KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma / Tietoverkkotekniikka

Riku Leinonen

Palomuurien IPv6-migraatio

Opinnäytetyö 2011

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU

Tietotekniikan koulutusohjelma

LEINONEN, RIKU	Palomuurien IPv6-migraatio
Opinnäytetyö	69 sivua + 18 liitesivua
Työn ohjaaja	yliopettaja Martti Kettunen
Toimeksiantaja	Optimiratkaisut Oy
Maaliskuu 2011	
Avainsanat	IPv6, palomuurit, ASA, SimuNet, VPN

Tämän työn tarkoituksena on ollut tutkia Cisco ASA -palomuurien IPv6-ominaisuuksia ja sitä, mitä pitää ottaa huomioon IPv6-osoitteisiin siirtyessä, erityisesti Cisco ASA 5510 -palomuureissa. Työssä selvitettiin, miten saatiin käytössä olevaan IPv4-palomuuriin lisättyä IPv6-liikenne ja mitä eri IPv6-tunneleita voitiin toteuttaa eri Cisco ASA –käyttöjärjestelmäversioilla. Työssä selvitettiin myös miten natiivi IPv6-palomuuri liitettiin verkkoon. Työ on tehty Optimiratkaisut Oy:n toimeksiantona ja toteutettu Kymenlaakson ammattikorkeakoulun SimuNet-ympäristössä sekä puhtaassa laboratorioympäristössä.

Työ aloitettiin selvittämällä IPv4- ja IPv6-protokollien tietoturvaeroja ja kertaamalla IPv6-osoitteiden rakennetta. Teoriaosuudessa esiteltiin myös Cisco ASA -palomuurien eri IPv6-perustoimintoja, kuten pääsylistoja, reititystä sekä liityntäporttien eri IPv6-osoitetyyppejä. Teoriaosuuden lopussa selvennettiin IPv6-tunneleiksi soveltuvien VPN-tunnelityyppien toimintaa.

Käytännön kokeissa lisättiin SimuNetin toiminnassa oleviin palomuureihin Dual-Stack-ominaisuus eli lisättiin IPv6-liikenne IPv4-liikenteen rinnalle. IPv6-yhteyksiä ja palomuurien IPv6-pääsylistoja testattiin eri palvelimien avulla SimuNetissä. Tunneleiden käytännön kokeet tehtiin erillisillä palomuureilla, koska SimuNetin palomuurit eivät tukeneet VPN-tunneleita käytetyssä toimintatilassa. IPv6 SSL VPN -tunneli saatiin muodostettua liikennöimällä IPv6-osoitteilla IPv4-verkon läpi suojattuun IPv6-testiverkkoon. IPv6 LAN-to-LAN VPN –tunneli saatiin muodostettua täysin natiivina IPv6-tunnelina viimeisimmällä käyttöjärjestelmäversiolla. Viimeiseksi SimuNetin reunalle lisättiin natiivi IPv6 Cisco ASA -palomuuri, jonka kautta yhdistettiin Kymenlaakson ammattikorkeakoulun ICLAB-ympäristön "tuotantoverkko" julkiseen IPv6-Internettiin. Tämän palomuurin läpi toimi muun muassa ICTLAB-ympäristön IPv6-kotisivut.

Cisco ASA 5510 -palomuuri todettiin toimivaksi IPv6-liikenteen kanssa Dual-Stackiä käyttämällä SimuNetissä. Eri IPv6-tunnelit onnistuivat laboratorioympäristössä mutta ympäristöt näissä testeissä olisivat voineet ehkä olla vielä haastavampia. Natiivi IPv6-palomuuri oli SimuNetin ensimmäisiä natiiveja IPv6-laitteita ja oli tärkeä lisä SimuNetille.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU

University of Applied Sciences

Information Technology

LEINONEN, RIKU	Firewall IPv6 Migration
Bachelor’s Thesis	69 pages + 18 pages of appendices
Supervisor	Martti Kettunen, Principal Lecturer
Commissioned by	Optimiratkaisut Oy
March 2011	
Keywords	IPv6, firewall, ASA, SimuNet, VPN

The purpose of this work was to study the Cisco ASA firewall's IPv6 features and what matters have to be taken into consideration in the transition to IPv6 addresses, in particular, the Cisco ASA 5510 firewalls. This thesis work was commissioned by Optimiratkaisut Oy and all the practical tests were made in Kymenlaakso University of Applied Sciences' laboratory called SimuNet and also in the separated pure laboratory environment.

This thesis work was started by exploring the security differences between the IPv4 and IPv6 protocols, investigating the structure of the IPv6 protocol and clarifying the ways to add IPv6 traffic to a firewall. The theory section of this work includes the basic IPv6 features of the Cisco ASA firewall such as IPv6 access-list, IPv6 routing and different types of IPv6 addresses which can be assigned to an interface. At the end of the theory section, different VPN tunnels are also introduced, which are implemented in the practical section of this thesis work.

In the practical tests of this thesis work, the Dual-Stack feature was added to the SimuNet laboratory's firewalls. IPv6 connections and access-lists were verified with the different types of servers in the SimuNet network. Practical tests of the VPN tunnels were made with separated Cisco ASA firewalls, because SimuNet's firewalls did not support VPN tunnels in the multiple context mode. IPv6 SSL VPN tunnel was established with IPv4 addresses and IPv6 traffic was sent through that tunnel. IPv6 LAN-to-LAN IPSec VPN tunnel was established only with the IPv6 addresses, using the latest OS version. Finally, the native IPv6 firewall was added to the edge of the SimuNet network, which connected the ICTLAB's “production network” to the IPv6 Internet. ICTLAB's web server was also connected to the public IPv6 Internet with that firewall.

Cisco ASA 5510 firewall was verified fully functional with the IPv6 traffic using the Dual-Stack feature in SimuNet. The two different types of VPN tunnels were established successfully in the pure laboratory environment but there could have been slightly more difficult environments for these tests. The native IPv6 firewall was one of the first components of the SimuNet network which worked natively with the IPv6 addresses and it was an important addition to SimuNet.

SISÄLLYS

1 JOHDANTO

IPv4 -osoitteiden nopea väheneminen maailmalla ajaa yrityksiä siirtymään IPv6 -osoitteisiin, joita on käytettävissä enemmän kuin tarpeeksi. Yritysten ja erityisesti operaattoreiden verkkoihin olisi jo suotavaa lisätä IPv6-valmiuksia, ettei IPv6-osoitteisiin siirtymisestä tulisi liian nopeaa ja riskialtista prosessia. Siirtyminen IPv4:sta IPv6-protokollaan ei ole varmasti mikään mutkaton prosessi, koska IPv6-protokollan tuomia mahdollisia ongelmia ei ole vielä täysin selvitetty. Aikaa IPv4-osoitteiden loppumiseen ei ole kauan, joten eri laitteiden IPv6-ominaisuuksiin on jo hyvä tutustua tässä vaiheessa.

Tämä opinnäytetyö on suuntautunut tutkimaan palomuurien IPv6-ominaisuuksia ja asioita, joita täytyy ottaa huomioon IPv6-liikenteeseen siirryttäessä, erityisesti Cisco Asa 5510 -palomuureissa. Työssä on ollut tarkoituksena käydä teoriassa läpi IPv6- ja IPv4-protokollien välisiä tietoturvaeroja ja Cisco ASA:n toimintaan liittyviä periaatteita IPv6-ominaisuuksien kannalta. Käytännön kokeissa on ollut tarkoituksena lisätä palomuureihin IPv6-valmiuksia IPv4-osoitteiden rinnalle sekä testata yhteyksiä palomuurien läpi. Työssä tutustuttiin myös aivan natiivin IPv6-palomuurin toimintaan ja eri tunneleiden toimivuuteen IPv6-osoitteilla ja samalla on tullut selvitettyä eri Cisco ASA käyttöjärjestelmä-versioiden IPv6-ominaisuuksia ja puutteita.

Tämä opinnäytetyö on tehty Optimiratkaisut Oy:n toimeksiantona. Työ on tehty pääosin Kymenlaakson ammattikorkeakoulun SimuNet-alustalle, joka vastaa lähestulkoon oikeaa operaattoriverkkoa. SimuNet mahdollistaa IPv6-ominaisuuksien lisäämiseen palomuureihin samalla, kun ne ovat aktiivisessa käytössä, mikä tekee tehtävästä realistisemman verrattaessa puhtaaseen laboratorioympäristöön. Työn palomuurilaitteiksi on valittu Ciscon Asa 5510 -palomuurit, koska ne ovat SimuNetin keskeisimpiä laitteita ja niitä löytyy myös Kymenlaakson ammattikorkeakoulun tietoverkkolaboratorion tiloista SimuNetin ulkopuolelta. SimuNetin ulkopuolelta löytyviä palomuureja on käytetty erilaisiin testitarkoituksiin ennen kuin itse SimuNetin palomuureihin on tehty muutoksia sekä VPN-tunneleiden toteutukseen.

SimuNet-ympäristössä tehtiin samaan aikaan montaa eri projektia ja opinnäytetyötä samoilla laitteilla ja samaan aihepiiriin liittyen, joten töiden aihealueiden päällekkäin menemistä ei voitu välttää. Tässä työssä on viitattu lähteet selvästi, kun on käsitelty muiden opiskelijoiden opinnäytetöihin liittyviä asioita. Samaan aikaan tehtyjä ja

samaan aihepiiriin liittyviä opinnäytetöitä SimuNetissä olivat Riku Oinosen työ MPLS L2VPN ja operaattoriverkon kahdennetut palvelut, Erno Tolosen työ VPN-Ratkaisut operaattorin siirtyessä IPv6-yhteyskäytäntöön ja Mika Koskisen työ Ohjelman etäkäyttö SSL VPN-yhteydellä.

2 IPV4-OSOITTEISTA IPV6-OSOITTEISIIN

1980-luvulla organisaatio nimeltä IETF(Internet Engineering Task Force) kehitti IPv4-protokollan. Kun IPv4 määriteltiin, ei siinä huomioitu tarpeeksi tietoturva–asioita eikä myöskään sen maailmanlaajuista nopeaa kasvua. Internetin räjähdysmäinen kasvu 1990-luvulla toi useimmat tietoturvaongelmat esiin sen aikaisissa tietoverkoissa, ja sitä mukaa huomattiin mitä olisi voitu IPv4:n suunnittelussa tehdä toisin. Jos Internet olisi ollut tässä tilanteessa silloin, kun IPv4 määriteltiin, olisi IPv4:n rakenne suunniteltu eri tavoin. (Hogg & Wyncke 2008, 3.)

IPv4-osoitteet koostuvat 32-bittisistä osoitteista, ja yhteensä osoitteita on maailmalla noin 4 miljardia. IPv4-osoitteet ovat tällä hetkellä vielä ylivoimaisesti käytetyimpiä osoitteita, kun osoitteita on vielä jäljellä, mutta niiden loppumisen jälkeen IPv6-osoitteiden käyttö tulee lisääntymään nopeasti. IPv4-osoitteita on yritetty säästää muun muassa osoitteenmuunnos-tekniikoilla lisäajan saamiseksi. (IPv4 ,Wikipedia 2011.)

1990-luvun alussa IETF huomasi, että uutta IP-protokollaa ehkä tarvittaisiin, ja IPv6:n kehitys alkoi. Aluksi IPv6:sta kutsuttiin nimellä IPng(Internet Protocol next generation), joka muutettiin myöhemmin IPv6:ksi. IPv6 tarjoaa monia uusia toimintoja ja on tuleva seuraava askel Internet protokollan evoluutiossa. IPv6 standardoitiin täydellisesti vuonna 1998 ja on siitä lähtien ollut käytettävissä. (Hogg & Wyncke 2008, 3)

Suuren IPv6-osoiteavaruuden myötä tulleita tärkeimpiä uusia verkko-ominaisuuksia ovat muun muassa päätelaitteelta päätelaitteelle kulkevat yhteydet ilman NAT-osoitteenmuutostekniikoita, osoitteiden automaattinen määritystoiminto autoconfiguration sekä Multihoming-ominaisuus. IPv6:ssa osoitteita riittää jokaiselle päätelaitteelle ilman osoitteenmuutosta ja jokaiselle laitteelle voidaan jakaa oma julkinen IPv6-osoite. Automaattinen osoitteenmääritys tapahtuu laitteen verkon tietoja ja oman MAC-osoitteen tietoja hyväksi käyttäen. Multihoming-ominaisuus sallii

laitteille monta eri IPv6-osoitetta, millä saadaan parannettua laitteiden yhteyksien luotettavuutta. (IPv6, Wikipedia 2011)

3 IPV6-OSOITTEET

IPv6-osoitteet muodostuvat 16-bittisistä kentistä, joita on 8 kappaletta. Jokaisessa 16-bittisessä kentässä on 2 tavua eli kokonaiseen osoiteeseen mahtuu 16 tavua. Osoitteiden kokonaispituus on 128 bittiä eli kokonaisuudessaan osoitteita löytyy 2^{128}, mikä on enemmän kuin tarpeeksi koko maailmalle. 16-bittiset kentät erotellaan toisistaan kaksoispisteillä ja jokainen kenttä esitetään neljän merkin pituisella heksadesimaaliluvulla eli kentän kummankin tavun arvo esitetään heksadesimaaliluvulla. Jos osoitteessa on monta nollaa peräkkäin, voidaan ne lyhentää kahdella kaksoispisteellä, mutta näin voi tehdä vain kerran yhdessä osoitteessa. Esimerkiksi osoitteesta **2001:0:130F:0:0:9C0:876A:130B** voidaan poistaa turhia nollia, jolloin saadaan osoitteesta seuraavan näköinen: **2001:0:130F::9C0:876A:130B**, joka vastaa aivan samaa osoitetta. Perus IPv6-osoitetyypit ovat unicast-osoite, multicast-osoite ja anycast-osoite. Unicast-osoitteisiin kuuluvat julkisesti käytettävät osoitteet ja linkkikohtaiset link-local-osoitteet. Link-localeita ei voida reitittää minnekään, ja ne voivat täten olla samoja eri verkoissa. Link-localeissa käytetty prefix on fe80::/10. Multicast-osoitteet ovat IPv6:ssa IPv4:n broadcast-osoitteita vastaavia osoitteita, joilla liikennöidään tietyn multicast-ryhmän jäseniin samanaikaisesti. Multicast-osoitteissa käytetty prefix on ff00::/8. Anycast-osoite lähetetään joukolle rajapintoja eli lähimmälle anycast-vastaanottajalle, joka vastaa reititysprotokollan mukaista liityntäporttia. Laitteiden loopback-osoitteet merkitään merkeillä *::1* ja oletusreitti merkeillä *::/0.* (IPv6, Wikipedia 2011.) (Hinden & Deering 1998) IPv6-osoitealueet

Seuraavat osoitealueet ja niihin liittyvät organisaatiot on määritelty IANA:n (Internet Assigned Numbers Authority) toimesta vuonna 2008, ja nämä kannattaa huomioida IPv6-liikennettä suodattaessa.

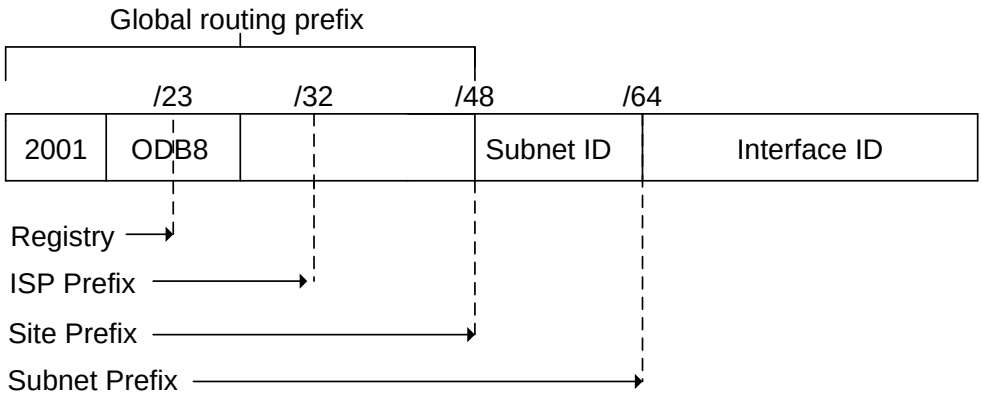
- 2001::/16 – IPv6 unicast-osoitteet
- 2002::/16 – 6to4-tunnelointi
- 2003::/18 - RIPE NCC
- 2400::/12 – APNIC

- 2600::/12 – ARIN (US DoD)
- 2610::/23 – ARIN
- 2620::/23 – ARIN
- 2800::/12 – LACNIC
- 2A00::/12 – RIPE NCC
- 2C00::/12 – AfriNIC

(Hogg & Wyncke 2008, 129.)

3.1 Julkinen IPv6 unicast-osoite

Julkinen IPv6 unicast-osoite koostuu julkisesta reititysosasta, aliverkko-ID:stä ja liityntäportti-ID:stä ja on yhteensä 128 bittiä pitkä. Julkisen IPv6 unicast-osoitteen rakenne esitetään kuvassa 1.



Kuva1. Unicast-osoite (Hinden, Deering & Nordmark 2003)

Julkisessa reititysosassa määritellään osoitteen rekisteriosa ja osoitteen sijainti(Site), missä näkyy esimerkiksi Internet-yhteyden tarjoajan tunniste. Julkisen reititysosan pituus on 48 bittiä. Aliverkko-ID kertoo kyseisen aliverkon tunnisteen, missä unicast-osoite sijaitsee. Aliverkkotunniste on 16 bittiä pitkä ja sen sisältämät aliverkot voidaan jakaa eri organisaatioissa aivan omanlaisella tavalla omaan käyttöön. Liityntäportti-ID on 64 bittiä pitkä ja se koostuu muokatusta EUI-64-tunnisteesta, joka generoidaan liityntäportin paikallisen laitteen MAC-osoitteen avulla. (Hinden, Deering & Nordmark 2003.)

3.2 IPv6-osoitteen otsikkokentät

IPv6-osoitteiden otsikot koostuvat kahdeksasta kentästä, kun taas IPv4:ssa niitä oli neljätoista. IPv6-otsikoiden koko on 40 tavua (320 bittiä), kun taas IPv4-otsikoiden vain 20 tavua(160 bittiä). IPv6:ssa on vähemmän kenttiä, mutta esimerkiksi osoitekentät ovat neljä kertaa suuremmat kuin IPv4:ssa. IPv4 ja IPv6-otsikkokentät näkyvät kuvassa 2. (Hinden & Deering 1998)

IPv6-otsikkokentät

Version: Versio-kenttä on neljän bitin pituinen kenttä, mikä on sama kuin IPv4:ssa sisältäen numeron 6, numeron 4 sijaan.

Traffic class: Liikenneluokka-kenttä koostuu kahdeksasta bitistä ja on saman tapainen kuin IPv4:n ToS-kenttä. Se merkitsee paketin liikenneluokka-merkinnällä, jota käytetään Differentiated Services(DiffServ)-palveluissa. Nämä toiminnot ovat samat IPv4:ssa ja IPv6:ssa.

Flow label: Flow label-kenttä koostuu 20-bitistä. Se sallii tietyn liikenteen, mihin lisätään labelit eli "liput". Tätä kenttää käytetään muun muassa multilayer-kytkimien pakettien siirtoon ja erityisesti pakettien siirron nopeuttamiseen.

Payload length: Kuorman pituus-kenttä on samantapainen kenttä kuin IPv4:n pituus-kenttä. Se määrittelee otsikoidun paketin kuorman pituuden tavuina.

Next header: Next header-kenttä määrittelee, mikä seuraava otsikko tulee IPv6-paketin otsikon jälkeen. Seuraava otsikko voi olla kuljetuskerroksen paketti, esimerkiksi TCP tai UDP, tai se voi olla jokin lisäotsikko.

Hop limit: Hop limit-kenttä määrittelee, kuinka monta hyppyä IPv6-paketti voi edetä maksimissaan. Jokainen hyppy vähentää tätä arvoa yhdellä. Tämä arvo vastaa IPv4:n TTL(Time To Leave)-kenttää. Koska IPv6-otsikossa ei ole tarkistussummaa, voidaan tätä kenttää vähentää laskematta tarkistussummaa, mikä nopeuttaa paketin prosessointiaikaa.

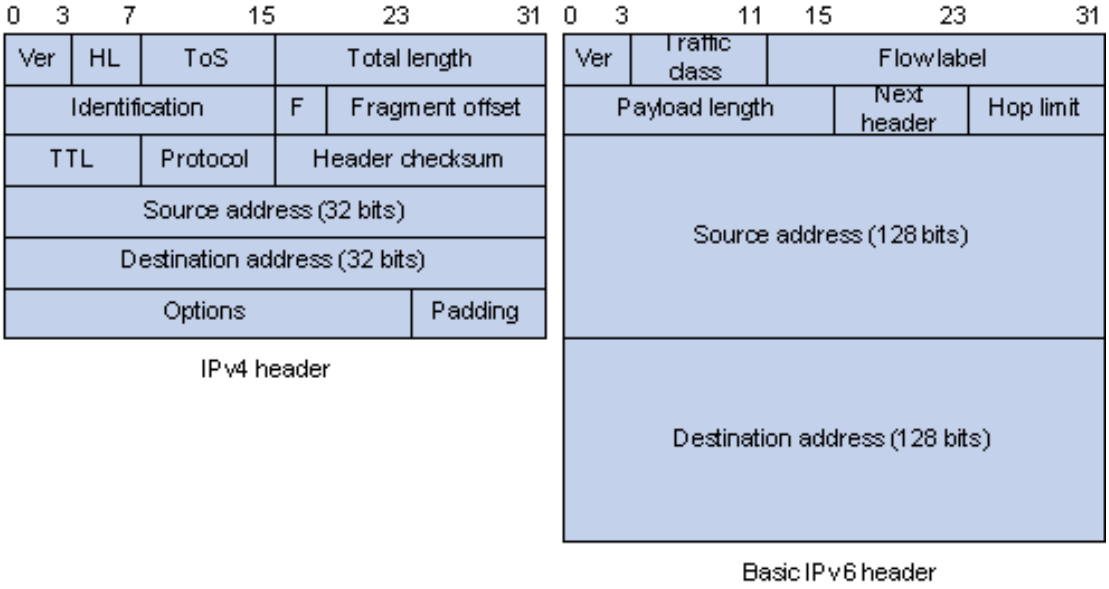
Source address: Paketin lähdeosoite on 128-bittiä pitkä ja kertoo, mistä paketti on lähtöisin.

Destination address: Paketin kohdeosoite on 128-bittiä pitkä ja kertoo minne paketti on menossa eli kohdeosoitteen.

(IPv6 Packet Headers, 2011)

3.3 IPv6- ja IPv4-pakettien vertailu

IPv6- ja IPv4–pakettien otsikkokenttien kokoerot näkyvät kuvasta 2. Kuvasta näkee myös, kuinka IP-paketin rakenne on muuttunut huomattavasti yksinkertaisemmaksi IPv6-protokollaan siirryttäessä.



Kuva2. IPv6 ja IPv4 paketit (IPv6 Basics, H3C Technologies Co 2011.)

IPv6-otsikon kenttien määrä on huomattavasti pienempi kuin IPv4-otsikoissa, mutta silti IPv6-otsikko on kaksi kertaa suurempi kuin IPv4-otsikko. Se ei kuitenkaan hidasta IPv6-pakettien prosessointia suuren otsikkokoon myötä, vaan päinvastoin se nopeuttaa sitä. IPv6-otsikkokenttä pudottaa joitakin otsikkokenttiä pois IPv4-otsikkoon verrattuna tai siirtää ne otsikon lisäkenttiin, tehden näin otsikosta yksinkertaisemmin käsiteltävän. Palomuurien täytyy käsitellä IPv6-pakettien otsikko ja tarkkailla osoitteita, hyppyjen maksimimäärää ja hyppyoptio-otsikoita, jos niitä on olemassa, toisin kuin IPv4-paketeissa, joista täytyy käsitellä monet erilaiset otsikkokentät, joihin kuuluvat muun muassa Time-to-Live(TTL), fragment offsets ja paketin pituus(Total lenght). IPv6-pakettien tavoite on, että otsikoita käsiteltäisiin enemmän raudalla(hardware) kuin ohjelmallisesti(software), kun parannetaan laitteiden suorituskykyä. IPv6-lisäotsikot kuitenkin hidastavat nimenomaan palomuureja, jos niitä on paljon. Palomuurien täytyy käsitellä otsikko ja myös kaikki

lisäotsikot päästäkseen käsiksi kuljetuskerrokseen liittyviin tietoihin ja ohjelmallisiin tietoihin. (Hogg & Wyncke 2008, 133.)

