Opinnäytetyö (AMK)

Tietotekniikan koulutusohjelma

Tietoliikenne ja sähköinen kauppa

2011

Tero Greijus

PK-YRITYKSEN TIETOVERKON ASTEITTAINEN PÄIVITYS

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ
Turun ammattikorkeakoulu
Tietotekniikka | Ohjelmistotuotanto
Joulukuu 2011 | 41 sivua
Ohjaaja Lehtori Tiina Ferm

Tero Greijus

PK-YRITYKSEN TIETOVERKON ASTEITTAINEN PÄIVITYS

Tässä opinnäytetyössä käydään läpi TCP/IP-verkossa oleva nykyinen laitteiden osoittaminen eli tunnistus sekä lähiverkkojen yhdistäminen eri toimipisteiden välillä virtuaalisesti, ei kiinteästi yhdistäen välimatkasta johtuen. Sen jälkeen kuvataan teoriassa siirtyminen uuteen laiteosoitemenetelmään.

Opinnäytetyön toimeksiantajana toimi Trivore Oy jolla on kiinnostus siirtyä IPv6-tekniikkaan nykyisin yleisestä ja hallitsevasta IPv4-tunnuksista. Suurin työmäärä muodostui virtuaalisista yhteyksistä toimipaikkojen välillä. Käytössä on tunnelointi eli yhdyskäytävät. Kunkin toimipaikan, nykyisten ja tulevien, operaattorit eli yhdysliikenteen toimittajat ovat erit. Työtä vaikeutti se, että verkko on tuotantokäytössä ja lisäksi siinä on kiinni asiakkaita. Heitä koskee myös vaitiolovelvollisuus ja asiakassopimukset, joten verkon laitteisiin ei voinut kajota.

Lähtötiedot kuitenkin annettiin ja tärkein tieto oli se, että käytössä on Cisco ASA 5505 – palomuurilaitteisto eli laitepohjaisesti toteutettu verkon suojaus. Tunnelointina on IPSec ja asiakkaille on SSL VPN -yhteydet. Nykyiset operaattorit ovat Turussa Sonera ja Helsingissä Elisa.

Opinnäytetyöstä muodostui teoreettinen selvitystyö ja siinä kerrotaan, mitä IPv6 tuo mukanaan ja miten tunnelointi muuttuu jos muuttuu. Pyrkimys on asteittaiseen siirtymiseen.

Ratkaisuehdotuksessa pitäydytään vielä Dual Stack –menetelmässä eli käytetään IPv4/IPv6-kaksoispinoa. Laitteen kapasiteetti saattaa muodostua ongelmaksi, mutta liikenteen hyvin suunnitellulla suodatuksella saatetaan välttää järjestelmän hidastuminen. Siirtyminen järeämpiin laitteisiin ylimenokaudella olisi suotavaa. Kun varsinainen käyttöönotto aikanaan tapahtuu, täytyy miettiä tietoturvan kannalta monimutkaisuuden välttämistä ja hallintaa.

ASIASANAT:

IPv6, palomuuri, Dual Stack, Cisco ASA, VPN, tunnelointi, IPSec

BACHELOR'S THESIS | ABSTRACT
TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology | Software Engineering

December 2011 | 41 pages

Instructor lecturer Tiina Ferm

Tero Greijus

GRADUAL UPGRADING OF NETWORK IN THE SME

This thesis looks into the actual addressing i.e. identification mechanism of the hardware in the TCP/IP network and virtual network connections (VPN) between offices. After that the transition into new technology is described in theory.

The commissioner was Tivore Oy who is interested in changing the current IPv4 technology into advanced IPv6 world. The major task was to handle with the virtual connections between offices using tunnelling, so called gateways. The operators in every local office are different. The work was complex due to usage of the network and installed customers. Also Trivore Oy is involved in confidentiality and customer contracts.

As input the company uses Cisco ASA 5505 firewalls i.e. network security is hardware based. The tunneling method is IPSec and for customers there are SSL connections. Actual operators are Sonera in Turku and Elisa in Helsinki.

The thesis is theoretical survey describing what IPv6 includes and how tunnelling method will eventually change it. The target is gradual improvement.

The conclusions show that IPv4/IPv6 Dual Stack should remain. The capacity, i.e. throughput of the data stream can then be a problem. After building a good filtering with accessing lists the system slowdown be avoided. Changing the firewall appliances into next generation even during the changeover period is suggested. When the final introduction is actual, the IT staff should think how to avoid the complex network and how to reach proper management due to network policy

KEYWORDS:

IPv6, firewall, Dual Stack, Cisco ASA, VPN, tunneling, IPSec

KUVAT

KÄYTETYT LYHENTEET

IPv4	Internet-protokolla, osoiteluokkia yli neljä miljardia
IPv6	IPV4:ää seurannut uusi versio. osoitteita tulee olemaan käytössä 2^{128}
TCP/IP	Transmission Control Protocol/Internet Protocol: tietosähkeiden valvontaan ja lähetykseen sekä vastaanottajan tunnistukseen tarkoitetut protokollat eli tietoliikennekurit
RFC	Request For Comments: dokumenttisarja, joka sisältää TCP/IP-prokollasta kaiken mahdollisen standardisoidun tiedon (määrityksiä, mittauksia, ehdotuksia, hyväksymisiä)
unicast	täsmälähetys eli viesti lähtee yhdelle kohteelle
multicast	ryhmälähetys, yhdeltä monelle
anycast	viestin lähetys ryhmälle, mutta vain yksi valitsee sen
globaali osoite	julkinen IP-osoite
link-local osoite	laitteen omaan käyttöön tarkoitettu osoite, ei ulkoverkkoon
OSI-malli	teoreettinen kerrosmalli, miten tietosähkettä käsitellään
broadcast osoite	yleislähetys (ei enää käytössä IPv6:ssa)
DHCP	Dynamic Host Control Protocol: IP-osoitteen välitysjärjestelmä verkkoon kykeytyville
NAT	Network Address Translation: osoitemuunnos tietosähkeen tullessa sisäverkkoon tai sieltä internetiin lähtiessä
CIDR	Classless Inter-Domain Routing: reititystapa
autoconfiguration,	autokonfiguraatio: automaattiset osoitteen jakamiset, asetusten määritykset ja uudelleennumeroinnit
VPN	Virtual Private Network: virtuaalinen yksityisverkko ts. ei kiinteästi kaapeloitu
platform	toteutustaso
IPSec	joukko TCP/IP-perheeseen kuuluvia prokollia tietoliikenneyhteyksien turvaamiseen
VoIP	IP-pohjaiset puhepalvelut tietoverkossa
Dual Stack	kaksoispino: IPv4/IPv6 –lähetysten muuntoon ja hallintaan

AH	Authentication Headers: IPSec-protokollassa todennusotsake tietosähkeessä
ESP	Encapsulation Security Payload: IPSec-paketissa salausotsake
tunnel, tunnelling	tunnelointi, yhdyskäytävä (suojattu muulta liikenteeltä)
PPTP	Point-to-Point Tunneling Protocol: pasta päähän -tunnelointi
L2TP	Ciscon ja Microsoftin yhdessä kehittämä tunnelointimalli, toimii OSI-mallin toisessa kerroksessa (Layer 2)
GRE	Generic Routing Ptotocol: Ciscon tekemä, geneerinen eli ottaa mahdollisimman vähän kantaa ympäristöön
Mobile IP	mobiiliratkaisuihin tarkoitetut mallit
DMZ	De-Militarized Zone: demilitarisoitu alue eli fyysinen tai looginen aliverkko, joka yhdistää tietoturvaltaan heikompaan alueeseen
WAN	Wide Area Network: laajaverkko, joka peittää maantieteellisesti suurempia alueita
outbound	tietoverkon rajalla olevasta reitittimestä katsoen ulkomaailma (vastakohta inbound)
RADIUS	Remote Authentication Dial in User Service: tietoverkon sisäänsoittopalvelu
RAS	Remote Access Services: etäkäyttö, tarkoitettu verkon etäkäyttäjille (tarvitsee useimmiten oman palvelimen)
UDP	User Datagram Protocol: TCP/IP-perheen yhteydetön protokolla eli kadonneita tietopaketteja ei pyydetä lähettämään uudelleen
Frame Relay	operaattorien tarjoama yhteydellinen verkkotekniikka
ATM	Asynchronous Transfer Mode: muuten sama kuin edellä, mutta perustuu solutekniikkaan
PDA	Personal Data Assistant: useimmiten kämmentietokone
TLA	Top Level Aggregator: ylin kenttä IP-tietosähkeessä, toimii kuin puhelinnumeron maakoodi
SLA	Site Level Aggregator: kenttä IP-tietosähkeessä, toimii kuin puhelinnumeron suuntanumero
NLA	Next Level Aggregator: kenttä IP-tietosähkeessä, toimii kuin puhelinnumeron tilaajanumeron alkuosa

ID	laitetunnus
MAC address	Media Access Control: verkkolaitteen fyysinen osoite
ND	Neigbor Discovery: protokolla, joka haistelee verkossa olijat
DNS	Domain Name Server: järjestelmä, joka muuttaa verkkotunnuksia IP-osoitteiksi
API	Application Program Interfaces: ohjelmointirajapinta
BGP	Border Gateway Protocol: tärkein internetissä käytetty ulkoinen yhdyskäytäväprotokolla
SNMP	Simple Network Management Protocol: verkon laitteiden hallintaan tarkoitettu protokolla (tilakyselyt ja laitehälytykset)
6to4	IPv6- ja IPv4-liikenteen välitykseen operaattorista välittämättä (ei asetuksia)
prefix	etuliite
6rd	IPv6 Rapid Deployment: operaattorikäyttöön tarkoitettu versio 6-to4:stä
Teredo	kuin 6to4, mutta tarkoitettu edelleen NAT-tekniikkaa käyttäviin tapauksiin, käytännössä ”IPv6 over UDP”
Isatap	Intra-Site Automatic Tunnel Addressing Protocol: tunnelin päätepisteille automaattisista johdettuja osoitteita
NAT-PT	Network Address Translation – Protocol Translation: siirtymävaiheen tekniikka. muuntaa IPv6:sta IPv4:ksi ja päinvastoin. Poistuu käytöstä
Stateless	tilaton muoto, määritys reitittimen portissa
EUI-64	Extended Unique Identifier: 64-bittinen OSI:n kakkoskerroksen standardi
FTP	File Transfer Procol: tiedostonsiirtoprotokolla
Telnet	etäkäyttöprotokolla, käytetään useimmiten reitittimen huoltoportteihin
ICMP	Internet Control Message Protocol: laitteen virhe- ja ohjaussanomien käsittelyyn. Olellinen osa reitittimen toimivuutta tarkastaeltassa tai testeissä
SSL	Secure Sockets Layer: ei RFC-asemaa. IPSecin rinnalla, mutta tarkoitettuna etäkäyttöön
TLS	edellisen uusi nimi

IETF	Internet Engineering Task Force: järjestö, joka yllä pita RFC-dokumentaatiota muun työn ohessa
HMAC	Hash-Based Message Authentication Code: tunnistuskoodi IPSecissä
IKE	Internet Key Exchange: salausavainten vaihtomenetelmä (IPSec). Olemassa version yksi ja kaksi (IKEv1, IKEv2)
SPD	Security Police Database: tietokanta, joka sisältää dynaamisesti salauskättelyt
SA	Security Associations: salauskäytännön attribuuttien vaihto

