä. Komennolla *ipv6 unicast-routing* otetaan käyttöön reitittimen staattiset ja dynaamiset reititysominaisuudet. Lisäksi asetetaan oletusreitti kohti laboratorion reitittävää kytkintä.

Vastapään reitittimelle asetetaan muuten samankaltaiset asetukset, mutta oletuksena Ciscon lähettämät RA-viestit halutaan laittaa pois päältä, jotta ne eivät häiritse muuta verkkoa. Tähän käytetään komentoa *ipv6 nd ra suppress all.*

```
interface FastEthernet0/0
 ip address 178.251.144.85 255.255.255.224
 duplex auto
 speed auto
 ipv6 address autoconfig
 ipv6 enable
 ipv6 nd ra suppress all
```

5.1.1 VRF (Virtual Routing and Forwarding) -tuki

Ciscon laitteissa voidaan käyttää VRF-tukea, jonka avulla reitittimellä voi olla useita toisistaan erotettuja reititystauluja. VRF:n avulla voidaan erotella asiakkaita toisistaan tai luoda verkkoja eri käyttötarkoituksiin, joita ovat hallinta ja data. Operaattoriverkoissa VRF:lle on tarvetta, sillä MPLS VPN -toteutuksissa asiakkaiden aliverkot voivat olla päällekkäisiä.

Normaalisti Ciscon VRF-tuki otetaan käyttöön reitittimen konfigurointitilassa komentamalla. Sen jälkeen VRF:ään pitää liittää jokin reittimen liitäntä, joka tässä tapauksessa on portti *GigabitEthernet 0/0*.

```
ipsecrtr1(config)#ip vrf hallinta
ipsecrtr1(config)#interface GigabitEthernet 0/0
ipsecrtr1(config-if)#ip vrf forwarding hallinta
```

Toisaalta IPv6-tuen myötä VRF:n konfigurointia Ciscon IOS:ssa on yhdenmukaistettu, koska entisessä syntaksissa komennot ovat ip-komentojen alaisuudessa, ja siten viittaavat IPv4:een.

Uudentyyppiseen VRF-määrittelyyn siirryttäessä voidaan ajaa seuraava komento ja siirtää vanhan tyyppiset VRF:t uuteen muotoon. Edellisen esimerkin mukaiset konfiguraatiot pysyvät samoina, mikäli valitaan non-common-policies.

```
ipsecrtr1(config)#vrf upgrade-cli multi-af-mode ?
common-policies IPv4 VRF policies are moved to common VRF
policies
non-common-policies IPv4 VRF policies are not moved to com-
mon VRF policies,but kept as ipv4 only VRF policies.
```

Valinnan jälkeen voidaan vielä määritellä päivitettävä VRF, jonka jälkeen IOS haluaa vahvistaa päivityksen. Huomattavaa on kuitenkin, että ip vrf forwarding -määrittelyn ja IPv6-osoitteen sisältävä liitäntä menettää IPv6-osoitteensa VRF:ää päivitettäessä. IPv4-osoitteet säilyvät ennallaan ja yhteyttä ei menetetä.

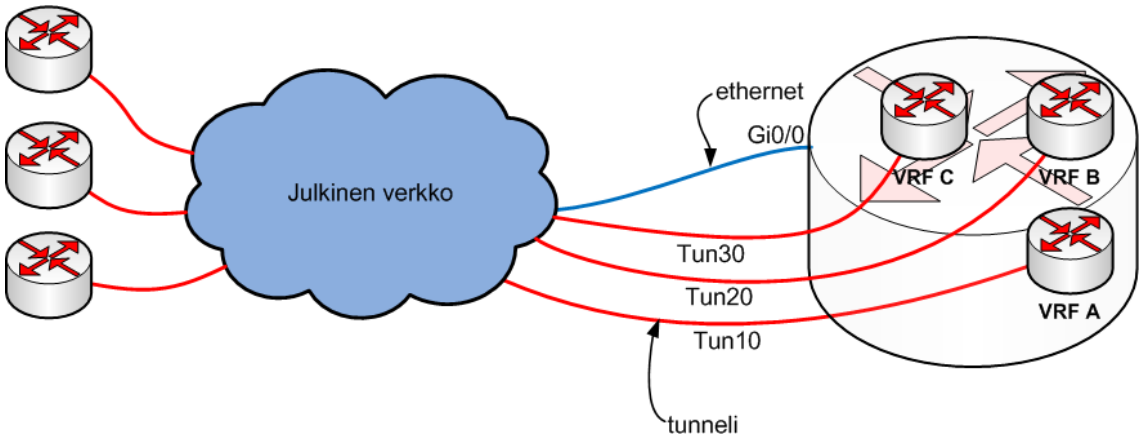
```
ipsecrtr1(config)#vrf upgrade-cli multi-af-mode common-
policies vrf vanhavrf
You are about to upgrade to the multi-AF VRF syntax com-
mands.
You will lose any IPv6 address configured on interfaces be-
long  ing to upgraded VRFs.
```

```
Are you sure ? [yes]: yes
Number of VRFs upgraded: 1
```

Tässä työssä konfiguroitiin uusi VRF kahta tunnelia varten, ja sille määriteltiin tuki kummallekin protokollalle. Liitännälle Tunnel10 ja Tunnel30 konfigurointiin VRF käyttämällä komentoa *vrf forwarding cisco_vrf*. Uutta VRF:aa luotaessa voidaan käyttää komentoa *vrf definition <vrf_nimi>*.

```
ipsecrtr1(config)#vrf definition cisco_vrf
ipsecrtr1(config)#address-family ipv4
ipsecrtr1(config)#exit
ipsecrtr1(config)#address-family ipv6
ipsecrtr1(config)#end
```

IPsec-tunneliliitäntä voidaan liittää tiettyyn VRF:ään, mutta varsinainen IPsec-yhteydessä käytettävä julkinen IP-osoite voidaan jakaa useiden asiakkaiden käytettäväksi. VRF:ia tarvitaan pitämään liikenne erillään eri verkkojen tai asiakkaiden välillä ennen palomuuria.



Kuvio 9. Periaatekuva VRF:n toiminnasta, liikenne eristetään IP-tasolla loogisten reitittimien alle.

Huomioitavaa on, ettei Cisco IOS tue VRF:n käyttöä OSPFv3:n kanssa. Konfiguraatiotilassa syötettävä komento *ipv6 router ospf [process]* ei anna täydentää VRF:n määrittelyä, toisin kuin vastaava OSPFv2-prosessin luova komento. Ciscon Feature Navigator –sivuston mukaan tukea ei vielä ole ja useat viestit Ciscon keskustelupalstalla viittaavat siihen, ettei tukea vielä ole. [21.] Tämän opinnäytetyön kirjoittamisen aikana Cisco on julkaissut IOS:n 7600-sarjan reitittimelle, jossa olisi kyseinen tuki. [20.]

5.1.2 IPv4- ja IPv6-liikenne IPv6 VPN:n ylitse

Ciscojen välisissä IPsec-yhteyksissä voidaan käyttää GRE-protokollaa (Generic Routing Encapsulation), jonka avulla saadaan sekä IPv6- ja IPv4-paketit välitettyä samassa tunnelissa. GRE-protokolla kulkee salattuna ESP:n hyötykuormassa, ja sen jälkeen voidaan sijaita IP-prokollien ohella esimerkiksi multicast-liikennettä.

Toinen vaihtoehto on käyttää normaalia tunnelointia, jossa ESP-kehys sisältää samatien IP-protokollan kehyksen ja datan. GRE:n käyttäminen kapselointina vähentää tunnelissa kuljetettavan hyötykuorman määrää, mutta se sallii toisen IP-protokolla version tai multicastin siirtämisen salattuna.