IPv6-lisäotsikot, jotka lisätään seuraavassa järjestyksessä tavallisen otsikon jälkeen:

1. **Hyppyoptio-otsikko** (Hop-by-Hop Options Header): Hyppyoptio-otsikkoa käytetään vaihtoehtoisen tiedon kuljettamiseen ja tämä otsikko pitää tutkia jokaisessa solmukohdassa paketin matkan varrella. Tämän otsikon next-header arvo on 0.

2. **Kohdeoptio-otsikko** (Destination Options Header): Kohdeoptio-otsikossa on vaihtoehtoista tietoa, jota pitää tutkia vain vastaanottaja-laitteessa. Tämän otsikon next-header arvo on 60.

3. **Reititysotsikko** (Routing Header): Reititysotsikko käyttää IPv6-lähettäjä, josta paketti lähetetään. Siinä listataan eri verkon solmukohtia, joiden kautta paketin täytyy kulkea päästäkseen kohdeosoitteeseen. Tämän otsikon next-header arvo on 43.

4. **Fragmentointiotsikko** (Fragment Header): Fragmentointiotsikkoa käyttää IPv6-lähettäjä ja sitä käytetään sellaisten isojen pakettien lähettämiseen, joita ei voi lähettää kyseisen polun MTU-arvon kanssa. Fragmentointi tapahtuu vain lähettäjä-laitteessa. Tämän otsikon next-header arvon on 44.

5. **Todennusotsikko** (Authentication header): Todennusotsikko huolehtii IPv6-paketin lähettäjän varmistuksesta, mikä tapahtuu otsikkoon lisätyn tarkistussumman avulla. Tätä otsikkoa käytetää muun muassa IPSecin todennuksessa ja tämän otsikon arvo on 51.

6. **Salausotsikko** (Encapsulating Security Payload Header): Salausotsikko huolehtii IPv6-paketin sisällön salauksesta. Salausotsikko on viimeinen selväkielinen lisäkenttä, jonka jälkeen tulevat lisäkentät ovat salattuja. Tätä otsikkoa käytetään IPSecin salauksessa, ja tämän otsikon arvo on 50.

7. **Ylemmän protokollakerroksen kehys** (Upper-layer header): Ylemmän protokollakerroksen kehystä käytetään datan kuljettamiseen, jossa tyypillisiä protokollia ovat TCP(arvo 6) ja UDP(arvo 17).

(Kaario 2008, 115-122.)

Palomuurien pitäisi yrittää välttää mahdollisimman paljon turhia paketteja, jotka käyttävät IPv6-lisäotsikoita, koska niiden suodatus vie palomuurin tehoja. IPv6-palomuurien pitäisi estää kaikki paketit, joilla on tuntemattomia lisäotsikoita. Myös kaikki turhat lisäotsikolliset paketit, joilla on RH0 tai mikä tahansa hyppyoptio-otsikko, pitäisi estää, esimerkiksi reitittimen hälytysoptio-otsikko(Router Alert option). (Hogg & Wyncke 2008, 133.)

4 IPV4- JA IPV6-TIETOTURVAN EROJA JA YHTÄLÄISYYKSIÄ

TCP/IP–protokollapinoa tarkastellessa OSI-mallin verkkokerros on ainut kerros, jossa IPv4:n ja IPv6:n väliset erot tulevat kunnolla esille. Käytännössä, jos web-sovellus on haavoittuvainen IPv4–ympäristössä, se on haavoittuvainen myös samanlaisille hyökkäyksille IPv6–ympäristössä. Molempien protokollien otsikoissa on monia yhtäläisyyksiä. Molemmissa otsikoissa on yhteistä vielä versio, QoS(Quality of service)-kenttä, kuorman pituuskenttä, laskuri paketin matkan mittaamiseen, seuraavan ylemmän kerroksen protokollan arvo ja tietysti lähde– ja kohdeosoite. Tämän vuoksi käytännössä monet hyökkäystavat ovat samanlaisia IPv4- ja IPv6–verkoissa. (Hogg & Wyncke 2008, 500.) Seuraavassa listassa on muutamia esimerkkejä:

- Sovellus-kerroksen hyökkäykset
- Luvaton sisäänpääsy
- Man-in-the-middle-hyökkäykset
- Sniffing/Eavesdropping- hyökkäykset
- DoS (Denial of service) – hyökkäykset
- Spoofed packets–hyökkäykset (pakotettuja osoitteita ja muita kenttiä)
- Hyökkäykset reitittimiä ja muita verkkolaitteita vastaan

- Hyökkäykset fyysistä- ja siirtokerrosta vastaan

  (Hogg & Wyncke 2008, 500.)

Samat parhaaksi todetut suojausmenetelmät IPv4–verkoissa pätevät myös hyvin IPv6–verkoissa. Fyysiset topologiat ja verkon suunnittelumallit pysyvät samanlaisina ja tavanmukaiset IPv4–verkkojen rajojen suojaamiseen käytetyt menetelmät toimivat myös IPv6–verkoissa. Verkon reunojen tarkka suodatus ja sisäverkon suojauksen jatkuva parantaminen on vieläkin nykypäivän järjestys IPv6-verkkojen turvaamisessa. (Hogg & Wyncke 2008, 500.)

IPv6 eroaa kuitenkin IPv4:sta vähän ja siksi on olemassa uhkia, jotka ovat muuttuneet hiukan sen takia, että IPv6 tekee asioita eri tavalla kuin IPv4. Seuraavassa listassa on uhkia, jotka ovat muuttuneet IPv6–protokollan mukaan tullessa:

- LAN –pohjaiset hyökkäykset (ARP[Address Resolution Protocol] tai NDP [Neighbor Discovery Protocol])
- Hyökkäykset DHCP:tä tai DHCPv6:ta vastaan
- DoS-hyökkäykset reitittimiä vastaan (hyppyoptio lisäotsikot mielummin kuin reititin hälytykset)
- Fragmentointi (IPv4-reitittimet suorittavat fragmentoinnin, mutta IPv6–päätelaitteet käyttävät fragment-lisäotsikkoa)
- Paketin vahvistus hyökkäykset, eli yritetään kuormittaa verkkoa tai kartoittaa lähettämällä mahdollisen moneen paikkaan multicast-liikennettä (IPv4 käyttää broadcastia; IPv6 käyttää multicastia)

  (Hogg & Wyncke 2008, 501.)

Kokonaisuudessa IPv6 ei ole yhtään sen turvallisempi kuin IPv4:kaan, mutta sillä on siitä huolimatta aivan omanlaatuisiakin huomioitavia ominaisuuksia. IPv6-otsikon sisäiset kentät kuten flow–table ja IPv6:n käyttämät laajennusotsikot ovat vain IPv6:n ominaisuuksia. On olemassa myös hyökkäyksiä, jotka uhkaavat vain IPv6–verkkoja. (Hogg & Wyncke 2008, 501.) Seuraavassa listassa on uhkia, jotka ovat ominaisia vain IPv6–verkoille:

- Haittaohjelmien tiedustelu ja matojen skannaus verkoissa vaikeampaa (Esimerkiksi Brute-force havainnointi on vaikeampaa)

- ICMPv6–hyökkäykset (ICMP6-paketit eroavat IPv4-protokollan ICMP-paketeista)
- Extension Header(EH)–hyökkäykset (Lisäotsikot pitävät käsitellä tarkasti palomuureissa)
- Autoconfiguration (NPD hyökkäykset ovat yksinkertaisesti tehtävissä)
- Protokollan muutos–hyökkäykset
- Mobile IPv6-hyökkäykset
- IPv6 protokollapino-hyökkäykset (Koska IPv6:n käyttö on vasta kasvussa, voi protokollapinosta löytyä vielä bugeja)

(Hogg & Wyncke 2008, 501.)

5 IPV6-MIGRAATIO PALOMUUREISSA

Palomuureissa on kaksi tapaa lisätä IPv6-liikenne sen toimintaan, joko lisäämällä palomuuriin Dual-Stack-ominaisuus tai konfiguroida palomuuri täysin natiiviksi IPv6-palomuuriksi. Dual-Stackin hyvä puoli on, että IPv6-osoitteet saadaan lisättyä jo käytössä olevaan IPv4-palomuuriin eikä IPv4-asetuksiin tarvitse koskea juuri ollenkaan. Natiivissa IPv6-palomuurissa taas palomuurin suorituskyvyt eivät kärsi niin paljon kuin Dual-Stackissä, koska palomuurin tarvitsee suodattaa vain yhden protokollan liikennettä. Palomuurin toimintaa IPv6-protokollan kanssa olisi myös yksinkertaisempi hallita natiivissa IPv6-palomuurissa, jos liikennettä olisi paljon. (Hogg & Wyncke 2008, 128.)

5.1 Dual-Stack

Cisco ASA-palomuurien käyttöjärjestelmäversio 8.0 ja uudemmat tukevat ainakin Dual-Stack-ominaisuutta, jossa IPv6-liikennettä varten liityntäportteihin määritellään IPv4-osoitteiden lisäksi vielä IPv6-osoitteet. Tämä on nopein tapa lisätä IPv6-liikenne laitteisiin, joissa on jo IPv4-osoitteet sekä IPv4-liikennettä. IPv6-osoitteet voidaan lisätä liityntäportteihin IPv4-osoitteiden rinnalle ja ne eivät vaikuta toistensa toimintaan mutta saattavat heikentää esimerkiksi palomuurin suorituskykyä. Palomuurien prosessointiteho saattaa laskea, koska kummankin protokollan liikenne pitää suodattaa samaan aikaan ja vielä erilaisilla pääsylistoilla. IPv6-osoitteita on

helppo lisätä liityntäportteihin, koska niitä voi lisätä useita ja ne eivät poista aikaisemmin syötettyjä osoitteita. Dual-Stack on hyvä ja varma tapa saada laitteet nopeasti tukemaan IPv6-liikennettä, ilman että IPv4-liikenteeseen tarvitsisi tehdä suuria muutoksia ja on varma askel IPv6-verkkoja kohti, jos natiiveihin IPv6-verkkoihin ei ole vielä mahdollisuutta. (Punithavathani, Sankaranarayanan, 2.)

5.2 Natiivi IPv6

Työn käytännönkokeiden verkossa oli kaksi palomuuria, jotka suodattivat jo IPv4-liikennettä. Natiivi IPv6 -palomuuri olisi hyvä lisä verkolle, varsinkin jos IPv4-liikennettä on paljon. IPv6-liikenteen suodattaminen suuren IPv4-liikenteen rinnalla voi tuottaa liian suurta kuormaa yhdelle palomuurille. Voisi olla järkevämpää muutenkin käyttää erillistä palomuuria kummankin protokollan liikenteelle, koska silloin niiden hallintaa olisi yksinkertaisempaa ja helpompi ylläpitää. Varsinkin IPv6-liikenteen kanssa, koska IPv6-liikennettä oli vielä vähän työtä tehdessä. Tämän työn käytännön kokeissa toteutettiin tämä idea lisäämällä natiivi IPv6-palomuuri SimuNetin reunalle. (Hogg & Wyncke 2008, 128.)

6 IPV6-OSOITETYYPIT LIITYNTÄPORTEISSA

Osoitetyyppejä on useita IPv6–verkoissa ja IPv6–osoitteet voidaan lisätä jokaiseen Cisco ASA-palomuurin liityntäporttiin IPv4–osoitteiden rinnalle. Yhdellä liityntäportilla voi olla monta eri IPv6-osoitetta samaan aikaan. Liityntäporteilla on automaattisesti link-local osoite esimerkiksi julkisen osoitteen lisäksi, kun vain IPv6–osoite on lisätty liityntäporttiin. IPv6–ominaisuudet käynnistyvät porteissa heti, kun siihen määritellään jonkinlainen IPv6–osoite. (Configuring IPv6, 2011.)

Global address

Julkinen osoite eli staattisesti määritelty on unicast-osoite, joka määritellään manuaalisesti liityntäporttiin. IPv6–osoitteessa täytyy myös ilmoittaa osoitteen prefix eli IPv6–verkon koko, johon osoite kuuluu. Kun liityntäporttiin lisätään julkinen osoite, lisätään sille myös automaattisesti link-local osoite. (Configuring IPv6, 2011.)

Esimerkki:
hostname(config-if)# ipv6 address 2a00:1dd0:100:a1fa::1/64

Stateless autoconfiguration

Yksinkertaisin tapa lisätä IPv6-osoite liityntäporttiin on konfiguroida siihen tilaton autokonfiguraatio. Se luo liityntäportille julkisen IPv6-osoitteen ja link-local osoitteen. Julkinen IPv6-osoite perustuu sen saamiin prefixeihin, joita se saa reitittimien mainostusviesteistä. Link-local–osoite generoituu automaattisesti liityntäportille sen muokatusta EUI-64 liityntäportti-ID:stä. Autoconfiguration–käskyllä portti saa myös automaattisen IPv6-oletusreitin. (Configuring IPv6, 2011.)

Esimerkki:
hostname(config-if)#ipv6 address autoconfig

Link–local

Link-local osoite on linkkikohtainen osoite ja voi tästä syystä olla vaikka sama useassa verkon liityntäportissa. Automaattisesti generoituna link-local osoite syntyy muokatun EUI-64 liityntäportti-ID:n kanssa, joka perustuu liityntäportin omaan MAC-osoitteeseen. Jos liityntäportille tarvitsee lisätä vain pelkkä link-local osoite, niin sen voi lisätä myös manuaalisesti seuraavassa esimerkissä näkyvällä käskyllä. (Configuring IPv6, 2011.)

Esimerkki:
hostname(config-if)#ipv6 address fe80::1111:2222:3333:4444 link - local

IPv6 enable

IPv6 enable–käskyllä saadaan liityntäportti nopeasti IPv6–portiksi. Käsky luo liityntäportille automaattisesti link-local osoitteen käyttämällä muokattua EUI-64 liityntäportti–ID:tä. IPv6 enable–käskyä ei tarvita IPv6–ominaisuuksien käyttöönottoon Cisco ASA-palomuureissa, jos liityntäporttiin on jo konfiguroitu jokin IPv6-osoite. (Configuring IPv6, 2011.)

Esimerkki:
hostname(config-if)# ipv6 enable

EUI–64

EUI (Extended Unique Identifier)-64 lisää liityntäporttiin 64-bittisen uniikin porttitunnisteen. Portti–ID:stä eli MAC -osoitteesta muodostettu osoitteen loppuosa lisätään manuaalisesti syötettyyn IPv6–osoitteeseen ilman manuaalista syöttöä tai DHCP–palvelinta. (Configuring IPv6, 2011.)

Esimerkki:
hostname(config-if)#ipv6 address 2001:db8:: /64 eui – 64

hostname# show ipv6 interface f0/0
Global unicast address(es):
*2001:DB8::**212:7FFF:FEEB:6B40**, subnet is 2001:DB8::/64 [EUI/TEN]*

IPv6 enforce EUI–64

EUI-64-tunnisteen käytön voi myös ottaa pakolliseksi tietyissä paikallisissa linkeissä käyttämällä enforce EUI-64 käskyä linkin liityntäportissa. Linkin liityntäporttien tunnistusosan on oltava 64 bittiä pitkä ja EUI-64–muodossa. Porttiin konfiguroitu enforce–käsky tarkistaa jokaisesta saapuneesta paketista lähdeosoitteen EUI-64–osan, minkä täytyy vastata lähdeportin MAC-osoitetta. Jos se ei vastaa sitä, syntyy virheilmoitus ja paketti tiputetaan. (Configuring IPv6, 2011.)

Esimerkki:
hostname(config-if)#ipv6 enforce - eui64 <interface_name>

7 IPV6-LIIKENTEEN SUODATUS PALOMUUREISSA

IPv6–liikenteen suodatus verkoissa kannattaa aloittaa tekemällä IPv6-Security Policy eli tietoturvapolitiikka, jota toteutetaan palomuureissa pääasiassa pääsylistoilla. Oletuksena palomuureissa ei ole minkäänlaisia pääsylistoja, ja kaikki liikenne estetään ulkoverkosta sisäverkkoon päin. Käytännössä tietoturvapolitiikan pääsylistoja voidaan alkaa tehdä kahdella tavalla. Aluksi joko sallitaan tai estetään kaikki liikenne palomuurin läpi. Jos kaikki liikenne sallitaan aluksi, niin kaikki liikenne mitä ei haluta päästää palomuurin läpi, pitää estää erikseen pääsylistoilla. Tämän työn käytännönkokeissa käytetyn menetelmän lähtökohta oli päinvastainen, eli kaikki palomuurin läpi kulkeva liikenne estettiin aluksi. Liikennettä avattiin sitä mukaa

pääsylistoilla, kun palvelimia tai palveluita lisättiin verkkoon. Tämä menetelmä oli tämän työn kannalta järkevin ja varmin vaihtoehto, ettei palomuuriin jäisi tuntemattomia tietoturva-aukkoja. (Hogg & Wyncke 2008, 164.)

Cisco ASA -palomuurien liikennettä suodatetaan pääasiassa pääsylistoilla, jotka tehdään erikseen sekä IPv4– ja IPv6-liikenteelle. Palomuureissa määritellään perinteisesti inside- ja outside–portit, jotka määrittelevät palomuurien toimintaa. Perussääntö on, että liikenne sallitaan luotettavammasta verkosta epäluotettavampaan verkkoon ja toiseen suuntaan kaikki liikenne on automaattisesti estetty. Inside–portti saa automaattisesti suojaustason 100 ja outside-portti saa suojaustason 0. Mitä suurempi suojaustason arvo, sitä luotettavampi verkko on kyseessä. Käytännössä kaikki liikenne mitä halutaan sallia palomuurin outside-portista sisään päin, täytyy erikseen sallia pääsylistojen avulla. Kaikki pääsylistat täytyy luomisen jälkeen liittää tiettyyn porttiin ja määritellä mihin suuntaan ne vaikuttavat. Tiettyjä poikkeuksia ovat esimerkiksi IPv6–pingien salliminen suoraan liityntäportteihin, jossa ei tarvita erillistä liityntäportin määritystä. (Hogg 2008, 164.)

7.1 Pääsylistat

IPv6-pääsylistat määritellään lähestulkoon samalla tavalla kuin IPv4-pääsylistatkin. Niissä täytyy vain määritellä erikseen että ne ovat nimenomaan IPv6-pääsylistoja. Ne eivät siis vaikuta ollenkaan IPv4–liikenteeseen. Muuten pääsylistojen rakenne koostuu aivan samalla tavalla kuin IPv4–pääsylistoissa. Pääsylistoissa sallitaan tai estetään tietyllä protokollalla kulkeva liikenne tietystä verkosta tiettyyn verkkoon. Pääsylistoja kannattaa tehdä yksi kumpaakin suuntaa kohden, koska liityntäporteilla voi olla käytössä vain yksi pääsylista kerrallaan, joko in- tai out-suuntaan päin. Eli suurin osa liikenteiden pääsylistoista kannattaa tehdä samalla pääsylistanimellä.

ipv6 access-list SPOLICY_IN permit icmp6 2a00:1dd0:100::/48 2a00:1dd0:100:b1::/64

Liikenteen yksittäinen lähdeosoite tai kohdeosoite voidaan myös erikseen sallia tai estää host-määrityksen avulla.

ipv6 access-list SPOLICY_IN permit icmp6 host 2a00:1dd0:100::10 host 2a00:1dd0:100:b1::10

Pääsylistojen loppuun lisätään erilaisia liikennetyyppimäärittelyjä joko tietyllä porttinumerolla tai porttinumeroita kuvaavilla liikenteen nimillä, jos pitää sallia jokin tietty protokolla, esimerkiksi HTTP-protokolla.

*ipv6 access-list SPOLICY_IN permit tcp 2a00:1dd0:100::10 host 2a00:1dd0:100:b1::10 (**www/ eq 80**)*

Kuvassa 3 on esimerkkinä erilaisia IPv6-pääsylistoja, jotka ovat luotu palomuuriin kyseisillä komentoriveillä. Kyseisillä pääsylistoilla sallitaan tietty liikenne palomuurin läpi ja kaikki muu liikenne on estetty. Pääsylistoja luodaan lisää sitä mukaan, kun tulee tarvetta päästää uutta liikennettä sen läpi. Kaikki pääsylistat ovat luotu samalla nimellä, jotta ne saataisiin nimettyä samanaikaisesti tiettyyn porttiin. Kuvan 3 pääsylistat ovat nimetty outside-liityntäporttiin ja sisäänpäin tulevalle liikenteelle. Kuvassa 3 näkyvällä access-group-käskyllä saadaan osoitettua IPv6-pääsylistat tiettyyn porttiin. (Adding an IPv6 access-list, 2011.)

```
ipv6 access-list SPOLICY_IN permit icmp6 2a00:1dd0:100::/48 host 2a00:1dd0:100:b1::10 echo
ipv6 access-list SPOLICY_IN permit udp any host 2a00:1dd0:100:b1::100 eq domain
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:b1::100 eq domain
ipv6 access-list SPOLICY_IN permit icmp6 2a00:1dd0:100::/48 host 2a00:1dd0:100:b1::100 echo
ipv6 access-list SPOLICY_IN permit icmp6 2a00:1dd0:100::/48 host 2a00:1dd0:100:b1::200 echo
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:b1::200 eq https
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:b1::200 eq www
ipv6 access-list SPOLICY_IN permit icmp6 any host 2a00:1dd0:100:b1::200 echo
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:b1::200 eq ftp
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:b1::200 eq ftp-data
ipv6 access-list SPOLICY_IN deny ip any any

access-group SPOLICY_IN in interface outside
```

Kuva3. IPv6 pääsylistat

7.2 ICMPv6:n salliminen

Kaikki ICMPv6–viestit ovat estetty oletuksena Cisco ASA-palomuureihin päin ja epäluotettavimmista verkoista luotettavimpiin verkkoihin. ICMPv6–viestit eli IPv6–pingit voidaan sallia kahdella tavalla: tekemällä normaali IPv6–pääsylista ICMP–protokollalle tai tekemällä ICMP-pääsylista suoraan liityntäporttiin. Näiden lisäksi palomuuriin täytyy lisätä ICMP–inspection, että saadaan minkäänlaisia ICMPv6–viestejä liikkumaan palomuurin läpi. (Hogg & Wyncke 2008, 165.)

7.2.1 ICMPv6–pääsylistat suoraan liityntäporttiin

ICMPv6–viestit voidaan sallia tekemällä pääsylista suoraan liityntäporttiin. Nämä pääsylistat tunnetaan nimellä ”ICMPv6 filter”. Nämä pääsylistat eroavat tavallisista IPv6–pääsylistoista siten, että nämä suodattavat liikennettä liityntäportteihin päin, eivätkä palomuurin läpi menevää liikennettä. Esimerkissä alla näkyy suoraan liityntäportteihin suunnattuja ICMPv6–pääsylistoja. Listoissa ei tarvitse olla erillistä ”deny any”–sääntöä, koska nämä säännöt vaikuttavat vain jos liikenne vastaa listassa olevia määrityksiä. Loput liikenteestä, jotka eivät vastaa listoissa sallittua liikennettä ovat automaattisesti estetty. (Hogg & Wyncke 2008, 165.)

Esimerkki:
ASA5510(config)# ipv6 icmp permit any echo outside
ASA5510(config)# ipv6 icmp permit any echo-reply outside
ASA5510(config)# ipv6 icmp permit any packet-too-big outside
ASA5510(config)# ipv6 icmp permit any time -exceeded outside
ASA5510(config)# ipv6 icmp permit any unreachable outside

7.2.2 ICMPv6-liikenteen tarkkailu (ICMPv6 inspection)

Ciscon ASA–palomuuri voi suorittaa ICMPv6:n ”tilallisen tarkkailun”(Stateful inspection) samalla tavalla kuin TCP-tai UDP–liikenteelle. ICMP–tarkkailu täytyy lisätä, jos haluaa minkäänlaisen ICMPv6–viestien menevän palomuurin läpi, ainakin ASA:n versiossa 8.2(3) ja multi-context-tilassa. ICMPv6:n tarkkailu täytyy sallia policy-mappia käyttämällä. Käskyn *inspect icmp* voi lisätä suoraan default inspection -luokkaan. (Hogg & Wyncke 2008, 164.)

Esimerkki:
```
policy-map global_policy
  class inspection_default
    inspect icmp
```

8 IPV6-LIIKENTEEN REITITYS PALOMUUREISSA

Vaikka Cisco ASA 5510 versio 8.2 tukee monia IPv4-reititysprotokollia, niin se ei tue IPv6-reititysprotokollia, vaan ainoa reititystapa on staattinen reititys. Staattisia IPv6–reittejä tarvitaan toisten IPv6–verkkojen tavoittamiseen. Jos palomuuriin saapuvan liikenteen kohdeosoite ei löydy staattisista reiteistä, se ohjataan oletusreitin kautta

eteenpäin. IPv6-oletusreittejä tarvitaan siis lähes aina, että liikenne saadaan kulkemaan varmasti haluttuun verkkoon. (Hogg & Wyncke 2008, 162.)