SISÄLTÖ

1 JOHDANTO

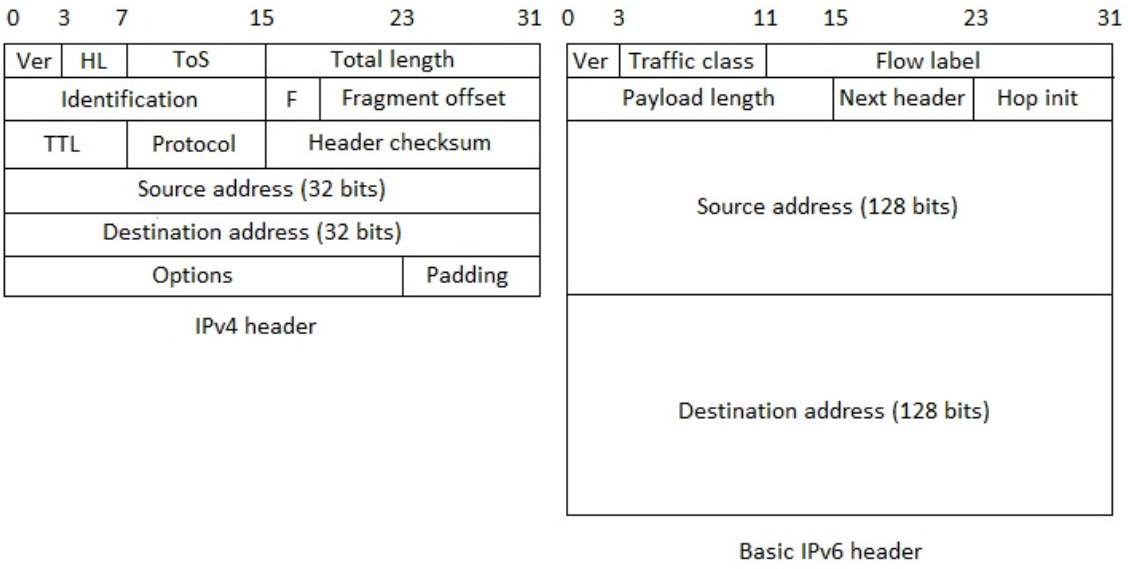
Opinnäytetyön tekijälle annettiin tehtäväksi selvitystyö, miten seuraavan sukupolven laiteosoitteistus otettaisiin käyttöön korvaten perinteinen. Tästä muodostui toimeksianto eli IPv4-IPv6 –hanke – lyhennetysti hanke, jota nimitystä jatkossa myös käytetään. Siinä oli tarkoitus tutkia julkista IPv6:tta (Internet Protocol, version 6: tietoliikennekäytäntö tietokoneiden yhdistämiseksi ja internetiin kytkeytymiseksi) ja mitä se tarkoittaisi IPv4-osoiteavaruuden (Internet Protocol version 4) käyttöön tottuneen PK-yrityksen - pieni tai keskisuuri yritys - verkon laiteosoitteiden siirtämiseen seuraavaan osoitesukupolveen (kuva 1. ja kuva 2.). Miten siis pitäisi valmistautua, mitä olisi odotettavissa ja jos havaittiin, pelättävissä? Suoritettaisiinko vain suoraviivainen vaihto vai porrastettu, vaiheittainen siirtyminen?

Päämääräksi toimeksiannolle asetettiin hallittu ja hyvin organisoitu kasvupolku IPv4- eli maailmanlaajuisesti tunnetuimmasta, käytetyimmästä ja perinteiseksi luokittelusta TCP/IP-laiteosoitteistosta (Transmission Control Protocol / Internet Protocol) IPv6-teknologiaan. Tunnelointi mielletään välivaiheeksi ja hankkeen tulikin johtaa julkiseen IPv6-osoitteistukseen. Ympäristöksi eli laitteiston ja järjestelmän alustaksi määritettiin dynaaminen ja nopeasti kasvava PK-yritys.

Toimeksiantajana toimi Trivore Oy ja ohjaajana heidän taholtaan toimitusjohtaja Kari Mattsson. Toimialakseen he ilmoittavat ICT-alan (Information and Communications Technology: tieto- ja viestintäala) infrastruktuuripalveluiden tuottamisen: peruspalvelut, taustajärjestelmät ja tietoliikenne. Yrityksen kotisivut löytyvät osoitteessa www.trivore.com (yhtiö, tuotteet, palvelut, asiakastuki, yhteystiedot). [25.]

IPv4	**IPv6**
32-bittiset osoitteet	128-bittiset osoitteet
4 294 967 296 osoitetta	340 282 366 920 938 463 463 374 607 431 768 211 456 osoitetta
esim. 10.162.22.111	esim. 2001:db8:1205:e14:250:daff:fe7d:42ec

Kuva 1. IPv4- ja IPv6-osoitteet [RFC 2373]

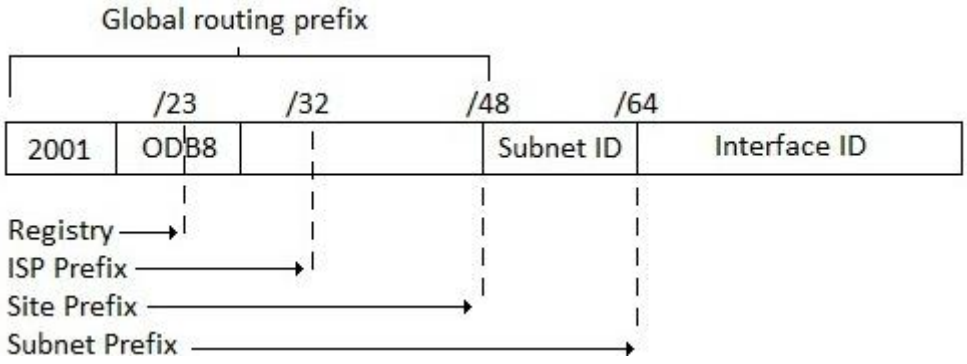


Kuva 2. IPv4- ja IPv6-paketit [IPv6 Basics, H3C Technologies Co 2011.]

Aivan alkuun tutkitaan IPv6:n teoriaa ja vertaillaan lyhyesti dominoivaan eli pääsääntöisesti edelleen käytössä olevaan IPv4-arkkitehtuuriin. Tiivistetysti sanottuna IPv4-osoitteet koostuvat 32-bittisistä osoitteista, kun taas IPv6-osoitteen kokonaispituus on 128-bittiä. Edellisillä voidaan osoittaa enimmillään noin 4 miljardia suoraa laiteosoitetta ilman osoitemuunnoksia ja jälkimmäisellä 2^{128} (kuva 1.).

Normitasolla IPv6-osoitetyypit ovat unicast (täsmälähetys: viestin lähettäminen yhdelle kohteelle), multicast (ryhmälähetys: yhdeltä monelle) ja anycast (viestin lähettäminen ryhmälle siten, se päätyy vain yhdelle ryhmän jäsenelle). Unicast-osoite on julkinen eli IPv6-globaaliosoite, joka näkyy ilman muunnoksia julkisessa verkossa sekä myös link-local –osoite (data link layer, OSI-mallin taso 2. OSI: Open Systems Reference Model – kuvaa tiedonsiirtojärjestelmän seitsemässä kerroksessa (kuva 3.).

Kuva 3. OSI-malli [Wikipedia, fi.wikipedia.org, 8.12.2011]



Kuva 4. IPv6-osoite [RFC 2373]

jotka eivät ole reitityskelpoisia – sama osoite voi olla käytössä useammassakin eri verkossa. Unicast-osoite (kuva 4.) määrittelee yhden ja vain yhden rajapinnan.

Multicast-osoitteet vastaavat IPv4:n broadcast-osoitteita eli yleislähetystä, poiketen siinä, että toimitaan tietyssä multicast-ryhmässä. Anycast-osoite on tunniste ryhmälle rajapintoja. Tuleva paketti menee jollekin anycast-osoitteen rajapinnoista – useimmiten ensimmäiseksi tunnistettavalle. Multicastissa ne taasen menevät kaikille rajapinnoille [8].

Ei ole ollut itsestään selvää siirtyä uuteen osoitteistukseen, vaan IPv4:ää on jatkettu käyttämällä dynaamisia osoitteita (DHCP, Dynamic Host Configuration Protocol, IP-osoitteen välitysmenetelmä verkkoon kytkeytyville), osoitteenmuunnoksia (NAT,

Network Address Translation) ja uudistamalla reititystapaa (CIDR, Classless Inter-Domain Routing).

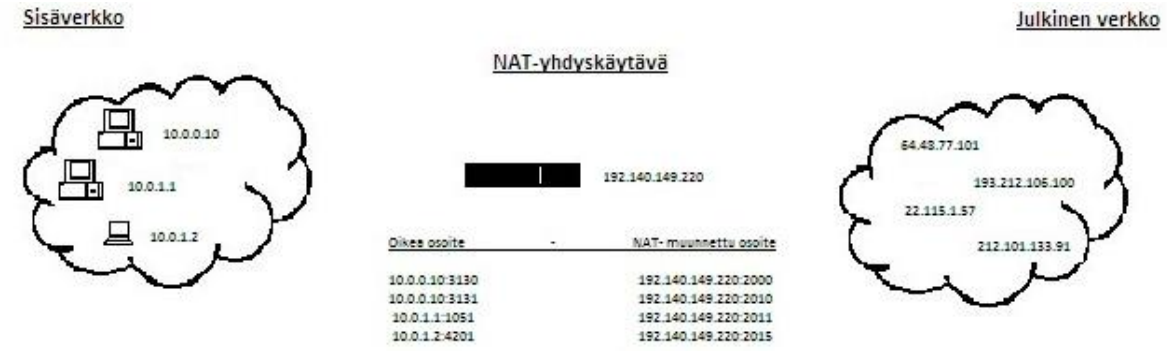
Seuraavaksi tutkitaan toteutusvaihtoehtoja (mikäli niitä on useampi varteenotettava) ja päädytään realistisimpaan, ehdotettavaan toteutukseen. Odotettavissa on jo nykyisillä resursseilla oleva toimiva ratkaisu, sillä viitteet löytyvät alan julkaisuissa ja lupaukset ovat niistä poimittavissa.

2 IPv4 JA IPv6

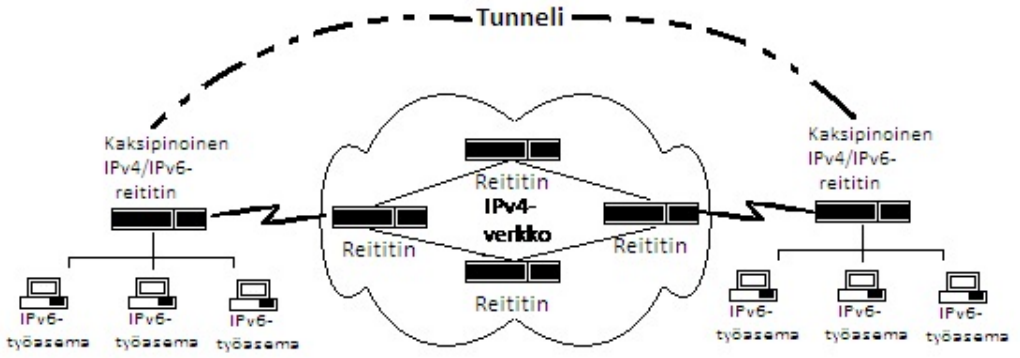
IPv6 on laadittu IPV4:stä saadulla kokemuksella, sen puutteita korjaamalla ja uusia ominaisuuksia lisäten. Toisin sanoen on suunniteltu täysin uusi arkkitehtuuri. IPv6 pitää sisällään joustavan ja laajennetun otsikkorakenteen, autokonfiguraation (automaattiset osoitteen jakamiset, asetusmääritykset ja uudelleennumeroinnit), palvelunlaadun, liikenteen suunnittelun, monilähetyksen [RFC 2375] - perinteinen yleislähetys on jätetty pois), todennuksen ja salaamisen. VPN-tunnelointikin (Virtual Private Network: virtuaaliset yksityisverkot) on ns. sisäänrakennettu ominaisuus. Uusi osoitteistusarkkitehtuuri poistaa protokollasta NAT:ien (Network Address Translation) (kuva 5.) tarpeellisuuden, jolloin sulautetut älyverkot ja mobiili- eli liikkuva tietojenkäsittely on helppo platformina eli toteutustasona toteuttaa. NAT ei olisi ollut pidemmän päälle ratkaisu, sillä

- verkko muuttuu yhdyskäytävässä monimutkaisemmaksi sovellustasolla protokollamuunnosten takia
- vikoja saattaisi ilmaantua ylimääräisen portaan kautta – osa, jota olisi pakko käyttää, mutta olisi vaikeasti ennustettavissa hankaluutensa takia siirtotiellä
- pääsy julkisesta verkosta: välityspalvelimien käyttötarve (liikenteen kierrätys)
- NAT ei toimi palomuurina – siihen ei voi, eikä saa luottaa
- IPSec (IP Security Architecture – joukko TCP/IP-perheeseen kuuluvia protokollia tietoliikenneyhteyksien turvaamiseen) ja VoIP (Voice over IP – eli IP-pohjaiset puhepalvelut) eivät voisi toimia ilman ylimääräistä työrupeamaa

Protokollassa on tiettyjä määrityksiä siirtymämalleista, joilla varaudutaan IPV6-isäntien ja verkkoreitittimien levityksessä tapahtuviin katkoksiin. Ehkä tärkein siirtymisstrategia on tunneloinnin käyttäminen, jotta IPv6-saarekkeet (dedikoidut verkot) voidaan yhdistää IPv4:ää käyttävän runkoyhteyden välityksellä. Runkoreitittimessä on tällöin Dual Stack eli IPv4/IPv6-kaksoispino (kuva 6.).