Konfiguroidaan laboratorioreititin VPN-yhteydelle ja käyttämään VRF:aa.

```
crypto keyring cisco_keyring
  pre-shared-key address ipv6
2A02:2340:FFFF:FFFF:213:60FF:FE7F:290E/128 key abcd1234

crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2

crypto isakmp profile cisco
 keyring cisco_keyring
 match identity address ipv6
2A02:2340:FFFF:FFFF:213:60FF:FE7F:290E/128
 keepalive 30 retry 30




crypto ipsec transform-set cisco-cisco ah-sha-hmac esp-3des
crypto ipsec profile cisco
 set transform-set cisco-cisco
 set pfs group2
 set isakmp-profile cisco

interface Tunnel10
 description to-Cisco_1841
 vrf forwarding cisco_vrf
 no ip address
 ipv6 address FD00:1000::1/64
 tunnel source 2001:67C:110:3003::2
 tunnel mode gre ipv6
 tunnel destination 2A02:2340:FFFF:FFFF:213:60FF:FE7F:290E
 tunnel protection ipsec profile cisco
```

Tunnelin toiminnan testaaminen tapahtui ensiksi ilman VRF:n konfigurointia. Tunneli nousi ylös, kun kaikki parametrit oli varmistettu kummastakin reitittimestä, jotta ne olisivat samat.

```
ipsecrtr1#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

IPv6 Crypto ISAKMP SA

 dst: 2001:67C:110:3009::2
 src: 2A02:2340:FFFF:FFFF:213:60FF:FE7F:290E
 conn-id: 1002  I-VRF:          Status: ACTIVE Encr: 3des Hash: sha  Auth: psk
 DH: 2  Lifetime: 23:01:47 Cap: D    Engine-id:Conn-id = SW:2
```

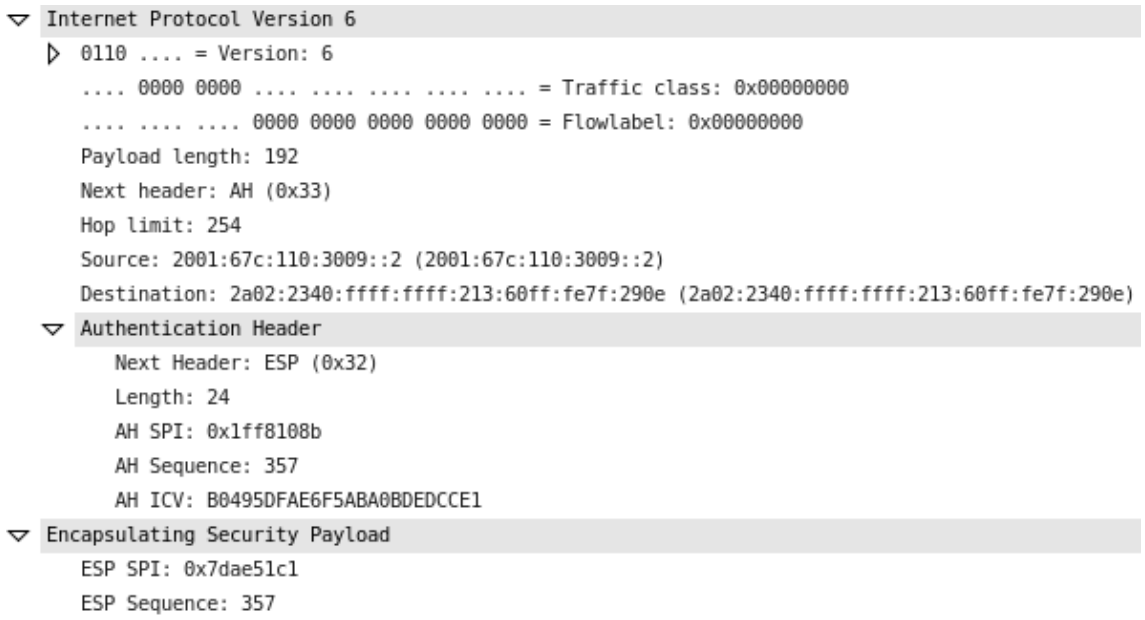
Kuvio 10. show crypto isakmp sa detail -komennolla voidaan tarkistaa IKE-neuvottelun lopputulos.

Kuviossa 7 nähdään onnistunut IKE/ISAKMP-kättely, jossa tila on aktiivinen ja seuraava avaimen uusiminen tapahtuu n. 23 tunnin kuluttua. Salaukseen on käytetty 3DES:ia. Varmenteena on SHA ja autentikoitumiseen on käytetty esijaettua-avainta (PSK). Avaimen pituus on 1024 bittiä, koska käytössä on Diffie-Hellmann ryhmä 2 [14.] Vastapää tukee DPD:ta, joka ilmenee kohdasta ”Cap: D”.

DPD (Dead Peer Detection) on tapa tunnistaa vastapään katoaminen, jolloin VPN:aa yritetään neuvotella ylös uudelleen [19.] Kaikki reitittimet ja palomuurit eivät tue DPD:ta, jolloin on suositeltavaa ottaa se pois käytöstä. Ciscon reitittimissä DPD voidaan ottaa pois käytöstä ISAKMP-profiilista komennolla *no keepalive*.

Yrittäessäni testata päästä päähän liikennettä huomasin, ettei vastausta saada onnistuneesta IPsecin neuvottelusta huolimatta. Liikenteen seuranta välissä olevalta reitittimeltä paljasti ESP-enkapsuloitujen pakettien hukkuvan matkalle, vaikka ne lähtivät virtuaalireitittimeltä kohti Internetiä.

Ongelma ratkesi avaamalla AH-protokolla välissä olevalta Juniper SSG520 -palomuurilta, koska AH-kehys sijaitsee paketissa ennen ESP:ta, jolloin palomuuri pudottaa sallimattoman liikenteen. Vaihtoehtoisesti Ciscon IPsec voidaan myös konfiguroida toimimaan ilman AH:ta, sillä ESP-protokolla tekee autentikoinnin.



Kuvio 11. Ulkopuolinen ei pääse tarkastelemaan Wiresharkia apuna käyttäen ESP-paketin sisältöä. Paketissa nähdään laajennettujen kehyksien ketjuttamista IPv6->AH->ESP.

Palomuurin konfiguroinnin jälkeen liikennöinti tunnelissa onnistui.

```
kotirtr1#ping fd00:1000::1 source fd00:1000::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FD00:1000::1, timeout is 2 seconds:
Packet sent with a source address of FD00:1000::2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/16 ms
```

Kuvio 12. Päästä päähän -liikenteen testaaminen ICMPv6-paketeilla käyttämällä ping-komentoa.

VRF:n käyttöönottamisen jälkeen liitännältä poistetaan kaikki olemassa olevat osoitteet, joten ne joudutaan konfiguroimaan uudestaan. Tästä huolimatta tunneloitua yhteyttä ei saatu toimimaan yllä olevalla ping-testillä. Syyn selvittämisessä käytin apuna *debug ipv6 packet* -komentoa, minkä avulla voidaan tarkastella pakettien kulkua niiden lähtiessä ja/tai saapuessa.