8.1 Oletusreitti

Oletusreitti voidaan määritellä Cisco ASA –palomuureissa joko inside- tai outside–puolelle kulkevalle liikenteelle. IPv4-verkkojen neljän nollan reittiä vastaava osoite IPv6–maailmassa on ::/0. (Hogg & Wyncke 2008, 163.) IPv6–oletusreitti konfiguroidaan seuraavalla tavalla:

ipv6 route if_name ::/0 <next_hop_ipv6_address>

8.2 Staattinen reitti

Staattiset IPv6–reitit määritellään joko inside– tai outside–liityntäportteihin. Niiden perään voi myös lisätä reitin maksimietäisyyden hyppyjen määränä(1-255) tai tunnelointi-määrityksen(tunneled). Tunneled-määrityksessä reittiä käytetään tunneloidulle liikenteelle, jolle ei ole määritelty erillistä tai automaattista reittiä ennestään ja etäisyysarvo on automaattisesti 255. (Hogg & Wyncke 2008, 163.) Staattinen reitti konfiguroidaan seuraavalla tavalla:

Esimerkkejä:

ipv6 route if_name <destination_ipv6_address> <next_hop_ipv6_address> [hop count <1-255> / tunneled]

ipv6 route outside 2a00:1dd0:100::/64 2a00:1dd0:a5a::2 ***230***
ipv6 route outside 2a00:1dd0:100::/64 2a00:1dd0:a5a::2 ***tunneled***

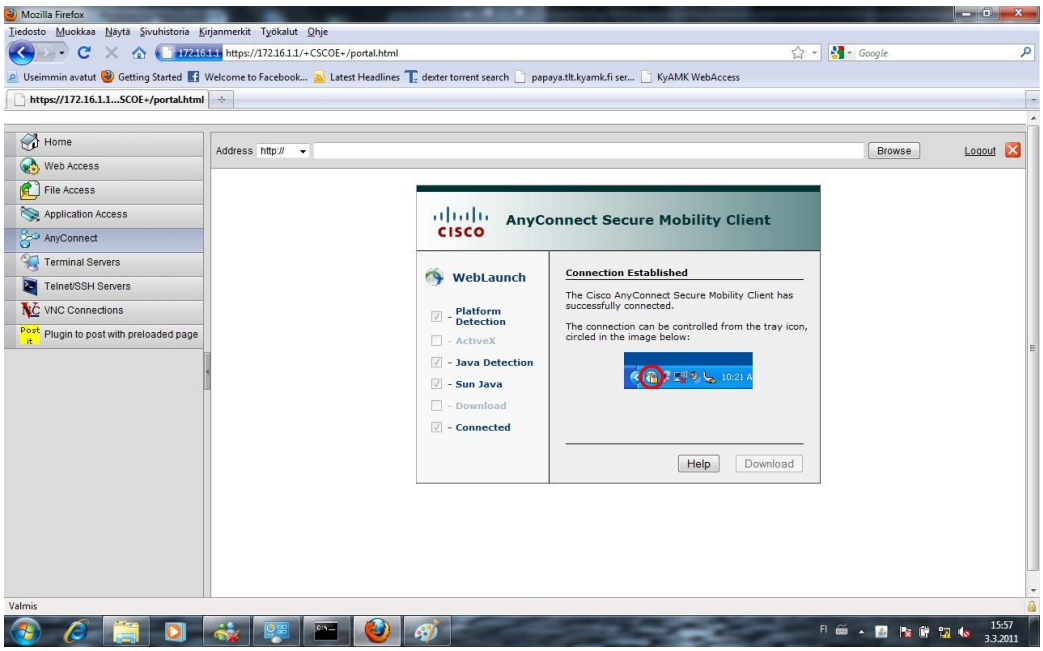
9 IPV6-TUNNELIT PALOMUUREISSA

Cisco ASA palomuurien LAN-to-LAN tunneleihin käytetään yleensä IPSec-protokollaa ja etäyhteyksiin SSL-salausprotokollaa (Hogg 2008, 368). LAN-to-LAN tunneli on mahdollista toteuttaa natiivina IPv6-tunnelina, mutta SSL VPN:ää ei voida toteuttaa täysin natiivina, vaan IPv6-liikenne täytyy siirtää IPv4 verkon läpi tunneloituna suojattuun IPv6-verkkoon. Syy tähän on, että uusimmatkaan Cisco ASA:n versiot eivät tue natiiveja IPv6 SSL VPN-tunneleita. (Configuring VPN , 2011)

9.1 SSL VPN

SSL VPN on käytännössä Cisco ASA palomuurien tarjoama VPN -tunneleiden muodostamiseen käytetty web-pohjainen hallintaliittymä. Tunnelit luodaan etätyöasemalta suljettuun verkkoon. Suljetun verkon reunalla on ASA–palomuuri, johon on konfiguroitu SSL VPN ja tunneli luodaan sen ja etäkäyttäjän välille. SSL VPN -tunneleita voidaan käyttää ilman erillistä asiakasohjelmaa vain kirjautumalla web-hallintaan internet-selaimen kanssa tai sitten asiakasohjelma AnyConnectin kanssa, josta kerrotaan myöhemmin tässä työssä. Etäyhteyden muodostanut asiakas saa itselleen suljetun verkon IPv6-osoitteen SSL-tunnelia pitkin ja voi liikennöidä tämän osoitteen kanssa suljettuun verkkoon. SSL VPN:ää ei voi luoda natiivina IPv6:na millään Cisco ASA:n versiolla, mutta IPv6-liikennettä voidaan siirtää IPv4-tunnelin läpi. SSL VPN:ää käytetään paljon nimenomaan etäkäyttötunnelointiin, kun taas IPseciä käytetään enemmän LAN-to-LAN käyttöön. (Hogg & Wyncke 2008, 368-373.)

Cisco ASA:n Clientless SSL VPN -tunneli muodostetaan kirjoittamalla selaimeen palomuurin IP-osoite, jonka jälkeen avautuvat kirjautumiskentät, johon pitää valita ryhmä ja kirjoittaa oikea käyttäjänimi ja salasana. Tämän jälkeen selaimeen avautuu SSL VPN:n hallintaan käytetty graafinen liittymä, josta esimerkki kuvassa 4. (Hogg 2008, 368-373.)



Kuva4. Clientless SSL VPN

9.1.1 SSL(Secure Sockets Layer)

SSL on VPN -tunnelointiin käytetty salausprotokolla, joka tunnetaan nykyään nimellä TLS, ja se toimii OSI -mallin kerroksilla 4-7. SSL-protokollalla suojataan IP-liikennettä ja yhteyksien suojauksen hoitaa OSI-mallin kuljetuskerros eli siinä ei tarvitse erikseen määrittää salaustapaa. SSL toimii HTTPS(TCP portti 443)-protokollan avulla ja on siksi usein jo valmiiksi sallittu eri verkkoihin ja on joissain tapauksissa helpompi käyttää kuin IPSec-protokollaa. Tavallisin SSL:n suojaama liikenne on nettiselaimen eli WWW-protokollan liikenne, minkä suojaamiseen SSL alun perin kehitettiin. (TLS, Wikipedia 2011.)

9.1.2 Anyconnect 3.0 -ohjelma

IPv6 SSL VPN -tunneloinnin asiakasohjelmana on käytetty paljon Anyconnect-ohjelmistoa, joka toteuttaa samanlaisen tunnelin kuin Clientless SSL VPN -yhteyskin. Anyconnectin asentamisen jälkeen Windowsin Käynnistä -palkkiin ilmestyy kuvake, josta saadaan helposti luotua SSL VPN -tunneli ilman Internet-selaimen käyttöä. Anyconnect ohjelmisto asennetaan asiakkaattoman SSL VPN -yhteyden kautta päätekoneelle, lataamalla se suoraan ASA–palomuurista. Asennustiedosto löytyy menemällä AnyConnect -osioon, jonka jälkeen asennus käynnistyy automaattisesti. (Hogg & Wyncke 2008, 368-373.)

Kuva5. AnyConnect 3.0 login

9.2 LAN-to-LAN IPSec VPN

LAN-to-LAN–tunneleita käytetään kahden suojatun verkon yhdistämiseen julkisen verkon yli, mikä toteutetaan luomalla tunneli näiden verkkojen reunalaitteiden välille. Cisco ASA versioista 8.3 ja myöhemmät tarjoavat IPv6-tuen myös LAN-to-LAN IPsec VPN -tunneleille. Cisco ASA:n versiot 8.2 ja sitä vanhemmat versiot eivät tue minkäänlaisia natiiveja IPv6-VPN- tunneleita. ASA:n versiot 8.3 ja uusin 8.4 tukevat vain yhdenlaisia natiiveja IPv6-tunneleita ja ne ovat LAN-to-LAN VPN-tunnelit. LAN-to-LAN-tunnelit täytyy muodostaa kahta Cisco ASA 5500–sarjan palomuuria käyttämällä, jotta ne toimivat eli näitä tunneleita ei pysty muodostamaan esimerkiksi ASA:n ja reitittimen välille. LAN-to-LAN-tunneleita pystyy muodostamaan joko pelkästään IPv6-osoitteita käyttämällä eri IPv6-verkkojen välillä tai sitten pitämällä sisäverkot IPv4-verkkoina ja ulkoverkko IPv6-verkkona tai päinvastoin. Ainut rajoite IPv6 LAN-to-LAN–tunneleilla on, että sisäverkkojen täytyyy muodostua saman protokollan osoitteista. Mahdolliset IPv6 LAN-to-LAN VPN topologiat ovat 8.3- ja 8.4-versioilla seuraavanlaiset:

- ASA:n sisäverkot IPv4-osoitteilla ja ulkoverkko IPv6-osoitteilla
- ASA:n sisäverkot IPv6-osoitteilla ja ulkoverkko IPv4-osoitteilla
- ASA:n sisäverkot IPv6-osoitteilla ja ulkoverkko IPv6-osoitteilla

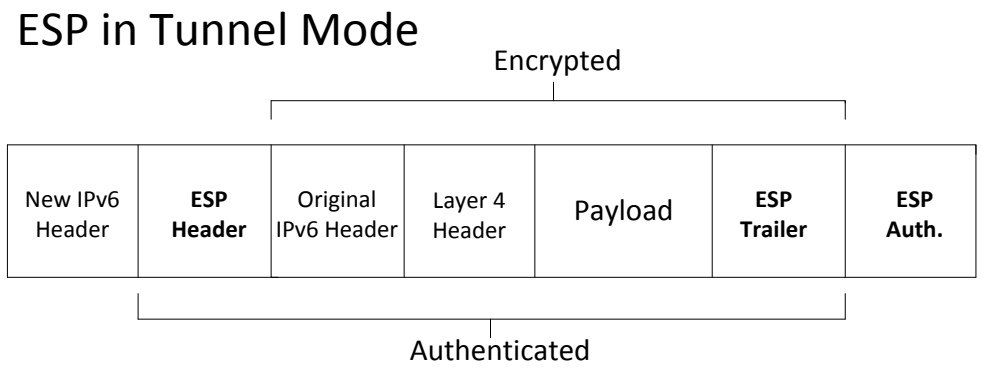
(Configuring LAN-to-LAN Ipsec VPNs, 2011.)

9.2.1 IPSec (IP Security Architecture)

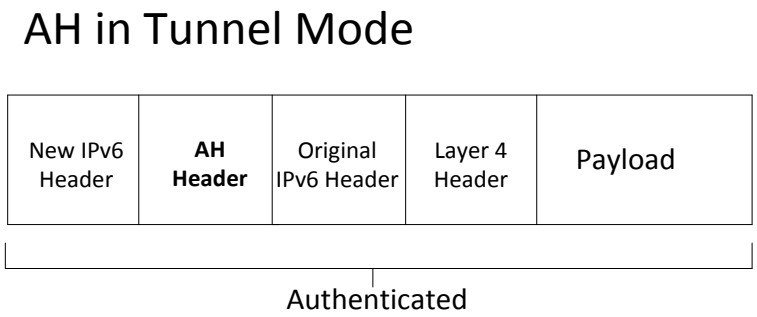
Alkuperäisessä IP-protokollan suunnittelussa ei ollut tarkoitus suojata yksittäisiä paketteja ja sen vuoksi lisäominaisuuksia lisättiin protokollaan. IETF(The Internet Engineering Task Force) kehitti IPSecin, että saataisiin IP-paketeille suojaukseen käytettävä kehys, joka voi sisältää monia erilaisia salaus- ja todennusmahdollisuuksia. Ideana oli, että IPSec ei olisi yksittäinen protokolla, millä olisi rajallinen määrä joitain salausalgoritmejä, vaan niitä voisi myös lisätä myöhemmin eikä protokollaa tarvitsisi uusia mitenkään. IPSec ei siis pakota käyttämään mitään tiettyä salausalgoritmiä. (Hogg & Wyncke 2008, 320.)

IPSec määrittää uudet protokollan otsikot, jotka lisäävät todennuksen ja luottamuksellisuuden IP-paketteihin. Näistä yksi on AH(Authentication Header)-otsikko, joka suojaa otsikkotietoja ja paketin tietoja. Toinen niistä on ESP(Encapsulation Security Payload), joka suojaa paketin sisältöä. IPsecin arkkitehtuuri on lähes samanlainen IPv4:ssa ja IPv6:ssa. IPv4:ssa AH ja ESP ovat IP-protokollan otsikoita, ja IPv6:ssa ne määritellään lisäotsikoiden avulla. ESP käyttää next-header–arvonaan lukua 50 ja AH:n luku on numero 51. AH:ta tai ESP:tä voi käyttää kumpaakin joko yksin tai sitten yhdistettynä toisiinsa. ESP huolehtii paketin kuorman luottamuksellisuudesta, todentaa paketin lähteen ja huolehtii viestin eheydestä. ESP käyttää salausalgoritmejä suojatakseen paketin sisällön ja on myös mukautunut käyttämään joitakin muotoja HMAC(Hash-based Message Authentication Code):stä huolehtiakseen viestin eheydestä. AH käyttää yhteydetöntä paketin eheyden varmistusta ja tietojen alkuperän todennusta. AH:n ensisijainen toiminto on hoitaa pakettien lähteiden todennus ja todeta paketin yhteneväisyys. AH tekee vain paketin todennuksen ja yhteneväisyyden todennuksen eikä hoida sulautettujen pakettien varmistusta. ESP taas hoitaa näiden pakettien varmistuksen/luottamuksellisuuden ja tuo myös lisää todennusominaisuuksia paketeille. Molemmat otsikot, AH sekä ESP perustuvat IKE:een(Internet Key Exchange) vaihtaakseen suojatusti symmetriset avaimet salauksessa ja todennuksessa. (Hogg & Wyncke 2008, 320.)

IPv6-tunnelointiin käytetyt IPSec paketit esitetään kuvissa 6 ja 7:



Kuva6. ESP (Hogg & Wyncke 2008, 323.)



Kuva7. AH (Hogg & Wyncke 2008, 323.)

9.2.2 IKEv1 (Internet Key Exchange version 1)

IPSec:n arkkitehtuurin tietty osa sisältää avainten vaihto- ja avainten hallintaprotokollia. IPSec tunneleiden molempien päiden on oltava yhtä mieltä siitä, mitä todennusalgoritmiä, todennusavainta, salausalgoritmiä ja salausavainta ne käyttävät sekä missä ajassa avaimet päivitetään uusiin. Näiden määrityksien täytyy olla samat molemmissa päissä tunnelia, jotta tunneli toimisi oikein. (Hogg 2009, 322.)

IKEv1 käyttää UDP-protokollan porttia 500 vaihtaakseen kaksivaiheisesti salausalgoritmejä ja avainmateriaaleja. Vaihe yksi avaa kanavan, jossa vaihdetaan tietoja, ja sen voi suorittaa joko normaalissa tilassa(Main-mode) tai aggressiivisessa tilassa(Aggressive-mode). Normaali tila suorittaa kolme kaksisuuntaista vaihtoa, kun taas Aggressiivinen tila vaatii vähemmän paketteja ja on nopeampi. Normaali tila on turvallisempi tapa mutta hitaampi. Vaihe kaksi neuvottelee IPSec-salaus-algoritmit, joitain parametreja ja avaimet/sertifikaatit, joita käytetään itse yhteyden muodostukseen. Kaikki salaukseen liittyvät tiedot löytyvät SDP(Sucure Policy

Database)-tietokannasta. Kummallakin puolella täytyy olla tämä tietokanta, josta löytyy lista algoritmeistä, avaimista, IP-osoitteista ja avainten voimassaoloajoista, jota tunnelin kumpikin osapuoli käyttää tunnelia aktivoidessa. (Hogg & Wyncke 2008, 322-323.)

Tunnelin molempien päiden hyväksyttyä salaustavat ja avaimet, syntyy niiden välille SA(Security Associations)-"yhteysistunnot". IKEv1:ssä SA:t pitää luoda molempiin suuntiin, molempiin vaiheisiin (1- sekä 2-vaiheeseen) ja ESP- sekä AH-protokollille. Tämän vuoksi tarvitaan kaksi SA:ta IKEv1:n ensimmäiseen vaiheeseen ja neljä SA:ta tarvitaan täydelliseen IPSec-yhteyteen. Ensimmäisessä vaiheessa luodaan IKE SA molempiin päihin eli kaksi SA:ta. Sitten toisessa vaiheessa luodaan AH:lle ja ESP:lle ja molempiin päihin samat eli yhteensä luodaan 4 SA:ta. (Hogg & Wyncke 2008, 324.)

Valid Encryption Methods	Valid Authentication Methods
esp-des	esp-md5-hmac
esp-3des (default)	esp-sha-hmac (default)
esp-aes (128-bit encryption)	
esp-aes-192	
esp-aes-256	
esp-null	

Kuva8. IKEv1 Encryption and Authentication Methods (Configuring LAN-to-LAN Ipsec VPNs, 2011.)

9.2.3 IKEv2 (Internet Key Exchange version 2)

IKEv1:n määritykset ovat levinneet niin moneen IETF:n RFC-dokumenttiin, ja se on kehittynyt niin monimutkaiseksi, että se haluttiin korvata versiolla kaksi. Version kaksi tarkoitus oli yksinkertaistaa tätä protokollaa, kasaamalla vain tärkeimmät määritykset yhteen dokumenttiin sekä poistamalla turhat osat kokonaan. IKEv1:n aggressiivinen tila on poistettu kokonaan IKEv2:sta, koska hakkerit ovat tehneet paljon hyökkäyksiä juuri tähän vaiheeseen. IKEv2:ssa on vain normaali tila ja nopea tila(Quick Mode). Normaali tila on neljän paketin pituinen ja Nopea tila vain kahden paketin pituinen. IKEv2 käyttää yksivaiheista yksinkertaisempaa neuvottelua tunnelin toisen pään kanssa ja luo tämän jälkeen vain yhdet SA:t molempiin päihin sekä generoi avaimet vain joko AH:lle tai ESP:lle. (Hogg 2009, 324.) (Riikonen, 6.) (Ding, 20.)

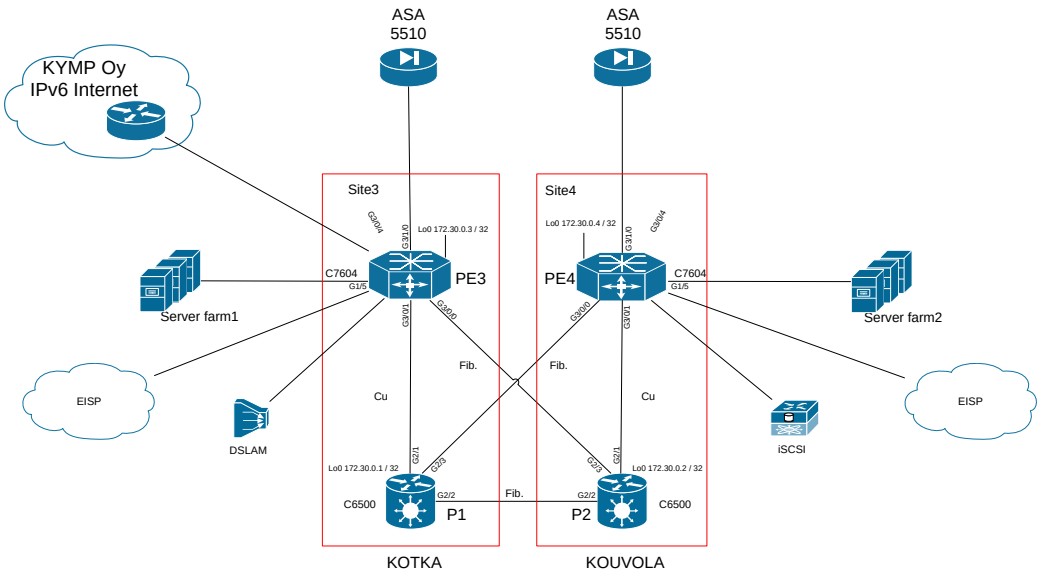
Valid Encryption Methods	Valid Integrity Methods
des	sha (default)
3des (default)	md5
aes	
aes-192	
aes-256	

Kuva9. IKEv2 Encryption and Integrity Methods Methods (Configuring LAN-to-LAN Ipsec VPNs, 2011.)

10 KÄYTÄNNÖN KOKEET SIMUNETISSÄ

SimuNet on Kymenlaakson ammattikorkeakoulun sekä paikallisten yritysten yhteinen hanke, jota kaikki osapuolet ovat pyrkineet kehittämään. Se on oikeaa operaattoriverkkoa mallintava testiverkko, jota voidaan käyttää monenlaisiin projekteihin. SimuNetin avulla tehtiin myös tämän työn käytännön kokeita.

Paikallisten yritysten tarjoamat avut olivat hyödyllisiä tämän työn käytännön kokeita tehdessä. Hyödyllisin oli Kymp Oy:n tarjoama IPv6-liittymä, joka oli yhdistetty suoraan SimuNetiin ja sen avulla päästiin testaamaan IPv6-yhteyksiä palomuurin läpi julkiseen IPv6-Internetiin. SimuNetin käyttöön rekisteröity IPv6-osoiteavaruus oli 2a00:1dd0:100::/48.



Kuva10. SimuNetin topologia

10.1 SimuNetin toiminta lyhyesti

Verkko koostui kahdesta eri puolesta, jotka toimivat ikään kuin ne olisivat kahdessa maantieteellisessä paikassa mutta kuuluivat silti samaan operaattoripilveen. Tämän työn aikana puolet olivat nimetty nimillä KOTKA ja KOUVOLA. SimuNetin reitittimien välillä toimi OSPF(Open Shortest Path First)-reititysprotokolla, reunareitittimien välillä BGP(Border Gateway Protocol)-reititysprotokolla ja kaikki reitittimet kuuluivat samaan MPLS(Multiprotocol Label Switching)-pilveen. OSPF-protokollalla reitittimet mainostivat reittejä toisilleen verkon sisällä ja BGP välitti reittejä reunareitittimien välillä sekä verkon reunoilta eri autonomisiin alueisiin ulos SimuNetistä. BGP:n avulla kulki muun muassa IPv6-reittien mainostukset, josta kerrotaan lisää myöhemmin tässä työssä. MPLS:n avulla IP-paketit kuljetettiin nopeasti verkossa MPLS-lippujen avulla, ilman että runkoreitittimien tarvitsi tehdä reititystä. MPLS:ää käytettiin IPv6-liikenteen siirtämiseen IPv4-runkoverkon yli, josta kerrotaan lisää myöhemmin tässä työssä. Näiden lisäksi verkon eri puolien välillä oli myös virtuaalisia lähiverkkotunneleita, joiden avulla esimerkiksi palomuurien väliset failover-yhteydet toimivat. SimuNetin reunareitittimissä(PE-laitteissa) toimi myös HSRP(Hot Standby Router Protocol)-protokolla, jotta koko verkosta saatiin reduntanttinen katkosten varalta. PE-laitteisiin on myös luotu eri VLANit, joihin määriteltiin IP-osoitteet, joita tarvittiin myös HSRP:ssä. Näiden protokollien avulla verkko oli täysin reduntanttinen linkkien katkeamisen varalta ja oli valmis muokattavaksi erilaisiin tarkoituksiin. SimuNetin palvelinfarmit sijaitsivat molemmilla puolilla verkkoa liitettynä PE-laitteisiin. Palvelinfarmeihin asennettiin erilaisia palvelimia ja palveluita. Näitä olivat muun muassa IPv6 WWW –palvelin, IPv6 FTP -palvelin, IPv6 DNS -palvelin ja verkkolevyjä. Näiden palvelimien edustalla toimivat Ciscon ASA -palomuurit, jotka varmensivat toisiaan failover-toiminnolla ja ne tarvitsivat IPv6-tuen, jotta eri palvelut saatiin käyttöön palvelinfarmeilta.