Kuva 5. Esimerkki NAT –yhdyskäytävästä [26]



Kuva 6. IPv6:n tunnelointi IPv4-runkoyhteyden välityksellä [1]

2.1 Virtual Private Network: VPN ja tunnelointi

VPN-palvelut ovat hajautetun verkon ydin. IPv6 ottaa kantaa erittäin moneen arkkitehtuurin osaan eli sen voidaan todeta oleva ratkaiseva tekijä koko infrastruktuurin laatimisessa ja eritoten VPN-palvelujen toteuttamisessa. IPv6:n pakettiotsake (kuva 7.) havainnollistaa muutosta edelliseen IP:n versioon ja hahmottaa IPv6:n reititystä.

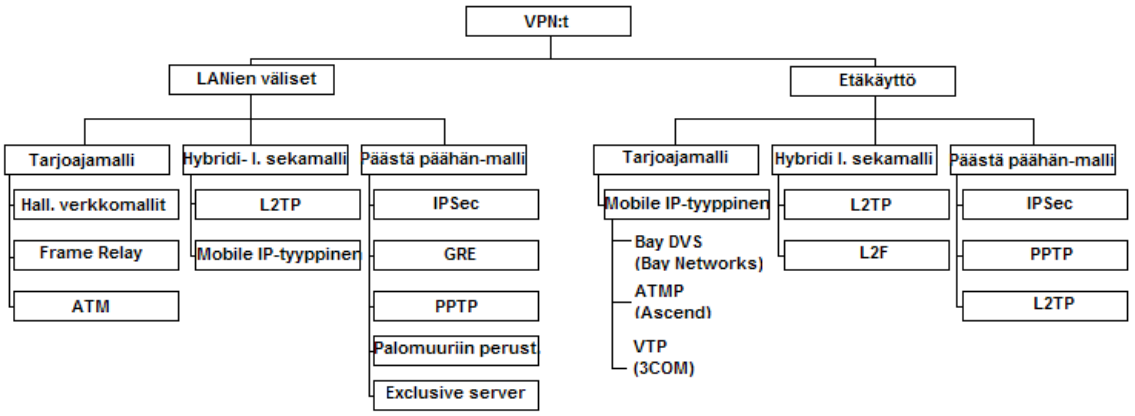
4 bittiä Versio	4 bittiä Prioriteetti	24 bittiä Datavuotunnus	
16 bittiä Datakuorman pituus		8 bittiä Seuraava otsake	8 bittiä Hyppyrajoitus
128 bittiä Lähdeosoite			
128 bittiä Kohdeosoite			

Kuva 7. IPv6:n reititysotsake [26]

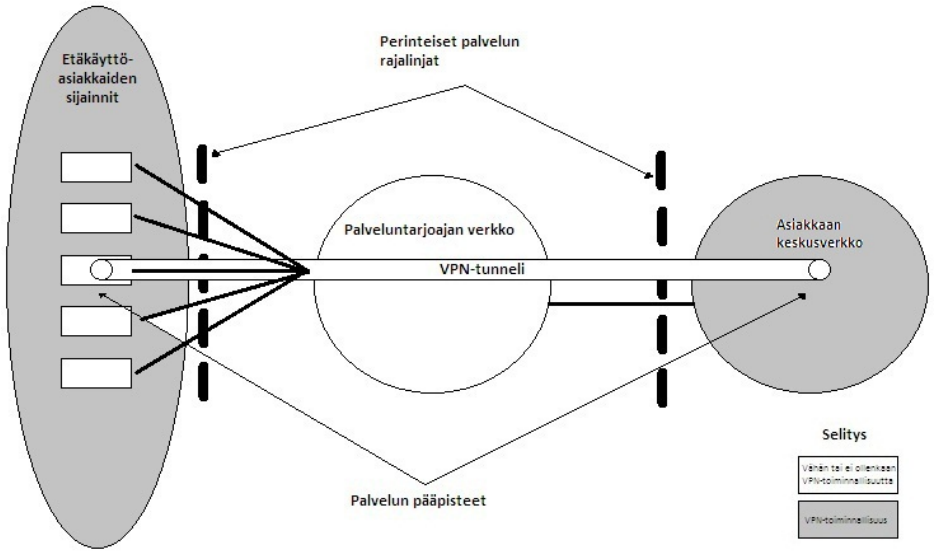
Edellistä arkkitehtuurisukupolvea hallitseva havaitsee, että otsakkeen pituus on kiinteästi 40 tavua sekä moni IPv4:n otsakkeen kentistä on nimetty uudelleen tai siirretty vaihtoehtoisiin laajennusotsakkeisiin poiketen edellisen sukupolven kiinteämittaisesta otsakkeesta [RFC:t 2373 ja 2374]. Kaiken kaikkiaan kiinteämittainen otsakekoko takaa tehokkaamman pakettien käsittelyn reitittimissä toisin, kuin IPV4:n vaihtelevat otsakekerrokset, jotka on jäsennettävä avainmääreiden löytämiseksi (Seuraava otsake –kenttä on avainasemassa). Tähdennettävää on, että IPv6-otsake sisältää suoran tuen datavirtaan liittyville tunnuksille. Näin tunnuskytkentäiset arkkitehtuurit ovat helpommin käsiteltävissä. Valinnanvaraisiin lisä- tai laajennusotsakkeisiin lukeutuvat todennusotsake (AH, Authenticating Headers) ja salausotsake (ESP, Encapsulating Security Payload), joita käytetään tarjoamaan IPSec:in tunnelointi-, autentikointi- ja salausominaisuuksia IPv4:ssä ja IPv6:ssa.

Kuva 8. IPSec –tunnelointi [RFC 2401], ESP-osa (b) [9]

Kiteytetysti voidaan sanoa, että VPN on pikemminkin sisäänrakennettu komponentti IPv6:een kuin lisävaruste. Tässä yhteydessä on todettava, että IPSec ottaa paikkansa tunnelointina, joka on yleisin päästä päähän –mallia toteuttavana (kuva 10.). Muita ovat PPTP (Point-to-Point Tunneling Protocol), L2TP (Ciscon ja Microsoftin yhdessä kehittämä VPN-tunnelointiprotokolla, joka toimii OSI-mallin kakkoskerroksessa), GRE (Generic Routing Encapsulation, Ciscon kehittämä) sekä palomuuriin perustuvat mallit: ne lunastavat sijansa tietyssä ympäristössä tai toimivat apuprotokollana. Mobile IP on sinällään oma luku sinänsä: mahdollisuuksien maailma. IPSec ei myöskään ole protokolla yksiselitteisesti, vaikka useassa yhteydessä näin sitä kutsutaankin, vaan kyseessä on protokollien kokoelma – yli 40 kappaletta [RFC 1825].



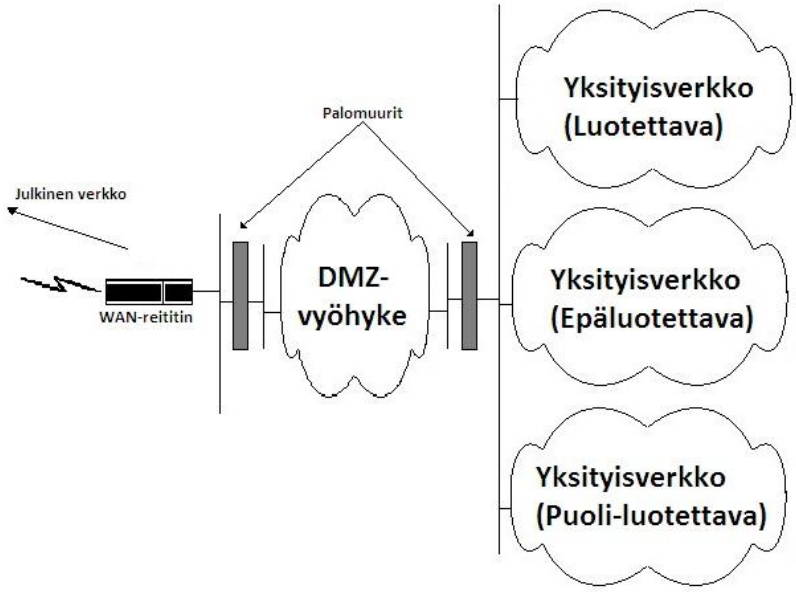
Kuva 9. VPN-protokollat, -mallit ja –sovellukset [1]



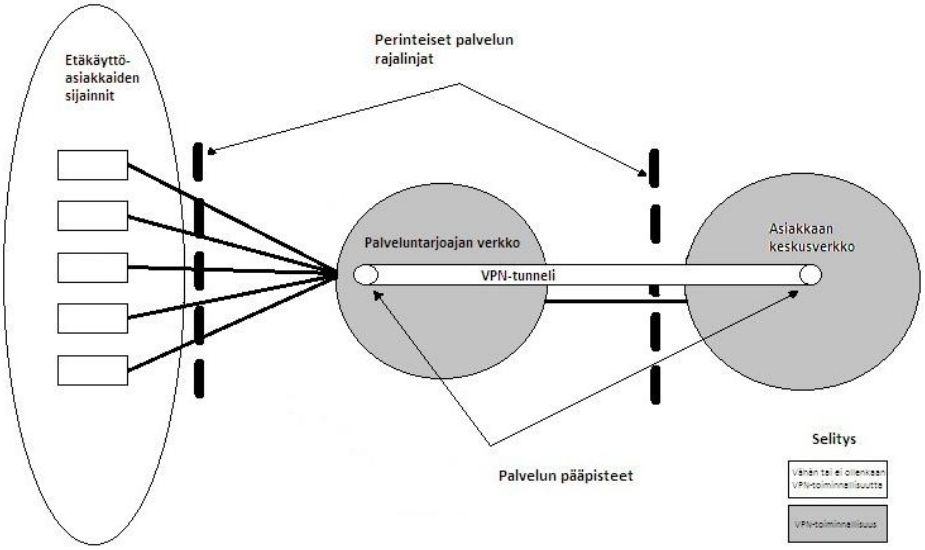
Kuva 10. Palvelun päätepisteet päästä päähän –mallissa [1]

Microsoft tukee PPTP:tä. Siinä on otettava huomioon, että se toimii parhaiten kun verkkoon on luotu demilitarisoitu vyöhyke eli DMZ (De-militarized Zone, tietoturvassa demilitarisoitu alue: tarkoittaa fyysistä tai loogista aliverkkoa, joka yhdistää järjestelmän turvattomampaan alueeseen, kuva 11.), joka on palomuurein eristetty kumpaankin suuntaan ja WAN-reititin (Wide Alea Network, laajaverkko, joka peittää laajoja maantieteellisiä alueita) on julkisessa verkossa (Outbound), ulkoisen palomuurin ulkopuolella, julkisessa verkossa. PPTP-palvelin sijoitetaan DMZ:aan, jonne voidaan sijoittaa yrityksen ulkoiset palvelimet. Sisäverkko Intranet-palvelimineen jää sisäisen palomuurin taakse (Inbound). Miksi valita helpon IPSecin sijaan PPTP? Tietyt sovellukset, varsinkin Microsoftin tekemät periaatteessa edellyttävät PPTP:tä ja DMZ:aa (kuva 11.).

VPN:n sekamallin (palvelun tarjoaja –mallin ja päästä päähän –mallin väliin asettuva eli siinä hallinnoidaan palveluntarjoajan verkkoa JA asiakaspäätä) L2TP:n kiistaton etu on etäkäytön optimointi ja RADIUS-palvelimen (Remote Authentication Dial in User Service, sisäänsoittopalvelu - RAS-käytössä (Remote Access Services – etäkäyttö: tarkoitettu verkon etäkäyttäjille) tarve ensimmäisen tason todennukseen, tunnelointiin ja tilinpitoon (kuva 12).