Debug-komennon tulosteessa erityisesti seuraavat rivit nousivat esille.

```
*Apr  7 22:22:42.176: IPv6-Fwd: Sending on
GigabitEthernet0/0
*Apr  7 22:22:42.180: IPv6-Fwd: No route to destination
2A02:2340:FFFF:FFFF:213:60FF:FE7F:290E
*Apr  7 22:22:42.184: IPv6-Sas: SAS picked source
FD00:1000::1 for 2001:67C:110:3009::2 (Tunnel10)
*Apr  7 22:22:42.184: IPv6-Fwd: No route to destination
2001:67C:110:3009::2
```

Tämän jälkeen jatkoin vianselvitystä tarkastelemalla cisco_vrf-nimisen VRF:n reititystaulua, josta puuttui reitti kohti julkista kohdeosoitetta.

```
ipsecrtr1#show ipv6 route vrf cisco_vrf
IPv6 Routing Table - cisco_vrf - 3 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, NM - NEMO, ND - Neighbor Discovery
       l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   FD00:1000::/64 [0/0]
     via Tunnel10, directly connected
L   FD00:1000::1/128 [0/0]
     via Tunnel10, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

Kuvio 13. VRF:n reititystaulu, josta ei löydy debug-tulosteen mukaisia kohteita.

VRF-instanssista tulee olla mahdollisuus liikennöidä tunnelin kohteeseen, joten lisäsin reitin kohdeosoitteeseen seuraavalla komennolla. Tämän jälkeen paketit liikkuivat reitittimien välillä ja ping-kyselyihin saatiin vastaus vastapäältä.

```
ipv6 route vrf cisco_vrf
2A02:2340:FFFF:FFFF:213:60FF:FE7F:290E/128
2001:67C:110:3009::1 nexthop-vrf default
```

IPv6-liikenteen välittämisen IPsecin ylitse todettiin toimivaksi, joten työn tarkoitus oli myös selvittää, voidaanko IPv4-paketteja lähettää natiivin IPv6-yhteyden ylitse salattuna. Käytössä kummallakin reitittimellä on GRE-kapsulaatio, joka voi välittää monia protokollia. Kummallekin reitittimelle konfigurointiin IPv4-osoite samasta aliverkosta, mutta esimerkiksi reititystä IPv4:n osalta ei säädetty lainkaan. Osoitteiden tulisi nyt olla tavoitettavissa esimerkiksi pingillä.

```
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/16/40 ms
```

Kuvio 14. IPv4-pakettien siirtäminen yli salatun IPv6-verkon onnistui.

Ciscon reitittimissä voidaan käyttää myös toisenlaista kapselointia, joka konfiguroidaan tunnel-liitännän alle komennolla *tunnel mode ipsec ipv6*. Edellä mainitussa menetelmässä uusi IPv6-kehys seuraa suoraan ESP:ta ilman välissä olevaa GRE-kehystä. Tämän jälkeen ping ei kuitenkaan onnistu, sillä IOS hylkää paketin seuraavalla virheviestillä.

```
*Apr  7 21:38:01.955: %IPSECV6-4-PKT_PROTOCOL_MISMATCH: IP
protocol in packet mismatched with tunnel mode, packet from
10.10.10.2 to 10.10.10.1 dropped by Tunnel10.
```

Virheestä voidaan päätellä, ettei IOS tue IPv4-paketin siirtämistä kyseisessä tilassa. Suurta etua ipsec ipv6 -tilasta ei saada, sillä MTU pienenee 1374 tavuun GRE:n sallimasta 1456 tavusta. Toisaalta kaikki reitittimet tai palomuurit eivät välttämättä tue GRE:n käyttöä. Ciscon laitteilla rakennettavia VPN-yhteyksiä voidaan tehdä GRE:n avulla, jotta IPv6:tta voidaan käyttää paikassa, johon sitä ei tarjota.

IPv4-pakettien siirtämisestä ipsec ipv6 -tilassa on tehty Ciscolle kehityspyyntö CSCtu09251, koska vastaavaan ongelmaan on törmätty asiaa tutkineiden keskuudessa. Ciscon ASA-palomuureissa osaavat eri protokollan tunneloinnin ilman GRE:ta, mutta ei IOS-pohjaiset reitittimet eivät. Vastaavanlaisesta tilanteesta löytyy maininta Ciscon omalta keskustelupalstalta. [16.]

Tunnelin kapseloinnin vaihtaminen aiheuttaa virheilmoituksia, joiden perusteella GRE-tunnelin käyttäminen on ainoa vaihtoehto, kun halutaan siirtää IPv6-liikennettä IPv4-verkon läpi salatusti. Tunnelin konfiguroiminen *tunnel mode ipv6ip* -komennolla aiheuttaa sen, ettei IPsec:ia voida ottaa käyttöön tunnelissa.

```
kotirtr1(config-if)#tun protection ipsec profile profile0
ERROR: tunnel protection is only valid on IPIP, GRE, IPSEC
and MGRE interfaces
```

Komennon *tunnel mode ipsec ipv4* ei vaikuta asiaan, sillä IPv6-paketit hukkuvat edelleen reitittimessä. Ainoaksi toimivaksi vaihtoehdoksi jää ajaa tunnelia GRE-

kapsuloinnilla, jos IPv4- ja IPv6-liikenne halutaan siirtää samassa tunnelissa. Kummallekin protokollalle voidaan tehdä oma tunneli, kun käytettävissä ovat Internetissä reitittyvät julkiset IPv4- ja IPv6-osoitteet.

5.1.3 IPv6-liikenne IPv4 VPN:n ylitse

Kummallekin reitittimelle konfiguroidaan uusi VTI (Virtual Tunnel Interface), jolle annetaan IPv6-osoite. Tunnelin kapsulointina käytetään oletusarvoisesti GRE:ta, mutta testaus suoritetaan myös ilman GRE-kapsulointia. VPN:n asetuksina käytetään samoja asetuksia kuin IPv6:n kanssa. Täten on riittävää, että IKE- ja IPsec-vaiheille lisätään vain uudet vastapään tunnistavat konfiguraatiot. IPv4 VPN:n toimintaan ei tässä kappaleessa perehdytä syvällisemmin. Käytännössä VPN-osuuden konfiguroimiseen riittää kahden rivin lisääminen.

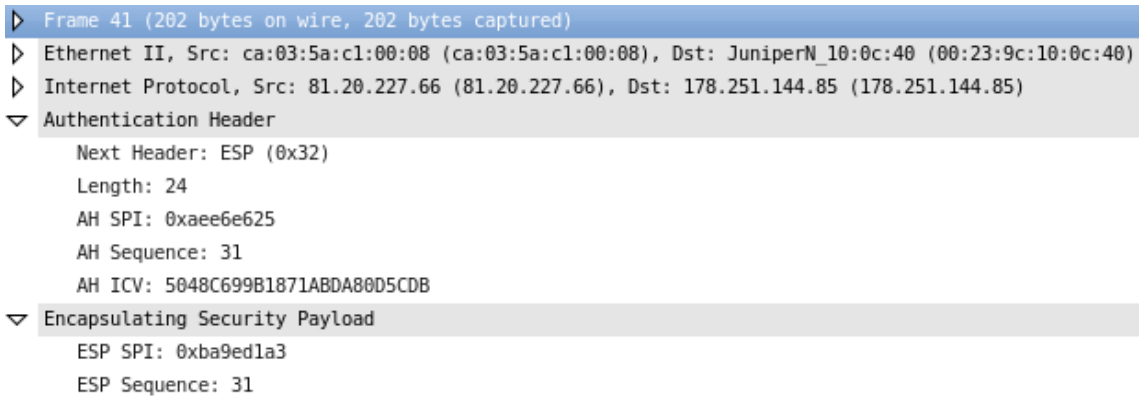
Uuden tunnelin asetukset laboratorioreitittimellä:

```
interface Tunnel30
 description Cisco_Cisco-IPv4-VPN
 vrf forwarding cisco_vrf
 no ip address
 ipv6 address FD00:1002::1/64
 tunnel source 81.20.227.66
 tunnel destination 178.251.144.85
 tunnel protection ipsec profile cisco
```

Uusi tunneli liitettiin myös cisco_vrf-nimiseen VRF-instanssiin, mutta erillistä IPv4-reittiä kohti tunnelin julkiseen kohdeosoitteeseen VRF:sta ulospäin ei tarvinnut lisätä. IPv4 ja IPv6 VRF:ssa on jokin ero toteutustavassa, jonka vuoksi IPv6:ssa tarvitaan reitti julkiseen verkkoon.