10.2 SimuNetin palomuurien toiminta ennen IPv6-liikennettä

Palomuurit toimivat SimuNetissä palvelinfarmien edustapalomuureina. Palvelinfarmien liikenne oli ainoa liikenne, jonka palomuurit suodattivat. Palomuurit olivat toimineet vain IPv4–liikenteen kanssa.

Palomuurit olivat kahdennettu eri konteksteja käyttämällä eli ne olivat multi-context-tilassa. Kontekstien nimet olivat KOTKA, KOUVOLA, admin ja system. Nämä

kontekstit sijaitsivat molemmissa palomuureissa, joita kumpikin laite pystyi käyttämään samanaikaisesti, jos toinen laite kaatui. Kaikki kontekstit olivat käytössä samaan aikaan molemmilla puolilla verkkoa eli ne olivat aktiivi-aktiivi-tilassa. KOTKA oli aktiivinen verkon vasemmalla puolella ja KOUVOLA verkon oikealla puolella SimuNetin topologiasta katsoen. Kontekstit olivat ikään kuin yhden palomuurilaitteen konfiguraatiot mutta ne sijaitsivat tässä tapauksessa molemmissa laitteissa. Jos toisen aktiivisen kontekstin konfiguraatiota muutettiin, niin toisenkin laitteen sama kyseinen konteksti päivittyi automaattisesti.

Työtä aloittaessa palomuureihin ei ollut tehty ollenkaan pääsylistoja mutta pingit kulkivat oletusasetuksilla palomuurin läpi. Liityntäporteille oli annettu IPv4-osoitteet ja palomuurin inside- ja outside-liityntäportit olivat määritelty. Eri konteksteihin oli määritelty niiden VLANit ja oletusreitit. Palomuurien failover-toiminnot toimivat hyvin eri kontekstien välillä ja näiden vaihdossa ei mennyt kuin muutama sekunti.

Failover–toiminto tarvitsi toisen kerroksen tunneleita toimiakseen, koska palomuurien failover-linkki piti muodostaa lähiverkkoyhteydellä. Nämä tunnelit olivat määritelty PE-laitteisiin ja ne olivat toteutettu pseudo-wire- ja VPLS(Virtual Private Lan Service)-ratkaisuiden avulla. Lisää VPLS-yhteyksistä sekä muista virtuaalisista tunneleista Riku Oinosen opinnäytetyössä, joka on tehty myös SimuNetiin. (Oinonen 2011.)

11 IPV6-LIIKENNE SIMUNETISSÄ

SimuNetin IPv6-liikenne kulki verkon läpi PE-laitteiden 6PE-ominaisuuksien avulla, jotta eri puolilta SimuNetiä päästiin IPv6-Internetiin ja kummankin puolen palvelinfarmeille. Palvelinfarmeilla sijaitsevat IPv6-palvelut täytyi suojata palomuureilla, koska SimuNet oli yhdistettynä julkiseen IPv6-Internetiin. IPv6-palveluita käyttäisivät SimuNetin ensimmäiset "asiakkaat", joita liitettiin SimuNetiin tämän työn aikana erillisellä natiivilla IPv6-palomuurilla.

11.1 IPv6-liikenteen kuljetus IPv4-runkoverkon läpi

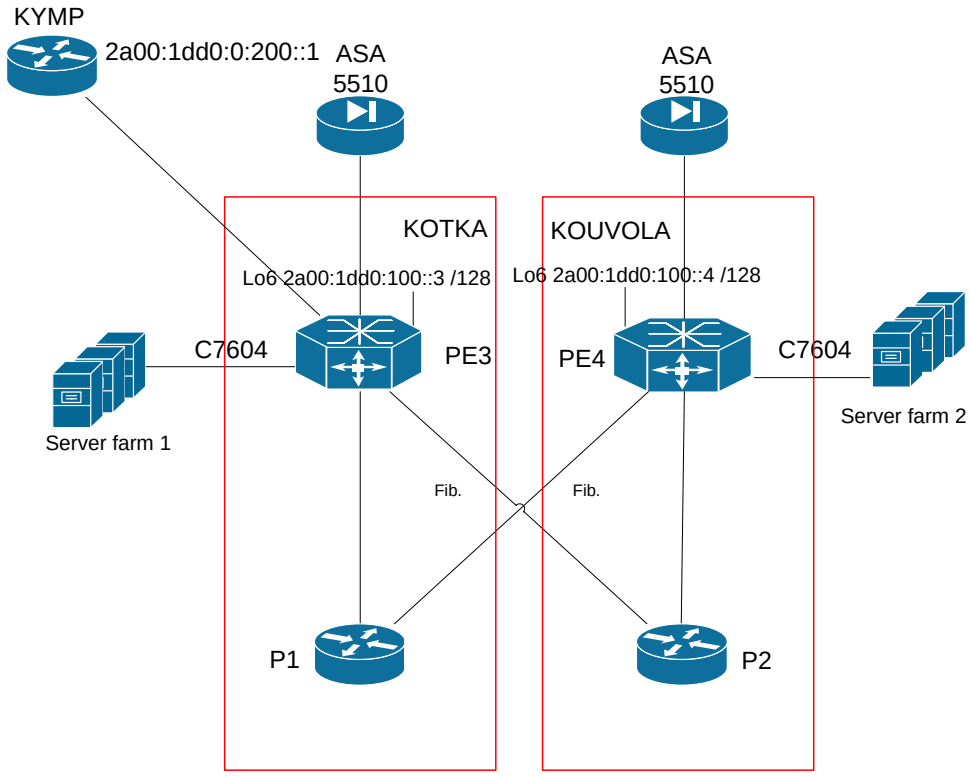
IPv6-liikenne kulki SimuNetissä verkon KOTKA-puolelta verkon KOUVOLA-puolelle ja takaisin PE-reitittimien avulla. P–laitteet olivat verkossa vain liikenteen välittäjinä eivätkä tienneet mitään IPv6–liikenteestä. IPv6–liikenne lisättiin verkkoon

Ciscon 6PE(IPv6 over MPLS)-menetelmällä, joka käytti hyväkseen laitteiden Dual–Stack-ominaisuutta. 6PE–tekniikka lisäsi IPv6–ominaisuudet vain verkon reunareitittimiin ja mahdollisti IPv6–liikenteen kulun verkon läpi ilman, että verkon sisäiset välittäjälaitteet tiesivät tästä mitään. 6PE–tekniikka oli hyvä tapa siirtyä IPv4-verkoista IPv6–verkkoihin nopeasti, pitäen verkon sisäiset muutokset mahdollisimman vähäisinä ja oli tästä syystä vain ensimmäinen vaihe IPv6–osoitteisiin siirtymisessä. Natiivit IPv6–verkot olivat vasta kehitysasteella työtä tehdessä ja niihin siirtymiseen liittyi paljon erilaisia riskejä. 6PE oli tässä vaiheessa järkevin ratkaisu SimuNetin monia osa-alueita silmällä pitäen. (Suurnäkki 2010, 3.)

6PE tarvitsi toimiakseen MPLS:ää, BGP4–reitystä ja laitteiden Dual-Stack–ominaisuutta. 6PE käytti hyväksi jo toimivaa IPv4–runkoverkkoa siten, että IPv6-liikenne siirrettiin kuormana MPLS–pakettien sisällä PE–reitittimien välillä. Paketoituna MPLS–paketteihin IPv6–liikenne pystyi liikkumaan verkossa samoja reittejä kuin IPv4–liikennenkin. MPLS:ää hallittiin ja konfiguroitiin vain IPv4–osoitteilla. IPv6–reiteistä vastasi BGP–protokolla ja vain se oli tietoinen verkon IPv6–osoitteista. Lisää SimuNetin PE-laitteiden IPv6-liikenteeseen liittyviä asioita löytyy Simo Suurnäkin projektityöstä 6PE, joka toteutettiin SimuNetissä ennen tämän työn aloitusta. (Suurnäkki 2010, 3.)

11.2 Käytännön kokeissa käytetyt SimuNetin laitteet

Tämän työn SimuNetiin kohdistuvissa käytännön kokeissa tarvittiin vain muutamaa SimuNetin laitetta ja siksi SimuNetin topologian kuvasta voidaan karsia muutamia laitteita pois ja keskittyä vain oleellisiin laitteisiin ja niiden toimintaan. Käytännön kokeissa käytettiin pääasiassa Ciscon laitteita: kolmea Cisco ASA -palomuuria, kahta PE(Provider Edge)-laitetta, kahta P(Provider)-laitetta sekä vielä molempia palvelinfarmeja.



Kuva11. Fyysinen kytkentä

Laitteet ja niiden tehtävät lyhyesti SimuNetissä:

Cisco Asa 5510 –palomuurit

SimuNetin palvelinfarmien edustalla toimivat Cisco ASA 5510 -palomuurit, jotka varmensivat toisiaan failover–toiminnolla. SimuNetin eri palvelut toimivat näiden palomuurien kautta. Kaikki liikenne, mitä palvelinfarmeille meni, kulki palomuurien läpi. Palomuureista toinen sijaitsi KOTKA-puolella ja toinen KOUVOLA-puolella SimuNetiä. Kolmas palomuuri on tämän työn lopussa SimuNetin reunalle lisätty natiivi IPv6-palomuuri.

Palvelimet sisäverkossa

Ohjelmistona palvelinfarmien palvelinlaitteissa toimi VMware ESX 4.0. Työtä tehdessä testipalvelimina käytettiin Linux-käyttöjärjestelmien päälle käynnistettyjä palveluita.

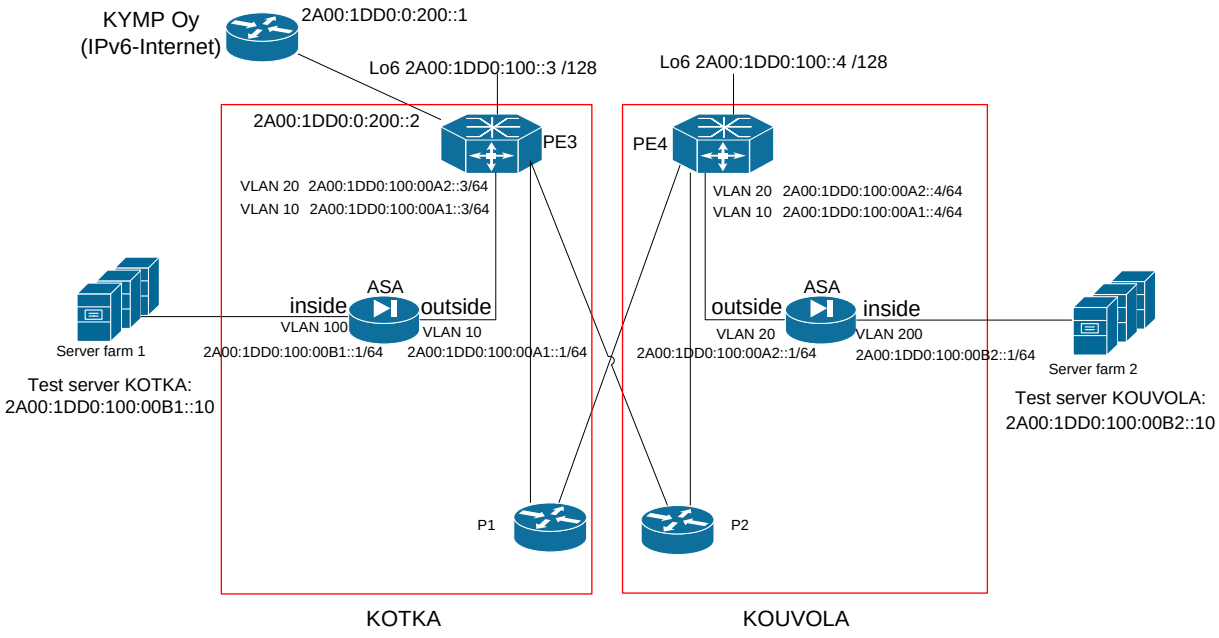
Provider Edge –reitittimet

Cisco 7604 -reitittimet toimivat SimuNet-verkon reunalaitteina, joihin verkon ”asiakkaiden” Customer Edger–laitteet liitettäisiin. Toiseen PE-laitteeseen on liitetty muun muassa KYMP Oy:n IPv6–liittymä.

Provider-kytkimet
SimuNetin runkolaitteet ovat Cisco Catalyst 6500 –kytkimiä, jotka toimivat vain MPLS-liikenteen välittäjinä verkon keskellä. Ne eivät tienneet esimerkiksi paketoidusta IPv6–liikenteestä mitään, jota niiden kautta kulki.

11.3 Verkon palomuurien looginen IPv6-toimintamalli

Kuvassa 12 näkyy, kuinka palomuurien oli tarkoitus toimivat serverifarmien edustalla ja mitä kautta IPv6-liikenteen oli tarkoitus kulkea loogisesti. Kuvassa 12 näkyy myös, mitä IPv6-osoitteita käytettiin eri laitteissa ja niiden välisissä verkoissa(VLANit) sekä IPv6-osoitteet, jotka lisättiin seuraavaksi ASA-palomuurien liityntäportteihin.



Kuva12. Palomuurien looginen toimintamalli

IPv6-osoitteet oltiin jo lisätty PE3- ja PE4-laitteisiin sekä kummallekin puolelle testi-palvelimille. PE-laitteilta lähteville VLANeille oltiin myös lisätty IPv6-osoitteet, jotta HSRP-protokolla toimisi IPv6-liikenteen kanssa. P-laitteisiin ei tarvinnut lisätä mitään

konfiguraatioita, koska IPv6-liikenne kulki MPLS-pakettien sisällä. Palomuureihin oli tarkoitus lisätä IPv6-osoitteet, että SimuNetin IPv6-liikenne saataisiin kulkemaan myös palvelinfarmeille ja niiden IPv6-liikennettä suodatettaisiin. Ennen kuin palomuureihin lisättiin Dual-Stack-ominaisuus, piti ne päivittää uudempaan versioon.

12 SIMUNETIN PALOMUURIEN PÄIVITYS

SimuNetin palvelinfarmien edustalla toimivien Cisco Asa 5510 -palomuurien päivittäminen oli ajankohtaista, koska käytönnön kokeita aloittaessa niiden käyttöjärjestelmäversiot olivat 8.0-versiot. Uudempia versioita oli kolme kappaletta: 8.2, 8.3 ja 8.4. Tässä tapauksessa piti asentaa 8.2(3)-versiot molempiin palomuureihin, koska niissä ei ollut 1Gb kokoista muistia, jota tarvittaisiin 8.3- tai uusimpaan 8.4-versioon päivittäessä. Palomuureissa oli vain 256Mb muistia, mikä riitti 8.2(3)-versiolle. SimuNetin ASA-palomuureihin täytyi päivittää myös ASDM–webhallinta, että saatiin siihen myös kaikki uusimmat ominaisuudet käyttöön esimerkiksi IPv6-ominaisuudet.

Päivittääkseen palomuurit tarvittiin aluksi yhteys yhdeltä virtuaalikoneelta ASAaan, johon oli asennettu uusien käyttöjärjestelmien siirtoon tarvittava TFTP(Trivial File Transfer Protocol)-palvelin. Tällä palvelimella siirrettiin ASA-palomuureihin tarvittavat päivitys-imaget. Virtuaalikoneelle täytyi antaa jokin IP-osoite, joka oli samalla tarvittavan TFTP -palvelimen osoite, johon palomuurilla otettiin yhteys. Päivitykseen tarvittavat tiedostot piti siirtää TFTP-palvelimen käyttämään kansioon, josta palomuuri löysi ne siirron yhteydessä. Asan (tässä tapauksessa nollatussa) konfiguraatioossa avattiin yksi portti siirtoa varten ja helpoiten tämä onnistui antamalla portille IP-osoite ja nimeämällä se sisäpuolen portiksi, ettei liikennettä estettäisi mitenkään. Kun yhteys palomuuriin oli muodostettu, niin seuraavaksi siirrettiin uudet käyttöjärjestelmäversiot ASAaan, tämän konsolilta annettujen käskyjen avulla. Siirron jälkeen oli tarpeellista tarkistaa, että menivätkö tiedostot varmasti flash-muistiin ja esiintyikö siirrossa yhtään virhettä. Kun käyttöjärjestelmä- ja ASDM-tiedostot näkyivät flash-muistissa, voitiin ne nimetä palomuurin ensisijaiseksi boottaus-imageksi ja ensisijaiseksi ASDM-imageksi. Vanhat järjestelmäversiot nimettiin uudelleen ja jätettiin flash-muistiin varmuuden vuoksi, jos vaikka vanha versio täytyisi palauttaa myöhemmin takaisin palomuuriin.

Päivitykseen tarvittavat konfiguraatiot:

ASA:

conf t
interface ethernet 0/0
ip address 192.168.1.1 255.255.255.0
nameif inside
no shutdown
!
boot system flash:/asa823-k8.bin
asdm image flash:/asdm-634-53.bin
write memory

TFTP-siirto:

copy tftp:asa823-k8.bin flash:
copy tftp:asdm-634-53.bin flash:

13 DUAL-STACK SIMUNETIN PALOMUUREISSA

Työn käytännönkokeissa tarkoituksena oli tutkia ja kokeilla SimuNetin Cisco ASA 5510 -palomuurien IPv6-ominaisuuksia. Työtä tehdessä SimuNetissä oli monta projektia käynnissä samaan aikaan ja IPv4-runkoverkko haluttiin pitää sellaisenaan, ilman suuria muutoksia. Tarkoitus oli, että IPv6-liikenne lisättäisiin SimuNetiin ja sen palomuureihin IPv4-liikenteen rinnalle Dual-Stackia ja 6PE:tä käyttämällä. SimuNetissä ei ollut aluksi kuin kaksi ASAn palomuuria, joihin ensimmäiseksi lisättiin Dual-Stack-ominaisuus. Käytännönkokeissa SimuNetin reunalle lisättiin myöhemmin vielä natiivi IPv6-palomuuri, joka oli myös Cisco ASA 5510 -palomuuri. Tämän työn käytännön kokeissa keskityttiin tarkemmin vain palomuurien eri IPv6-ominaisuuksiin ja niiden testaamiseen. Palomuurien välinen failover-toiminto ei tarvinnut IPv6:n myötä mitään muutoksia sen konfiguraatioon mutta failover-osoitteet olisi voitu muuttaa myös IPv6-osoitteiksi. tästä ei olisi kumminkaan ollut mitään hyötyä SimuNetille eikä palomuureille, koska runkoverkko oli muutenkin IPv4-protokollaa. Asan versiot 8.2(1) ja sitä uudemmat tukevat failoveria IPv6-osoitteilla.

13.1 Liityntäporttien määrittäminen

Liityntäportteihin konfiguroitiin IPv6-osoitteet Dual-Stackina IPv4-osoitteiden rinnalle. Liityntäportteihin lisättiin julkiset unicast-osoitteet ja joihinkin myös Link-local-osoitteet. Link-local-osoitteet lisättiin manuaalisesti kummankin puolen inside-

portteihin, koska Linux-pohjaiset palvelimet käyttivät oletusreittinään oletuksena link-local-osoitteita ja ne haluttiin yksinkertaisemmiksi. Link-local-osoitteiksi pystyi määrittämään helposti muistettavat osoitteet, jotka helpottivat paljon palvelimien oletusreitin testausta, esimerkiksi KOTKA-puolen osoitteeksi *fe80:a1::1*. Julkisia unicast-osoitteita tarvittiin palomuurin outside-porteissa ulkoisten yhteyksien testaamiseen ja myös etähallintayhteyksiin, joita voitiin koittaa esimerkiksi SSH:lla (Secure Shell).

KOTKA-kontekstiin lisättiin seuraavat konfiguraatiot:

```
interface Ethernet0/0.10
 nameif outside
 security-level 0
 ipv6 address 2a00:1dd0:100:00a1::1/64
 ipv6 address fe80:a1::1 link-local
!
interface Ethernet0/0.100
 nameif inside
 security-level 100
 ipv6 address 2a00:1dd0:100:00b1::1/64
 ipv6 address fe80:b1::1 link-local
```

KOUVOLA-kontekstiin lisättiin seuraavat konfiguraatiot:

```
interface Ethernet0/0.20
 nameif outside
 security-level 0
 ipv6 address 2a00:1dd0:100:00a2::1/64
 ipv6 address fe80:a2::1 link-local
!
interface Ethernet0/0.200
 nameif inside
 security-level 100
 ipv6 address 2a00:1dd0:100:00b2::1/64
 ipv6 address fe80:b2::1 link-local
```

Liityntäportin tiedoissa näkyi että palomuurilla oli juuri ne IPv6-osoitteet, jotka haluttiinkin. *Show ipv6 interface inside* -käskyllä nähtiin kuinka inside-portti sai määrätyt IPv6-osoitteet:

```
ciscoasa/KOTKA# show ipv6 interface inside
inside is up, line protocol is up
  IPv6 is enabled, link-local address is fe80:b1::1
  Global unicast address(es):
    2a00:1dd0:100:b1::1, subnet is 2a00:1dd0:100:b1::/64
```

13.2 IPv6-reititys

SimuNetin palomuureihin ei tarvinnut lisätä kuin IPv6–oletusreitti outside-puolen suuntaan, että IPv6-liikenne saatiin kulkemaan oikeaan verkkoon. Palomuurin oletusreitteihin lisättiin PE -laitteiden HSRP:n tarjoama virtuaalinen IPv6–osoite. Tämä oletusreitti lisättiin molempiin konteksteihin, että yhteydet osaisivat siirtyä tarvittaessa toiselle puolelle verkkoa. Seuraavassa esimerkissä näkyy, kuinka oletusreitti lisättiin ja miltä IPv6-reititystaulu näytti tämän jälkeen.

KOTKA sekä KOUVOLA-konteksteihin lisättiin seuraavanlaiset oletusreitit:

KOTKA:
ipv6 route outside ::/0 fe80::1

KOUVOLA:
ipv6 route outside ::/0 fe80::2

Kuvassa 13 näkyy KOTKA-puolen IPv6-reititystaulu, jossa näkyy IPv6-sisäverkko 2a00:1dd0:100:b1::/64, IPv6-ulkoverkko 2a00:1dd0:100:a1::/64 ja IPv6-oletusreitti fe80::1.

```
ciscoasa/KOTKA# show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static
L   2a00:1dd0:100:a1::1/128 [0/0]
     via ::, outside
C   2a00:1dd0:100:a1::/64 [0/0]
     via ::, outside
L   2a00:1dd0:100:b1::1/128 [0/0]
     via ::, inside
C   2a00:1dd0:100:b1::/64 [0/0]
     via ::, inside
L   fe80::/10 [0/0]
     via ::, outside
     via ::, inside
L   ff00::/8 [0/0]
     via ::, outside
     via ::, inside
S   ::/0 [0/0]
     via fe80::1, outside
ciscoasa/KOTKA#
```

Kuva13. Show ipv6 route (KOTKA)

14 IPV6-PÄÄSYLISTAT JA IPV6-YHTEYKSIEN TESTAAMINEN

SimuNetin molemmille puolille oli käynnistetty aluksi yhdet testiserverit, joilla testattiin IPv6-yhteyksien ja pääsylistojen toimivuutta palomuureissa, pääasiassa IPv6-pingien kulkua eri laitteisiin ja takaisin. Eri palveluiden kokeilemiseen tarvittiin lisää virtuaalipalvelimia, joita tarvittaessa luotiin. Pääsylistat luotiin kaikki samaan pääsylistaan nimellä SPOLICY_IN, koska jokaiseen porttiin voi luoda vain yhden pääsylistan kumpaakin suuntaa kohden.

14.1 ICMP6–viestit

ICMP6-pingeillä testattiin IPv6-yhteyksien toimivuutta ja ne eivät kulkeneet palomuurin läpi samalla tavalla kuin IPv4-pingit ASAn versiossa 8.2(3). ICMP6-viestejä varten täytyi kytkeä palomuureissa päälle ICMP-inspection, joka ohjasi ICMP6-viestit ASAn läpi. Tämän lisäksi IPv6 pääsylistoissa täytyi sallia ICMP6-viestit outside-portista sisäänpäin. Ensimmäiseksi luotiin pääsylistat palomuureihin.