Kuva 11. DMZ [26]

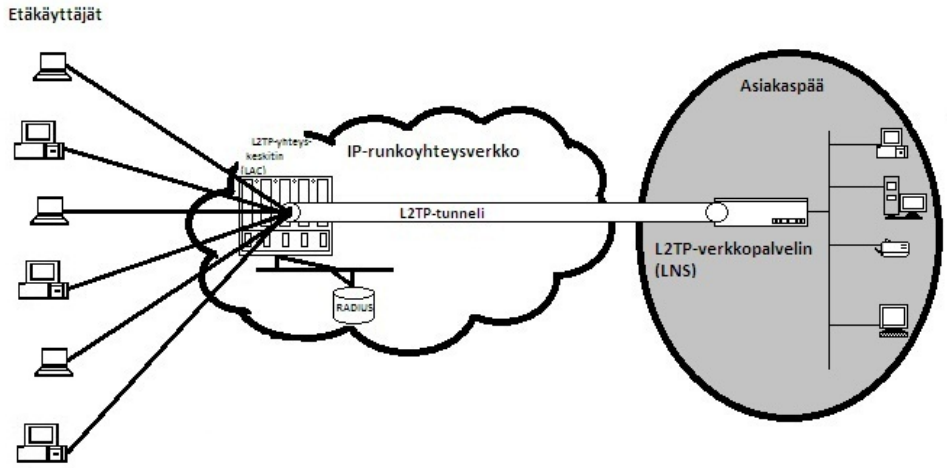


Kuva 12. Palvelun päätepisteet hybridi- eli sekamallissa [1]

Kuitenkin PPP-yhteys (Point-to-Point –protokolla: suora yhteys verkkolaitteiden välillä) muodostuu päästä päähän. On huomattavaa, että L2TP-paketit ovat UDP-kapseloituja (yhteydetön protokolla), toisin kuin PPTP:ssä, jossa käytetään TCP-istuntoa komento- ja valvontapakettien kuljetukseen. L2TP on näin ollen ns. yhteydetön. Komento- ja valvontapaketteja joudutaan käyttämään enemmän, mutta kun saantiviiveet ovat ongelma verkossa, löytää L2TP (kuva 13.) perustelut helposti käytölleen.

GRE harvoin mielletään omaksi tunnelointiprotokollakseen, sillä se on käytössä useimmiten toisten protokollien kapseloinnissa, kuten PPTP:ssä ja useimmissa Mobile IP –tunneloinneissa. GRE on ns. toimitusprotokolla (sillä on dedikoidut otsakkeet) ja se on siinä tehokas: pelkistetty rakenne [RFC 1702]. Toimitusotsake on jätetty avoimeksi GRE:ssä – siksi se on lisäksi kevyt, sillä se on tavallaan huomaamaton: tavanomainen IP-reititin ei edes tiedä, että se lähettää eteenpäin GRE-paketteja, koska sen ainoa huolenaihe on IP-otsake. GRE on käytössä apuprotokollana ja toimii kuten RADIUS ja NAT → korvaa Layer2 –virtuaaliyhteyksiä (Frame Relay, ATM)

- Frame Relay: alueverkkotekniikka, poistuu käytöstä kalleutensa ja vanhentuvan tekniikan vuoksi
- ATM: Asynchronous Transfer Mode: asynkroninen tiedonsiirtotapa (tieto siirtyy eri nopeudella tulo- tai lähtösuuntaan nähden)



Kuva 13. L2TP-verkko [1]

3 bittiä	13 bittiä	32 bittiä	16 bittiä	64 bittiä
Osoite-tyyppi	TLA	NLA	SLA	Liittymätunniste

Kuva 14. Tyypillinen IPv6:n 128-bittinen osoiteformaatti [8]

IPv6:n merkittävyys keskittyy sen uuteen 128-bittiseen osoitekenttään [RFC 2373]. Laajempi osoiteavaruus mahdollistaa perustan IP-verkottumiselle, joka tukee sulautetun ja piilotetun verkottumisen alati kiihtyvää leviämistä aivan lähitulevaisuudessa.

Hyvinkin pian ja osin jo nyt PDA- laitteet (Personal Digital Assistant, kämmentietokone) – esim. iPadit tai Samsung Galaxy Tabin kaltaiset lukulaitteet, autot, myyntiautomaatit ja jopa yleiset kodinkoneet vaativat IP-osoitteita. Suuri osoitekoko luo perustan tehokkaan hierarkisen (tasomalli, perustuu arvojärjestykseen) reititysrakenteen ylläpitämään verkottumista globaalisella tasolla. IPv6:n osoitteenmuodostus (kuva 14.) voi ottaa huomioon TLA:t (Top Level Aggregator), NLA:t (Next Level Aggregator) ja SLA:t (Site Level Aggregator), jotka antavat verkkoreitittimille mahdollisuuden reitittää paketteja aivan puhelinverkon periaatteen mukaisesti. Tällöin TLA vastaa maanumeroa ja NLA suuntanumeroa, johon lisätään puhelinnumeron alkuosa (SLA). Puhelinverkosta poiketen aggregaatit eivät ole välttämättä tiukasti maantieteellisiä, koska varsinkin suurissa verkoissa rajat ylittyvät helposti ja ovat käsitteellisiä. NLA:t voidaan peräti jakaa edelleen alakenttiin, jotta ne vastaisivat paremmin pienempien palveluntarjoajien hierarkioita [RFC 2450].

Uusi 64-bittinen liittymätunnistekenttä (Interface ID) luo edellytykset verkossa verkossa sijaitsevan isäntäkoneen osoitteen yksinkertaiselle autokonfiguroinnille, joka itse asiassa perustuu LAN-kortin ID:hen – käytännössä MAC-osoitteeseen (laiteosoite, esimerkiksi verkkokortti: perustuu laitteelle koodattuun valmistajan sarjanumeroon). Lokalisoinnin jälkeen uusi ND-protokolla [Neighbor Discovery, RCF:t 2461 ja 1970] mahdollistaa sen, että asema voi pyytää reititysetuliitteensä outbound- eli ulospäin ohjaavalta reitittimeltä. Toisin kuin DHCP-palvelussa, tällä metodilla ei vaadita osoitepalvelimelta, että se ylläpitää jaettujen osoitteiden tilaa tai hallinnoi osoitteiden varauksia (tosin tilallinen osoitteen osoittaminen DHCP:n välityksellä on lisätty IPv6:een ja se on aina käytettävissä). Autokonfigurointi säästää ns. solmujen siirtojen ja muutosten uudelleenmäärittelyiltä ja tarvittaessa jopa helpottaa yritystä vaihtamaan internet-palveluntarjoajia eli IP-operaattoreita. On pääteltävissä, että teoriassa globaalit julkiset IPv6-osoitteet ovat heti toteutettavissa pohjautuen LAN ID:hin liittymätunnistekentässä.

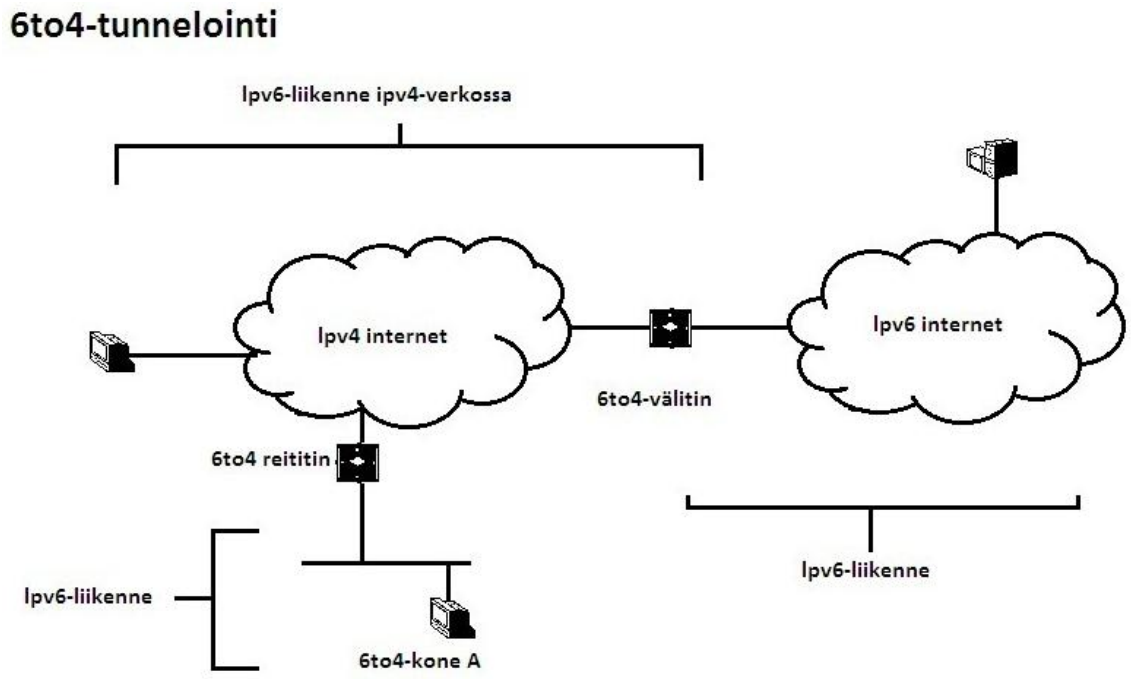
Olemassa olevat IPv4-pohjaiset DNS-nimipalvelimet (Domain Name System: järjestelmä, joka muuttaa verkkotunnuksia IP-osoitteiksi) eivät yksinkertaisesti toimi uudessa arkkitehtuurissa ja ne on päivitettävä – ne eivät enää selviä uusiin 128-bittisiin osoitteisiin kohdistuvista hauista ja niiden säilytyksestä. Tällöin Dual Stack astuu kuvioon eli rakennetaan uusi kaksinkertainen IPv4/IPv6-tominnallisuutta tukeva nimipalvelimien verkko nimien kääntämiseksi IPv6-osoitteiksi. Näitä nimipalvelimia voidaan käyttää myös siirtymävaiheenmalleissa. Jos nimihaku palauttaisi IPv4-osoitteen, kaksinkertaisen IP-pinon omaava isäntä käyttäisi yhteydessä IPv4:ää ja jos tuloksena olisi IPv6-osoite, käyttöön otettaisiin IPv6. Suurin osa sovelluksista käyttää API:a (Application Program Interfaces, ohjelmointirajapinta) kyselyjen suorittamisessa nimipalvelimilta, mutta toisin toimivat voivat vaatia päivityksiä toimiakseen uusien 128-bittisten tietueiden kanssa. Muut verkkoprotokollat kuten BGP (Border Gateway Protocol) ja SNMP (Simple Network Management Protocol, verkossa olevien laitteiden tilakyselyihin tai laitehälytyksiin), tarvitsevat vastaavasti parannuksia selviytyäkseen uudessa ympäristössä.

2.2 Tunnelointi ilman operaattorin tukea

Edellä käsiteltiin kiinteästi konfiguroituja tunnelointeja. IPv6-palveluihin voi kytkeytyä, vaikka oma operaattori ei tekniikkaa tukisikaan. IPv6-liikennettä voi nimittäin siirtää IPv4-verkon yli helppokäyttöisillä, automaattisilla (oletusarvoisena laitteessa)

tunnelointimekanismeilla. Niiden avulla IPv6-työasema voi kommunikoida IPv6-palvelimen kanssa, vaikka jompikumpi tai molemmat olisi liitetty vain IPv4-verkkoon.

Käytännöistä yleisin lienee 6to4 [RFC 3056] (kuva 15.), joka on oletuksena aktivoitu esimerkiksi Microsoft Windows Vistassa ja 7:ssä sekä Windows Server 2008:ssa. Oletusaktivoiti tekee siitä siis automaattisen.



Kuva 15. 6to4 -tunnelointi [4]

Tarkoitusta varten on veloituksetta käytettävissä useiden eri tahojen ylläpitämiä julkisia 6to4-liikennettä välittäviä reitittimiä. Käyttäjän kannalta menettely on helppo, koska se etsii tunnelin päätepisteen automaattisesti IPv4-verkosta. Haittapuolena on, että käyttäjä ei voi vaikuttaa tunnelin päätepisteiden valintaan, vaan päätepisteeksi valikoituu lähin 6to4-osoitetta ”mainostava” reititin.. Palvelun laatua ei takaa mikään, vaan liikenne voi kulkea vähemmän optimaalista reittiä pitkin ja tunnelin päätepisteet voivat olla suorituskyvyltään epäsymmetriset.