```
kotirtr1#ping fd00:1002::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FD00:1002::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
```

Kuvio 15. IPv6-paketit kulkevat salattuina päästä päähän IPv4 VPN:n avulla, minkä kapsulointina on käytössä GRE.



Kuvio 16. ICMPv6-paketit näyttävät verkkoliikenteen puolella kuin miltä tahansa muulta IPsec-liikenteeltä.

```
ipsecrtr1#show ipv6 route vrf cisco_vrf
IPv6 Routing Table - cisco_vrf - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, NM - NEMO, ND - Neighbor Discovery
       l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   ::/0 [1/0]
     via 2001:67C:110:3009::1%default
C   FD00:1000::/64 [0/0]
     via Tunnel10, directly connected
L   FD00:1000::1/128 [0/0]
     via Tunnel10, receive
C   FD00:1002::/64 [0/0]
     via Tunnel30, directly connected
L   FD00:1002::1/128 [0/0]
     via Tunnel30, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

Kuvio 17. IPv4- ja IPv6-tunnelien liitäntöjen verkot näkyvät nyt samassa cisco_vrf-reititystaulussa, mutta liikenne kulkee omissa tunneleissaan.

5.2 Cisco – Juniper Networks SSG5 (Netscreen) – VPN -yhteydet

Juniperin valmistama SSG5 on pieni palomuurituote, jonka käyttöjärjestelmänä on ScreenOS. Laite on suunniteltu pienten toimipisteiden etäyhteyksien rakentamiseen, ja se voidaan jopa klusteroida yhteyksien varmistamiseksi.

Palomuurin konfigurointi tapahtuu komentoriviltä tai vaihtoehtoisesti web-pohjaisen käyttöliittymän avulla. Useiden laitteiden keskitettyyn hallintaan Juniper Networksilla on Network Security Manager eli NSM, jonka asentaminen tämän työn kannalta ei ollut tarpeellista. Laitteen ohjelmistoversio päivitettiin uusimpaan versioon 6.3.0r10.0, jossa on mukana OSPFv3-tuki.

Ennen IPv6:n käyttöönottoa Netscreenille tulee antaa komento *set envar ipv6=yes*, minkä jälkeen laite pyytää uudelleenkäynnistystä asetuksien aktivoimiseksi [15]. Tämän jälkeen palomuuri konfiguroitiin asettamaan IPv6-osoitteensa lähiverkon IPv6-reitittimen RA-viesteistä.

5.2.1 IPv6 VPN:n konfigurointi

VPN:n pystyttämisessä jouduin kokeilemaan useita erilaisia asetuksia ennen kuin liikennettä voitiin siirtää laitteiden välillä. Hyödylliseksi osoittautui IPv4 VPN:ia käsittelevä artikkeli Mozilla Firefoxin kehittäjän blogista, mistä oli apua sopivien neuvotteluasetuksien löytämisessä [17.] Ensimmäisen vaiheen neuvotteluasetuksissa toimiviksi osoittautuivat taulukon 1 mukaiset asetukset.

Taulukko 1. Toimivat P1-asetukset Juniperin ja Ciscon välillä.

Encryption	3DES
Hash	MD5
PFS	Group2

Ciscossa konfigurointi tapahtui lisäämällä sopiva isakmp politiikka. IKE-neuvottelun alkaessa vastapään tarjoamia asetuksia verrataan järjestysnumeron mukaisesti konfiguroituihin politiikkoihin. Avainten elinajaksi asetettiin 28 800 sekuntia, joka on Netscreenin mukainen oletusarvo. Alla oleva ote konfiguraatiosta määrittelee taulukon mukaiset asetukset.

```
crypto isakmp policy 5
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 28800
```

Muut asetukset Netscreenia varten konfiguroitiin seuraavanlaisesti. Liitännän Tunnel20-konfiguraatiossa on käytössä OSPFv3-reititysprotokolla.

```
crypto isakmp profile juniperssg
 keyring juniperssg_keyring
 match identity address ipv6
2A02:2340:FFFF:FFFF:217:CBFF:FEF4:C1C0/128
 no keepalive

crypto ipsec transform-set juniperssg esp-3des esp-sha-hmac

crypto ipsec profile juniperssg
 set transform-set juniperssg
 set pfs group2
 set isakmp-profile juniperssg

interface Tunnel20
 description Cisco_Netscreen-IPv6-VPN
 ip address 10.10.20.1 255.255.255.0
 ipv6 address FD00:1001::1/64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 10 area 0
 tunnel source 2001:67C:110:3009::2
 tunnel mode ipsec ipv6
 tunnel destination 2A02:2340:FFFF:FFFF:217:CBFF:FEF4:C1C0
 tunnel protection ipsec profile juniperssg
```

Netscreenissa löytyy vastaavasti valmiiksi määriteltyjä IKE-asetuksia, joten pre-g2-3des-md5-nimistä asetusta voidaan käyttää IKE-neuvottelussa.

pre-g2-3des-md5	Preshare	2	3DES/MD5	28800

Kuvio 18. Netscreenin P1-asetukset, jossa luku 2 tarkoittaa DH-ryhmää ja 28800 avaimen elinaikaa.

VPN-yhteys luodaan Netscreenin web-käyttöliittymällä valitsemalla kirjautumisen jälkeen vasemmasta valikosta VPNs ja sen jälkeen AutoKey IKE. New-painikkeella päästään luomaan uusi VPN ja asetukset uudelle yhteydelle valitaan taulukon 2 mukaisesti.

Taulukko 2. Juniper Netscreenin VPN-asetukset.

VPN Name	v6-vpn-to-lab
Gateway Name	lab-gw
Type Static IP: Address/Hostname	2001:67c:110:3009::2
Local ID	jätetään tyhjäksi
Preshared Key	abcd1234 (ei ruksia kohdassa Use as seed)
Security Level	Standard, joka vaihdetaan myöhemmin gateway-asetuksista tilaan Custom ja pre-g2-3des-md5

Web-käyttöliittymä luo tarvittavat komennot Netscreenin konfiguraatiotiedostoon. Erityisesti asetuksien kokeilemisen yhteydessä käyttöliittymän nopeus helpotti vaihtoehtojen läpikäymistä. Sopivat asetukset toisen vaiheen neuvottelulle selvitettiin kokeilemalla ja toimivat asetukset nimettiin nimellä *cisco*.

```
set ike p2-proposal "cisco" group2 esp 3des sha-1 second
3600
set ike gateway "lab-gw" address 2001:67c:110:3009::2 Main
outgoing-interface "ethernet0/0" local-address
"2a02:2340:ffff:ffff:217:cbff:fef4:c1c0" preshare
"fXaHlgU2Nb7C7qsmVTC64n7tkUniedygqQ==" proposal "pre-g2-
3des-md5"
set vpn "v6-vpn-to-lab" gateway "lab-gw" replay tunnel
idletime 0 proposal "cisco"
set vpn "v6-vpn-to-lab" id 0x2 bind interface tunnel.1
```

IPsec-asetuksissa jouduttiin käyttämään autentikointina SHA1-algoritmia, mikä on SHA256:sta heikompi. Syynä lienee GNS3:n alla emuloitava Ciscon reititin, joka normaalisti käyttäisi fyysistä kryptomodulia pakettien kryptaamiseen ja purkamiseen. Emuloitavassa ympäristössä kryptomoduli puuttuu, jolloin salatut paketit eivät kulje onnistuneesta IPsec-neuvottelusta huolimatta. Virhe näkyy reitittimen logissa tai debug-tulosteessa *%CRYPTO-4-RECVD_PKT_MAC_ERR: decrypt: mac verify failed* -virheenä.