Kaikki ICMP6-pingit SimuNetin IPv6-osoitealueesta KOTKA-puolen sisäverkkoon sallittiin seuraavalla pääsylistalla KOTKA-puolen ASAan:

ipv6 access-list SPOLICY_IN permit icmp6 2a00:1dd0:100::/48
2a00:1dd0:100:00b1::/64 echo
ipv6 access-list SPOLICY_IN deny ip any any
access-group SPOLICY_IN in interface outside

Kaikki ICMP6-pingit SimuNetin IPv6-osoitealueesta KOUVOLA-puolen sisäverkkoon sallittiin seuraavalla pääsylistalla KOUVOLA-puolen ASAan:

ipv6 access-list SPOLICY_IN permit icmp6 2a00:1dd0:100::/48
2a00:1dd0:100:00b2::/64 echo
ipv6 access-list SPOLICY_IN deny ip any any
access-group SPOLICY_IN in interface outside

ICMP-inspectioniä varten tehtiin oma class-map ja policy-map. Aluksi luotiin class-map nimellä icmp_class, joka määriteltiin vastaamaan oletus-inspection-liikennettä. Tämän jälkeen luotiin policy-map, joka nimettiin nimellä icmp_policy. Tähän policyyn lisättii luokka icmp_class ja lisättiin määritys *inspect icmp*. Lopuksi icmp_policy lisättiin outside-liityntäporttiin.

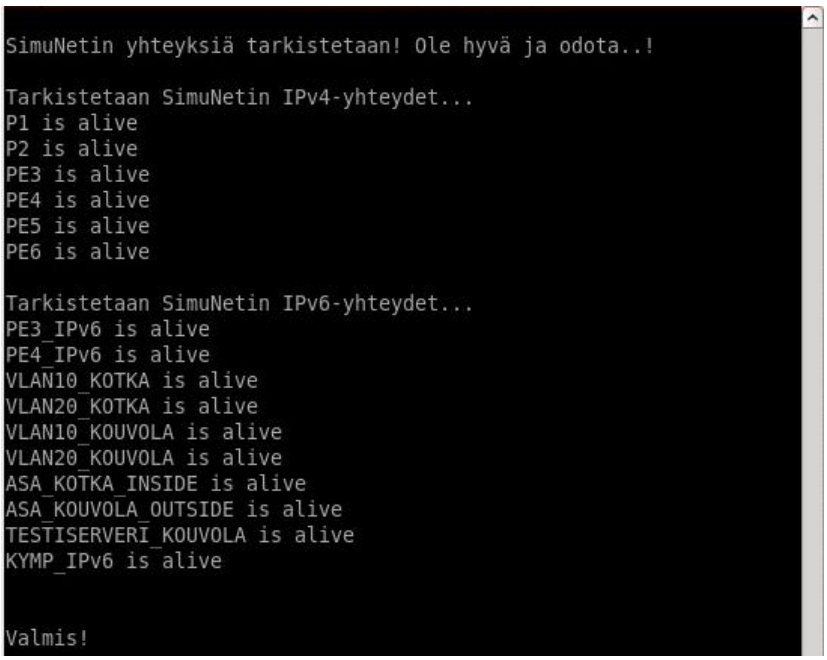
ICMP inspection lisättiin molempien puolien palomuureihin. ICMP inspection lisättiin KOTKA-puolen ASAan seuraavilla konfiguraatioilla:

ciscoasa/KOTKA(config)# class-map icmp_class
ciscoasa/KOTKA (config-cmap)# match default-inspection-traffic
ciscoasa/KOTKA (config-cmap)# exit
ciscoasa/KOTKA (config)# policy-map icmp_policy
ciscoasa/KOTKA (config-pmap)# class icmp_class
ciscoasa/KOTKA (config-pmap-c)# inspect icmp
ciscoasa/KOTKA (config-pmap-c)# exit
ciscoasa/KOTKA (config)# service-policy icmp_policy interface outside

```
class-map icmp_class
 match default-inspection-traffic
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map icmp_policy
 class icmp_class
  inspect icmp
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
service-policy icmp_policy interface outside
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
ciscoasa/KOTKA#
```

Kuva14. Show running-config, ICMP inspection

ICMP6-viestien testaus KOTKA-puolen testipalvelimelta onnistui FPING-scriptillä, joka näkyy kuvassa 15. FPING-scriptillä saatiin testattua kaikki SimuNetin IPv6-yhteydet. Scripti pingaa KOTKA-puolen testiserveriltä palomuurin läpi jokaista IPv6-osoitetta, jotka verkossa oli sillä hetkellä ja ilmoitti oliko laite hengissä eli vastasiko se ping-viestiin. FPING-scriptin tarkemmat tiedot löytyvät työn liitteestä 8. Cisco ASAn ICMP6-viestien käsittely saatiin todettua lisäämällä palomuurin konsoliin debug-käsky *debug icmp trace*, joka ilmoitti jokaisen ICMP6-viestin, joka saapui sen liityntäporttiin sekä minne viestit ohjattiin siitä eteenpäin.



Kuva15. SimuNetin ICMP6-viestien testaus

14.2 IPv6 WWW–palvelin

IPV6 WWW-palvelinta testattiin Linux-pohjalle asennetulla Apache-palvelimella, joka sijaitsi ensisijaisesti KOTKA-puolen serverifarmissa. Tarkoitus oli sijoittaa IPv6-testisivusto kyseiselle palvelimelle ja mennä sivuille julkisen IPv6-verkon läpi ja todeta vain, että sivut toimivat IPv6-osoitteilla.

Palvelimen asennus

Apache-palvelin asennettiin Linuxissa käskyllä *yum install apache*, jonka jälkeen palvelin pitää käynnistää käskyllä *service httpd start*. Apache loi Linuxiin automaattisesti testikansion mahdollisille nettisivuille polkuun */var/www/*. WWW-kansioon luotiin index.html–tiedosto käskyllä *touch index.html*, johon lisättiin haluttu sivujen sisältö käskyllä *nano index.html*, että saatiin sopiva testisivu näkyviin.

Tämän jälkeen muutettiin palvelimen IPv6-osoitteeksi 2a00:1dd0:100:00b1::200. Se tehtiin muokkaamalla ifcfg-eth0-tiedostoa käskyllä *nano /etc/sysconfig/network-scripts/ifcfg-eth0.* Palvelimen verkkokortti täytyi käynnistää uudelleen muutoksien mahdollistamiseksi käskyllä *service network restart*, jonka jälkeen palvelimessa oli IPv6-sivusto ja IPv6-osoite.

Pääsylistat ASAan WWW-palvelinta varten:

IPv6 ICMP6-viestit sallittiin mistä vain IPv6-Internetistä WWW-palvelimelle seuraavalla pääsylistalla:

ipv6 access-list SPOLICY_IN permit icmp6 any host 2a00:1dd0:100:00b1::200 echo

HTTPS ja WWW –protokollan yhteydet sallittiin mistä vain Internetistä WWW-palvelimelle seuraavilla käskyillä:

ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:00b1::200 eq https
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:00b1::200 eq www

pääsylistan määrittäminen outside-liityntäportista sisään tulevalle liikenteelle:

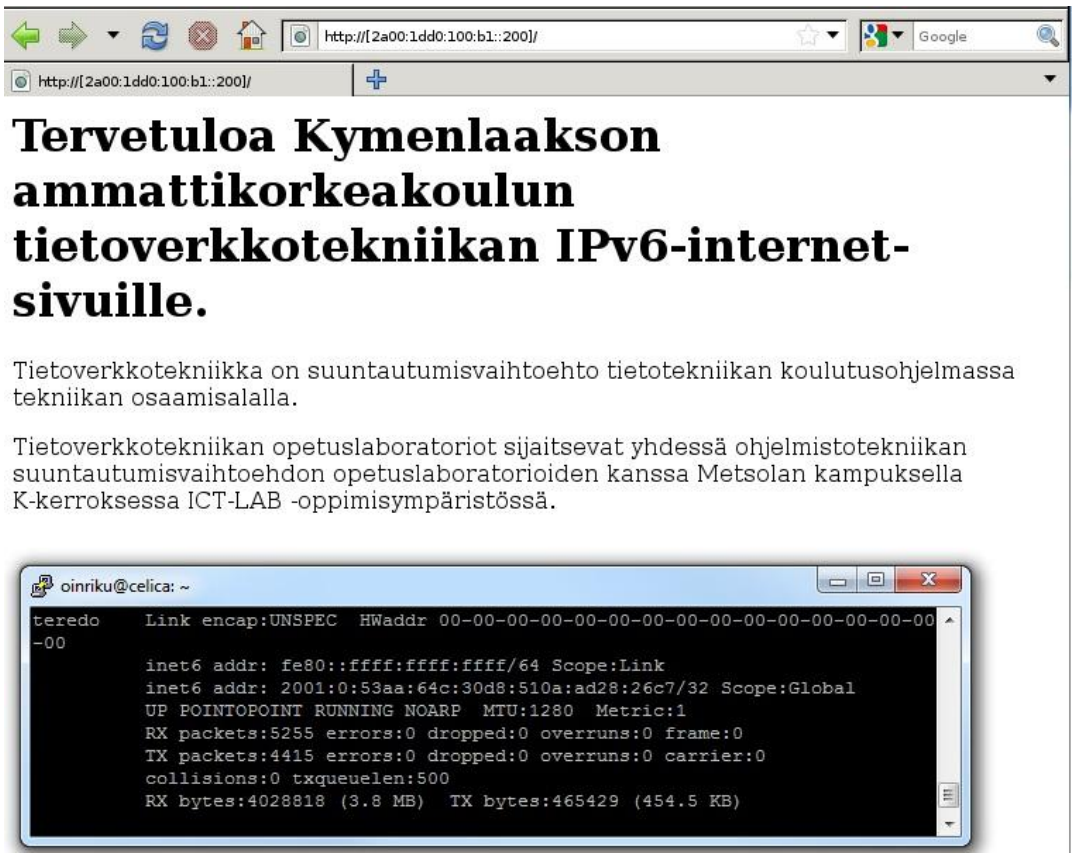
access-group SPOLICY_IN in interface outside

Yhteyden testaus

Sivuja testattiin aluksi syöttämällä palvelimen Mozilla Firefox-selaimeen osoite http://[::1], joka on palvelimen oma IPv6-loopback-osoite ja sivut avautuivat niin kuin pitikin. Yhteyden testaus julkisen IPv6-verkon kautta onnistui Teredo-tunnelointia käyttämällä, jolla päästiin tunneloidusti IPv4-verkon läpi microsoftin palvelimille, josta päästiin IPv6-internettiin. Teredo-tunneli käynnistettiin seuraavilla käskyillä Linux-ympäristössä, jossa se tunnetaan nimellä Miredo:

yum install miredo
etc/init.d/miredo start

Aluksi pingattiin WWW-palvelimen osoitetta onnistuneesti ja myös sivut avautuivat nettiselaimella osoitteella http://[2a00:1dd0:100:00b1::200], mikä oli palvelimen osoite KOTKA-puolen ASA:n takana sijaitsevassa 00b1-verkossa. Kuvassa 16 näkyy selaimella avattu IPv6-testisivu ja Teredo- tunnelin IP-osoite, jolla yhteys muodostettiin.



Kuva16. IPv6 WWW-palvelin

14.3 IPv6 FTP–palvelin

IPv6-FTP-palvelin asennettiin samaan palvelimeen kuin WWW-palvelin. Tarkoitus tässäkin kokeessa oli vain todeta FTP-palvelimen toimivuus julkisen IPv6-verkon ja ASAn läpi.

Palvelimen asennus

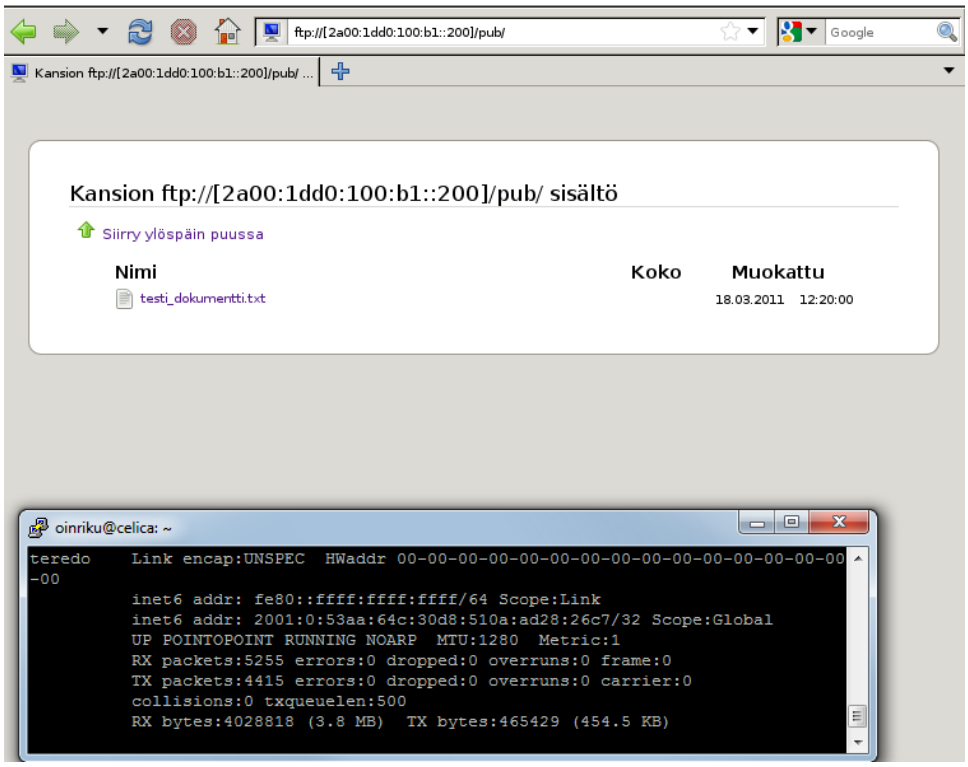
FTP-palvelimeksi valittiin vsftpd(Very Secure FTP)-palvelin, jonka konfiguraatioista piti poistaa IPv4-ominaisuudet ja vaihtaa tilalle IPv6-ominaisuudet, koska ne eivät toimineet tässä palvelimessa rinnakkain. Tällä ei ollut väliä tätä koetta tehdessä sillä tässä tapauksessa tarvittiin vain IPv6 FTP-palvelin.

Pääsylistat ASAaan FTP-palvelinta varten, jossa sallitaan FTP-yhteydet mistä vain Internetistä FTP-palvelimelle, olivat seuraavanlaiset:

ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:00b1::200 eq ftp
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:00b1::200 eq ftp-data
access-group SPOLICY_IN in interface outside

FTP-palvelimen testaus:

FTP-palvelinta testattiin Teredo-tunnelin avulla julkisesta IPv6-verkosta. FTP-palvelun toimivuus todettiin kirjoittamalla selaimeen osoitteen: ftp://[2a00:1dd0:100:00b1::200]. FTP-yhteyden toimivuus nähtiin myös palomuurin pääsylistojen osumien määristä(hit-count), joista näki, kuinka monta yhteyttä on vastannut pääsylistassa määriteltyä yhteyttä. Pääsylistat ja osumien määrät näkyvät työn liitteessä 7.



kuva17. FTP-palvelin

14.4 IPv6 SSH–hallintayhteys

SSH-yhteyttä käytetään usein laitteiden etähallintaan, minkä takia se on hyvä testata ASA-palomuureissa myös IPv6-osoitteilla. Käytännössä yhdistämiseen käytetään laitteen inside– tai outside-portin osoitetta, minkä jälkeen syötetään käyttäjä ja salasana. Kun käyttäjä ja salasana vastaavat palomuuriin määriteltyä käyttäjää, avautuu etähallintakoneelle palomuurin hallintakonsoli. IPv6 SSH-hallintayhteys lisättiin KOTKA-puolen Cisco ASA -palomuuriin.

ASA-palomuuriin lisättiin enable-salasana, joka jätettiin tässä tapauksessa tyhjäksi. Sen jälkeen luotiin käyttäjätunnus ja salasana, joita etäkäyttäjä käyttää SSH-

yhteydessä. AAA-todennukseksi valittiin SSH ja käyttäjiksi laitteen omat käyttäjätunnukset(LOCAL). Sitten avattiin SSH-yhteyksiä eri IPv6-osoitealueille ja samalla määriteltiin mihin porttiin ne avattiin. Tässä tapauksessa avattiin kaikille mahdollisille IPv6-osoitteille outside-portista ulospäin käskyllä *ssh ::/0 outside* ja KOTKA-puolen ASAn sisäverkon osoitteille inside-portin puolelle käskyllä *ssh 2a00:1dd0:100:00b1::/64 inside.* Outside-puolen IPv6 SSH-yhteydet tarvitsivat myös pääsylistan, jossa sallittiin kaikki SSH-yhteydet outside-porttiin. Lopuksi määriteltiin toimialueen nimi ja generoitiin RSA-avaimet, jotka SSH tarvitsee toimiakseen. Mitä suuremmaksi avainparit määrittää, sitä kauemmin niiden generoimiseen menee aikaa. Avainten kooksi valittiin suositeltu 1024-bittiä käskyllä *crypto key generate rsa modulus 1024*. Seuraavassa esimerkissä on kaikki tarvitut konfiguraatiot IPv6 SSH-yhteyden muodostamiseen.

enable password “enter”
*username asakotka password **********
aaa authentication ssh console LOCAL
ssh ::/0 outside
ssh 2a00:1dd0:100:00b1::/64 inside
domain-name CISCO.ORG
crypto key generate rsa modulus 1024
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:00a1::1 eq ssh
access-group SPOLICY_IN in interface outside

Yhteyden avaaminen päätekoneelta onnistui esimerkiksi inside-puolen verkosta Linux–käyttöjärjestelmällä kirjoittamalla konsoliin *ssh asakotka@2a00:1dd0:100:*00b1*::1* ja tämän jälkeen salasana. Windows-käyttöjärjestelmien kautta yhteyden testaus onnistui Putty-ohjelmalla, josta löytyi SSH-ominaisuus.

14.5 IPv6 ja ASDM

ASA-palomuurien hallintaan kokeiltiin myös web-pohjaista ASDM-hallintaohjelmaa. Ohjelmalla pystyi määrittämään eri ominaisuuksia vain muutamalla yksinkertaisilla vaiheilla, käyttämällä esimerkiksi erilaisia asennusvelhoja. IPv6-ominaisuuksia löytyi ainakin 6.2 versiota uudemmilla versioilla. Testissä käytettiin versiota 6.3(3) ja tämä versio tarvitsi ASAn käyttöjärjestelmäversion 8.2(3) toimiakseen.

ASDM–hallintayhteyden muodostaminen IPv6-osoitteilla

Muodostaakseen IPv6 ASDM-yhteyden täytyi System-konfiguraatiossa mennä admin-kontekstin asetuksiin ja lisätä sinne portti management0/0 ja avata se erikseen. Management-portti otettiin käyttöön admin-kontekstissa, mihin ASDM:ää käyttävä kone liitettiin ja sille lisättiin IPv6-osoite. Admin-kontekstiin avattiin myös HTTP-palvelin, johon määritettiin verkko mistä hallintayhteys muodostettaisiin. Verkko oli tässä tapauksessa testikäyttöön luotu 2a00:1dd0:100:ffff::/64. Hallintayhteys piti sallia system-kontekstiin erikseen IPv6-pääsylistalla, jossa sallittiin yhteydet tietystä verkosta management-portin osoitteeseen ja yhteyksien tyypeiksi valittiin WWW- ja HTTPS-protokollat, mitä ASDM voi käyttää. Lopuksi päätekoneelle piti antaa osoitteeksi jokin IPv6-osoite, mikä kuului samaan verkkoon kuin management-portti.

IPv6 ASDM-yhteyden muodostukseen tarvittavat konfiguraatiot:

System-context:

```
context admin
 allocate-interface Management0/0
!
interface Management0/0
no shutdown
```

Admin-context:

```
interface Management0/0
 nameif management
 ipv6 address  2a00:1dd0:100:ffff::1/64
 management-only
!
http server enable
http 2a00:1dd0:100:ffff::/64 management
```

Pääsylistat System-kontekstiin:

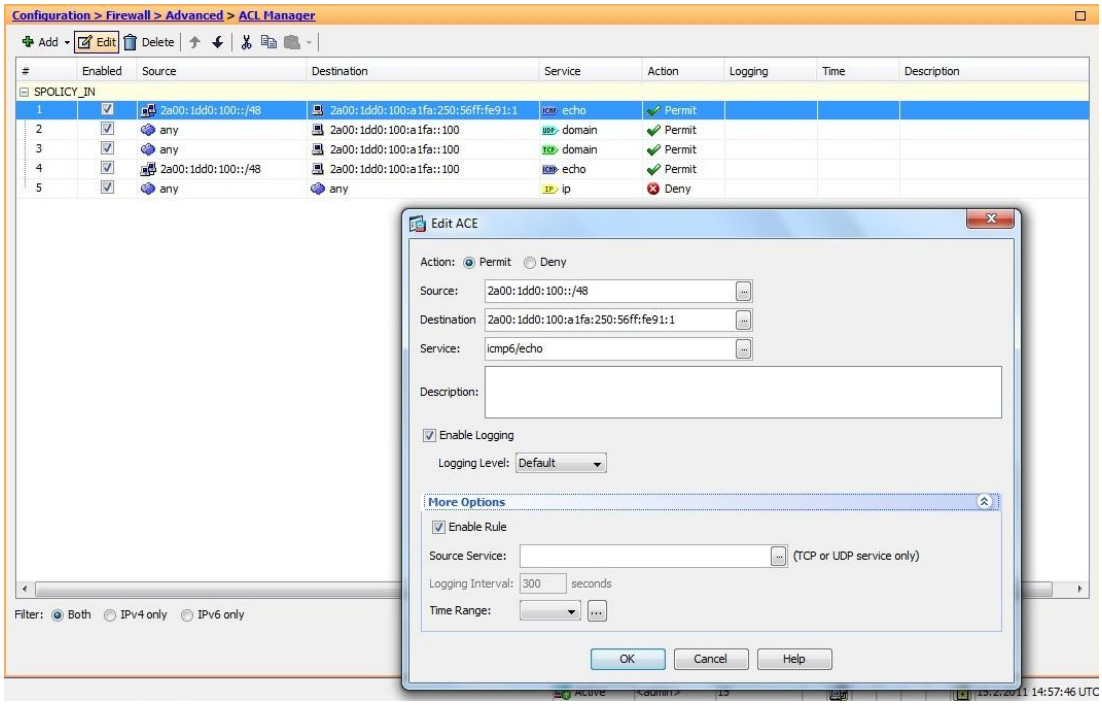
```
ipv6 access-list V6MGMT permit tcp 2a00:1dd0:100:ffff::/64 host
2a00:1dd0:100:ffff::1 eq www
ipv6 access-list V6MGMT permit tcp 2a00:1dd0:100:ffff::/64 host
2a00:1dd0:100:ffff::1 eq https
access-group V6MGMT in interface management
```

Käytettävän päätekoneen asetukset:

ipv6 address: 2a00:1dd0:100:ffff::2/64

ASDM:n IPv6-ominaisuuksien testaaminen

ASDM:n käynnistys onnistui selaimelta kirjoittamalla siihen management-portin IPv6-osoitteen muotoon: http://[2a00:1dd0:100:ffff::1]. ASDM 6.3(3) tuki lähestulkoon kaikkia IPv6-ominaisuuksia, lukuun ottamatta VPN-tunneleita, joihin 8.2–käyttöjärjestelmäversio ASAsta ei kyennyt. IPv6 VPN-ominaisuuksia esitetään lyhyesti ASDM:llä käytännönkokeiden VPN-osiossa.



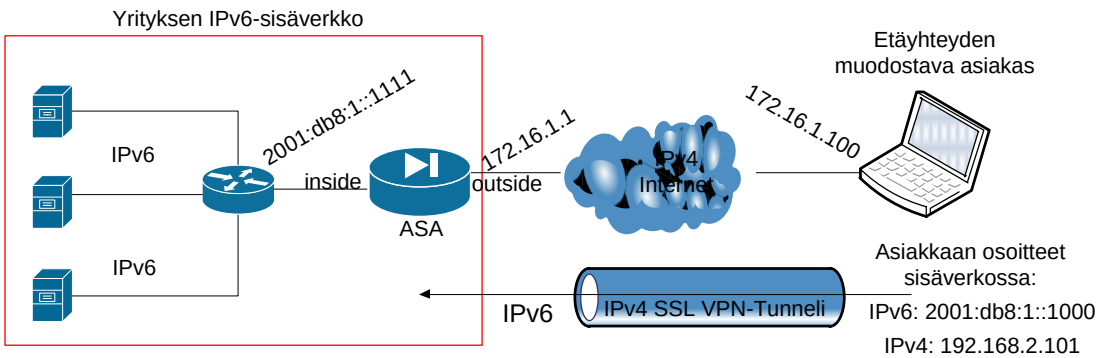
Kuva18. ASDM-IPv6 ACL

15 IPV6 JA VPN–TUNNELIT

Yksi tärkeä Cisco ASA palomuurien ominaisuus oli erilaisten VPN-tunneleiden muodostaminen, mitä myös testattiin tässä työssä IPv6-osoitteilla. Koska Cisco ASA -palomuurit eivät tukeneet minkäänlaisia VPN-tunneleita multi-context-tilassa, tarvittiin SimuNetin ulkoisia palomuureja. Ulkoisia palomuureja oli työtä tehdessä aluksi vapaana vain yksi eli kokeet oli aloitettava vain yhtä palomuuria käyttämällä. Palomuuriin asennettiin 8.2(3) versio, koska tässäkään palomuurissa ei ollut vielä tarvittavaa muistipäivitystä. 8.2(3) version kanssa yhteen sopivassa asdm-634-53-versiossa ei ollut tukea IPv6 VPN-tunneleille, niinpä tunnelit pitivät muodostaa tämän version kanssa konsolin kautta. Cisco ASAn uusin versiokaan (8.4) ei tukenut minkäänlaisia natiiveja remote-access-tunneleita IPv6-osoitteilla mutta tuki natiiveja LAN-to-LAN/Site-to-Site IPv6-tunneleita. Koska aluksi käytössä ei ollut kuin yksi ASA näiden tunneleiden muodostamiseen, niin ensimmäiseksi testattiin remote-access-tunneleita ja tässä vaiheessa oli käytössä versio 8.2(3). Remote-access-tunneleiden muodostamiseen täytyi käyttää IPv4 SSL VPN -tunnelia ja liikennöidä sen läpi IPv6-osoitteilla.