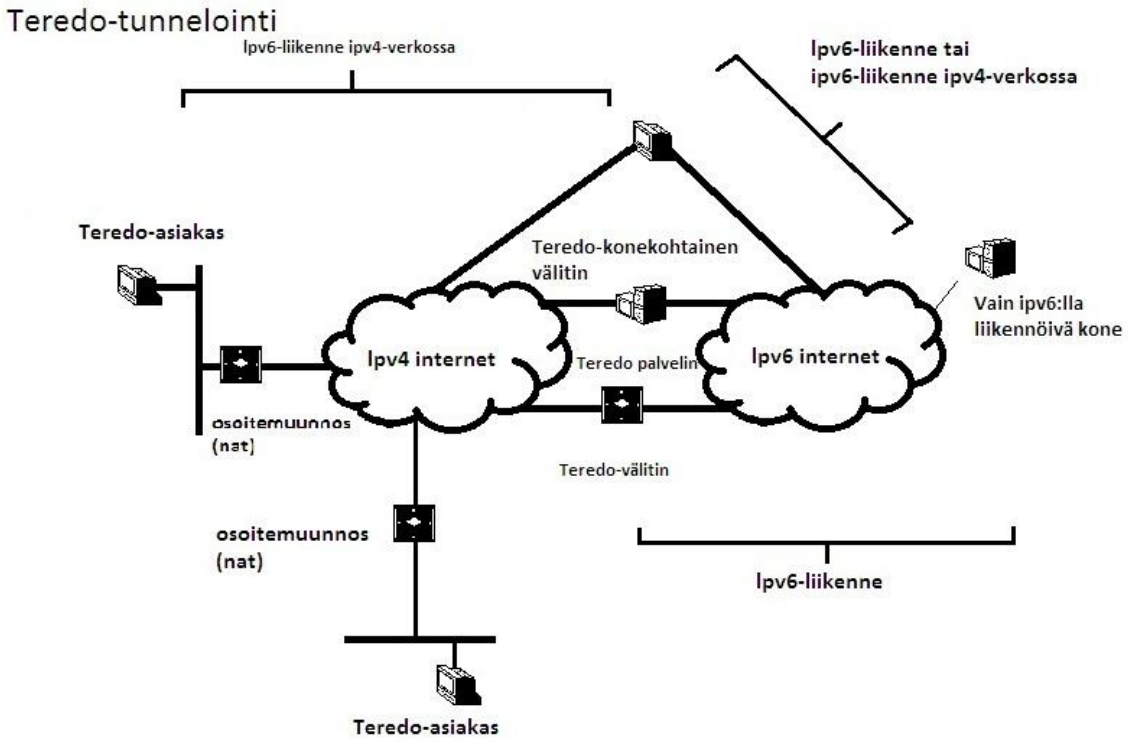
Hyviä puoliakin on: toimiakseen 6to4 vaatii vain yhden globaalin IPv4-osoitteen, joka voi kuulua NAT-muunnoksen tekevälle laitteellekin. NATin takana olevat verkot saadaan osaksi globaalia IPv6-maailmaa ja IPv4:n osalta ne ovat edelleen yksityisiä. Tarjoaa siis käyttäjälle /48-kokoisen globaalin prefiksin eli etuliitteen se: mahdollistaa

IPv6-aliverkotuksen. Esimerkiksi 2002:82E6:3671::/48 kun käytetään osoitetta 130.230.54.113.

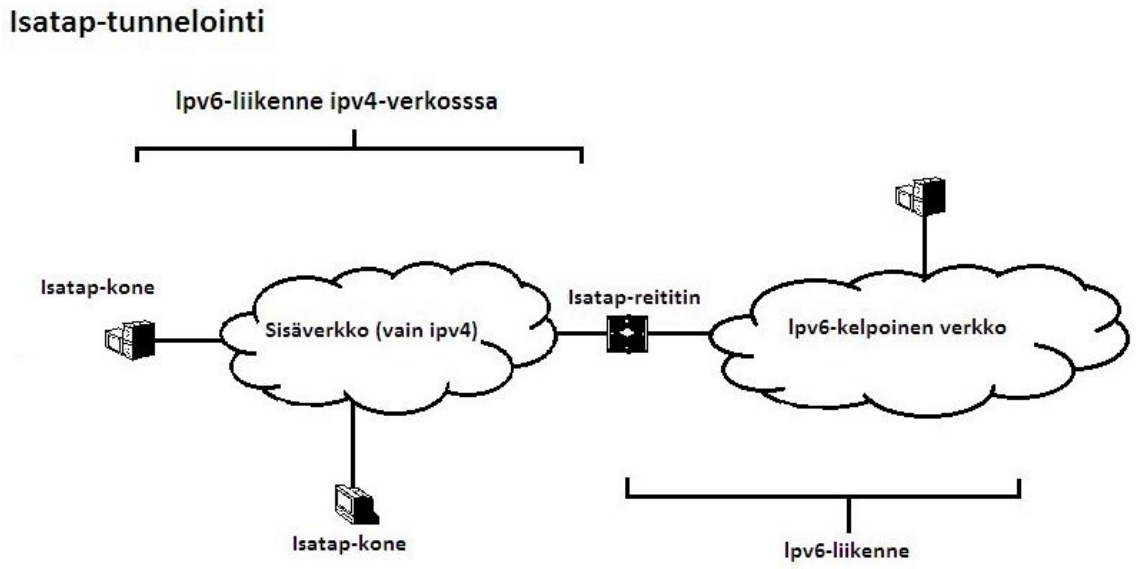
Eräs vastaus tähän hallitsemattomuuteen on 6rd (IPv6 Rapid Deployment [RFC 5969]), joka on operaattorikäyttöön tarkoitettu versio 6to4:stä. Sen avulla palveluntarjoaja voi pakottaa tunneloidun IPv6-liikenteen omiin yhdyskäytäviinsä ja rajata sen omiin asiakkaisiinsa. Ranskalainen Free (palveluntuottaja) otti sen käyttöön jo vuonna 2007. [http://en.wikipedia.org/wiki/IPv6_transition_mechanisms].

6to4 sopii käytettäväksi vain koneilta, joilla on julkinen IP-osoite. Osoitemuunnoksen takana (NAT) toimivia koneita varten on kehitetty Teredo-käytäntö [RFC 4380, 5991 ja 6081], joka sekin on Microsoftin tukema (kuva16.).

Teredo tulee kyseeseen myös silloin, kun palomuuri ei salli tavallista IPv6-tunnelointia. Käytännössä Teredo on ”IPv6 over UDP”. Teredoa käytetään useimmiten silloin kun 6to4 ei tule kyseeseen eli yksi tai useampi NAT- osoite tarvitsee IPv6:tta. Toimii myös silloin, kun molemmat osapuolet ovat NATin takana. Huomioon on otettava, että Teredon käyttämät osoitteet ovat osa globaalia IPv6-osoiteavaruutta.



Kuva 16. Teredo-tunnelointi [5]



Kuva 17. Isatap-tunnelointi [6]

Jos yritys on päivittämässä omaa verkkoaan vähin erin IPv6-aikaan, eteen tulee usein tarve tunneloida IPv6-liikennettä oman IPv4-verkon sisällä, esimerkiksi toimipisteiden välillä. Yrityksen sisäistä liikennettä ei ole suotavaa kuljettaa julkisten tunnelointireitittimien kautta, joten edellä kuvatut menettelyt eivät ole suositeltavia. Tarkoitusta varten onkin kehitetty Isatap-käytäntö (Intra-Site Automatic Tunnel Addressing Protocol [RFC 5214] (kuva 17.), joka käyttää tunnelin päätepisteille automaattisesti paikallisia, IPv4-osoitteista johdettuja IPv6-osoitteita. Sillekin löytyy tuki esimerkiksi Windowseista. Tietoturvan kannalta on tärkeää suodattaa liikenne Isatap-reitittimen IPv4-osoitteeseen organisaation rajalla.

Muita julkaisuissa olleita menetelmiä ovat mm.

- Tunnel Broker [RFC 3053]: käyttää Configured Tunneling –tekniikkaa, ei siis määrittele protokollaa. Käyttäjä rekisteröi palvelun käyttöönsä. Palveluntarjoaja antaa käyttöjärjestelmäkohtaiset ohjeet, ohjelman tai skriptin, jolla tunneli konfiguroidaan käyttäjän ja Tunnel Broker –palveluntarjoajan välillä.
- 6in4: poistunut käytöstä 20.5.2006, ei enää RFC-numeroa
- 6over4 [RFC 2529]: vaatii kuitenkin toimivan IPv4 multicast –reitityksen. Tämä on poistuva menetelmä

Näitä kutsutaan puoliautomaattisiksi (ne eivät ole oletusarvoisesti aktivoitu).

2.3 NAT-PT

Vielä mainitsematon transitio- eli siirtymävaiheen menetelmä on NAT-PT (täydelliseltä nimeltään Network Address Translation – Protocol Translation [RFC 2766]). NAT-PT:ssä IPv6-paketit muunnetaan IPv4-paketeiksi. Toimii myös toiseen suuntaan. Muunnos tehdään reitittimessä tai paketin lähettäjän toimesta. NAT-PT on tarkoitettu lähinnä laitteille, jotka osaavat vain yhtä protokollaa, mutta tarvitsevat palveluita toiselta osapuolelta, joka käyttää IPv6:tta. DNS on tätä käytettäessä suuri ongelma, sillä DNS-pakettien sisältökin pitää muuntaa. NAT-PT:ssä on täysin mahdotonta käyttää protokollia, jotka kuljettavat IP-osoitetta ja myös IPSec vaatii muutoksia

Liikennemäärän ja etenkin osoitteiston kasvaessa vasteajat saattavat muodostua ongelmaksi. Tämä on jo luokiteltu poistuneeksi menetelmäksi (Historic Status) [RFC 4966]. Yleisin käyttötapa oli DNS ja sovellustason yhdyskäytävä [7].

3 TOIMEKSIANTO: SIIRTYMINEN IPv6:EEN

Lähtökohdaksi ideoitiin tarvekartoitus ja suunnittelun konsultaatio simuloidulle eli keksitylle ja pöytätestatulle yritykselle, jolla on useampia toimipisteitä – aloitusvaiheessa kaksi. Sanomattakin on selvää, että toimeksiantajalla eli Trivore Oy:llä oli ajatus hyödyntää tutkimusta, määrittelyjä, suunnittelua ja raportointia tuotantokäytössään. Aiheen lähtökartoituksessa todettiin, että lopputyöntekijän on tukeuduttava laajalti käytettävissä olevaan tietouteen, joka olisi saatavilla internetin, kirjallisuuden, toimittajien ja asiantuntijoiden haastattelujen välityksellä. Jo spesifiointivaiheessa ilmeni ja tuli selväksi, ettei mitään konkreettista käyttöönottoa ja testausta ole tarkoitus tehdä – ainakaan käytettävissä olevalla aikataululla. Opinnäytetyön tekijälle jäi vastuu luottaa omiin kykyihinsä sekä luovasti etsiä ja hyödyntää lähteitä itsekriittisesti.

Itse osoitteistusversioiden vaihtoon ei tekijälle ollut suunniteltu roolia ja kun käyttöönotto mahdollisesti realisoituu, tilanne katsotaan molemminpuolisesti uudestaan sen hetkisessä tilanteessa. Laitteisto on jo olemassa eli kyseessä oli puhdas tutkimus- ja kehitystyö.

Heti ensitapaamisessa toimitusjohtaja Mattsson kertoi tiukasti rajatut raamit. Tehtäväkenttänä on simuloitu PK-yritys: päätoimipaikkaa sijaitsee Turussa ja yrityksessä on käytössä Cisco ASA 5505 –laitteistopalomuuri (oppiva palomuuri, suodatusjärjestelmä, kaistanrajoitus, sisältöseuranta ja reititys sekä VoIP, suojattuna - kaikki yhdessä laitekokoonpanossa). Toinen toimipaikka on Helsingissä ja sinne päätettiin hankkia vastaavanlainen Cisco-laitteisto. Koko yrityksessä on käytössä sovellus, joka olettaa, että lähiverkossa on mistään osatekijästä riippumatta käytettävissä IPv6 (osoiteavaruus 2^{128}). Tämä on ohjelmiston toimittajan vaatimus. Oletusoperaattoreina ovat Turussa Telia Sonera ja Helsingissä Elisa [27]. Kyseiset operaattorit tarjoavat liikennöintiprotokollasta versiota IPv4 toimipaikkojen välille, mutta IPv6 onnistuu yrityksen sisällä, kunhan se on palomuurin takana ja omassa valvonnassa, omalla vastuulla.