Autentikointialgoritmin vaihdon jälkeen paketit kulkevat kumpaankin suuntaan ja logeista voidaan tarkastella, että IPsec-vaihe on onnistunut. Netscreenin komentorivillä

VPN:iin liittyviä tapahtumia voidaan tarkastella komennolla *get event type 536* tai vaihtoehtoisesti käytetään web-käyttöliittymän *Reports->System Log*:n alla olevaa *Event*-näkymää. Seuraavana on esimerkki onnistuneesta IPsec-neuvottelusta.

```
2012-04-11 00:54:19 info IKE 2001:67c:110:3009::2 Phase 2
msg ID fec51971: Completed negotiations with SPI d46fba2c,
tunnel ID 2, and lifetime 3600 seconds/4194303 KB.
2012-04-11 00:54:19 info IKE 2001:67c:110:3009::2 phase
2:The symmetric crypto key has been generated successfully.
```

Tarkistetaan muodostunut yhteys ping-komennolla ja todetaan se toimivaksi.

```
kotifw1-> ping fd00:1001::1
Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to fd00:1001::1, timeout is 1 seconds
!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=7/8/12 ms
```

Kuvio 19. Toimiva IPv6 VPN-yhteys Ciscolta Juniper SSG5 -palomuurille.

Juniperin ja Ciscon tunneliliitännöille konfiguroitiin IPv4-osoitteet, joilla voidaan testata menetelmien yhteensopivuutta. Ciscon reitittimestä johtuen IPv4-liikennettä ei voitu välittää tässäkään tapauksessa, kun käytössä on ipsec ipv6 -tila. Reitittimeltä ping-komentoa ajettaessa saadaan seuraava virheilmoitus.

```
*Apr 11 00:40:15.106: %IPSECV6-4-PKT_PROTOCOL_MISMATCH: IP
protocol in packet mismatched with tunnel mode, packet from
10.10.20.1 to 10.10.20.2 dropped by Tunnel20.
```

Netscreen-palomuurin tunneliliitäntä voidaan asettaa toimimaan GRE-tilassa, mutta IPsec ei tarjoa vastapäälle proxy ID -asetuksina samanlaisia arvoja. Tällöin proxy ID -arvot joudutaan asettamaan käsin tunnelin up-tilaan saamiseksi. Lisäksi tunnelin local interface asetus pitää olla ethernet0/0 tai tunneli ei nouse ylös. Ciscon reitittimellä tunnelin toiminnan vaihtaminen GRE:ksi riittää, mutta *mac verify failed* -virheitä kertyy logiin, eikä liikenne tunnelissa kulje.

Juniper Networksin palomuurin GRE-toteutuksen vuoksi Ciscon reitittimien ja Netscreen-palomuurien välillä ei voida siirtää IPv4-liikennettä salattuna samassa tunnelissa IPv6-liikenteen kanssa. Netscreenin konfigurointimahdollisuudet antavat viitteitä myös

siitä, ettei GRE ole tarkoitettu käytettäväksi yhdessä IPsecin ja erityisesti IPv6:n yhteydessä.

Juniperin konfigurointiopas Netscreenille sisältää esimerkkejä 6in6, 4in6 ja 6in4 IPsec-yhteyksien rakentamisesta valmistajan omilla palomuureilla, mutta GRE:sta ei ole mainittu mitään [18.] Saman valmistajan tuotteilla on siis mahdollista rakentaa siirtymävaiheen verkko, jossa kummatkin protokollat ovat salattuina samassa VPN-putkessa. Siirtymävaiheella tarkoitetaan tässä tilannetta, jossa ulkoista yhteyttä toisella protokollalla ei ole käytettävissä, minkä vuoksi sisäisten palveluiden liikenne tunneloidaan julkisen verkon ylitse.

5.2.2 OSPFv3:n toimivuuden testaaminen

Cygate Oy:n hallintayhteyksien kannalta OSPFv3:n tuki on yksi olennainen osa IPv6-protokollaan käyttöönotossa, joten aihetta sivutaan tässä työssä. Juniperia varten Ciscolle ei lisätty erillistä VRF:aa, joten OSPFv3 voidaan konfiguroida kummallekin laitteelle.

Tunnelille konfiguroitavat OSPFv3-asetukset ovat kappaleen 5.2.1 konfiguraatiolistauksessa. Juniperille on OSPFv3 on konfiguroitu seuraavalla tavalla. OSPFv3:n vaatima router-id asetetaan kummankin laitteen julkiseksi IPv4-osoitteeksi.

```
kotifw1-> get config | i ospfv3
set protocol ospfv3
set router-id 178.251.144.84
set interface tunnel.1 protocol ospfv3 area 0.0.0.0
set interface tunnel.1 protocol ospfv3 enable
set interface tunnel.1 protocol ospfv3 cost 10
```

```
kotifw1-> get vrouter trust-vr protocol ospfv3 neighbor
VR: trust-vr RouterId: 178.251.144.84
-----------------------------------
                Neighbor(s) on interface tunnel.1 (Area 0.0.0.0)
RouterId        Nbr-saw-DR      Nbr-saw-BDR     Nbr-If-Id  Opt      Pri State   (Down, Up)
-------------------------------------------------------------------------------
81.20.227.66    0.0.0.0         0.0.0.0         0x00000007 --V6|E|R 1   FULL    (+5    -0)
```

Kuvio 20. OSPFv3-naapuruus reitittimien välillä on kunnossa, joten GRE:ta ei tarvitse käyttää Netscreenin ja Ciscon välillä.

Testataan prefiksien mainostamista Netscreenille luomalla Ciscoon loopback-liitäntä, jolle annetaan IPv6-osoite.

```
interface Loopback1210
 no ip address
 ipv6 address FEED:CAFE::BEEF/64
 ipv6 ospf network point-to-point
 ipv6 ospf 10 area 0
```

Netscreen lisää mainostetun prefiksin trust-vr-virtuaalireitittimen IPv6-reititystauluun. Point-to-point-määrittelyn vuoksi vastapää saa tiedokseen koko aliverkon koon /64, eikä vain yksittäistä osoitetta /128.

```
kotifw1-> get route protocol ospfv3

IPv6 Dest-Routes for <untrust-vr> (0 entries)
------------------------------------------------------------------------------
H: Host C: Connected S: Static A: Auto-Exported
I: Imported R: RIP/RIPng P: Permanent D: Auto-Discovered
N: NHRP
iB: IBGP eB: EBGP O: OSPF/OSPFv3 E1: OSPF external type 1
E2: OSPF/OSPFv3 external type 2 trailing B: backup route

IPv6 Dest-Routes for <trust-vr> (8 entries)
------------------------------------------------------------------------------
         ID                                   IP-Prefix       Interface
                                                Gateway   P Pref    Mtr     Vsys
------------------------------------------------------------------------------
*        23                             feed:cafe::/64          tun.1
                               fe80::c803:5aff:fec1:6   O   60     11     Root
```

Kuvio 21. Tulos ja komento Netscreenin OSPFv3:lla opittujen reittien tarkastelua varten.

5.2.3 IPv4- ja IPv6-liikenne IPv4 VPN:n ylitse

Netscreenin tuki GRE-protokollan käyttämiseen IPsecin kanssa ilmeni heikoksi jo aikaisemmassa testissä, joten tarkastetaan voiko Netscreen tunneloida IPv6:tta GRE:n sisällä ilman IPsecia. Ciscolle lisätään normaali tunneliliitäntä, joka oletusarvoisesti on GRE-tunneli.

```
interface Tunnel40
 description Cisco_Netscreen-IPv4-VPN
 no ip address
 ipv6 address FD00:1004::1/64
 tunnel source 81.20.227.66
 tunnel destination 178.251.144.84
```

Vastaavasti luodaan Netscreeniin liitäntä tunnel.2.

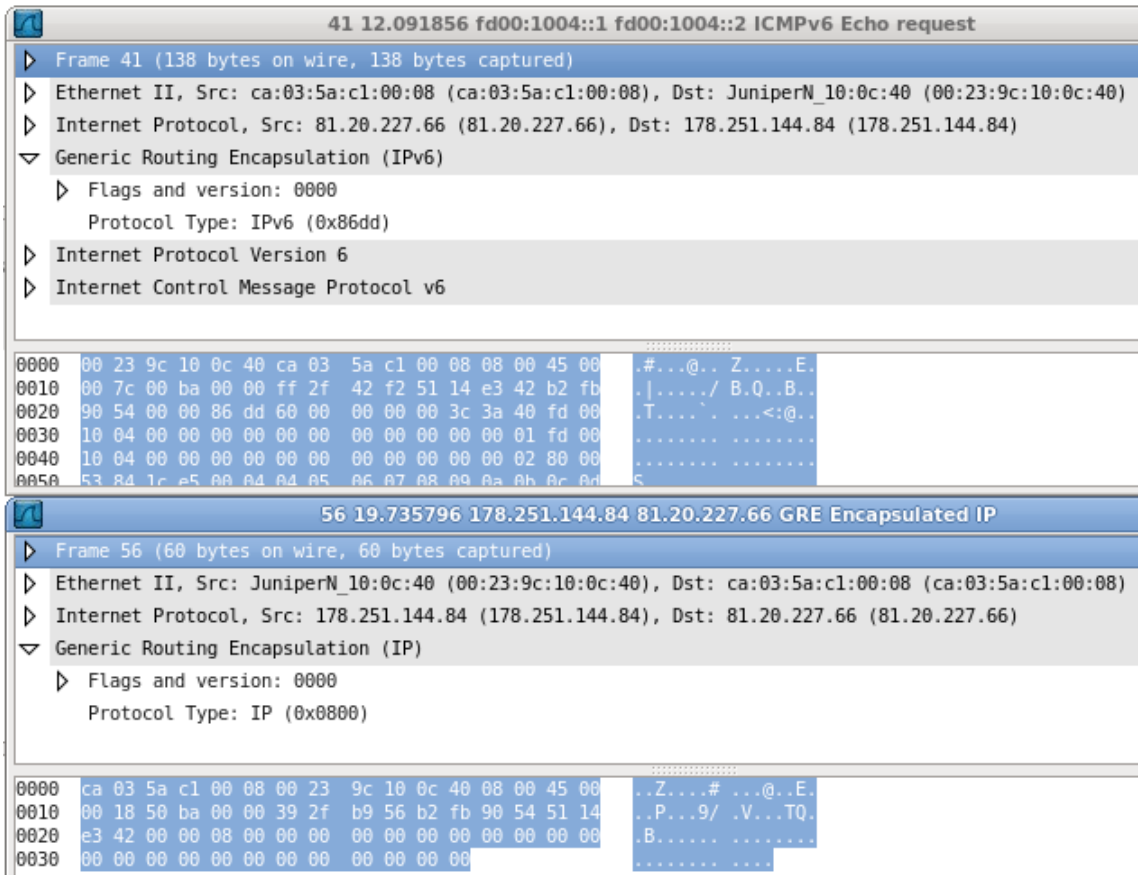
```
set interface "tunnel.2" zone "Untrust"
set interface "tunnel.2" ipv6 mode "host"
set interface "tunnel.2" ipv6 ip fd00:1004::2/64
set interface "tunnel.2" ipv6 enable
set interface tunnel.2 tunnel encap gre
set interface tunnel.2 tunnel local-if ethernet0/0 dst-ip
81.20.227.66
```

Tunneliliitännät ovat ylhäällä kummassakin laitteessa.

```
Interface tunnel.2:
  link ready, admin status up

Interface Status Protocol Description
Tu40      up     up       Cisco_Netscreen-IPv4-VPN
```

Tästä huolimatta pingin ajaminen virtuaalireitittimeltä ei anna vastausta. Syyn löytämiseksi tarkistetaan pakettien oikeellisuus Wiresharkilla ennen suurempia muutoksia. Laboratoriomuurissa labfw on sallittu GRE-liikenne kumpaankin suuntaan.



Kuvio 22. Wiresharkin pakettikaappaus. Ylempi ikkuna on Ciscon reitittimeltä lähtevän GRE-kapsuloidun ICMPv6-paketin sisältö. Alemmassa ikkunassa on Netscreenilta lähtenyt paketti pingia suoritettaessa.

Kuviossa 22 ylemmässä ikkunassa havaitaan ping-paketin lähtevän oikeanlaisena eli se sisältää GRE-kehyksen jälkeen IPv6- ja ICMPv6-kehykset. Sen sijaan alemmassa ikkunassa nähdään GRE-kehys, mutta sen sisältämän protokollan tyyppi on IPv4 (0x800) ilman mitään hyötykuormaa. Oikean paketin koko on 138 tavua, kun taas Netscreenin lähettämä puutteellinen paketti on kooltaan vain 60 tavua. Netscreenin puutteellisen GRE-toteutus vuoksi IPv6:tta tukevaa VPN-yhteyttä ei voida rakentaa, kun käytössä on vain IPv4-yhteys. Vastaavasti Ciscossa IPv6- ja IPv4-protokollia ei voida salata IPsecin avulla ilman GRE-protokollaa.

6 Johtopäätökset

Opinnäytetyössä perehdyttiin IPv6-protokollan toimintaan ja esiteltiin myös edeltävä IPv4-protokolla. Tietoliikenteen salaamiseen tarvittava kokoelma protokollia eli IPsec esiteltiin eri komponentteineen. Työn toisessa osuudessa käytiin läpi miten protokollat konfiguroidaan Cisco Systemsin ja Juniper Networksin laitteilla. Lisäksi näiden välistä yhteensopivuutta testattiin, jotta valmistajien välinen yhteensopivuus selviäisi.

IPv6-protokolla yleistyy hitaasti nykyisissä IPv4:een perustuvissa verkoissa, mutta useat valmistajat markkinoivat laitteitaan IPv6:ta tukevina. Tästä huolimatta tietoa erilaisten laitteiden yhteensopivuudesta on vain vähän. Työn kannalta ja kokonaiskuvan muodostamiseksi useiden laitteiden testaaminen olisi ollut hyödyllistä, mutta aikaavievää. Työ tuotti uutta tietoa Cygate Oy:lle IPv6-tukeen liittyvistä ongelmakohdista, mikä huomioidaan yrityksen käynnistämässä IPv6-projektissa.

Työssä tuli eteen useita laitteiden ohjelmistosta johtuvia rajoituksia, jotka lienevät tyypillisiä, kun verkkoympäristö on laitteistoltaan hyvin erilainen. Lähtökohtaisesti näitä ongelmia voidaan vähentää valitsemalla suunniteltavaan verkkoon samanlaiset laitteet.

Cygate Oy:n kannalta työssä saatiin hyvää tietoa Ciscon VRF- ja OSPFv3-toteutuksien yhteensopivuudesta. Työn kirjoittamishetkellä OSPFv3-tuki VRF-instansseille oli vasta tulossa, mikä vaatisi vielä lisää testaamista mahdollisten ohjelmistovirheiden varalta. Cygaten hallintayhteyksien kannalta puute on suuri, minkä vuoksi aivan täyttä tuotantovalmiutta ei saavuteta IPv6:n kanssa. Kysyntä IPv6-protokollalle on kuitenkin hitaasti kasvamassa, joten Cygatella tulee olla tiedossa keinot vastata siihen.

Lähteet

1 Free pool of IPv4 address space depleted. Verkkodokumentti. Luettu 15.10.2011. Saatavissa: http://www.nro.net/news/ipv4-free-pool-depleted.

2 World IPv6 Day. Verkkodokumentti. Luettu 16.10.2011. Saatavissa: http://www.worldipv6day.org.

3 Hagen, Silvia. IPv6 Essentials, 2nd Edition. O'Reilly 2006.

4 IPv6 and IPv4 headers. Verkkodokumentti. Luettu 19.11.2011. Saatavissa: http://startnetworks.blogspot.com/2011/08/ipv6-and-ipv4-headers.html.

5 IPv6 header. Verkkodokumentti. Luettu 19.11.2011. Saatavissa: http://www.ietf.org/rfc/rfc2460.txt.

6 IPv6 Global Unicast Address Format. Verkkodokumentti. Luettu 20.11.2011. Saatavissa: http://www.ietf.org/rfc/rfc3587.txt.

7 Internet Control Message Protocol (ICMPv6). Verkkodokumentti. Luettu 20.11.2011. Saatavissa: http://www.ietf.org/rfc/rfc4443.txt.

8 VPNs and VPN Technology. Verkkodokumentti. Luettu 21.11.2011. Saatavissa: http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=7.

9 IPv6 IPsec Availability. Luettu 2.1.2012. Verkkodokumentti. Saatavissa: https://www.arin.net/participate/meetings/reports/ARIN_XXI/PDF/tuesday/ARIN-IPsecv6.pdf.

10 Verkkosivusto. Luettu 23.12.2011. Verkkodokumentti. Saatavissa: http://www.networkworld.com/community/blog/world-ipv6-day-results.

11 RH header security. Luettu 2.1.2012. Verkkodokumentti. Saatavissa: http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf.

12 Firewall Design Considerations for IPv6. Verkkodokumentti. Luettu 2.1.2012. Saatavissa: http://www.nsa.gov/ia/_files/ipv6/I733-041R-2007.pdf

13 Rautanen, Jaakko. Keskustelu 2.1.2012.

14 Diffie-Hellman (DH). Verkkodokumentti. Luettu 7.4.2012. Saatavissa: https://supportforums.cisco.com/docs/DOC-1061.

15 IPv6 on ScreenOS devices. Verkkodokumentti. Luettu 8.4.2012. Saatavissa: http://kb.juniper.net/InfoCenter/index?page=content&id=KB15692.

16 IPSec VPN IPv6 Between Asa 5550 and 881. Verkkodokumentti. Luettu 11.4.2012. Saatavissa: https://supportforums.cisco.com/message/3437874.

17 IPsec VPN between Cisco IOS & Netscreen. Verkkodokumentti. Luettu 8.4.2012. Saatavissa: http://blog.mozilla.com/mrz/2007/07/16/ipsec-vpn-between-cisco-ios-netscreen-solved/.

18 ScreenOS Reference Guide: Dual-Stack Architecture with IPv6. Verkkodokumentti. Luettu 11.4.2012. Saatavissa: http://www.juniper.net/techpubs/software/screenos/screenos6.3.0/630_ce_Dual_Stack_IPv6.pdf.

19 IPSec Dead Peer Detection Periodic Message Option. Verkkodokumentti. Luettu 11.4.2012. Saatavissa: http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtdpmo.html.

20 OSPFv3 in a VRF on a 7600 – Mailing list. Verkkodokumentti. Luettu 12.4.2012. http://www.gossamer-threads.com/lists/cisco/nsp/159721.

21 IPv6 OSPF routing within VRF context. Verkkodokumentti. Luettu 12.4.2012. https://supportforums.cisco.com/thread/2073440.

22 IPv6 Node Requirements. Verkkodokumentti. Luettu 16.4.2012. Saatavissa: https://tools.ietf.org/html/rfc4294#section-8.1.

Laboratorioreitittimen ipsecrtr1 konfiguraatio

```
hostname ipsecrtr1
!
vrf definition abc
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition cisco_vrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
ip cef
!
!
no ip domain lookup
ip domain name lab.cygate.fi
ipv6 unicast-routing
ipv6 cef
!
!
crypto pki token default removal timeout 0
!
!
crypto keyring juniperssg_keyring
  pre-shared-key address ipv6
2A02:2340:FFFF:FFFF:217:CBFF:FEF4:C1C0/128 key abcd1234
crypto keyring cisco_keyring
  pre-shared-key address 178.251.144.85 key abcd4321
  pre-shared-key address ipv6
2A02:2340:FFFF:FFFF:213:60FF:FE7F:290E/128 key abcd1234
!
crypto isakmp policy 5
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 28800
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp profile juniperssg
   keyring juniperssg_keyring
   match identity address ipv6
2A02:2340:FFFF:FFFF:217:CBFF:FEF4:C1C0/128
   no keepalive
crypto isakmp profile cisco
```

```
   keyring cisco_keyring
   match identity address ipv6
2A02:2340:FFFF:FFFF:213:60FF:FE7F:290E/128
   match identity address 178.251.144.85 255.255.255.255
   keepalive 30 retry 30
!
!
crypto ipsec transform-set juniperssg esp-3des esp-sha-hmac
crypto ipsec transform-set cisco-cisco ah-sha-hmac esp-3des
!
crypto ipsec profile cisco
 set transform-set cisco-cisco
 set pfs group2
 set isakmp-profile cisco
!
crypto ipsec profile juniperssg
 set transform-set juniperssg
 set pfs group2
 set isakmp-profile juniperssg
!
!
interface Loopback1210
 no ip address
 ipv6 address FEED:CAFE::BEEF/64
 ipv6 ospf network point-to-point
 ipv6 ospf 10 area 0
!
interface Tunnel10
 description Cisco_Cisco-IPv6-VPN
 vrf forwarding cisco_vrf
 ip address 10.10.10.1 255.255.255.0
 ipv6 address FD00:1000::1/64
 ipv6 enable
 tunnel source 2001:67C:110:3009::2
 tunnel mode gre ipv6
 tunnel destination 2A02:2340:FFFF:FFFF:213:60FF:FE7F:290E
 tunnel protection ipsec profile cisco
!
interface Tunnel20
 description Cisco_Netscreen-IPv6-VPN
 ip address 10.10.20.1 255.255.255.0
 ipv6 address FD00:1001::1/64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 10 area 0
 tunnel source 2001:67C:110:3009::2
 tunnel mode ipsec ipv6
 tunnel destination 2A02:2340:FFFF:FFFF:217:CBFF:FEF4:C1C0
 tunnel protection ipsec profile juniperssg
!
interface Tunnel30
 description Cisco_Cisco-IPv4-VPN
 vrf forwarding cisco_vrf
 no ip address
 ipv6 address FD00:1002::1/64
 tunnel source 81.20.227.66
 tunnel mode ipsec ipv4
 tunnel destination 178.251.144.85
 tunnel protection ipsec profile cisco
!
```

```
interface Tunnel40
 description Cisco_Netscreen-IPv4-VPN
 no ip address
 ipv6 address FD00:1004::1/64
 tunnel source 81.20.227.66
 tunnel destination 178.251.144.84
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 ip address 81.20.227.66 255.255.255.248
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 ipv6 address 2001:67C:110:3009::2/64
 ipv6 enable
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 0.0.0.0 0.0.0.0 81.20.227.65
!
ipv6 route vrf cisco_vrf
2A02:2340:FFFF:FFFF:213:60FF:FE7F:290E/128
2001:67C:110:3009::1 nexthop-vrf default
ipv6 route ::/0 2001:67C:110:3009::1
ipv6 router ospf 10
 router-id 81.20.227.66
!
!
```

Juniper Netscreen -palomuurin konfiguraatio

```
unset key protection enable
set clock timezone 2
set clock dst recurring start-weekday 2 0 3 02:00 end-
weekday 1 0 11 02:00
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
set protocol ospfv3
set enable
set area 0.0.0.0
exit
exit
set alg appleichat enable
unset alg appleichat re-assembly enable
set alg sctp enable
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 1646
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
unset zone "V1-Trust" tcp-rst
unset zone "V1-Untrust" tcp-rst
set zone "DMZ" tcp-rst
unset zone "V1-DMZ" tcp-rst
unset zone "VLAN" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet0/0" zone "Untrust"
set interface "ethernet0/1" zone "DMZ"
set interface "bgroup0" zone "Trust"
set interface "tunnel.1" zone "Trust"
set interface "tunnel.2" zone "Untrust"
set interface bgroup0 port ethernet0/2
set interface bgroup0 port ethernet0/3
set interface bgroup0 port ethernet0/4
set interface bgroup0 port ethernet0/5
set interface bgroup0 port ethernet0/6
```

```
unset interface vlan1 ip
set interface ethernet0/0 ip 178.251.144.84/27
set interface "ethernet0/0" ipv6 mode "host"
set interface "ethernet0/0" ipv6 ip
2a02:2340:ffff:ffff::/64
set interface "ethernet0/0" ipv6 enable
set interface ethernet0/0 route
set interface bgroup0 ip 192.168.100.101/24
set interface bgroup0 nat
set interface tunnel.1 ip 10.10.20.2/24
set interface "tunnel.1" ipv6 mode "router"
set interface "tunnel.1" ipv6 ip fd00:1001::2/64
set interface "tunnel.1" ipv6 enable
set interface "tunnel.2" ipv6 mode "host"
set interface "tunnel.2" ipv6 ip fd00:1004::2/64
set interface "tunnel.2" ipv6 enable
set interface tunnel.2 tunnel encap gre
set interface tunnel.2 tunnel local-if ethernet0/0 dst-ip
81.20.227.66
set interface tunnel.1 mtu 1390
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
unset interface vlan1 bypass-ipv6-others-ipsec
set interface vlan1 bypass-icmpv6-ndp
set interface vlan1 bypass-icmpv6-mld
unset interface vlan1 bypass-icmpv6-mrd
unset interface vlan1 bypass-icmpv6-msp
set interface vlan1 bypass-icmpv6-snd
set interface ethernet0/0 ip manageable
set interface bgroup0 ip manageable
set interface ethernet0/0 manage ping
set interface ethernet0/0 manage ssh
set interface ethernet0/0 manage web
set interface ethernet0/0 ipv6 ra accept
set interface tunnel.1 ipv6 ra link-mtu
unset interface tunnel.1 ipv6 ra link-address
unset interface ethernet0/0 ipv6 nd nud
set interface tunnel.1 ipv6 nd nud
set interface tunnel.1 ipv6 nd dad-count 0
set interface tunnel.2 ipv6 nd nud
set interface tunnel.2 ipv6 nd dad-count 0
set interface bgroup0 dhcp server service
set interface bgroup0 dhcp server auto
set interface bgroup0 dhcp server option netmask
255.255.255.0
unset interface bgroup0 dhcp server config next-server-ip
set flow tcp-mss
unset flow no-tcp-seq-check
set flow tcp-syn-check
unset flow tcp-syn-bit-check
set flow reverse-route clear-text prefer
set flow reverse-route tunnel always
set hostname kotifw1
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set address "Trust" "fd00:1001::/64" fd00:1001::/64
set address "Untrust" "178.251.144.131/32" 178.251.144.131
255.255.255.255
set address "Untrust" "fd00:1001::/64" fd00:1001::/64
set crypto-policy
```

```
exit
set ike p2-proposal "cisco" group2 esp 3des sha-1 second
3600
set ike gateway "lab-gw" address 2001:67c:110:3009::2 Main
outgoing-interface "ethernet0/0" local-address
"2a02:2340:ffff:ffff:217:cbff:fef4:c1c0" preshare
"fXaHlgU2Nb7C7qsmVTC64n7tkUniedygqQ==" proposal "pre-g2-
3des-md5"
set ike respond-bad-spi 1
set ike ikev2 ike-sa-soft-lifetime 60
unset ike ikeid-enumeration
unset ike dos-protection
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
set ipsec access-session log-error
set ipsec access-session info-exch-connected
set ipsec access-session use-error-log
set vpn "v6-vpn-to-lab" gateway "lab-gw" replay tunnel
idletime 0 proposal "cisco"
set vpn "v6-vpn-to-lab" id 0x3 bind interface tunnel.1
unset interface tunnel.2 acvpn-dynamic-routing
set url protocol websense
exit
set policy id 1 from "Trust" to "Untrust"  "Any-IPv4" "Any-
IPv4" "ANY" permit
set policy id 1
exit
set syslog config "178.251.144.131"
set syslog config "178.251.144.131" facilities local0 lo-
cal1
set syslog src-interface ethernet0/0
set syslog enable
set nsmgmt bulkcli reboot-timeout 60
set ssh version v2
set ssh enable
set config lock timeout 5
set license-key auto-update
set telnet client enable
set snmp port listen 161
set snmp port trap 162
set snmpv3 local-engine id "0162022007000107"
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
set router-id 178.251.144.84
unset add-default-route
set route 192.168.20.0/24 interface tunnel.1
set route 0.0.0.0/0 gateway 178.251.144.65
exit
set interface tunnel.1 protocol ospfv3 area 0.0.0.0
set interface tunnel.1 protocol ospfv3 enable
set interface tunnel.1 protocol ospfv3 cost 10
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
```

Cisco 1841 (kotirtr1) -reitittimen konfiguraatio

```
hostname kotirtr1
!
ip cef
ip domain name crisu.fi
ipv6 unicast-routing
ipv6 cef
!
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key vq2305i+sfgjh address ipv6
2001:67C:110:3009::2/128
crypto isakmp keepalive 30 30
crypto ipsec transform-set 3des ah-sha-hmac esp-3des
!
crypto ipsec profile profile0
 set transform-set 3des
 set pfs group2
!
interface Tunnel10
 ip address 10.10.10.2 255.255.255.0
 ipv6 address FD00:1000::2/64
 ipv6 enable
 tunnel source FastEthernet0/0
 tunnel mode gre ipv6
 tunnel destination 2001:67C:110:3009::2
 tunnel protection ipsec profile profile0
!
interface FastEthernet0/0
 ip address 178.251.144.85 255.255.255.224
 duplex auto
 speed auto
 ipv6 address autoconfig
 ipv6 enable
 ipv6 nd ra suppress all
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 nd ra suppress
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 0.0.0.0 0.0.0.0 178.251.144.65
!
ipv6 route ::/0 2A02:2340:FFFF:FFFF::1
ipv6 router ospf 10
 router-id 178.251.144.85
```