15.1 Remote-Access IPv6 SSL VPN-tunneli

IPv6 SSL VPN-tunnelin tarkoitus oli, että etäyhteyden muodostama asiakas-laite liikennöi IPv6-osoitteella IPv4-SSL- tunnelin läpi palomuurin takana olevaan IPv6-sisäverkkoon. IPv6-osoitteen asiakas saa palomuurilta, minkä palomuuri jakaa asiakkaalle tunnelin muodostamisen aikana. Asiakas pystyy käyttämään käytännössä yrityksen sisäverkon IPv6-palveluita ihan mistä vain IPv4-verkon yli. Kuvassa 19 näkyy tämän tunnelin testiympäristön topologia.



Kuva19. IPv6 SSL VPN

15.1.1 Tunnelin konfigurointi konsolilla

IPv6 SSL VPN -tunneli muodostettiin samaan tyyliin kuin IPv4 SSL VPN -tunnelikin. Käytännössä palomuuriin konfiguroitiin aluksi toimiva IPv4 SSL VPN -tunneli ja tämän jälkeen lisättiin vain IPv6 SSL VPN -tunnelin vaatimat lisäkonfiguraatiot.

IPv4 SSL VPN -tunneli saatiin toimimaan muutamia esimerkkikonfiguraatioita muokkaamalla, joista saatiin muokattua toimiva IPv4 SSL VPN testitarkoitukseen. Yksi hyvä lähde oli Mika Koskisen opinnäytetyö, jossa käsiteltiin IPv4 SSL VPN -asioita (Koskinen 2011.) IPv4 SSL VPN -tunnelin toimivuuden toteamisen jälkeen palomuuriin täytyi tehdä seuraavat toimenpiteet:

1. IPv6-osoitteen lisääminen inside-liityntäporttiin, josta etäyhteyden muodostava käyttäjä liikennöi IPv6-sisäverkkoon.

interface Ethernet0/1
nameif inside
***ipv6 address** 2001:db8:1::100/64*

2. IPv6-osoite-"pool":in luominen. Etäkäyttäjän saama IPv6-osoite tuli tästä osoitealueesta ja osoitteita jaettiin kymmenen kappaletta maksimissaan.

*ipv6 local pool **ipv6pool** 2001:db8:1::1000/64 10*

3. IPv6-poolin lisääminen tunnelointi-ryhmien asetuksiin

tunnel-group TestiVPN general-attributes
address-pool insidepool
*ipv6-address-pool **ipv6pool***

tunnel-group ipsecvpn general-attributes
address-pool insidepool
*ipv6-address-pool **ipv6pool***

4. IPv6 oletusreitin lisääminen inside-puolelle käyttäen komennon lopussa määritettä "tunneled", mikä tarkoittaa että kaikki vain tunnelista tuleva liikenne, mitä ei voida reitittää staattisilla tai automaattisesti opituilla reiteillä ohjataan tähän reittiin.

*ipv6 route inside ::/0 2001:db8:1::1111 **tunneled***

(Enabling IPv6 VPN Access, Cisco Networks 2011)
(Hogg 2008, 369-371)

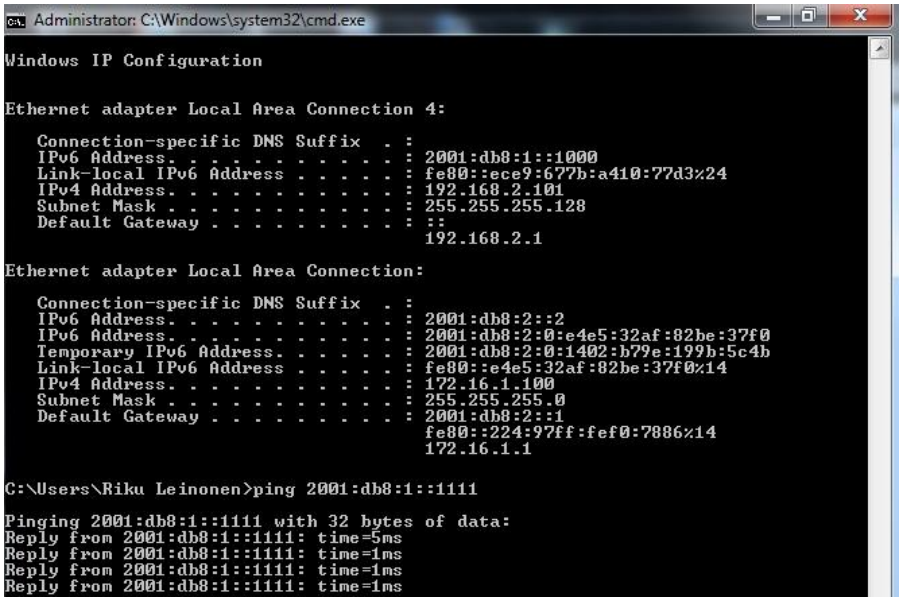
ASAn täydelliset tarvittavat konfiguraatiot löytyvät liitteestä 3.

15.1.2 Tunnelin testaus

IPv6 SSL VPN –tunneli teki IPv4-tunnelin, jota pitkin asiakas pystyi liikennöidä IPv6-osoitteilla yrityksen sisäverkkoon ja takaisin sille annetun IPv6-osoitteen kanssa. Asiakaskone sai tässä tapauksessa IPv6- sekä IPv4-osoitteen palomuurilta, johon oli luotu sekä IPv6- että IPv4-osoite-poolit.

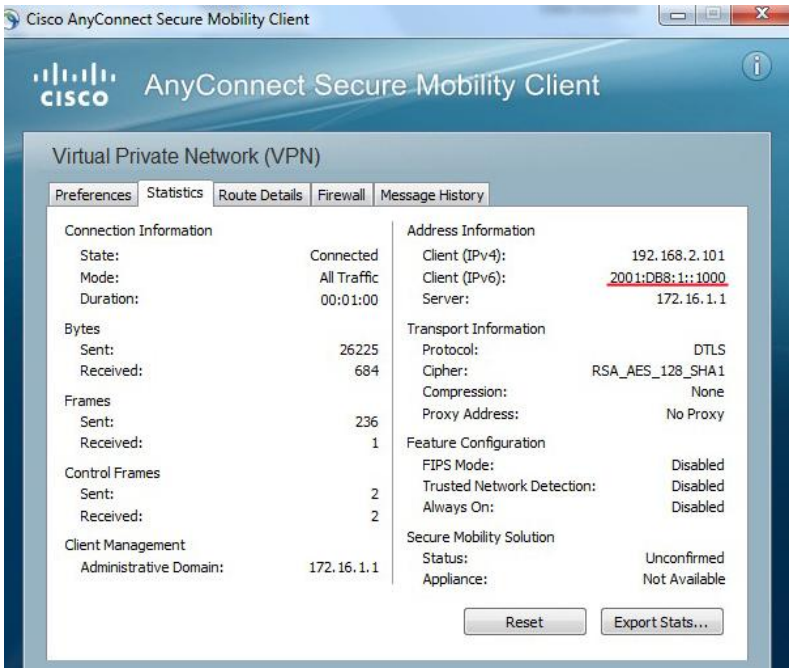
Cisco ASA:n uusin versio 8.4 ei tukenut natiivia IPv6 SSL VPN –tunneleita työtä tehdessä, joten tämä oli ainoa keino toteuttaa SSL–tunneli ja liikennöidä sitä pitkin IPv6-osoitteilla. Kun asiakas liikennöi IPv6-osoitteilla IPv4-tunnelia pitkin, niin samaan aikaan ei pystynyt pingaamaan palomuurin outside-portin IPv6-osoitetta. Kun tunneli suljettiin, niin tätä porttia pystyi taas pingaamaan. SSL VPN –hallintayhteyttä ei pystynyt muodostamaan IPv6-osoitteilla selaimen kautta eikä myöskään AnyConnect 3.0-asiakasohjelman kanssa.

Tunnelia testattiin pingaamalla etäyhteyden muodostaneella koneella tunnelin toisessa päässä olevaa IPv6-reititintä. Kuvan 20 ylemmät verkkosovittimen tiedot olivat tunnelin antamat IP-osoitteet ja oletusreitit. Alemmat olivat asiakaskoneen oman verkkosovittimen asetukset. IPv6-osoite 2001:db8:1::1111 oli tunnelin toisessa päässä sijaitsevan IPv6-reitittimen osoite, jota pingattiin onnistuneesti tunnelin läpi.



kuva20. IPv6-ping etäkäyttäjältä sisäverkkoon.

Kuvassa 21 näkyy, kuinka etäyhteyden muodostanut AnyConnect-asiakas saa IPv6-osoitteen, jolla se liikennöi SSL-tunnelin läpi IPv6-sisäverkkoon ja IPv4-osoite, jolla tunneli oli muodostettu (Administrative Domain).



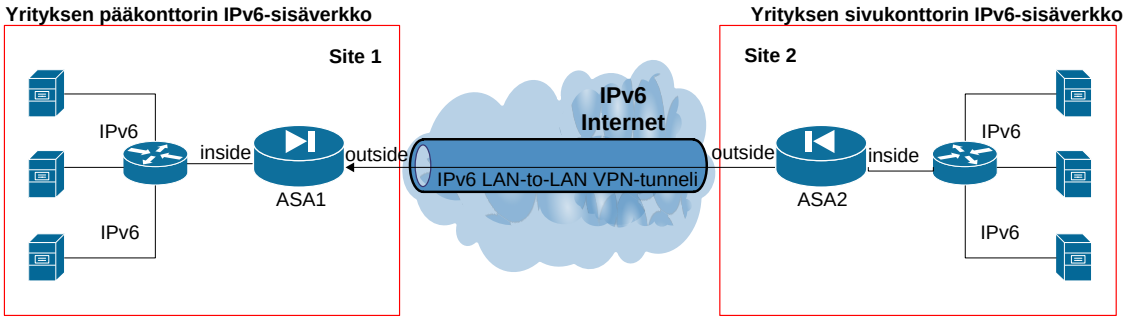
Kuva21. AnyConnect 3.0 Stats

Syöttämällä *Show vpn-sessiondb detail svc* –käskyn Cisco ASAn konsoliin, nähtiin testikäyttäjä remote, joka oli saanut IPv6-osoitteen tunnelin läpi ja siinä näkyi myös eri tunnelityypit, joissa IPv6-liikennöinti onnistui. Asiakasohjelmana näkyi AnyConnect Windows 3.0. Clientless-tunnelissa näkyi, että IPv6-osoitetta ei voitu käyttää tämän yhteyden muodostamiseen. Eli käytännössä web-pohjaista VPN-hallintayhteyttä ei voitu muodostaa IPv6-osoitteilla. Kuva *Show vpn-sessiondb detail svc* -käskystä löytyy liitteestä 6.

15.2 IPv6 LAN-to-LAN IPSec VPN-tunneli

Käytännön kokeissa kokeiltiin vain IPv6-osoitteita käyttävää IPv6 LAN-to-LAN tunnelia, jossa sisäverkotkin koostuivat IPv6-osoitteista. Koe tehtii uusimmalla Cisco ASA:n versiolla 8.4(1). Cisco ASA:n versio 8.4(1) täytyi päivittää laboratorioympärissä olevaan Cisco ASA 5510:aan kuten myös toiseen lainaksi saatuun Cisco ASA 5510:aan. Tämä tunneli muodostettiin näiden laitteiden välille ilman tarvittavaa lisämuistia, mikä ei rajoittanut laitteiden toimintaa niin että tunneleiden muodostus olisi ollut mahdotonta. Tunneliin konfiguroitiin mahdollisiksi

avaintenvaihtoprotokollaksi molemmat IKEv1 ja IKEv2, joista suojatumpaa IKEv2:sta käytettiin testatessa tunnelia.



Kuva22. LAN-to-LAN IPSec VPN topologia

Käytettävän topologian normaalien IP-yhteyksien toimivuus piti varmistaa ennen kuin itse tunnelia käytiin konfiguroimaan. Reitittimiin täytyi lisätä IPv6-oletusreitti ASA:n inside-puolen liityntäportin IPv6-osoitteeseen. Palomuureihin piti lisätä reitti haluttuun tunnelin toisen pään kohdeverkkoon, jossa next-hop-osoitteena käytettiin tunnelin toisen pään liityntäportin IPv6-osoitetta. Palomuureihin luotiin myös pääsylistat IPv6-pingeille, jotta yhteyksiä päästiin testaamaan päästä päähän pingaamalla ennen kuin itse tunnelia käytiin konfiguroimaan. Kun tunnelin molempien päiden reitittimet pingasivat toisiaan palomuurien läpi, niin sen jälkeen päästiin konfiguroimaan itse tunneli.

15.2.1 Tunnelin konfigurointi konsolilla

Seuraavissa vaiheissa esitetään, mitä konfiguraatioita IPv6 LAN-to-LAN VPN -tunnelin tekemiseen kuului molempien palomuurien osalta. IP-yhteyden muodostamiseen tarvittavat liityntäportit, reitit ja pääsylistat konfiguroitiin ASA-palomuureihin seuraavalla tavalla:

Site1 -puolen tunnelin muodostanut outside-portti sai osoitteen 2001:db8:100::**1**/64 ja sisäverkoksi määriteltiin 2001:a1fa:100::/64-verkko. Staattinen reitti luotiin Site2-puolen kohdeverkkoon osoittamalla tähän verkkoon menevälle liikenteelle next-hop-osoitteeksi 2001:db8:100::2, joka oli Site2-puolen outside-portti. Lopuksi luotiin pääsylistat icmp6-viesteille, että päästiin toteamaan yhteyden toimivuus.

ASA1:

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ipv6 address 2001:db8:100::1/64
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ipv6 address 2001:a1fa:100::1/64
!
ipv6 route outside 2001:be7a:100::/64 2001:db8:100::2
!
ipv6 access-list SPOLICY_IN permit icmp6 any any echo
ipv6 access-list SPOLICY_IN permit icmp6 any any echo-reply
access-group SPOLICY_IN in interface outside
```

Site2 -puolen tunnelin muodostanut outside-portti sai osoitteen 2001:db8:100::**2**/64 ja sisäverkoksi määriteltiin 2001:be7a:100::/64-verkko. Reititys tehtiin tunnelin toiselle puolelle kohdeverkkoon samalla tavalla kuin Site1-puolen ASA1:ssä. Tämän puolen pääsylistoissa sallittiin myös kaikki icmp6-viestit.

ASA2:

```
interface Ethernet0/0
 nameif outside
 security-level 0
ipv6 address 2001:db8:100::2/64
!
interface Ethernet0/1
 nameif inside
 security-level 100
ipv6 address 2001:be7a:100::1/64
!
ipv6 route outside 2001:a1fa:100::/64 2001:db8:100::1
!
ipv6 access-list SPOLICY_IN permit icmp6 any any echo
ipv6 access-list SPOLICY_IN permit icmp6 any any echo-reply
access-group SPOLICY_IN in interface outside
```

ISAKMP-policyn konfigurointi ja sen liittäminen outside porttiin (Molempiin ASA-palomuureihin samat konfiguraatiot):

IKEv1:ssä autentikointitavaksi valittiin jaettu avain, salaustavaksi 3des, HMAC-tavaksi SHA-1, Diffie-Hellman ryhmäksi group 2 ja salausavaimen voimassaoloaika 12 tunniksi.

IPsec IKEv1:

hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption 3des
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)# lifetime 43200
hostname(config)# crypto ikev1 outside

IKEv2:ssa salaustavaksi valittiin 3DES, Diffie-Hellman ryhmäksi group 2, PRF:ksi(Pseudo-random function) SHA-1 ja salausavaimen voimassaoloajaksi 12 tuntia.

IPsec IKEv2:

hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# encryption 3des
hostname(config-ikev2-policy)# group 2
hostname(config-ikev12-policy)# prf sha
hostname(config-ikev2-policy)# lifetime seconds 43200
hostname(config)# crypto ikev2 enable outside

IKEv1 transform set:in konfigurointi(Molempiin ASA-palomuureihin samat konfiguraatiot):

IKEv1:ssä yhdistetään salaus- ja todennustapa. Salaus- ja todennustapojen täytyivät olla samat kummassakin palomuurissa, että tunnelin sai muodostettua. FirstSet on transform-setin nimi tässä esimerkissä. Salaustapa oli esp-3des ja todennustapa esp-md5-hmac.

hostname(config)# crypto ipsec ikev1 transform-set FirstSet esp-3des esp-md5-hmac

IKEv2 Proposal-asetusten konfigurointi (Molempiin ASA-palomuureihin samat konfiguraatiot):

IKEv2:ssa pystyy ehdottamaan montaa salaus- ja todennustapaa samalla kertaa. ASA-palomuurit valitsevat sitten niistä parhaimman. Tässä esimerkissä IPsec-proposalin nimi oli secure. Protokolla oli ainoa valittavissa oleva ESP ja salaustavat olivat 3DES,AES ja DES. ESP:n integrity-tyypiksi valittiin SHA-1.

hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes des
hostname(config-ipsec-proposal)# protocol esp integrity sha-1

Pääsylistat sisäverkkojen välillä:

Kumpaakin ASA-palomuuriin täytyi lisätä pääsylistat, jotka määräsivät minkä verkon liikenne pääsi tunneliin. Kumpaakin ASA:an tuli pääsylistan lähdeverkoksi oma paikallinen sisäverkko ja kohdeosoitteeksi tunnelin toisessa päässä oleva kohdeverkko. Eli määriteltiin minkä verkkojen liikenne pääsee palomuurin outside-portista ulospäin, ei sisäänpäin.

ASA1:

ASA1(config)# ipv6 access-list l2l_list permit ip 2001:a1fa:100::/64 2001:be7a:100::/64

ASA2:

ASA2(config)# ipv6 access-list l2l_list permit ip 2001:be7a:100::/64 2001:a1fa:100::/64

Tunnel group -määritykset:

Tunnelointiryhmän asetuksiin täytyi lisätä tunnelin toisen pään IPv6-osoite ja tunnelin tyyppi, joita olivat esimerkiksi remote-access (IPsec, SSL ja clientless SSL remote access) tai ipsec-l2l (IPsec LAN to LAN). Tässä tapauksessa valittiin ipsec-l2l. Myös molempien tunneleiden jaetut avaimet täytyi määrittää tässä vaiheessa. Avaimien piti olla aivan samat molemmissa palomuureissa.

ASA1:

ASA1(config)# tunnel-group 2001:db8:100::2 type ipsec-l2l
ASA1(config)# tunnel-group 2001:db8:100::2 ipsec-attributes
*ASA1(config-tunnel-ipsec)# ikev1 pre-shared-key ******
*ASA1(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key ******
*ASA1(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key ******

ASA2:

ASA2(config)# tunnel-group 2001:db8:100::1 type ipsec-l2l
ASA2(config)# tunnel-group 2001:db8:100::1 ipsec-attributes
*ASA2(config-tunnel-ipsec)# ikev1 pre-shared-key ******
*ASA2(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key ******
*ASA2(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key ******

Crypto Map –määritykset:

Crypto map määrittää, mitä liikennettä IPsec suojelee, minne lähettää suojattu liikenne, mikä transform-set liittyy tähän liikenteeseen ja mihin liityntäporttiin luotu crypto map vaikuttaa. Tässä tapauksessa ASA1:n peer-osoite oli 2001:db8:100::2 ja ASA2:n 2001:db8:100::1. Crypto mapin liikenteeksi määriteltiin pääsylistan l2l_list liikenne. Transform-setiksi määriteltiin FirstSet, jossa määriteltiin jo IKEv1:ssä käytettävä salaus- ja todennustapa. IKEv2:n vastaavaksi proposaliksi lisättiin aikaisemmin luotu secure-proposal, johon oli määritelty monta eri käytettävää salaus- ja todennustapaa.

ASA1:

ASA1(config)# crypto map abcmap 1 match address l2l_list
ASA1(config)# crypto map abcmap 1 set peer 2001:db8:100::2
ASA1(config)# crypto map abcmap 1 set ikev1 transform-set FirstSet
ASA1(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
ASA1(config)# crypto map abcmap interface outside

ASA2:

ASA2(config)# crypto map abcmap 1 match address l2l_list
ASA2(config)# crypto map abcmap 1 set peer 2001:db8:100::1
ASA2(config)# crypto map abcmap 1 set ikev1 transform-set FirstSet
ASA2(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
ASA2(config)# crypto map abcmap interface outside

Täydelliset Cisco ASA IPv6 LAN-to-LAN IPSec VPN -konfiguraatiot löytyvät liitteistä 4-5. Konfigurointiohjeet löytyivät Cisco.com-sivustolta Cisco ASA 8.4-version konfiguraatio-oppaasta (Configuring LAN-to-LAN Ipsec VPNs, Cisco Networking 2011).

15.2.2 Tunnelin testaus konsolilla

IPv6 LAN-to-LAN VPN-tunneli aktivoidaan lähettämällä liikennettä määrätystä lähdeverkosta määrättyyn kohdeverkkoon. Liikenteeksi käy esimerkiksi IPv6-pingin testaus. Kun pingi kulki tunnelin läpi, pystyi IPv6-pingejä varten tehdyt pääsylistat poistaa kokonaan, jotka aluksi luotiin IP-yhteyden testaamista varten. Tämän jälkeen IPv6-pingien pitäisi kulkea suoraan tunnelin läpi ilman pääsylistoja.