Hankkeenvetäjä joutui miettimään seuraavia asioita:

- Turun toimipisteessä on nyt käytössä osoiteavaruus 172.17.1.0/24 ja Helsingissä 172.17.2.0/24. Mitä näiden IPv4-luokkien kanssa nyt tehdään?
- tunnelointi (IPSec –suojausmenetelmä siirtotiellä ja VPN).

- kapselointimenetelmä. On olemassa useampia protokollia. Mikä on järkevin?
- Globaalista Localiksi (julkisesta suljettuun eli lähiverkon sisäpuoliseen osoitteistukseen)
- mitä nämä osoiteavaruudet tarkoittavat tietokoneiden ja kaikkien laitteiden osalta, joilla on kiinteä IP-osoite? MAC-perusteinen IP-numero: onko se lähtökohta (kyseessähän on uniikki eli laitekohtainen osoite, jota ei ole muualla käytössä)?
- miten käyttäytyy julkinen IPv6 ja mitkä numerot kannattaa hankkia? Mistä ne hankitaan, mitä tällä saavutetaan (edut/haitat). Kokonaiskustannukset (kiinteät ja muuttuvat kustannukset) jäävät kuitenkin käyttöönottovaiheeseen
- mitä on oma autonominen IPv6 ja miten sellaisen saa?

Vaiheessa yksi ei IPv6 näy ekstranetissä eli lähiverkkoympäristössä, joihin dedikoiduilla eli oikeudet omaavilla asiakkailla on mahdollisuus päästä ja käyttää – vain palomuuri ja reititin ovat sen piirissä. Vaiheessa kaksi on jo globaali numerointi käytössä. Miten siis julkinen IPv6 kannattaa toteuttaa ja miten reititys palomuurissa saadaan luotettavasti ja helposti toteutettua? Mihin tilaan jää siis Local (inbound) eli lähiverkon sisäpuoli? Tunnelointi on jo kuitenkin lopetettu [3] ja riskianalyysissä täytyy olla tyhjentävä selvitys testauksesta ja havaituista tietoturvariskeistä. [25.]

4 KÄYTÄNNÖN TYÖ: OHJEISTUS

Ensimmäiset keskustelut käytiin jo joulukuussa 2008. Yrityksessä elettiin kuitenkin hektisiä aikoja ja työntoteuttajalla opiskelut olivat kurssien ja tenttien johdosta kiireellisessä vaiheessa. Yhteensovittamisten jälkeen varsinaisesti sopimukseen päästiin maaliskuun alussa 2010.

Suunnitteluvaiheessa oli mahdotonta luoda yksiselitteinen ja tiukasti jaksotettu aikataulu. Toimeksianto muuttui ja eli jonkin verran puolin ja toisin. Osioimisen jälkeen tehtävän vaiheiden päällekkäisyydet ja ristiin menot ajanjaksollisesti muokkasivat vaikeasti hallittavan mutta hyvin joustavan aikataulutuksen, joka vaati tilanneherkkyyttä ja itsekuria. Lisäksi sesongit (yritysmaailma), muut tehtävät sekä kesälomat kaikilla osapuolilla vaikeuttivat aikahaarukassa pysymistä.

Alkuperäisenä tavoitteena oli saada toimeksianto valmiiksi saman vuoden kesäkuun alkuun mennessä ja se havaittiin heti mahdottomaksi. Työntoteuttajan anottua opiskelulleen lisäaikaa lopulliseksi takarajaksi asettui vuodenvaihde 2011-2012.

Toimeksiantajalla on käytössään Cisco ASA 5505 –laitteistopalomuurit, yksi kummassakin toimipaikassa. Todennäköisesti tuotantokäyttöön tulevat uudemman Cisco ASA -laitesukupolven laitteet.

4.1 Osoitetyypit IPv6-rajapintoihin eli liityntäportteihin

IPv6:n käytettävyyttä helpottaa se, että IPv6-avaruutta käyttävässä verkossa IPv6-osoite voidaan määrittää IPv4-osoitteen rinnalle kuhunkin Cisco ASA –palomuurin liityntäporttiin. Portissa voi olla konfiguroituna useampi IPv6-osoite yhtäaikaisesti. Kun globaaliosoite määritetään porttiin, siihen automaattisesti määräytyy link-local –osoite määritetyn julkisen osoitteen lisäksi. IPv6-palvelut käynnistyvät porteissa välittömästi, kun IPv6-osoitemääritys on tehty. [11].

1) Julkinen osoite: staattiseksi eli globaaliksi määritelty unicast-osoite on asetettu porttiin käsin - pysyväksi. Sen lisäksi IPv6-osoitteessa pitää määriteltynä prefiksi eli IPv6-verkon koko – tavallaan pooli (rajattu osoiteavaruus), johon

osoite kuuluu. Kun liityntäporttiin on asetettu globaaliosoite sillä on automaattisesti link-local –osoite. [11.]

esim. `hostname(config-if)# ipv6 address 2001:1dd0:10a0:1b11::1/64`

2) Stateless autoconfiguration: helpointa on määrittää liityntäporttiin tilaton autokonfiguraatio, jolloin portti saa julkisen IPv6-osoitteen ja link-local –osoitteen ilman käsin luotuja määrityksiä. Reuna-alueen reitittimien lähettämät RA:t (Router Advertisiment Message) eli mainostusviestit sisältävät prefiksejä, jotka määräävät globaalin osoitteen. Liityntäportin link-local –osoite tulee automaattisesti luoduksi sen muokatusta EUI-64 liityntäportti-ID:stä. Samalla generoituu automaattisesti oletusreititin. [11.]

esim. `hostname(config-if)# ipv6 address autoconfig`

3) Link-local: tämä on linkkikohtainen osoite, joka voi olla samakin monessakin liityntäportissa. Link-local –osoite tulee luoduksi automaattisesti yhdessä muokatun EUI-64 –liityntäportti-ID:n kanssa. Tämä taasen perustuu portin dedikoituun MAC-osoitteeseen. Link-local voidaan luoda myös käsin, ellei porttiin haluta luoda mitään osoitetta, esimerkiksi unicastia. [11.]

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

IPv6 enable: tällä komennolla aktivoidaan suoraan liityntäportti noudattamaan IPv6:tta. Link-local –osoite generoituu automaattisesti käyttämällä muokattua EUI-64 liityntäportti-ID:tä. Tätä komentoa ei tarvita IPv6:n aktivoimiseen Cisco ASA –palomuureissa, jos jokin IPv6-osoite on jo luotu käsiteltävään porttiin. [11.]

esim. `hostname(config-if)# ipv6 enable`

4) EUI-64: EUI (Extended Unique Identifier) ja sen käytössä oleva muoto EUI-64 luo liityntärajapintaan 64-bittisen yksilöidyn porttitunnisteen. Portti-ID:stä eli MAC-osoitteesta saatu osoitteen loppuosa liitetään käsin tehtyyn IPv6-osoitteeseen ilman konfigurointia tai DHCP-palvelinta. [11.]

esim. `hostname(config-if)# ipv6 address 2001:c3a::/64 eui-64`

```
hostname# show ipv6 interface f0/0
Global unicast address(es):
2001:C3A::202:2DFF:FE01:BC01, subnet is 2001:C3A::/64[EUI/TEN]
```

5) IPv6 enforce EUI-64: EUI-64-tunniste voidaan pakottaa otettavaksi käyttöön paikallisissa linkeissä komennolla `enforce eui-64` linkin liityntäportissa. Liityntäportin tunnisteosa pitää olla 64 bittiä ja EUI-64 -formaatissa. Tällöin kaikki saapuvat paketit tarkistetaan ja lähdeosoitteen EUI-64 –osan on oltava yhtä MAC-osoitteen kanssa. Jollei vastaavuutta löydy, muodostetaan virheilmoitus ja paketti pudotetaan pois. [11.]

esim. `hostname(config-if)# ipv6 enforce-eui64 <interface_name>`
(<interface_name> on aiemmin täytynyt tulla määritetyksi nameif-komennolla, kun luotiin osoiteformaatti)

4.2 Palomuurien IPv6-liikenteen suodatus

Palomuurilaitteistoa, esimerkiksi Cisco ASA 5505, käyttöönotettaessa se estää kaiken liikenteen internetistä intranetiin (outboundista inboundiin). Käyttöönottoa pitää edeltää suunnitelma eli periaatteet tietoturvalle ja pääsyoikeuksille. Tällöin puhutaan suodatuksesta ja käytännössä se toteutetaan pääsylistoilla. Pääsylistat [10] pitää määritellä suunnitelman pohjalta, sillä oletuksena Cisco ASA:ssa ei ole minkäänlaisia pääsylistoja. Pääsylistat voi tehdä myös käänteisinä: avataan kaikki liikenne ja estetään tietty liikenne tai porttikohtaisesti kielletään esimerkiksi FTP-liikenne (File Transfer Protocol, tiedoston siirto). Tämä käytäntö tulee kyseeseen harvemmin – tuskin koskaan yritysmaailmassa. Johdonmukaisinta on, että pidetään kaikki liikenne estettynä ja avataan pääsylistoilla liikenneryhmille pääsy tarpeen tullen verkossa oleville tai siihen liitettäville laitteille ja palveluille. Tämä on tietoturvariskien kannalta turvallisin ja hallittavin tapa.

IPv4- ja IPv6-liikenteelle tehdään Cisco ASA:ssa liikenteen suodatusta varten kummallekin omat pääsylistansa [14, 15]. Määritellään erikseen inside- ja outside-portit palomuurin toiminnan hallitsemiseksi. Lähtökohtana on, että luotettavammasta verkosta liikenne sallitaan ulos ja epäluotettavammasta liikenne on estetty. Luonnollisesti inside-porttia pidetään luotettavuudeltaan korkea-arvoisempana ja se

saa arvon 100 ja outside-portin portin suojaustaso on 0. Tästä on pääteltävissä, että suojaustason arvonnosto tarkoittaa parempaa uskottavuutta verkon luotettavuudessa. Koska oletusarvoisesti kaikki sisään tuleva liikenne on estetty, täytyy pääsylistoilla avata liikennettä tarkoitusperien ja tietoturvapolitiikan puitteissa. Pääsylistojen luontien jälkeen ne täytyy asetuksilla liittää haluttuihin portteihin ja määrittää vielä vaikutussuunta (sisään tuleva – uloslähtevä). IPv6-pingit (menetelmä, jolla tarkistetaan, onko kohdelaite verkkoon kytketty) kannattaa sallia, ellei eri rajoitusta haluta. [16.]

Teknisesti IPv4- ja IPv6-pääsylistojen luonti ei poikkea toisistaan, mutta IPv6:n tapauksessa täytyy luontia tehdessä erikseen huolehtia, että ne ovat juuri IPv6-pääsylistoja. Niihin tehdyt määritykset eivät lainkaan koske IPv4-liikennettä. Proseduuri (toimenpide) on se, että määrätystä verkosta tietty liikenne sallitaan tai estetään määrättyyn verkkoon. Pääsylistoja täytyy tehdä sekä tulevaa että lähtevää liikennettä varten, sillä liityntäportit käsittelevät liikennettä kulkusuunnan mukaan. Hallittavuuden vuoksi enin osa liikenteiden pääsylistoista on syytä tehdä samalla pääsylistanimellä

Esim. `hostname(config)# ipv6 access-list acl_out deny tcp any host 3001:1::203:A0FF:FED6:162D eq ftp`

Erikseen voidaan siis estää tai sallia lähde- tai kohdeosoitteen liikenne host-asetuksella tapauskohtaisesti. Edellisestä esimerkistä havaitaan myös, että lisättäessä pääsylistan loppuun TCP-porttia kuvaava nimi tai sen numero, joka kertoo, saako se kyseisen liikenteen välitykseen luvan vai evätäänkö tämä toimenpide.

Esimerkissä pääsylistan nimi on ACL-out. tähän samaan listaan voidaan lisätä useampia määrityksiä, jotka koskevat tiettyä porttia, tiettyä suuntaa tai tiettyä liikennettä (esimerkiksi FTP , HTTP tai Telnet). Ne näkyvät palomuurin konfiguraatiossa omina riveinään. Pääsylistoja luodaan tarpeen mukaan eli liikennettä pitää sallia palomuurin yli. Kun pääsylistat on luotu, access-group –komennolla ne määritetään tiettyyn porttiin.

Esim. `hostname# access-group acl_in in interface outside`

Cisco ASA –palomuureissa myös ICMPv6-viestit on oletusarvoisesti estetty inboundiin. ICMPv6- eli IPv6-pingit saadaan toimimaan joko määrittämällä IPv6-pääsylista tälle protokollalle tai asettamalla suoraan liityntäporttiin ICMP-pääsylista. Tämä toimenpide

päätetään lisäämällä ICMP-inspection (ICMP-tarkistus) palomuuriin. Ilman sitä ICMP-liikenne ei edelleenkään kulje ASA:n läpi. [14.]

On muistettavaa, että tehtäessä pääsylistat suoraan liityntäportteihin tarkoituksena sallia ICPv6-viestit, eroavat ne normaaleista listoista siinä, että ne suodattavat liikennettä liityntäportteihin päin eivätkä liikennettä palomuurin läpi. Nämä käskyt ovat sallivia (oletusarvo on estää), joten erikseen muuta ICMPv6-liikennettä ei tarvitse estää.

esim. `hostname# ipv6 icmp permit any time-exceeded outside`

Vastaavanlaisia rivejä voi täten olla useampia alekkain (ICMPv6-viesteinä mm. echo, unreachable tai packet-too-big)

Lopuksi ICPv6-liikenteelle täytyy sallia tarkkailu (ICMPv6 Inspection), joka Cisco ASA:ssa on tilallista (Stateful Inspection) – aivan yhtäläisesti kuin TCP- tai UDP-liikenteelle. Tämä tehdään käyttäen asetusta policy-map. [RFC 4890.]

esim.

```
policy-map global_policy
class inspection_default
inspection icmp
```

4.3 Palomuurien IPv6-liikenteen reititys

Cisco ASA 5505 tukee monia IPv4-reititysprotokollia, mutta IPv6-ympäristössä ei dynaamista reititystä tueta [24]. Tällöin siis ainoaksi vaihtoehdoksi jää staattinen reititys ja oletusreitti. Ilman staattisia reittejä toisia IPv6-verkkoja ei tavoiteta. Jos kohdeosoite, joka saapuu palomuuriin inboundista, ei ole yksikään staattisista reiteistä, se ohjataan oletusreitille. Täten lähes poikkeuksetta reititysosoitteeksi muodostuu oletusreitti (jotta haluttu kohdeverkko saavutettaisiin).

Oletusreitti voidaan määritellä Cisco ASA –palomuureissa joko inside- tai outside-puolen liikenteelle. IPv4-verkkojen 0.0.0.0 –reittiä vastaa IPv6-ympäristössä ::/0. IPv6-oletusreitti määritetään komennolla

```
hostname(config)# ipv6 route if_name ::/0 <next_hop_ipv6_addr>
```

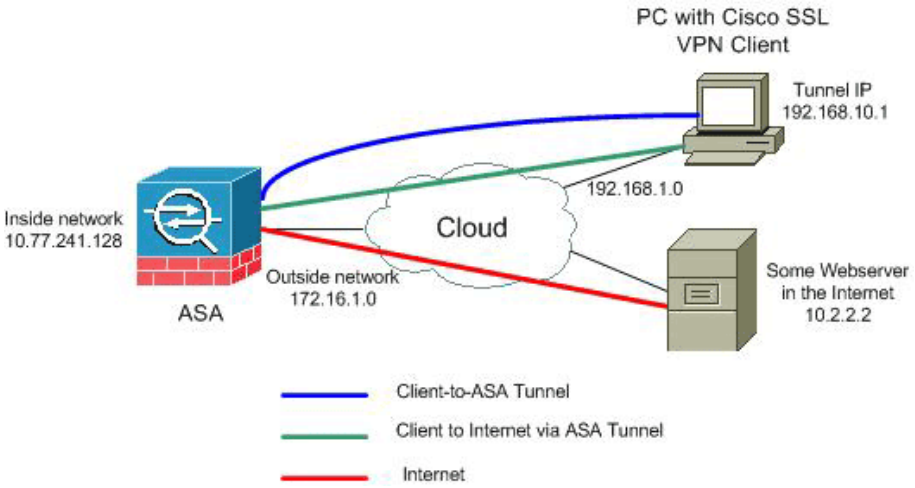
Staattiset IPv6-osoitteet asetetaan joko inside- tai outside-liityntäportteihin . Parametrina voi antaa maksimi hyppyjen määrän väliltä 1-255 tai määrittää tunneloinnin (tunneled). Tunneloidulle liikenteelle ei ole määritelty dedikoitua tai automaattista reittiä valmiiksi ja etäisyysarvoksi tulee aina 255

esim. `hostname# ipv6 route outside 2a00:4c21:101::/64 2a00:4c21:1e11::2 tunneled`

4.4 Palomuurien IPv6-tunnelit

Päästä päähän –mallissa tai kuten yleisemmin puhutaan LAN-to-LAN –tunneloinnista, käytetään pääsääntöisesti IPSec-protokollaa ja etäkäytössä SSL-salausprotokollaa (Secure Sockets Layer). LAN-to-LAN –tunneli voidaan muodostaa puhtaasti alkuperäisenä (engl. native, natiivi) IPv6-tunnelina ilman muunnoksia, mutta SSL VPN:ää ei täysin siihen kykene, vaan IPv6-liikenne täytyy tunneloida IPv4-verkon läpi suojattuun IPV6-ympäristöön. Cisco ASA –laitteiden viimeisimmätkään versiot eivät pysty native-tilaan. [13.]

Pelkistetysti kuvattuna SSL VPN:ää [13] voisi oikeastaan pitää HTML-pohjaisena hallintaliittymänä, jolla Cisco ASA –palomuureissa luodaan VPN-tunneleita. Etätyöasemalta on määritettävissä tunneli suljettuun verkkoon ilman pääkäyttäjän tekemiä määrityksiä. ASA-palomuurin on sijaittava suljetun verkon, intranetin edustalla (kuva 18.) ja siihen on asennettu SSL VPN sekä luotu tunneli sen ja asiakkaan (etäkäyttäjän) välille. Määritellyt tunnelit ovat käytettävissä sisäänkirjautuen käyttämällä tiedossaan olevaa WebVPN IP-osoitetta, jonka etäkäyttäjä kirjoittaa selaimen osoiteriville. Vasteeksi hän saa sisäänkirjautumisikkunan. Etäkäyttäjälle siirretään suljetun verkon IPv6-osoite SSL-tunnelin kautta, jolla hän pääsee liikennöimään intranetiin. IP-osoitteen kirjoittamisen jälkeen käynnistyvät sisäänkirjausrutiinit (kysytään ryhmää, käyttäjänimeä ja salasanaa) ja lopuksi aukeaa hallinnoiva graafinen liittymä. Toinen tapa on käyttää etäkoneeseen asennettua Ciscon AnyConnect-ohjelmistoa. Ellei sitä ole asennettuna, sen saa ASA – palomuurista ladattua SSL VPN –yhteyden muodostamisen jälkeen (laitteen hallinnassa oma valittava automaattiasennus).



Kuva 18. SSL VPN Client eli SVC-sovellus IPv4:ssä [17]

Käyttämällä AnyConnectia jää selainosuus pois, sillä Windowsin Käynnistä -palkkiin on ilmestynyt kuvake, jolla tunnelin muodostaminen on helpompaa.

SSL (Secure Sockets Layer on VPN-tunnelointiin tarkoitettu salausprotokolla, jonka nimi on nyttemmin muuttunut TLS:ksi [RFC 5246]. SSL käyttää IP-liikenteessä HTTPS-protokollaa (TCP-portti 443), jolla suojataan etenkin WWW-sivujen siirtoa. Nyttemmin SSL suojaa muutakin TCP-porttien liikennettä, kuten mm. SMTP-, POP-, IMAP-, LDAP- ja IRC-yhteyksiä. SSL perustuu varmenteisiin, joilla sivustot todistavat olevansa tarkistettuja ja oikealla asialla. Teknisesti SSL/TLS:n käyttämien yhteyksien suojauksen hoitaa kuljetuskerros. [18.]

Monessa yhteydessä on jo tullut mainituksi, että päästä päähän –mallissa on käytetyin tunnelointi LAN-to-LAN IPSec. Tällöin tunneli ulottuu suojattuun verkkoon kummassakin käyttöpäässä. Cisco ASA –laitteiden uusimmissa käytössä olevissa versioissa IPv6 VPN:n native-tila on tuettu LAN-to-LAN IPsecille – ei edelleenkään millekään muulle. Teoriassa ja varmasti käytännössäkin vastapäiden ASA-palomuurilaitteiden pitää olla samanlaiset. Tällöin saadaan transparentti (läpinäkyvä, esteetön) yhteys joko pelkästään IPv6-osoitteilla - sisäverkon käyttäessä IPv4:ää ja runkoyhteyden ollessa IPv6-maailmassa tai päinvastoin. Joka tapauksessa sisäverkoissa täytyy olla saman luokan osoitteet. [12.]

Aikoinaan lähdettäessä suunnittelemaan IP-protokollaa ei ollut edes tarvetta suojata jokaista kuljetettua datapakettia ja siksi lisäyksiä on hyväksytty ja otettu käyttöön protokollassa. IETF (Internet Engineering Task Force, avoin kansainvälinen järjestö) on

määritellyt IPSecin, joka on käytännössä joukko protokollia, jotka mahdollistavat käyttäjän tunnistuksen ja suojatut palvelut IP-kerroksessa. On korostettava, että IETF päätti tehdä järjestelmästä joustavan ja laajennettavan sen sijaan, että olisi tarkoin määritellyt käytettävät toiminnot ja salakirjoitusalgoritmit. Esimerkiksi IPSeciä käyttävä sovellus voi valita, käyttääkö se laillisuustarkistuksia, jolla tunnistetaan lähettäjä vai salataanko se, jolloin myös lähetettävät tiedot suojataan. Menetelmiä voidaan käyttää epäsymmetrisesti (laillisuustarkistus suoritetaan vain toisen lähteen osalta). IPSec tarjoaakin vain yleisen kehyksen ja kommunikoivat osapuolet voivat valita käyttämänsä algoritmit ja parametrit (esim. avaimen pituuden). Jotta yhteensopivuus voidaan taata, IPSec määrittelee joukon salausalgoritmeja, jotka kaikkien toteutusten on tunnistettava. Todennus, salaus ja luottamuksellisuus ovat IPSecin avainsanoja [16]. Tähän se tarjoaa ESP-otsikkoa (Encapsulation Security Payload) salaukseen ja luottamuksellisuuden tarkistukseen. Sen next-header arvo on 50 Rinnakkaiseen käyttöön on tarjolla AH-otsikko (Authentication Header), joka toteuttaa todennuksen ja takaa viestien eheyden (next-header arvo on 51). Nämä otsikot voivat olla käytössä yhdessä tai vain toinen niistä. IPv6:ssa ESP ja AH [19] toteutetaan lisäotsikoissa, kun taas IPv4:ssä ne ovat IP-protokollan otsikoita. IPSec:ssä on liuta pakollisia suojausalgoritmeja, jotka erityisesti koskevat ESP:iä. ESP on mukautunut käyttämään myös joitakin muotoja HMAC:sta (Hash-based Message Authentication Code) (kuva 19.).

Tunnistus	
HMAC ja MD5	RFC 2403
HMAC ja SHA-1	RFC 2404
ESP (Encapsulating Security Payload)	
DES CBC-tilassa	RFC 2405
HMAC ja MD5	RFC 2403
HMAC ja SHA-1	RFC 2404
Ei todennusta	
Ei salakirjoittamista	

Kuva 19. IPSecin pakolliset suojausalgoritmit [20]

Kuva 20. AH-otsikko [21]

Merkittävää on, että AH käyttää yhteydetöntä paketin eheydentarkistusta. Se riittää, jotta lähteiden todennus ja pakettien yhteneväisyys tulevat selvitettyä ja taattua. Molemmat otsikot perustuvat IKE:een (Internet Key Exchange, salausavainten vaihtomenetelmä), jotta symmetriset avaimet tulisivat suojatusti vaihdettua. IPSec-tunneleiden molempien päiden täytyy siinä mielessä synkronoituja eli millainen

- todennusalgoritmi
- todennusavain
- salausalgoritmi ja
- salausavain

on käytössä ja millaisella intervallilla ne päivitetään.

IKE koostuu protokollien ISAKMP (Internet Security Association and Key Management Protocol), Oakley ja SKEME (Secure Key Management Exchange for Internet) yhdistelmästä. IKE:stä on olemassa versiot 1 ja 2. IKEv1:ssä on käytössä UDP:n portti 500 ja se vaihtaa kahdessa vaiheessa salausalgoritmin ja avainmateriaalin. Ensin avataan kanava tiedonvaihtoa varten, joko normaalissa (Main Mode) tai aggressiivisessa (Aggressive Mode) tilassa. Ensin mainitussa tehdään kolme kaksisuuntaista vaihtoa - hitaasti ja turvallisesti ja jälkimmäisessä taasen vaaditaan vähemmän paketteja ja toimitaan nopeasti. Vaiheessa kaksi neuvotellaan IPSec – salausalgoritmit sekä muutama parametri ja avaimet tai sertifikaatit (käytössä yhteyden muodostuksessa). Nämä salauskättelyt ovat sijoitettuna SPD-tietokantaan (Secure Policy Database). Molemmissa päissä pitää olla sama tietokanta. Tietokanta sisältää tiedot algoritmeista, avaimista, IP-osoitteista ja avainten voimassaoloajoista – tärkeää tunnelin aktivoimisessa. [22.]

Kun tunnelin hyväksymiskättely on onnistunut eli salaustavat ja avaimet on lyöty lukkoon molemmissa tunnelin päissä, muodostuu SA-yhteys (Security Associations,

salauskäytännön attribuuttien vaihto). IKEv1:ssä ne pitää muodostua molempiin suuntiin, molempiin vaiheisiin ja ESP- sekä AH-protokollille. Siksi tarvitaan kaksi SA:ta IKEv1:n 1-vaiheeseen ja neljä täydelliseen IPSec-yhteyteen.

IKEv1 on havaittu kasvaneen monimutkaiseksi ja se oli aika korvata versio kahdella. Kehittyneemmässä versiossa yleensä karsitaan pois ja yksinkertaistetaan. Näkyvin muutos ja joidenkin tahojen mielestä parannus on aggressiivisen tilan poisjättö. Se alkoi muodostua tietoturvariskiksi. IKEv2:ssa on vain normaali ja nopea tila (Quick Mode). Ensimmäinen on neljän paketin mittainen ja jälkimmäisessä siirretään vain kaksi pakettia. Kättely on vain yksivaiheinen ja yksisuuntainen eli neuvotellaan tunnelin toisen pään kanssa, jonka jälkeen muodostetaan vain yhdet SA:t molempiin päihin sekä luodaan avaimet vaihtoehtoisesti ESP:lle tiai AH:lle. [23.]

5 JOHTOPÄÄTÖKSET

Reuna-alueen laitteina monet VPN-laitteet (varsinkin etäkäyttösovelluksille tarkoitetut) ovat työlistalla viimeisinä yrityksen verkosta vastaavalle. Avainasemassa on yhteensopivuuden varmistaminen niiden todennus-, nimeämis- ja osoitepalvelimien kanssa, jotka tukevat VPN-sovellusta. Ei sovi unohtaa, että etäkäyttöasiakkaat voivat yhä tavoittaa kaikki ne kaksinkertaisella IP-pinolla varustetut isäntäkoneet, jotka ovat sellaisiksi muutettu siirtymävaihetta luotaessa.

Summa summarum: IPv6:ssa tuetaan suoraan LANien välistä sovellusta. Voiko yritys sitten käyttää tätä ominaisuutta, riippuu pitkälti operaattorin eli palveluntarjoajan runkoyhteyden IPv6-valmiuksista. Useamman maan runkoyhteysoperaattorit ovat olleet mukana kokeellisessa IPv6-verkossa – 6Bone [RFC 2546], joka on elinkaarensa lopussa. Alunperin kysyttäessä tätä Soneran Yritysverkoista Anne Vuorisalolta ja Elisalta (Yritysverkot) asiantuntija Asko Kalliolta ei yksiselitteistä vastausta saatu [27]. Erittäin suurella todennäköisyydellä kummankin palveluntarjoajan oman verkon ydinalueet ovat jo täysin IPv6:ssa, mutta leviäminen reuna-alueille on hidasta työmäärän laajuuden ja kalleuden vuoksi, vaikka teknisesti se ei ole iso asia. Tunnelointi on tällä hetkellä tapa toimia ja sitä kumpikin ensisijaisesti tarjoaa. Minkään IPV6-osoitteistusta edellyttävän verkkosovelluksen käyttöönotolle VPN:ssä ei ole estettä. Täten opinnäytetyössä ei saavutettu suoraa ohjeistusta vaiheesta kaksi eteenpäin, kuten toimeksiannossa edellytettiin. Todettavissa kuitenkin on, että tietoturvariskit (kuten pyydettiin selvittämään) ovat kuten yleisesti IPv6:ssa tiedetään olevan: IPv6 ei ole yhtään turvallisempi kuin IPv4. Käsittääkseni MobileIP –hyökkäykset Cisco ASA –palomuureissa ovat uusi ilmiö. Muita arkoja alueita lienevät Dual Stack –pinoihin tulevat hyökkäykset ja luonnollisesti Stateless autoconfiguration-osoitteet (jos niitä jostakin syystä käytetään – ei suositeltavaa yritysmaailmassa).

Totaalinen verkottuminen ja uudenlainen identifiointi on jo aivan ovella - kuten futuristiset, mielenkiintoiset toteutukset, joista osa on jo toteutunut mm. biometriset tunnisteet: IP-osoitteen liittäminen henkilötunnukseen – ihonalainen siru tms.. Tämä ei ole enää tiedekirjallisuuden visiointia ja proosaa. Avainasemassa on se tosiasia, että IPv6 on automaattisesti julkinen, mikä on sen paras uudistus IPv4-sukupolveen verrattuna: jokainen laite saa globaalisen osoitteen automaattisesti eli operaattori ei voi jatkossa manipuloida verkko-osoitetta korvausperusteisesti – varaus, hallinta ja ylläpito - kuten IPv4-tekniikan aikana on ollut tähän asti tapana. Mahdollisuuksia on

suunnattomasti, mutta hallinnoitavaa on paljon ja ennen kaikkea tietoturvan puolesta on yritettävä pitää etumatka niihin, joille palomuuri on pelkkä haaste ja sen ohittaminen ajanviete. Onko IPv6 turvallisempi kuin IPv4 – sitä ei paljonpuhuttu IPSec voi millään taata, vaikka se monen mielestä tekee salatuista yhteyksistä hyvin varman. Yritysverkoissa globaalit osoitteet (operaattorilta anottavat) poistavat osoitemuunnokset niin haluttaessa lopullisesti, jolloin suora liikennöinti ilman ylimääräistä työtä (NAT) onnistuu. Ryhmälähetykset toimivat sovelluksissa tällöin päästä päähän ilman konversioita.

Toinenkin mahdollisuus on olemassa niille, jotka haluavat peittää verkkotopologian palomuurin IP-osoitteen taakse tietoturvanäkökantaansa vedoten: IPv6:ssa on hyödynnettävissä IPv4:n privaattiosoitteiden kaltaiset ULA-osoitteet (Unique Local Addressing [RFC 4193]. Nämä eivät ole reititettävissä internetiin. Globaaleja ja ULA-osoitteita ei kannattane käyttää rinnan – hallittavuuden kannalta. Pullonkaula on joka tapauksessa palomuuri siirtymävaiheen aikana – sen haavoittuvuus. Sen merkitystä ei saa unohtaa työtä aloittaessa, sitä tehdessä eikä sen jälkeenkään.

Lopuksi: eräs johtopäätös on myöskin se, että ns. ”pilvipalvelun” nimikkeellä asiakkaalle saatetaan myydä mitä tahansa ja ilman osaavaa, varauksetonta konsulttia tai yrityksestä löytyvää ITC-alan osaajaa (jota kuunnellaan) saatetaan tehdä hätiköityjä tai turhia – jopa harhaan meneviä päätöksiä.

LÄHTEET

Kirjallisuus ja julkaistu materiaali

- Microsoft: Windows 2008 Server

Elektroniset lähteet

- [1] Net Academy: Cisco Systems, NetAcademy (CCNA1 – CCNA4 opiskelumateriaalit syksy 2008 – kevät 2009)
- [2] RFC-dokumentit: http://www.ietf.org/rfc.html (RFC-hakuautomaatti kaikille opinnäytetyössä mainituille RFC:ille)
- [3] Tunnelien poisto: http://features.techworld.com/networking/3667/ipv6-migration-tactics/
- [4] 6to4: http://en.wikipedia.org/wiki/6to4
- [5] Teredo: http://en.wikipedia.org/wiki/Teredo_tunneling
- [6] Isatap: http://en.wikipedia.org/wiki/ISATAP
- [7] NAT-PT: http://en.wikipedia.org/wiki/IPv6_transition_mechanisms (viitattu 29.11.2011)
- [8] IPv6-osoitetyypit: http://msdn.microsoft.com/en-us/library/ms880932.aspx (viitattu 29.11.2011)
- [9] IPSec-tunnelointi: http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf (viitattu 4.11.2011 ja 22.11.2011)
- [10] Pääsylistan lisäys:]http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/acl_ipv6.html (viitattu 29.11.2011)
- [11] IPv6-konfigurointi: http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/ipv6.html (viitattu 22.11.2011)
- [12]päästä päähän -IPSec: http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/vpn_site2site.html (viitattu 28.11.2011)
- [13] SSL VPN: http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htwebvpn.html (viitattu 30.11.2011)
- [14] IPv6 -perusteet: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con.html (viitattu 30.11.2011)
- [15] IPSec-suodatus, palomuurit: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-sec_trfltr_fw.html (viitattu 30.11.2011)
- [16] Suodatus ja pääsylistat: http://www.cisco.com/en/US/docs/security/asa/asa70/configuration/guide/intparam.html (viitattu 30.11.2011)
- [17] SSL VPN 2: http://www.cisco.com/en/US/products/ps6496/products_configuration_example09186a008096fcf5.shtml (viitattu 30.11.2011)

- [18] TLS: http://fi.wikipedia.org/wiki/TLS ja http://openmaniak.com/openvpn.php (viitattu 28.11.2011)
- [19] ESP ja AH: http://fi.wikipedia.org/wiki/IPsec (viitattu 30.11.2011)
- [20] ESP ja HMAC: https://supportforums.cisco.com/docs/DOC-1125#Complete_Definition (viitattu 28.11.2011)
- [21] AH: http://technet.microsoft.com/en-us/library/cc959540.aspx (viitattu 30.11.2011)
- [22] IKEv1: http://www.waset.org/journals/waset/v6/v6-46.pdf (viitattu 28.11.2011)
- [23] IKEv2: http://www.cs.ust.hk/faculty/cding/COMP685/SLIDES/slide23.pdf ja http://en.wikipedia.org/wiki/Internet_Key_Exchange (viitattu 30.11.2011)
- [24] Cisco ASA 5505: http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/ipv6.html (viitattu 23.11.2011)

Haastattelut ja luennot

- [25] Trivore: Trivore Oy: toimitusjohtaja Kari Mattsson (useampaan otteeseen, mm. 24.3.2009; 3.3., 9.4., 19.10.2010)
- [26] CCNA-luennot: Turun AMK, Salon yksikkö: tuntiopettaja Mika Silvennoinen, CCNA1-CCNA4 –luennot (syksy 2008-kevät 2009)
- [27] Operaattorit: Telia-Sonera Oy, Yritysverkot: Anne Vuorisalo, puhelinkeskustelut 2.9.ja 9.9.2010, Elisa Oy, Yrityspalvelut: Asko Kallio, puhelinkeskustelu 8.11.2010