```
Router#show ipv6 interface brief
FastEthernet0/0            [up/up]
    FE80::21E:13FF:FE75:89E4
    2001:A1FA:100::10
FastEthernet0/1            [administratively down/down]
    unassigned
Serial0/1/0                [administratively down/down]
    unassigned
Serial0/1/1                [administratively down/down]
    unassigned
Router#
Router#
Router#
Router#ping 2001:be7a:100::10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:BE7A:100::10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
Router#
```

kuva23. LAN-to-LAN IPv6-ping

Tunnelin toimivuutta pystyi myös testaamaan suoraan ASA:n konsoliriviltä. Käskyllä *show ipsec stats* nähtiin, kuinka monta IPsec-tunnelia oli aktiivisena sekä muita IPseciin liittyviä arvoja. Toinen tarkempi käsky suoraan IKEv2-tunneleiden ja sen arvojen näkemiseen oli show *crypto ikev2 stats*. Tällä nähtiin vain IKEv2-tunnelin arvoja ja oli tässä tapauksessa tarpeellinen, koska tunneli oli luotu IKEv2:lla. ASA-palomuurit valitsevat tunnelin luomiseen turvallisimman tavan mitä on käytettävissä ja tässä tapauksessa IKEv2 oli turvallisin.

Show crypto isakmp sa–käsky näytti sekä IKEv1- että IKEv2–tunnelit ja olivatko ne aktiivisia. Se näytti myös tunneleiden päiden peer-IPv6-osoitteet, paikallisen verkon ja kohdeverkon osoitteet sekä salaus ja todennustavat. *Show crypto ipsec sa*- käsky näytti myös lähde- ja kohdeverkot sekä pakettien määrät. Näistä havainnollistavin oli selvästi show crypto isakmp sa-käsky, josta esimerkki seuraavassa kuvassa 24.

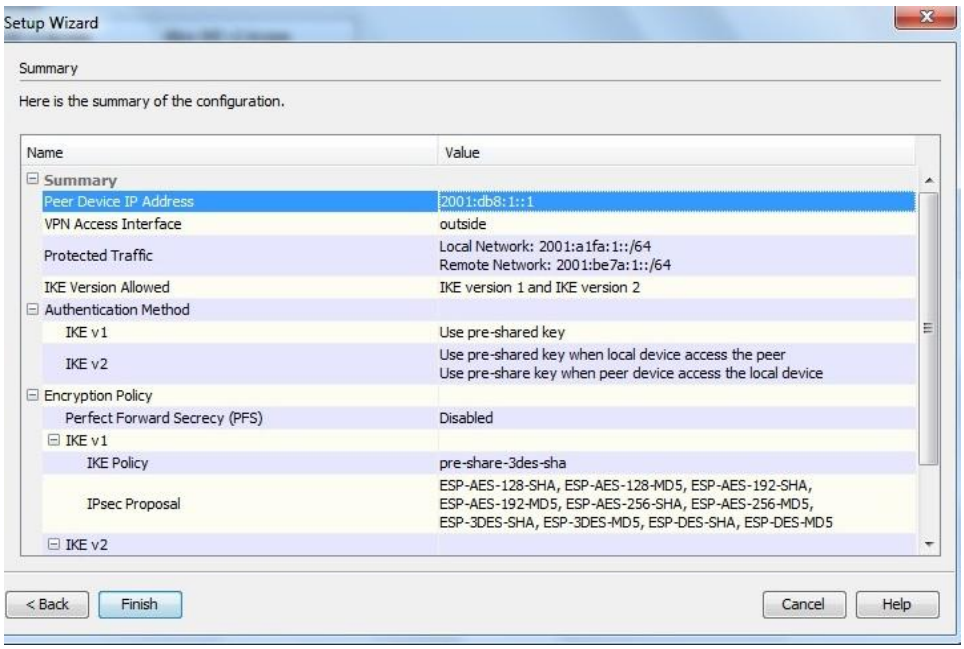
```
Site1# show crypto isakmp sa

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote     Status         Role
 38274043   2001:db8:100::1/500   2001:db8:100::2/500      READY    INITIATOR
      Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 43200/221 sec
Child sa: local selector  2001:a1fa:100::/0 - 2001:a1fa:100:0:ffff:ffff:ffff:ffff/65535
          remote selector 2001:be7a:100::/0 - 2001:be7a:100:0:ffff:ffff:ffff:ffff/65535
          ESP spi in/out: 0xcb1c7c66/0xf2f18175
Site1#
```

kuva24. show crypto isakmp sa

Tunnelin toimivuus tarkistettiin vielä ASDM 6.4(1):stä käyttämällä, jossa oli Monitor-tila. Monitor-tilassa pystyi tarkkailemaan luotuja tunneleita ja niiden eri tilastoja. Itse tunnelin luominen oli ASDM:llä nopeampaa, mutta vikojen paikantaminen sen luomasta konfiguraatiosta oli hitaampaa ja vaikeampaa.

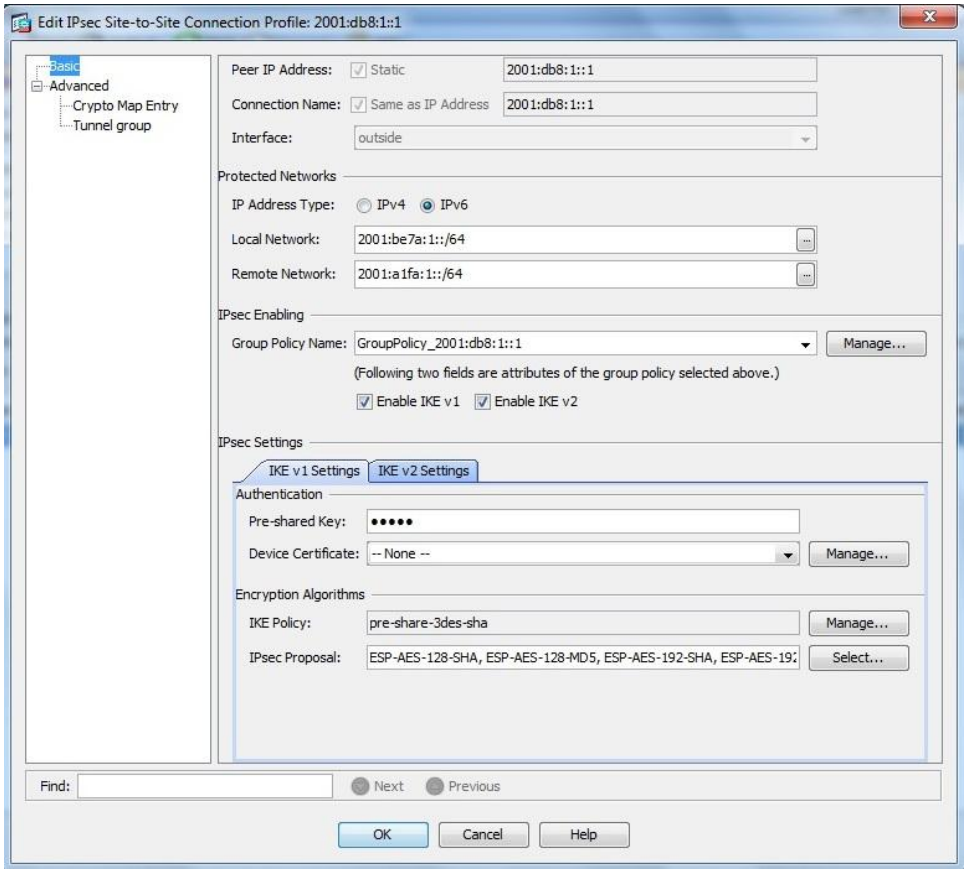
15.2.3 Tunnelin konfigurointi ASDM:llä

LAN-to-LAN VPN–tunnelin pystyi luomaan ASDM-version 6.4(1) tunnelointi-velhon avulla, missä oli vain kahdeksan eri vaihetta, joissa tunneli määriteltiin. Näissä vaiheissa määriteltiin käytännössä samat asiat kuin suoraan konsoliltakin. Vaiheet olivat Introduction, Peer Device Identification, IKE Version, Traffic to protect, Authentication Methods, Encryption Algorithms, Miscellaneous ja Summary. Summary-vaiheessa tunnelin kaikki määritykset näytettiin lyhyesti, josta näkyy esimerkki kuvassa 25.



Kuva25. LAN-to-LAN wizard

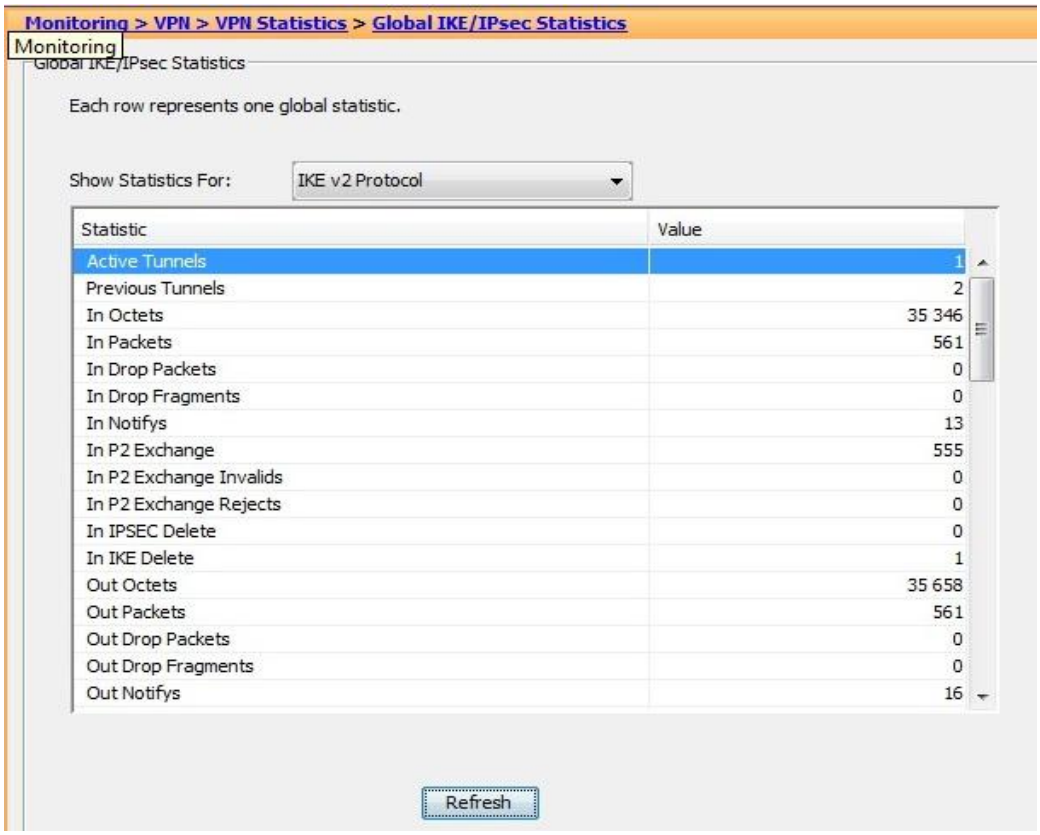
Kun tunneli oli luotuna, ilmestyi se yhteys-profiileihin ja sitä pystyi editoimaan vapaasti vielä jälkeenpäinkin helposti. Seuraavassa kuvassa 26 näkyy esimerkki LAN-to-LAN–tunnelin edit-ikkunasta.



Kuva26. ASDM LAN-to-LAN Edit

15.2.4 Tunnelin testaus ASDM:llä

Tunnelia pystyi tarkastelemaan ASDM:llä samalla tapaa kuin konsoliltakin, menemällä Monitorointi-tilaan ja sieltä VPN-osioon. Monitorointi-tilasta pystyi nähdä erityyppistä statistiikkaa luodusta tunnelista. Kuvassa 27 näkyy eri tilastoja IKEv2–protokollasta. Tilastoista pystyi päättelemään, että tunneli oli muodostunut ja paketteja oli kulkenut sen läpi.

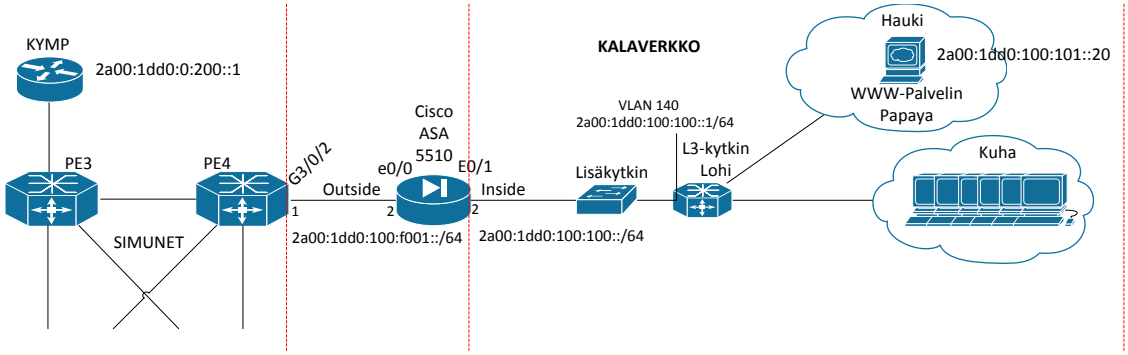


Kuva27. ASDM VPN Monitor

16 NATIIVI IPV6-PALOMUURI SIMUNETTIIN

Käytännön kokeiden loppupuolella saatiin yhteen SimuNetin ulkopuoliseen Cisco ASA 5510:aan 8.4-version vaatima muistilaajennus, jonka jälkeen päätettiin tehdä tästä palomuurista natiivi IPv6-palomuuri SimuNetin reunalle, joka yhdistäisi niin sanotut ensimmäiset asiakkaat IPv6-verkkoon. Tämä palomuuri suodattaisi vain IPv6-liikennettä ja sen taakse pistettäisiin myös ICTLAB-ympäristön IPv6-kotisivut osoitteella ipv6.ictlab.kyamk.fi. Sivut olisivat siis julkisessa IPv6-internetissä ja jäisivät aktiiviseen käyttöön. ICTLAB-ympäristön tuotantoverkon eli ns. Kalaverkon päätteet/asiakkaat jäisivät myös kiinni julkiseen IPv6-verkkoon ja pystyisivät liikennöimään IPv6-Internetissä.

Työssä tarvittiin Cisco ASA 5510-palomuuri, joka piti siirtää SimuNetin laitteiden kanssa samaan laitekaappiin ja linjat vedettiin sieltä viereiseen laitetilaan, jossa oli ICTLAB-ympäristön verkkoja yhdistävä multilayer-kytkin nimeltä Lohi. Asiakasverkko, joka oli tarkoitus liittää SimuNettiin, oli ns. Kalaverkko. Kalaverkossa sijaitsi muun muassa verkko nimeltä Kuha, jossa oli tietoverkkolaboratorion päätteet sekä Hauki-verkko, jossa sijaitsi WWW-palvelin nimeltä Papaya. Kokeen tavoitteena oli käytännössä saada asiakaskoneet pingaamaan esimerkiksi ipv6.google.com-sivuston osoitetta ja saada ICTLAB:in kotisivut auki esimerkiksi Teredo-tunnelin avulla julkisen IPv6-verkon kautta. Seuraavassa kuvassa 28 on tämän käytännön kokeen topologia ja käytetyt osoitteet.



Kuva28. Natiivi IPv6-palomuuri SimuNetissä topologia

16.1 Natiivin IPv6-palomuurin ja yhteyksien konfigurointi

Käytännönkoe aloitettiin avaamalla PE4-reunalaitteeseen uusi portti kyseiselle yhteydelle. Liityntäporttiin määriteltiin osoite 2a00:1dd0:100:f001::1/64, joka oli

palomuurin oletusreitissä määritelty next-hop-osoite. Palomuuri liitettiin PE4-laitteeseen konfiguroimalla ASA:an outside-portille IPv6-osoite 2a00:1dd0:100:f001::2/64 ja nimeämällä se outside-portiksi. Sitten tätä väliä testattiin pingaamalla, mikä onnistui. Sitten inside-portille lisättiin siitä lähtevän verkon osoite 2a00:1dd0:100:100::2/64, josta oli tarkoitus liikennöidä Lohi-kytkimeen luotuun uuteen VLAN 140:een, johon puolestaan luotiin virtuaalinen liityntäportti osoitteella 2a00:1dd0:100:100::1/64. Lohi-kytkimeen luotiin myös IPv6-oletusreitti, joka osoitti osoitteeseen 2a00:1dd0:100:100::2, joka oli palomuurin inside-puolen portti. Tässä vaiheessa ASA:an lisättiin pääsylistat pingeille outside-portista sisäänpäin ja tämän jälkeen sieltä voitiin pingata PE4-laitetta ja Lohi-kytkintä. Jotta ASA:sta saatiin IPv6-pingit läpi, piti siihen lisätä ICMP-incpection samalla tavalla kuin SimuNetin KOTKA- ja KOUVOLA-puolen palomuureihin. Tämän jälkeen Lohi-kytkin pingasi PE4-laitteelle ja takaisin.

Asiakaskoneelta pingattaessa pingit eivät lähteneet oikeaan osoitteeseen, koska Kuha-verkon eräs etäkäyttöpalvelin mainosti omaa IPv6-oletusreittiään ja koneille tarjottiin kahta IPv6-oletusreittiä samaan aikaan. Tämä saatiin estettyä poistamalla etäkäyttöpalvelimelta käsky *ipv6 unicast-routing*. Tämän jälkeen pingattaessa asiakaskoneelta PE4:sta pingi pysähtyi yllättäen ASA:n ja Lohi-kytkimen välillä takaisin päin tullessa. Tämä saatiin selvitettyä *debug icmp trace*-käskyllä ASA:ssa. ASA:an piti lisätä erillinen staattinen reitti, että paketit saatiin takaisin oikeaan verkkoon, vaikka tämä verkko lähti ASA:n inside-portista. Staattinen reitti tarvittiin inside-puolelle, koska ASA:n ja kohdeverkon välillä oli yksi multilayer-kytkin. ASA:n reititystaulussa näkyi jo kohdeverkko, joka lähti inside-portista, ja tämän takia aluksi oli mahdollista erehtyä että erillistä reittiä ei tarvinnut määrittää inside-puolelle lähtevälle liikenteelle.

Tämän jälkeen asiakaskoneet pingasivat PE4-laitteen porttia, mutta eivät siitä eteenpäin. PE4-reunalaitteen BGP-asetuksiin piti lisätä verkko 2a00:1dd0:100:00::/56, että uusien liitettyjen verkkojen reitit saatiin mainostettua toiselle puolelle SimuNettiä. Reitit täytyi siirtää BGP:tä käyttämällä, koska SimuNetin runko oli edelleen IPv4-protokollaa käyttävä ja tämä oli myös tarkoituksena. Tämän jälkeen PE4-laitteen reittien mainostukset toimivat ja liikenne kulki asiakaskoneelta KYMP Oy:n IPv6-liittymään ja siitä Internetiin. Lopuksi palomuuriin lisättiin pääsylista, joka salli kaiken IPv6 WWW-protokollan liikenteen Papaya-palvelimelle.

Laitteisiin lisätyt konfiguraatiot:

ASA 5510:

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ipv6 address 2a00:1dd0:100:f001::2/64
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ipv6 address 2a00:1dd0:100:100::2/64
!
ipv6 route inside 2a00:1dd0:100:100::/56 2a00:1dd0:100:100::1
ipv6 route outside ::/0 2a00:1dd0:100:f001::1
!
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:101::20 eq www
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:101::20 eq https
ipv6 access-list SPOLICY_IN permit icmp6 any any echo
ipv6 access-list SPOLICY_IN permit icmp6 any any echo-reply
ipv6 access-list SPOLICY_IN deny ip any any
access-group SPOLICY_IN in interface outside
!
class-map icmp_class
match default-inspection-traffic
policy-map icmp_policy
class icmp_class
inspect icmp
service-policy icmp_policy interface outside
```

PE4:

```
interface g3/0/2
ipv6 address 2a00:1dd0:f001::1/64
ipv6 enable
!
bgp 65001
address-family ipv6
network 2a00:1dd0:100:100::/56
```

Lohi-Multilayerkytkin:

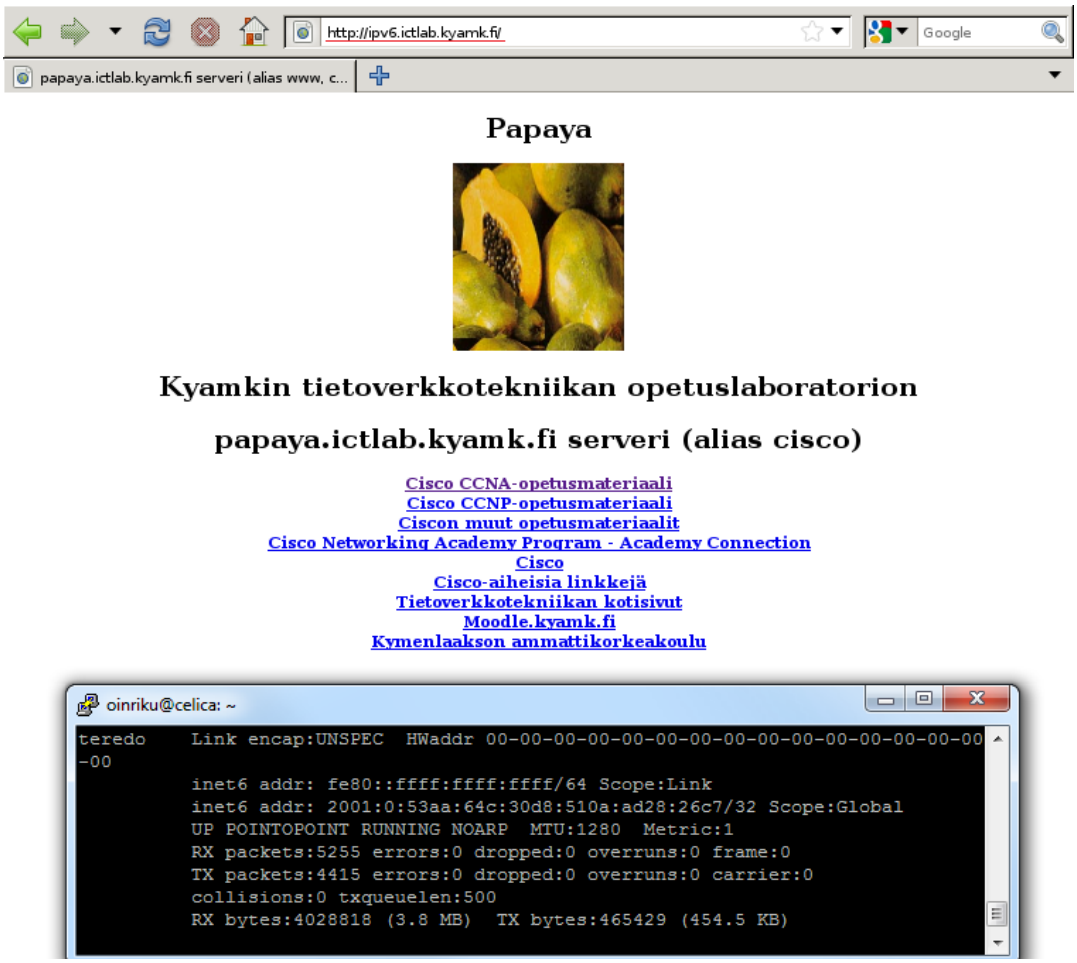
```
vlan 140
 name IPv6
!
interface Vlan140
 no ip address
 ipv6 address 2a00:1dd0:100:100::1/64
 ipv6 enable
!
ipv6 route ::/0 2a00:1dd0:100:100::2
```

Lisäkytkin:

vlan 140
name IPv6
!
interface fastethernet0/5
switchport access vlan 140

16.2 Natiivin IPv6-palomuurin ja yhteyksien testaus

Yhteyttä testattiin pingaamalla ipv6.google.comia onnistuneesti Kuha-verkon asiakaskoneelta ja tämän jälkeen avattiin ICTLAB-ympäristön IPv6-kotisivut Teredo-tunnelin avulla, mikä näkyy seuraavassa kuvassa 29.



Kuva29. ipv6.ictlab.kyamk.fi

17 YHTEENVETO

Tämän opinnäytetyön tarkoituksena oli testata eri IPv6-ominaisuuksia Cisco ASA 5510 –palomuureissa, ja tämä onnistui hyvin. Ensimmäisenä tavoitteena oli saada SimuNetin palomuurit toimimaan Dual-Stackina IPv6-osoitteiden kanssa, niin että IPv6-liikenne kulkisi SimuNetin eri serverifarmien välillä sekä myös IPv6-Internetiin, ja tämä saatiin aikaiseksi suhteellisen nopeasti. Aikaa meni tämän jälkeen enemmän eri yhteyksien testaamiseen erilaisilla palvelimilla ja nimenomaan tunneleiden kanssa, joihin tarvittiin erillisiä palomuureja SimuNetin ulkopuolelta. IPv6 LAN-to-LAN IPSec VPN-tunneleiden kanssa ei ollut varmuutta, toimisivatko nämä Cisco ASA 5510 järjestelmäversio 8.4 kanssa, jossa ei ollut tarvittavaa muistipäivitystä, mutta onneksi mitään ongelmia ei tähän liittyen tullut. Oikeassa käytössähän ei pystyisi luottamaan, että palomuurit toimisivat ilman suositeltavaa muistipäivitystä. Lopulta kun yksi muistipäivitys saatiin kokeisiin mukaan, ei sitä olisi voinut käyttää ainakaan tunneleihin, koska LAN-to-LAN-tunneliin olisi tarvittu kaksi muistipäivitystä ja natiivi IPv6 SSL VPN-tunneli oli muutenkin mahdoton toteuttaa. Käytännön kokeet onnistuivat tunneleiden osalta hyvin, mutta ne olisivat voineet olla jossakin monimutkaisemmassa ympäristössä, jotta niiden käyttö olisi ollut realistisempaa. SimuNetin alusta olisi sopinut tähän tarkoitukseen hyvin, mutta oli harmi, etteivät Cisco ASA:t tukeneet VPN-tunneleita multi-context-tilassa.

Natiivi IPv6-palomuuri oli todella hyödyllinen lisäys SimuNetille ja tämän yhteyden muodostaminen oli mielenkiintoista, koska siinä käytettiin vain IPv6-osoitteita ja se päätyi julkiseen IPv6-Internetiin. Palomuuriin ei tarvinnut lisätä montaa komentoa, mutta se oli SimuNetin ensimmäisiä laitteita, jotka toimivat natiivisesti IPv6-osoitteilla. Palomuuriin ei tehty eri konteksteja eli siihen voisi tulevaisuudessa yhdistää esimerkiksi tässä työssä toteutetun IPv6 LAN-to-LAN IPSec VPN-tunnelin jostain toiselta puolelta SimuNetiä.

Cisco ASA 5510 järjestelmäversio 8.2(3) toimi Dual-Stackina SimuNetissä hyvin perus-IPv6-liikenteen kanssa sekä suodatti liikennettä niin kuin pitikin. Yleisesti, jos Cisco ASA-palomuurin tehtäviin kuuluisi erilaisia IPv6-tunneleita tai esimerkiksi automaattisten reititysprotokollien käyttöä, eivät uusimmankaan käyttöjärjestelmäversion 8.4 ominaisuudet riittäisi siihen. Cisco ASA:n versio 8.4 toimisi hyvin IPv6-osoitteiden kanssa, jos palomuuri olisi esimerkiksi reitittimen

takana eli reititin hoitaisi reitityksen ja eri IPv6-tunnelit. Muuten ASA:n uudempia versioita täytyisi vielä odotella, että saataisiin IPv6-ominaisuudet kunnolla käyttöön Cisco ASA 5510 -palomuureissa.

18 LÄHTEET

Adding an Ipv6 Access List. Saatavissa: http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/acl_ipv6.html[viitattu 12.2.2011]

Configuring IPv6. Saatavissa: http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/ipv6.html[viitattu 23.2.2011]

Configuring LAN-to-LAN Ipsec VPNs. Saatavissa: http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/vpn_site2site.pdf[viitattu 20.3.2011]

Configuring VPN. Saatavissa: Configuring LAN-to-LAN Ipsec VPNs, Cisco Networks 2011)[viitattu 28.3.2011]

Ding Cunsheng. IKEv2: IPSec Key Management Protocol. Saatavissa: http://www.cs.ust.hk/faculty/cding/COMP685/SLIDES/slide23.pdf[viitattu: 4.4.2011]

Enabling IPv6 VPN Access. Saatavissa: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect23/administration/23admin3.html#wp1002258[viitattu 23.3.2011]

Hinden, R & Deering, S. 1998. IP Version 6 Addressing Architecture. IETF(Internet Engineering Task Force). Saatavissa: ftp://ftp.funet.fi/pub/standards/RFC/rfc2373.txt(viitattu 4.4.2011)

Hinden,R; Deering,S & Nordmark,E. 2003. IPv6 Global Unicast Address Format. Saatavissa: ftp://ftp.rfc-editor.org/in-notes/rfc3587.txt[viitattu 4.4.2011]

Hogg, S. & Vyncke, E. 2008. IPv6 Security. Indianapolis: Cisco Press.

IPSec. Saatavissa: http://en.wikipedia.org/wiki/IPsec[viitattu 3.3.2011]

IPv4. Saatavissa: http://en.wikipedia.org/wiki/IPv4[viitattu 3.1.2011]

IPv6. Saatavissa: http://en.wikipedia.org/wiki/IPv6[viitattu 4.4.2011]

IPv6 Basics. Saatavissa:
http://www.h3c.com/portal/Products___Solutions/Technology/IPv4___IPv6_Services/Technology_Introduction/200702/201238_57_0.htm[viitattu 4.4.2011]

IPv6 Packet Headers.Saatavissa:
http://www.juniper.net/techpubs/software/erx/erx50x/swconfig-routing-vol1/html/ipv6-config4.html[viitattu 4.4.2011]

Kaario, K. 2002. TCP/IP–verkot. Jyväskylä: Docendo.

Koskinen, M. 2011. Ohjelman etäkäyttö SSL VPN-yhteydellä. Opinnäytetyö. Kymenlaakson ammattikorkeakoulu.

Oinonen, R. 2011. MPLS L2VPN ja operaattoriverkon kahdennetut palvelut. Opinnäytetyö. Kymenlaakson ammattikorkeakoulu.

Riikonen, P. IKE Internet Key Exchange. Saatavissa:
http://xtrmntr.org/priikone/docs/ike.pdf[viitattu 4.4.2011]

Shalini Punithavathani, D. & Sankaranarayanan, K. 2009.IPv4/IPv6 Transition Mechanisms. European Journal of Scientific Research 1/2009, s.110-124. Saatavissa:
http://www.eurojournals.com/ejsr_34_1_12.pdf[viitattu 15.2.2011]

Suurnäkki,S. 2010. SimuNet 6PE Harjoitustyöraportti. Kymenlaakson ammattikorkeakoulu, tietotekniikka. Saatavissa:
http://papaya.ictlab.kyamk.fi/~amake/SimuNet/SimuNet_6PE.pdf[viitattu 4.4.2011]

TLS. Saatavissa: http://fi.wikipedia.org/wiki/TLS[viitattu 20.3.2011]

Cisco ASA 5510: Context-KOTKA konfiguraatiot (SimuNet):

```
ciscoasa/KOTKA# show run
:
ASA Version 8.2(3) <context>
!
hostname KOTKA
domain-name CISCO.ORG
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0.10
 nameif outside
 security-level 0
 ip address 172.30.1.1 255.255.255.248 standby 172.30.1.2
 ipv6 address 2a00:1dd0:100:a1::1/64
 ipv6 address fe80:a1::1 link-local
!
interface Ethernet0/0.100
 nameif inside
 security-level 100
 ip address 172.30.2.1 255.255.255.0 standby 172.30.2.2
 ipv6 address 2a00:1dd0:100:b1::1/64
 ipv6 address fe80:b1::1 link-local
!
dns server-group DefaultDNS
 domain-name CISCO.ORG
pager lines 24
mtu outside 1500
mtu inside 1500
ipv6 route outside ::/0 fe80::1
ipv6 access-list SPOLICY_IN permit icmp6 2a00:1dd0:100::/48 host
2a00:1dd0:100:b1::10 echo
ipv6 access-list SPOLICY_IN permit udp any host 2a00:1dd0:100:b1::100 eq domain
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:b1::100 eq domain
ipv6 access-list SPOLICY_IN permit icmp6 2a00:1dd0:100::/48 host
2a00:1dd0:100:b1::100 echo
ipv6 access-list SPOLICY_IN permit icmp6 2a00:1dd0:100::/48 host
2a00:1dd0:100:b1::200 echo
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:b1::200 eq https
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:b1::200 eq www
ipv6 access-list SPOLICY_IN permit icmp6 any host 2a00:1dd0:100:b1::200 echo
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:b1::200 eq ftp
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:b1::200 eq ftp-data
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:a1::1 eq ssh
ipv6 access-list SPOLICY_IN deny ip any any
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
```

Liite1 (2/2)

```
arp timeout 14400
access-group SPOLICY_IN in interface outside
route outside 0.0.0.0 0.0.0.0 172.30.1.5 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
aaa authentication ssh console LOCAL
no snmp-server location
no snmp-server contact
telnet timeout 5
ssh ::/0 outside
ssh 2a00:1dd0:100:b1::/64 inside
ssh timeout 5
no threat-detection statistics tcp-intercept
username asakotka password TfAcbC6FrjgnqiMH encrypted
!
class-map icmp_class
 match default-inspection-traffic
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map icmp_policy
 class icmp_class
  inspect icmp
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
service-policy icmp_policy interface outside
Cryptochecksum:87c9ddd219917b4cb553fd645177025c
: end
```

Cisco ASA 5510: Context-KOUVOLA konfiguraatiot (SimuNet):

ciscoasa/KOUVOLA# show run

ASA Version 8.2(3) <context>!

```
hostname KOUVOLA
domain-name CISCO.ORG
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0.20
 nameif outside
 security-level 0
 ip address 172.31.1.1 255.255.255.248 standby 172.31.1.2
 ipv6 address 2a00:1dd0:100:a2::1/64
 ipv6 address fe80:a2::1 link-local
!
interface Ethernet0/0.200
 nameif inside
 security-level 100
 ip address 172.31.2.1 255.255.255.0 standby 172.31.2.2
 ipv6 address 2a00:1dd0:100:b2::1/64
 ipv6 address fe80:b2::1 link-local
!
dns server-group DefaultDNS
 domain-name CISCO.ORG
pager lines 24
mtu outside 1500
mtu inside 1500
ipv6 route outside ::/0 fe80::2
ipv6 access-list SPOLICY_IN permit icmp6 2a00:1dd0:100::/48 host
2a00:1dd0:100:b2::10 echo
ipv6 access-list SPOLICY_IN permit icmp6 2a00:1dd0:100::/48 host
2a00:1dd0:100:b2::222 echo
ipv6 access-list SPOLICY_IN permit icmp6 any host 2a00:1dd0:100:b2::11 echo
ipv6 access-list SPOLICY_IN permit tcp any host 2a00:1dd0:100:a2::1 eq ssh
ipv6 access-list SPOLICY_IN deny ip any any
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
route outside 0.0.0.0 0.0.0.0 172.31.1.5 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
```

```
timeout tcp-proxy-reassembly 0:01:00
aaa authentication ssh console LOCAL
no snmp-server location
no snmp-server contact
telnet timeout 5
ssh ::/0 outside
ssh 2a00:1dd0:100:b2::/64 inside
ssh timeout 5
no threat-detection statistics tcp-intercept
username asakouvola password TfAcbC6FrjgnqiMH encrypted
!
class-map icmp-class
 match default-inspection-traffic
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map icmp_policy
 class icmp-class
  inspect icmp
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
service-policy icmp_policy interface outside
Cryptochecksum:2ebbd8f4ce9c24d2378331e829b9c50b
: end
ciscoasa/KOUVOLA#
```

Cisco ASA 5510: IPv6 SSL VPN & AnyConnect 3.0 konfiguraatiot (Laboratorioympäristö):

```
ciscoasa# show run
: Saved
:
ASA Version 8.2(3)
!
hostname ciscoasa
domain-name ciscoasa.com
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
 ipv6 address 2001:db8:2::1/64
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.2.1 255.255.255.0
 ipv6 address 2001:db8:1::100/64
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
boot system disk0:/asa823-k8.bin
ftp mode passive
clock timezone EEST 2
clock summer-time EEDT recurring last Sun Mar 3:00 last Sun Oct 4:00
dns domain-lookup outside
dns domain-lookup inside
dns domain-lookup management
dns server-group DefaultDNS
 domain-name ciscoasa.com
access-list inside_nat0_outbound extended permit ip host 192.168.2.2 192.168.2.0
255.255.255.0
access-list MGMT4 extended permit tcp 192.168.1.0 255.255.255.0 interface man-
agement eq https
access-list MGMT4 extended permit tcp 192.168.1.0 255.255.255.0 interface man-
agement eq www
pager lines 24
```

logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu management 1500
ip local pool insidepool 192.168.2.100-192.168.2.228 mask 255.255.255.128
ipv6 local pool ipv6pool 2001:db8:1::1000/64 10
ipv6 route inside ::/0 2001:db8:1::1111 tunneled
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-634-53.bin
no asdm history enable
arp timeout 14400
global (outside) 101 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 101 0.0.0.0 0.0.0.0
access-group MGMT4 in interface management
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.1.0 255.255.255.0 management
http 192.168.2.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set pfs
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP

```
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 enable outside
 svc image disk0:/anyconnect-win-3.0.0629-k9.pkg 1
 svc enable
 tunnel-group-list enable
 smart-tunnel list IPv6REMOTE IPv6REMOTE IPv6REMOTE.exe platform windows
group-policy remote internal
group-policy remote attributes
 vpn-tunnel-protocol svc webvpn
 group-lock value TestiVPN
 split-tunnel-policy tunnelall
 webvpn
  svc dtls enable
  svc keep-installer installed
  svc ask enable default svc timeout 15
  smart-tunnel auto-start IPv6REMOTE
  activex-relay enable
group-policy ipsecvpn internal
group-policy ipsecvpn attributes
 vpn-tunnel-protocol IPSec
 default-domain value ciscoasa.com
username remote password CxAh5EQ/8f4FVvNi encrypted privilege 0
username remote attributes
 vpn-group-policy remote
 vpn-tunnel-protocol svc webvpn
 group-lock value TestiVPN
 webvpn
  smart-tunnel auto-start IPv6REMOTE
  activex-relay enable
username remote2 password CxAh5EQ/8f4FVvNi encrypted privilege 0
username remote2 attributes
 vpn-group-policy ipsecvpn
```

```
vpn-tunnel-protocol IPSec
 group-lock value ipsecvpn
username MGMT4 password eYf/tWK5GF6Sv8L7 encrypted privilege 15
tunnel-group TestiVPN type remote-access
tunnel-group TestiVPN general-attributes
 address-pool insidepool
 ipv6-address-pool ipv6pool
 default-group-policy remote
tunnel-group TestiVPN webvpn-attributes
 group-alias IPv6REMOTE enable
tunnel-group ipsecvpn type remote-access
tunnel-group ipsecvpn general-attributes
 address-pool insidepool
 ipv6-address-pool ipv6pool
 default-group-policy ipsecvpn
tunnel-group ipsecvpn ipsec-attributes
 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
call-home
 profile CiscoTAC-1
  no active
```

destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:deadaf61d86ba35d415b1d4a2821e209

Cisco ASA 5510: IPv6 LAN-to-LAN VPN -tunnelin SITE1-konfiguraatiot (Laboratorioympäristö):

```
Site1# show run
: Saved
:
ASA Version 8.4(1)
!
hostname Site1
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 no ip address
 ipv6 address 2001:db8:100::1/64
!
interface Ethernet0/1
 nameif inside
 security-level 100
 no ip address
 ipv6 address 2001:a1fa:100::1/64
!
boot system disk0:/asa841-k8.bin
ftp mode passive
pager lines 24
mtu outside 1500
mtu inside 1500
ipv6 route outside 2001:be7a:100::/64 2001:db8:100::2
ipv6 access-list SPOLICY_IN permit icmp6 any any echo
ipv6 access-list SPOLICY_IN permit icmp6 any any echo-reply
ipv6 access-list l2l_list permit ip 2001:a1fa:100::/64 2001:be7a:100::/64
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

```
crypto ipsec ikev1 transform-set FirstSet esp-3des esp-md5-hmac
crypto ipsec ikev2 ipsec-proposal secure
 protocol esp encryption aes 3des des
 protocol esp integrity sha-1
crypto map abcmap 1 match address l2l_list
crypto map abcmap 1 set peer 2001:db8:100::2
crypto map abcmap 1 set ikev1 transform-set FirstSet
crypto map abcmap 1 set ikev2 ipsec-proposal secure
crypto map abcmap interface outside
crypto ikev2 policy 1
 encryption 3des
 integrity sha
 group 2
 prf sha
 lifetime seconds 43200
crypto ikev2 enable outside
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 43200
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
tunnel-group 2001:db8:100::2 type ipsec-l2l
tunnel-group 2001:db8:100::2 ipsec-attributes
 ikev1 pre-shared-key *****
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
```

```
 inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
call-home
 profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:5f91397d6208ff259fe43a4a6c1eae05
: end
```

Cisco ASA 5510: IPv6 LAN-to-LAN VPN -tunnelin SITE2-konfiguraatiot (laboratorioympäristö):

```
Site2# show run
: Saved
:
ASA Version 8.4(1)
!
hostname Site2
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 no ip address
 ipv6 address 2001:db8:100::2/64
!
interface Ethernet0/1
 nameif inside
 security-level 100
 no ip address
 ipv6 address 2001:be7a:100::1/64
!
boot system disk0:/asa841-k8.bin
ftp mode passive
pager lines 24
mtu outside 1500
mtu inside 1500
ipv6 route outside 2001:a1fa:100::/64 2001:db8:100::1
ipv6 access-list SPOLICY_IN permit icmp6 any any echo
ipv6 access-list SPOLICY_IN permit icmp6 any any echo-reply
ipv6 access-list l2l_list permit ip 2001:be7a:100::/64 2001:a1fa:100::/64
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

```
crypto ipsec ikev1 transform-set FirstSet esp-3des esp-md5-hmac
crypto ipsec ikev2 ipsec-proposal secure
 protocol esp encryption aes 3des des
 protocol esp integrity sha-1
crypto map abcmap 1 match address l2l_list
crypto map abcmap 1 set peer 2001:db8:100::1
crypto map abcmap 1 set ikev1 transform-set FirstSet
crypto map abcmap 1 set ikev2 ipsec-proposal secure
crypto map abcmap interface outside
crypto ikev2 policy 1
 encryption 3des
 integrity sha
 group 2
 prf sha
 lifetime seconds 43200
crypto ikev2 enable outside
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 43200
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
tunnel-group 2001:db8:100::1 type ipsec-l2l
tunnel-group 2001:db8:100::1 ipsec-attributes
 ikev1 pre-shared-key *****
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
```

```
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
call-home
 profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

Liite 6

Show VPN-Sessiondb detail svc:

```
ciscoasa# show vpn-sessiondb detail svc

Session Type: SVC Detailed

Username     : remote                 Index        : 12
Assigned IP  : 192.168.2.101          Public IP    : 172.16.1.100
Assigned IPv6: 2001:db8:1::1000
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : SSL VPN
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 12743                  Bytes Rx     : 59175
Pkts Tx      : 15                     Pkts Rx      : 576
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : remote                 Tunnel Group : TestiVPN
Login Time   : 07:52:39 EEST Thu Mar 3 2011
Duration     : 0h:06m:01s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

Clientless Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

Clientless:
  Tunnel ID    : 12.1
  Public IP    : 172.16.1.100
  Encryption   : RC4                    Hashing      : SHA1
  Encapsulation: SSLv3                  TCP Dst Port : 443
  Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 25 Minutes
  Client Type  : Web Browser
  Client Ver   : AnyConnect Windows 3.0.0629
  Bytes Tx     : 12051                  Bytes Rx     : 3025

SSL-Tunnel:
  Tunnel ID    : 12.2
  Assigned IP  : 192.168.2.101          Public IP    : 172.16.1.100
  Assigned IPv6: 2001:db8:1::1000
  Encryption   : RC4                    Hashing      : SHA1
  Encapsulation: TLSv1.0                TCP Src Port : 51569
  TCP Dst Port : 443                    Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 25 Minutes
  Client Type  : SSL VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.0.0629
  Bytes Tx     : 692                    Bytes Rx     : 2712
  Pkts Tx      : 1                      Pkts Rx      : 23
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0

DTLS-Tunnel:
  Tunnel ID    : 12.3
  Assigned IP  : 192.168.2.101          Public IP    : 172.16.1.100
  Assigned IPv6: 2001:db8:1::1000
  Encryption   : AES128                 Hashing      : SHA1
  Encapsulation: DTLSv1.0               UDP Src Port : 62800
  UDP Dst Port : 443                    Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client Type  : DTLS VPN Client
  Client Ver   : AnyConnect Windows 3.0.0629
  Bytes Tx     : 0                      Bytes Rx     : 53438
  Pkts Tx      : 0                      Pkts Rx      : 547
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
```

Liite 7

Show ipv6 access-list (KOTKA, SimuNet):

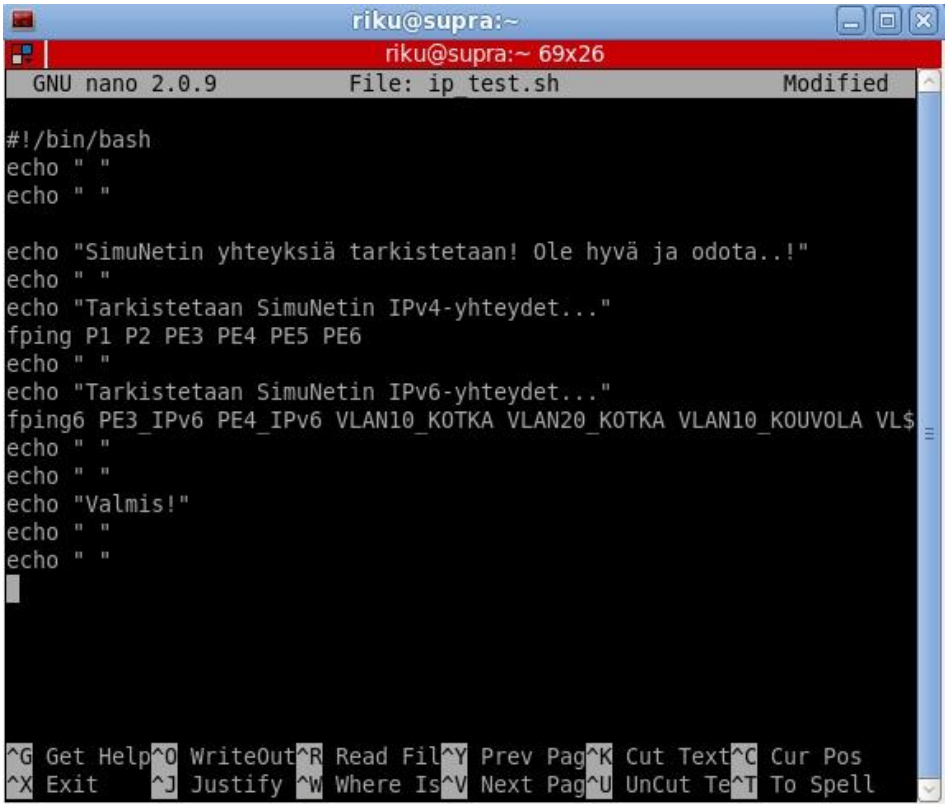
```
ciscoasa/KOTKA# show  ipv6 access-list
ipv6 access-list SPOLICY_IN; 12 elements; name hash: 0x6e154794
ipv6 access-list SPOLICY_IN line 1 permit icmp6 2a00:1dd0:100::/48 host 2a00:1dd0:100:b1::10 echo (hitcnt=0) 0xa62d8cee
ipv6 access-list SPOLICY_IN line 2 permit udp any host 2a00:1dd0:100:b1::100 eq domain (hitcnt=0) 0xce338666
ipv6 access-list SPOLICY_IN line 3 permit tcp any host 2a00:1dd0:100:b1::100 eq domain (hitcnt=0) 0xf695e354
ipv6 access-list SPOLICY_IN line 4 permit icmp6 2a00:1dd0:100::/48 host 2a00:1dd0:100:b1::100 echo (hitcnt=0) 0xc7f11b89
ipv6 access-list SPOLICY_IN line 5 permit icmp6 2a00:1dd0:100::/48 host 2a00:1dd0:100:b1::200 echo (hitcnt=0) 0x8cf7f962
ipv6 access-list SPOLICY_IN line 6 permit tcp any host 2a00:1dd0:100:b1::200 eq https (hitcnt=3) 0x30c9305b
ipv6 access-list SPOLICY_IN line 7 permit tcp any host 2a00:1dd0:100:b1::200 eq www (hitcnt=3) 0x55179957
ipv6 access-list SPOLICY_IN line 8 permit icmp6 any host 2a00:1dd0:100:b1::200 echo (hitcnt=13) 0x50ef8076
ipv6 access-list SPOLICY_IN line 9 permit tcp any host 2a00:1dd0:100:b1::200 eq ftp (hitcnt=1) 0xa41be1c6
ipv6 access-list SPOLICY_IN line 10 permit tcp any host 2a00:1dd0:100:b1::200 eq ftp-data (hitcnt=0) 0x3e82f41e
ipv6 access-list SPOLICY_IN line 11 permit tcp any host 2a00:1dd0:100:a1::1 eq ssh (hitcnt=0) 0xd15ae3e4
ipv6 access-list SPOLICY_IN line 12 deny ip any any (hitcnt=158) 0x448cb0c6
ciscoasa/KOTKA#
```

Show ipv6 access-list (ASA - natiivi IPv6, SimuNet):

```
ciscoasa# show ipv6 access-list
ipv6 access-list SPOLICY_IN; 7 elements; name hash: 0x6e154794
ipv6 access-list SPOLICY_IN line 1 permit tcp any host 2a00:1dd0:100:101::20 eq www (hitcnt=5) 0xa8f27f5d
ipv6 access-list SPOLICY_IN line 2 permit icmp6 any any echo (hitcnt=69) 0x3ea7f204
ipv6 access-list SPOLICY_IN line 3 permit icmp6 any any echo-reply (hitcnt=0) 0x30b93096
ipv6 access-list SPOLICY_IN line 4 permit tcp any host 2a00:1dd0:100:101::20 eq https (hitcnt=0) 0xa9b2b7d5
ipv6 access-list SPOLICY_IN line 5 permit tcp any host 2a00:1dd0:100:f001::2 eq ssh (hitcnt=0) 0xf7b28d25
ipv6 access-list SPOLICY_IN line 6 permit udp any any eq domain (hitcnt=0) 0x245322c2
ipv6 access-list SPOLICY_IN line 7 permit ip host 2a00:1dd0:100:c1:250:56ff:fe91:b any (hitcnt=70) 0xd85bf8bc
ciscoasa#
```

Liite 8

ICMP6-testi script:



ICMP6-testin tarvitsemien host-nimien määritys: