FI0001104648

(12) **PATENTTIJULKAISU**
PATENTSKRIFT

(10) **FI 110464 B**

(45) Patentti myönnetty - Patent beviljats **31.01.2003**

(51) Kv.lk.7 - Int.kl.7
H04L 29/06

(21) Patenttihakemus - Patentansökning **20010876**

(22) Hakemispäivä - Ansökningsdag **26.04.2001**

(24) Alkupäivä - Löpdag **26.04.2001**

(41) Tullut julkiseksi - Blivit offentlig **27.10.2002**

SUOMI – FINLAND
(FI)

PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN

(73) Haltija - Innehavare

1 •Nokia Corporation, Helsinki, Keilalahdentie 4, 02150 Espoo, SUOMI - FINLAND, (FI)

(72) Keksijä - Uppfinnare

1 •Haverinen,Henry, Arkkitehdinkatu 15 A 3, 33720 Tampere, SUOMI - FINLAND, (FI)
2 •Honkanen,Jukka-Pekka, Aleksanterinkatu 17 A 46, 33100 Tampere, SUOMI - FINLAND, (FI)
3 •Kuikka,Antti, Kattilaistentie 28 D 17, 33960 Pirkkala, SUOMI - FINLAND, (FI)

(74) Asiamies - Ombud: Papula Oy
Fredrikinkatu 61 A, 6.krs, 00100 Helsinki

(54) Keksinnön nimitys - Uppfinningens benämning

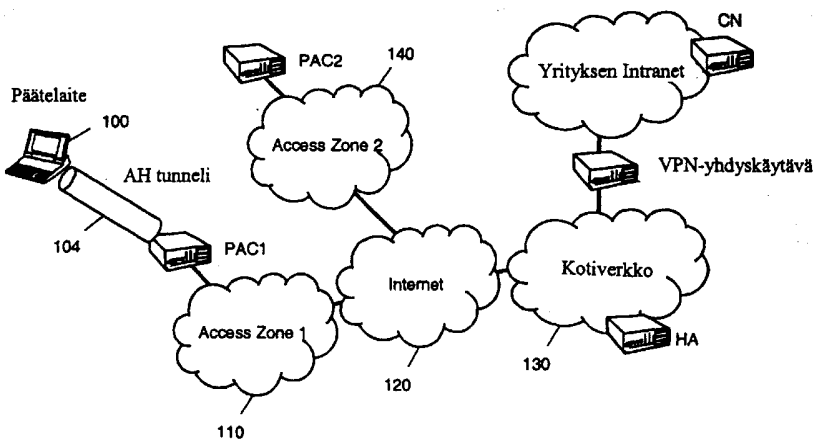
IP-tietoturva ja liikkuvat verkkoyhteydet
IP-säkerhet och mobila nätförbindelser

(56) Viitejulkaisut - Anförda publikationer

US A 2001/0047474 (H04L 9/00), WO A 0143329 (H04L), WO A 0154379 (H04L 29/06)

(57) Tiivistelmä - Sammandrag

Keksintö esittelee menetelmän, jolla paketteja siirretään matkaviestinpäätelaitteen (100) ja lähtösolmun välillä useiden itsenäisten tietoverkkojen kautta ja samalla taataan turvallinen yhteys. Itsenäisiin verkkoihin voi sisältyä esimerkiksi Internet (120), paikalliset Access Zone -vyöhykkeet (110,140), yhtiön Intranetit ja kotiverkko (130). Ongelmia saattaa tulla esimerkiksi silloin, kun liikkuva solmu käyttää yhteissijainnissa olevaa toista osoitetta, jolloin suoritetaan sekä IP-in-IP- että IPsec-tunnelointimuutos, ja nykyiset IPsec- ja IP-in-IP-toteutukset eivät pysty suorittamaan vaadittavia tunnelointitoimintoja matkaviestinterminaalissa. Tämä johtuu IP-in-IP- ja IPsec-tunneloinnista, kun IP-in-IP-tunneli ei ole uloin muunnos. Keksinnön eräässä suoritusmuodossa matkaviestinterminaalin käyttämä turvamenettely sisältää ensisijaisen turvamenettelyn ja dynaamisen toissijaisen turvamenettelyn, jotka soveltavat valikoiden määritettyjä muunnoksia tiettyihin paketteihin tiedonsiirron aikana.



Uppfinningen presenterar en metod med vilken paket överförs mellan en mobilterminal (100) och en startnod via flera självständiga datanät och med vilken en säker förbindelse samtidigt garanteras. De självständiga näten kan omfatta till exempel Internet (120), lokala accesszoner (110, 140), ett bolags Intränat samt hemnät (130). Problem kan uppstå till exempel när en mobil nod använder en samlokaliserad annan adress, varvid såväl IP-in-IP- som IPsec-tunnlingsändring utförs och de nuvarande IPsec- och IP-in-IP-utförandena inte kan utföra de krävda tunnlingsfunktionerna i mobilterminalen. Detta beror på IP-in-IP- och IPsec-tunnlingen, då IP-in-IP-tunneln inte är den yttersta förändringen. I en av uppfinningens utförandeformer innehåller det av mobilterminalen utnyttjade säkerhetsförfarandet ett primärt säkerhetsförfarande och ett dynamiskt sekundärt säkerhetsförfarande, vilka selektivt tillämpar definierade förändringar på vissa paket under dataöverföringen.

IP-TIETOTURVA JA LIIKKUVAT VERKKOYHTEYDET

KEKSINNÖN KOHDE

Esillä oleva keksintö liittyy yleisesti matkaviestinverkkoyhteyksiin ja erityisesti IP-tietoturvaa sekä yhteyksiä koskeviin menettelyihin.

KEKSINNÖN TAUSTA

Internetin ja sen osan WWW:n (World Wide Web) edut verkossa olevan laajan tietomäärän hyödyntämisessä tunnustetaan laajalti. Internetiin on perinteisesti muodostettu yhteys kiinteistä liityntäpisteistä, esimerkiksi työpaikalta, koulusta tai kotoa. Kiinteiden liityntäpisteiden käsite on ollut Internet-mallin perustana alusta lähtien. Esimerkiksi IP-protokolla reitittää paketit oikeisiin kohteisiin IP-osoitteiden mukaisesti. IP-osoitteet liitetään kiinteään fyysiseen paikkaan paljolti samalla tavalla kuin perinteiset puhelinnumerot liitetään lankapuhelinten fyysiseen sijaintiin. Tämän ansiosta IP-paketit voidaan reitittää aiottuun määränpäähän virheettömästi ja tehokkaasti.

Perinteinen yhteyskäsite on muuttunut liikkuvuuden lisääntyessä. Tämä on tullut esiin viime vuosina esimerkiksi matkapuhelinten käytön yleistyessä. Kannettavien tietokoneiden käyttö on toinen yhä suositumpi alue, jossa saadaan aikaan selviä etuja, jos käyttäjät pystyvät tekemään työtä paikasta riippumatta. Luotettavan Internet-yhteyden ansiosta liikkuvat verkkoyhteydet lisäävät myös kaikkien käyttäjien tuottavuutta, koska käyttäjät eivät ole enää sidottuja työpaikoilleen. Nykyisin ollaan yhä useammin siirtymässä langattomiin yhteyksiin, jotka tuovat lisää vapautta tarjoamalla yhteysmahdollisuuksia ajasta ja paikasta riippumatta, esimerkiksi lentokoneissa ja autoissa.

Perinteinen Internet-malli, jossa käytetään kiinteitä osoitteita, tekee kuitenkin Internetin saumattoman ja luotettavan käytön matkaviestinlaitteilla hieman ongelmalliseksi. Tämä johtuu siitä, että kun matkaviestinlaite muodostaa yhteyden uuteen verkkoon tai liityntäpisteeseen, uuteen verkkoon yhdistetyn IP-osoitteen kautta matkaviestinlaitteelle muodostuu uusi IP-osoite. Näin ollen alkuperäiseen IP-osoitteeseen kohdistetut paketit

eivät välity uuteen IP-osoitteeseen. Näihin ongelmiin on esitetty ratkaisuksi muun muassa Mobile IP:tä (RFC2002). Mobile IP on IETF (Internet Engineering Task Force) -ohjeistossa ehdotettu standardi, jolla liikkuvien yhteyksien ongelma ratkaistaan niin, että matkaviestinlaitteella on kaksi IP-osoitetta: kotiosoite ja toinen osoite, joka muuttuu aina uuden liityntäpisteen myötä. Mobile IP:n perusajatus on se, että se mahdollistaa saumattoman vierailun eri verkoissa. Matkaviestinlaitteeseen lähetetyt paketit pystyvät kulkemaan määränpäähänsä oikein huolimatta siitä, mihin verkkoon laite on kytkeytynyt.

Tyypillisesti lähtösolmusta lähtevät paketit kulkevat kohdesolmuun niin, että ne reititetään saapuvista verkkorajapinnoista lähteviin rajapintoihin reititystaulujen avulla. Reititystaulut sisältävät tietoja seuraavasta hypystä kuhunkin IP-kohdeosoitteeseen. Paketit voivat edetä matkaviestinlaitteeseen staattisen kotiosoitteen avulla, joka antaa sen vaikutelman, että liikkuva solmu pystyy jatkuvasti vastaanottamaan tietoja kotiverkossaan. Tällöin käytetään kotiagenttiverkkosolmua, joka noutaa liikkuvaan solmuun osoitetut paketit ja välittää ne solmun toiseen osoitteeseen, kun solmu on kytkeytyneenä vieraaseen verkkoon. Koska toinen osoite muuttuu aina uuden verkon kiinnityspisteen myötä, kotiagentin on tunnettava kyseiset tiedot, jotta se pystyisi ohjaamaan paketit uudelleen. Tämän vuoksi toinen osoite rekisteröidään kotiagenttinsa mukana aina, kun liikkuva solmu siirtyy tai saa uuden IP-osoitteen.

Pakettien toimittaminen liikkuvaan solmuun edellyttää, että paketti muotoillaan niin, että toinen osoite on IP-kohdeosoite pakettimuunnoksena tunnetussa prosessissa. Liikkuvalle solmulle määritetty uusi otsikko muodostuu muunnoksessa, jossa alkuperäinen paketti kapseloidaan (tätä kutsutaan myös tunneloinniksi) niin, että kotiverkko ei vaikuta reititykseen, kunnes paketti on turvallisesti perillä liikkuvassa solmussa. Määränpäässä pakettiin sovelletaan käänteistä muunnosta niin, että liikkuvan solmun kotiosoite näyttää olevan paketin kohdeosoitteena, jotta siirtoprotokolla, esimerkiksi TCP (Transmission Control Protocol) pystyy käsittelemään pakettia oikein. Vierasta agenttia käytetään tyypillisesti purkamaan sellaisten pakettien kapselointi, jotka on vastaanotettu kotiagentilta välitettäviksi liikkuvaan solmuun.

Edellä on kuvattu IP-tunneloinnin perusmuoto. Mobile IP kuitenkin tukee tyypillisesti kolmea tunnelointimekanismia: IP-kapselointi IP:n sisällä (RFC 2003), minimaalinen

kapselointi IP:n sisällä (RFC 2004) ja GRE (Generic Routing Encapsulation, RFC 1701). Usean IP-tunnelointimekanismin toteutusta kutsutaan IP-in-IP-tunneloinniksi. Näitä IP-in-IP-tunnelointimekanismeja voidaan käyttää paitsi Mobile IP:n kanssa myös tilanteissa, joissa on toivottavaa esimerkiksi yhdistää yksityisiä osoitetiloja käyttäviä verkkoja Internetin kautta tai tunneloida monijakeluliikennettä tunnelointia tukemattoman verkon kautta.

Mobile IP:ssä tärkeimpiä huolenaiheita on tietoturva. Internet on luonteeltaan avoin, joten lähetetyt paketit altistuvat turvariskeille. Niitä lisää entisestään liikkuvien solmujen liikkuminen aliverkkojen välillä. Turvariskeihin liittyen kehitettiin IP-turvaprotokolla eli IPsec (esitetty RFC2401:ssä) tuottamaan päästä-päähän-tietoturvaa pakettihyötykuormaa varten IP-terminaalien välisessä siirrossa. Tämä voidaan saavuttaa pääasiassa niin, että terminaaleille tuotetaan pakettien tietosähketasoinen tunnistus ja salaus, tyypillisesti käyttämällä symmetristä salakirjoitustekniikkaa, jossa samoja avaimia on käytettävä molemmissa päissä. Avainten hallintaprotokollalla (esimerkiksi IKE) voidaan luoda symmetriset avaimet käytettäviksi IPsec-pinossa, esimerkiksi samanlaiset, joita käytetään VPN-verkoissa.

IPseciä käyttävä terminaali pitää yllä tietoturvamenettelyä SPD (Security Policy Database) -tietokannassa, kuten on esitetty esimerkiksi RFC2401:ssä. SPD tunnistaa, millaista tietoturvaa liikenteeseen sovelletaan; esimerkiksi IPsec-menettely voi edellyttää, että kaikki liikenteessä olevat paketit tunneloidaan ESP (Encapsulating Security Payload) -hyötykuormalla VPN-yhdyskäytävään lukuun ottamatta tiettyjä paketteja, jotka pääsevät läpi ilman IP-käsittelyä. Tässä kuvatun kaltaista turvamenettelyesimerkkiä käytetään kaikkiin paketteihin, jotka kulkevat terminaalin solmun läpi. Koska turvamenettely on tyypillisesti staattinen ja konfiguroitu terminaaliin verkko-ohjelmiston asennuksen aikana, eräät yhteysnäkymät tuottavat erityisiä hankaluuksia käytettäessä staattisesti konfiguroitua turvamenettelyä. Asiaa voidaan selventää seuraavalla esimerkillä: jos matkaviestinterminaali vierailee vieraassa verkossa, jossa on IPsec-turvayhdyskäytävä vierailun kohteena olevan verkon ja kotiagentin välillä, ja jos liikkuva solmu käyttää yhteisessä sijainnissa olevaa toista osoitetta (jolloin sen on suoritettava sekä IP-in-IP- että IPsec-tunnelointi), nykyiset IPsec- ja IP-in-IP -toteutukset eivät pysty suorittamaan tarvittavia

matkaviestinterminaalin tunnelointitoimintoja. Tämä johtuu IP-in-IP- ja IPsec-tunneloinnista, kun IP-in-IP-tunneli ei ole uloin muunnos.

Nykyisissä käyttöjärjestelmissä IP-in-IP-tunnelit konfiguroidaan tyypillisesti näennäisinä verkkorajapintoina. Jos liikenteeseen tarvitaan IP-in-IP-tunnelointia, tällöin luodaan reititystaulutietue, joka reitittää liikenteen näennäiseen tunnelointirajapintaan. Koska reititystaulua sovelletaan protokollapinossa IPsec-menettelyn alapuolella, tämän toteutuksen takia IP-in-IP-tunneloinnin on aina oltava ulommainen muunnos paketille. Tämä ei ole kuitenkaan aina toivottava toimenpide. Jos esimerkiksi liikkuva solmu, joka käyttää yhteisessä sijainnissa olevaa toista osoitetta, haluaa AH (Authentication Header- eli tunnistusotsikkotunneli) -tunneloida kaiken liikenteen oletusyhdyskäytävään (yhteysreititin), AH-tunneloinnin tulisi olla ulommainen muunnos ja IP-in-IP-tunneloinnin toiseksi ulommainen muunnos, jotta paketti voidaan elvyttää.

Edellä esitetyn valossa keksinnön tavoitteena on tarjota tekniikka, jossa puututaan onnistuneesti aiempien toteutusten puutteisiin, jotka liittyvät IP-tietoturvaan sekä pakettien reititykseen liikkuviin solmuihin ja niistä pois.

YHTEENVETO KEKSINNÖSTÄ

Lyhyesti kuvattu ja keksinnön suoritusmuodon sekä siihen liittyvien ominaisuuksien mukainen menetelmä, jossa menetelmäaspektin mukaisesti paketit lähetetään ja vastaanotetaan turvallisessa yhteydessä ensimmäisen ja toisen verkkosolmun välillä. Menetelmän mukaisesti kyseisiä paketteja voidaan siirtää useissa itsenäisissä tietoverkoissa ensimmäisen ja toisen verkkosolmun välisellä polulla, ja ensimmäinen verkkosolmu ja kukin tietoverkko voivat noudattaa eri turvamenettelyjä, jotka määrittävät paketteihin sovellettavia tiettyjä muunnoksia; kyseinen menetelmä on **tunnettu siitä, että** ensimmäinen verkkosolmu pystyy dynaamisesti muuttamaan turvamenettelyään niin, että paketteihin sovelletaan sopivia muunnoksia turvallisen yhteyden ylläpitämiseksi.

Laiteaspektin mukainen matkaviestinlaite pystyy muodostamaan yhteyden verkon kanssa ja siinä on tiedonsiirtoa koskeva turvamenettely, jonka mukaan paketteja

siirretään matkaviestinlaitteeseen ja siitä pois. Kyseinen tiedonsiirron turvamenettely käsittää:

ensimmäisen muunnossarjan, joka liittyy ensisijaiseen turvamenettelyyn, jota sovelletaan siirrettyihin paketteihin

toisen muunnossarjan, joka liittyy toissijaiseen turvamenettelyyn, jota sovelletaan sopivalla tavalla siirrettyihin paketteihin.

KUVIEN LYHYT ESITTELY

Keksintö sekä siihen liittyvät muut tavoitteet ja edut ovat ehkä helpoimmin ymmärrettävissä viittaamalla seuraavaan kuvaukseen, johon liittyvissä kuvissa:

Kuviossa 1 on esimerkki käyttötavasta, joka ei sovi yhteen aiempien toteutusten kanssa.

Kuviossa 2 on esitetty aiempien toteutusten mukainen TCP/IP-pino IPseciä käyttävässä terminaalissa.

Kuviossa 3 on esimerkki käyttötavasta seuraavasta IP-paketista.

Kuviossa 4 on esitetty protokollapino, joka toimii keksinnön erään suoritusmuodon mukaisesti.

Kuviossa 5 on esitetty reititystaulutietueiden käyttö keksinnön erään vaihtoehtoisen suoritusmuodon mukaisesti.

Kuviossa 6 on esitetty kuvion 5 reititystaulusuoritusmuodon laajennus.

Kuviossa 7a on esitetty IPsec-käsittely lähtevälle liikenteelle keksinnön suoritusmuodon mukaisesti.

Kuvio 7b on jatke kuviolle 7a suoritusmuodon mukaisesta lähtevästä liikenteestä.

Kuviossa 8 on esitetty IPsec-käsittely saapuvalle liikenteelle keksinnön suoritusmuodon mukaisesti.

YKSITYISKOHTAINEN KUVAUS KEKSINNÖSTÄ

Kuviossa 1 on esitetty esimerkkinä käyttötapa, jota ei voida käyttää perinteisessä staattisessa IP-turvamenettelytoteutuksessa. Selvennyksen vuoksi näin voi käydä esimerkiksi silloin, kun käyttäjä yrittää muodostaa yhteyden yhtiönsä Intranet-verkkoon kannettavalla päätelaitteella muualta kuin toimistosta käsin. Yhteyden on ehkä kuljettava useiden erillisten liityntävyöhykkeiden ja -verkkojen kautta, joista jokainen saattaa noudattaa eri turvamenettelyä. Tällöin paketin käänteiset muunnokset eivät ole yhteensopivia. Päätelaite 100 muodostaa esitetyllä tavalla yhteyden Internetiin 120 Access Zone -vyöhykkeen 1 110 kautta. Tämän seurauksena päätelaitteen 100 ja lähimmän reitittimen PAC1 (Public Access Controller 1) välille muodostuu IPsec AH tunneli 104. AH-tunnelin päätarkoituksena on estää tunnistamattomia käyttäjiä käyttämästä päätelaitteen IP-osoitetta pakettien lähettämiseen Internetiin.

Liikkuva toiminnallisuus voidaan mahdollistaa käyttämällä Mobile IP:tä liityntävyöhykkeiden välisiin tai esimerkiksi WLAN-liityntävyöhykkeen ja langattoman GPRS-tietoverkon välisiin tukiaseman vaihtoihin. Mobile IP käyttää tyypillisesti IP-in-IP-tunnelia päätelaitteen nykyisen toisen osoitteen ja kotiagentin (HA) välillä. Kun päätelaite 100 haluaa yhteyden vertaissolmun (CN) tarjoamiin yhtiön tietoihin, tämä tapahtuisi normaalisti VPN-yhdyskäytävän kautta. VPN-yhdyskäytävälle voidaan toteuttaa oma turvamenettely, esimerkiksi IPsec ESP (Encapsulating Security Payload) -tunneli päätelaitteen kotiosoitteen 100 ja VPN-yhdyskäytävän välille. Kannettavan päätelaitteen 100 vieraillessa toisessa verkossa tapahtuu tukiaseman vaihto, jossa muodostuu AH-tunneli reitittimen PAC2 (Public Access Controller 2) kanssa. Näin saadaan yhteys yhtiön Intranetiin Access Zone -vyöhykkeen 2 140 kautta vertaissolmuun. IP-paketit, jotka kulkevat CN-vertaissolmun ja liikkuvan solmun välillä, käyvät läpi useita muunnoksia, jotka noudattavat voimassa olevia useita turvamenettelyjä. Tämän tuloksena voi muodostua sekä IP-in-IP- että IPsec-tunneleita. Tällöin IP-in-IP-tunneli ei ole ulommainen muunnos, mikä aiheuttaa voi hankaluuksia pakettien elvyttämisessä, kun aikaisemmilla toteutuksilla yritetään purkaa Mobile IP:n IP-in-IP-tunnelien kapselointi ennen muita IPsec-kapselointien purkamista.

Kuviossa 2 on esitetty aiempien toteutusten mukainen TCP/IP-pino IPseciä käyttävässä terminaalissa. IP-in-IP-tunnelointi on toteutettu näennäisenä verkkolaitteena. Reititystaulutietue voi ohjata lähtevän liikenteen IP-in-IP-tunnelilaitteeseen. Saapuvaa liikennettä varten IP-in-IP-tunnelointi poistetaan ennen kuin paketti luovutetaan IPsec-menettelyyn. IPsec-muunnokset tehdään kuviossa esitetyllä tavalla reitityksen yläpuolella niin, että IP-in-IP-tunnelointimuunnos on aina ulommainen muunnos. Toisin sanoen tuloksena syntyvä IP-in-IP-tunnelointiotsikko on aina ulommainen IP-otsikko, mikä aiheuttaa ongelmia, kun paketti yritetään elvyttää tekemällä muunnokset käänteisesti.

Kuviossa 3 on esitetty esimerkkinä, miltä tuloksena oleva IP-paketti näyttää liikkuvassa solmussa, kun siihen on sovellettu asiaan liittyvien verkkojen erilaisia turvamenettelyjä. Ulommainen muunnos on kuviossa 1 esitetty AH-tunneli 104, joka käsittää IP-otsikon 300 päätelaitteen nykyisen toisen osoitteen ja PAC:n välillä. AH-tunnelissa 305 on Mobile IP:n IP-in-IP-tunneli päätelaitteen nykyisen toisen osoitteen ja kotiagentin (HA) välillä käsittäen IP-otsikon 310. AH-tunneli saattaa käsittää erilaisia prosesseja, esimerkiksi tarkistussumma- ja tunnistuskoodit paketin tietoturvan varmistamiseksi. IP-in-IP-tunnelin sisällä on lisäksi VPN-tunneli päätelaitteen kotiosoitteen ja VPN-yhdyskäytävän välillä käsittäen IP-otsikon 320. VPN-tunnelissa on alkuperäinen IP-paketti, joka käsittää otsikon 330 ja hyötykuorman 340, joka siirtyy päätelaitteen kotiverkon ja vertaissolmun välillä. VPN-yhdyskäytävän turvamenettely voi määrittää ESP (Encapsulating Security Payload) -hyötykuorman kaikille vertaissolmusta tuleville paketeille, kuten viitenumero 325 osoittaa. Tämän vuoksi AH-tunneloinnin tulisi välttämättä olla ulommainen muunnos ja IP-in-IP-tunneloinnin toiseksi ulommainen muunnos. Otsikkorakenteesta käy selvästi ilmi, että IP-in-IP-tunnelointimuunnos ei ole ulommainen muunnos, ja näin ollen aiempien toteutusten mukainen TCP/IP-pino ei pysty elvyttämään pakettia kunnolla.

Keksinnön mukaisesti edellä mainittu ongelma voidaan korjata tekemällä IP-in-IP-tunnelointi niin, että se on osa IPsec-käsittelyä. Tämä voidaan tehdä toteuttamalla dynaaminen IPsec-strategia, joka sallii useiden turvamenettelyjen soveltamisen, jolloin erilaisia käsittelyjä voidaan soveltaa erilaiseen liikenteeseen. Keksinnön eräässä suoritusmuodossa IPsec-toteutus ylläpitää kahta turvamenettelytietokantaa (SPD):

ensisijaista SPD-tietokantaa VPN:ää ja dynaamista toissijaista SPD-tietokantaa Mobile IP:tä varten.

Kuviossa 4 on esitetty protokollapino, joka toimii keksinnön erään suoritusmuodon mukaisesti. Suoritusmuodon proseduurissa IP-in-IP-tunnelointimuunnos pystytään lisäämään IPsec-muunnosten väliin, koska IP-in-IP-tunnelointi toteutetaan toissijaisessa IPsec-menettelyssä eikä osana IP-reititystä. Tällöin käänteiset muunnokset voidaan tehdä oikeassa järjestyksessä. Edullisessa suoritusmuodossa ensisijainen menettely konfiguroidaan niin, että kukin ensisijainen SPD-tietue sisältää lipun, joka määrittää, sovelletaanko toissijaista menettelyä paketteihin. Koska toissijainen menettely on ensisijaisen alapuolella protokollapinossa, tällöin lähtevään liikenteeseen sovelletaan ensisijaista menettelyä ennen toissijaista. Saapuvaan liikenteeseen sovelletaan puolestaan toissijaista menettelyä ennen ensisijaista. Toissijainen menettely voidaan konfiguroida dynaamisesti kannettavan tietokoneen liikkuvalla ohjelmistolla, joka saattaa määrittää esimerkiksi, että liikenne on AH-tunneloitava yhteysreitittimeen nykyisellä liityntävyöhykkeellä. Ensi- ja toissijaisten turvamenettelyjen yläpuolella protokollapinossa toimivat korkeamman tason siirtoprotokollat, esimerkiksi TCP tai UDP (User Datagram Protocol) sekä niiden päällä käytettävät sovellukset.

Kuviossa 5 on esitetty eräs keksinnön vaihtoehtoinen suoritusmuoto. Siinä reititystaulua on laajennettu tietueilla, jotka pystyvät välittämään lähtevän paketin takaisin IPsec-käsittelyyn. Tässä tapauksessa IPsec-menettelyn ensimmäisessä ajossa sovelletaan kaikkia staattisia (ensisijaisia) IPsec-muunnoksia, esimerkiksi VPN-muunnosta. Lähtevässä liikenteessä liikkuva ohjelmisto voi dynaamisesti konfiguroida reititystaulun. Tässä suoritusmuodossa liikkuva ohjelmisto voi määrittää IP-in-IP-tunneleita reititystauluun. Taulussa voi olla tietueita, jotka vaativat IPsec-menettelyn ajamista uudelleen. Jos pakettiin sovelletaan IP-in-IP-tunnelointia, silloin IPsec-menettelyn eri säännöt voivat soveltua toisen ajon aikana. IPsec-menettelyn toisessa ajossa sovelletaan kaikkia dynaamisia (toissijaisia) muunnoksia. Saapuvassa liikenteessä käänteiset muunnokset tarkistetaan ja mukautetaan paikalliseen IPsec-menettelyyn, ja tällöin tarkistuksessa voidaan ottaa huomioon paikallisen IP-in-IP-tunneloinnin konfigurointi ja reititystaulu.

Kuviossa 6 on esitetty reititystaulun lisälaajennus kuvion 5 mukaiseen vaihtoehtoiseen suoritusmuotoon. Tässä suoritusmuodossa turvamenettely on jaettu kahteen osaan: ensisijaiseen turvamenettelyyn IPseciä varten ja toissijaiseen menettelyyn liikkuvaa ohjelmistoa varten. Loogisesti erotellun toissijaisen menettelyn etu on siinä, että ajon aikaiset muutokset eivät vaaranna ensisijaista menettelyä. Toissijaista menettelyä voidaan soveltaa pakettiin, jos reititystaulu ilmoittaa sen tarpeelliseksi. Tämä voidaan tehdä esimerkiksi attribuutilla, vaikkapa lipulla, joka lisätään reititystaulutietueeseen osoittamaan, että tällainen toimenpide on tarpeen.

Keksinnön mukaisesti protokollapinon toiminta tuottaa tulokseksi erilaisia proseduureja lähtevien ja saapuvien IP-pakettien käsittelyyn lähtöverkon ja sovelluksen näkökulmasta.

Lähtevä käsittely

Kuviossa 7a on esitetty IPsec-käsittely lähtevälle liikenteelle keksinnön suoritusmuodon mukaisesti. Esimerkkipaketti saapuu lähdesovelluksesta siirtoprotokollan, esimerkiksi TCP:n kautta vaiheessa 700 esitetyllä tavalla. Vaiheessa 702 toiminta alkaa vaadittavien muunnosten etsimisellä ensisijaisesta lähtevästä SPD-tietokannasta. Kun etsintä on suoritettu, tämän jälkeen määritetään, tarvitaanko IPSec-käsittelyä, vaiheessa 704 esitetyllä tavalla. Jos ensisijaisia muunnoksia ei tarvita, paketti tarkistetaan ja määritetään, vaatiiko toissijainen menettely käsittelyn vaiheessa 724. Jos osumia ei löydy tai jos menettely vaatii paketin pudottamista, paketti hylätään tässä kohtaa vaiheessa 708. Jos löytyy SPD-osuma, joka vaatii IPsec-käsittelyn, lähtevässä SAD (Security Association Database) -tietokannassa suoritetaan haku vaiheessa 710.

SPD (Security Policy Database) -tietokanta sisältää menettelyjä, jotka määrittävät, miten tietyt paketit on käsiteltävä. SAD-tietokannan turvakäytännöt sisältävät parametrit, joita tarvitaan menettelyn sanelemien toimintojen suorittamiseen. Esimerkkiparametrit sisältävät erilaisia kohteita, esimerkiksi salaus- ja tunnistusavaimia. Turvakäytännöt merkitään kokonaislukutunnisteella, jota kutsutaan SPI (Security Parameter Index) -indeksiksi. Tämä numero sisältyy IPsec-otsikoihin (AH ja ESP), ja sen avulla tehdään haku SAD-tietokannasta lähtevien pakettien käsittelyssä, jolloin (lähtevässä käsittelyssä) sopivaa turvakäytäntöä (SA) etsitään

vastaavan turvamenettelyn perusteella. Tyypillisesti avaimenhallintaprotokolla, esimerkiksi IKE (Internet Key Exchange), joka on IPsecin avaimenhallinnan vakioprotokolla, luo turvakäytännöt dynaamisesti. Turvakäytäntö vaaditaan aina, ennen kuin IPsec-muunnosta voidaan soveltaa. IP-in-IP-muunnoksissa ei tarvita avaimia, SPI-indeksejä tai muita parametreja, eli näihin muunnoksiin ei tarvita SAD-tietuetta, jos ne toteutetaan IPsec-menettelyssä.

Vaiheessa 712 tehdään tarkistus, jolla määritetään, löytyykö SAD-tietokannasta osumaa. Jos osuma löytyy, IPsec suorittaa turvamenettelyssä määritetyn IPsec-muunnoksen käyttämällä turvakäytännön parametreja vaiheessa 718 esitetyllä tavalla. Jos SAD:sta ei löydy osumaa, turvakäytäntö (Security Association eli SA) luodaan avaimenhallintakokonaisuudella, esimerkiksi IKE-protokollalla, vaiheessa 714 esitetyllä tavalla. Jos SA-turvakäytännön luominen epäonnistui tarkistuksen jälkeen vaiheessa 716, paketti hylätään vaiheessa 720 esitetyllä tavalla. Jos SA-turvakäytännön luominen onnistuu, muunnos voidaan aloittaa vaiheessa 718. Koska turvakäytäntöjä ei tarvita IP-in-IP-kapseloinnin purkamismuunnoksiin, SAD-hakua (vaihe 710) ei välttämättä tarvita SPD-tietueisiin, jotka määrittävät IP-in-IP-muunnokset. Kun tällainen menettely löytyy vaiheessa 704, toiminto voi suoraan edetä vaiheeseen 718 ja muunnos voidaan suorittaa. Vaihtoehtoisesti toteutus voi käyttää "täyteturvakäytäntöjä" IP-in-IP-muunnoksiin, jolloin IPsec- ja IP-in-IP-käsittelyt ovat samanlaiset. Ensisijainen SPD määrittää tyypillisesti vain varsinaisia IPsec-muunnoksia, ei IP-in-IP-muunnoksia. Vaiheessa 722 tehdään tarkistus lisämuunnosten tarpeen selvittämiseksi. Jos lisämuunnoksia tarvitaan, SAD-haku toistetaan vaiheessa 710. Kun kaikkia ensisijaisia muunnoksia on sovellettu, tämän jälkeen tarkistetaan, vaatiiko ensisijainen menettely toissijaisen menettelyn käsittelyä vaiheessa 724 esitetyllä tavalla.

Kuvio 7b on jatkoa kuvioon 7a, ja siinä toissijaisen käsittelyn osalta tarkistettu paketti välitetään vaiheessa 746 liikkuvaan solmuun, mikäli toissijaista käsittelyä ei tarvita. Jos toissijainen käsittely tarvitaan, toissijaisessa SPD-tietokannassa tehdään haku vaiheessa 726. Jos osumia ei löydy tai toissijainen menettely vaatii pudottamaan paketin, paketti hylätään vaiheessa 730. Jos osuma löytyy, suoritetaan haku lähtevästä SAD-tietokannasta vaiheessa 732. Joskus saattaa käydä niin, että toissijainen SPD-tietue vastaa hakua mutta ei vaadi käsittelyä. Tätä tapausta ei ole kuitenkaan esitetty yksikäsitteisesti. Tässä tapauksessa paketti välitetään vaiheeseen 746. Kuten

ensisijaisessa SPD-käsittelyssä, IP-in-IP-muunnoksiin ei tarvita turvakäytäntöä, ja näin ollen nämä muunnokset voidaan tehdä ilman SAD-tietokantahakua. IPsec-muunnoksissa tehdään aina tarkistus, jonka avulla määritetään, löytyikö lähtevästä SAD-tietokannasta osumaa vaiheessa 734. Muunnos suoritetaan vaiheessa 742. Jos lähtevästä SAD:sta ei löydy osumaa, turvakäytäntö (Security Association eli SA) luodaan avaimenhallintakokonaisuudella vaiheessa 736 esitetyllä tavalla. Jos SA-turvakäytännön luominen epäonnistui tarkistuksen jälkeen (vaiheessa 738), paketti hylätään vaiheessa 740. Jos SA-turvakäytännön luominen onnistuu, IPsec-muunnos pääsee alkuun vaiheessa 742. Vaiheessa 744 tarkistetaan, tarvitaanko lisää toissijaisen menettelyn tekemiä muunnoksia. Jos muunnoksia tarvitaan, toiminto palaa vaiheeseen 732. Jos muunnoksia ei tarvita lisää, paketti siirretään verkkoon vaiheessa 746 esitetyllä tavalla.

Keksinnön suoritusmuodossa IPsec-toteutukselle annetaan lupa suorittaa IP-in-IP-tunnelointi, kun taas aiemmissa toteutuksissa IPsec ei suorita IP-in-IP-tunnelointia. Ensisijaisen SPD:n tietueisiin on lisätty lippu, joka osoittaa, tarvitaanko toissijaista IPsec-käsittelyä paketeille, jotka vastaavat ensisijaisen SPD:n tietuetta. Kun lippu lisätään, IPsec-toteutus etenee toissijaisella käsittelyllä sen jälkeen, kun kaikki ensisijaisen SPD:n vaatimat IPsec-muunnokset on tehty. Jos lippua ei lisätä, toissijaista IPsec-käsittelyä ei tehdä. Tällöin IPsec-käsittely on samanlainen kuin aiempien toteutusten mukainen käsittelytoiminta. Jos toissijainen IPsec-käsittely tarvitaan, tällöin IPsec-toteutus suorittaa IPsec-muunnokset toissijaisen SPD:n vaatimalla tavalla.

Saapuva käsittely

Kuviossa 8 on esitetty IPsec-käsittely saapuvalle liikenteelle keksinnön mukaisesti. Vaiheessa 800 on esitetty verkosta vastaanotettu paketti. Vaiheessa 805 ulommaisesta otsikosta tarkistetaan, onko se IP-in-IP- tai IPsec-otsikko. Jos ulommainen otsikko ei ole IP-in-IP- tai IPsec-otsikko, käsittely jatkuu vaiheessa 830. Jos ulommainen otsikko on IP-in-IP- tai IPsec-otsikko, SAD:sta haetaan turvakäytäntöä vaiheessa 807. SAD-haku vaaditaan aina, kun muunnos on IPsec-muunnos (AH tai ESP). IP-in-IP-muunnoksissa turvakäytäntöjä ei välttämättä tarvita, joskin toteutus saattaa käyttää "täyteturvakäytäntöä", jotta käsittely olisi samanlainen IPsec- ja IP-in-IP-muunnoksissa.

Vaiheessa 810 tehdään tarkistus, jotta saataisiin selville, löytyykö osumia. Jos osumia ei löydy, paketti hylätään vaiheessa 815 osoitetulla tavalla. Jos osuma löytyy, IPsec suorittaa muunnoksen vaiheessa 820, ja samalla käytetyt turvakäytännöt (tai IP-in-IP-muunnokset, jotka tehdään ilman turvakäytäntöjä) ja niiden soveltamisjärjestys pannaan merkille. Vaiheessa 805 tarkistetaan, onko IPsec- ja/tai IP-in-IP-otsikoita jäljellä. Jos on, vaiheen 807 saapuva SAD-haku toistetaan. Jos otsikoita ei ole jäljellä, ensisijainen saapuva SPD tarkistetaan vaiheessa 830, jotta voitaisiin määrittää, onko tarvittavia muunnoksia sovellettu. Tämä vaihe on esitetty vaiheessa 835. Jos vastaavaa menettelyä ei löydy, paketti hylätään vaiheessa 840 osoitetulla tavalla. Jos vastaavuus löytyy, vaiheessa 845 tehdään tarkistus, jotta voitaisiin määrittää, vastaako nykyinen ensisijainen SPD-tietue sovellettua käsittelyä kokonaan tai osittain. Jos nykyinen ensisijainen SPD-tietue vastaa sovellettua käsittelyä kokonaan ja jos se ei vaadi toissijaista menettelyä, paketti lähetetään tarkistukseen, jossa määritetään kohdeterminaali, vaiheessa 860.

Jos nykyinen ensisijainen saapuva SPD-tietue vastaa sovellettua käsittelyä kokonaan tai osittain sekä vaatii toissijaisen menettelyn käyttöä, toissijaiseen saapuvaan SPD-tietokantaan tehdään haku, jotta voitaisiin määrittää, onko olemassa toissijaista saapuva SPD-tietuetta, joka vastaa sovellettua käsittelyä muilta osin, vaiheessa 850 esitetyllä tavalla. Jos ensisijaisen menettelyn tietue vastaa jo nykyisellään sovellettua käsittelyä kokonaan, tällöin on pakko olla myös toissijainen menettely, joka ei vaadi muunnoksia. Vaiheessa 855 tehdään tarkistus, jotta voitaisiin määrittää, vastaako sovellettu käsittely muilta osin toissijaista SPD-tietuetta. Jos vastaavaa toissijaista menettelyä ei löydy, ensisijainen saapuva SPD tarkistetaan jälleen vaiheessa 830. Ensisijaisen saapuvan SPD:n tarkistaminen jatkuu seuraavasta tarkistamattomasta menettelystä.

Keksinnön suoritusmuodon mukaisesti toimiva saapuva käsittely suorittaa käänteiset IPsec- ja IP-in-IP-muunnokset, jotka se havaitsee pakettien otsikoissa, SAD:n parametrien mukaisesti. Vaihtoehtoisesti toteutus voi suorittaa IP-in-IP-muunnoksia ilman vastaavaa SAD-tietuetta. Keksinnön mukaisesti IP-in-IP-tunnelointi on sallittu muunnos, toisin kuin aiemmissa toteutuksissa. Kun kaikki IP-in-IP- ja IPsec-otsikot on käsitelty, IPsec-toteutukset tarkistavat, että paketti vastaa SPD:tä. Tämän jälkeen

ensisijainen menettely tarkistetaan, ja tietueista tarkistetaan, vastaavatko ne sovellettua käsittelyä.

Jos ensisijaisen SPD:n tietue vastaa sovellettua käsittelyä ja tietue ei vaadi toissijaista menettelyä, tällöin IPsec-toteutus luovuttaa paketin ylempiin protokollakerroksiin tai välittää sen.

Toisaalta jos ensisijaisen SPD:n tietue vastaa sovellettua käsittelyä kokonaan ja tietue vaatii toissijaisen menettelyn, tällöin IPsec-toteutus tarkistaa, onko olemassa toissijaista menettelyä, joka ei vaadi käsittelyä. Jos ensisijaisen SPD:n tietue vastaa sovellettua käsittelyä osittain ja tietue vaatii toissijaisen menettelyn, IPsec-toteutus tarkistaa, onko olemassa toissijaista menettelyä, joka vastaa sovellettua menettelyä muilta osin, toisin sanoen sitä osuutta, jota ensisijainen SPD-tietue ei kata. Jos toissijaisesta SPD:stä löytyy osuma, IPsec-toteutus luovuttaa tämän jälkeen paketin ylempiin protokollakerroksiin tai välittää sen. Jos vastaavaa toissijaista menettelyä ei löydy, IPsec-toteutus jatkaa ensisijaisen SPD:n kääntämistä.

On syytä huomata, että suoritusmuodossa kuvatut ensi- ja toissijaiset turvamenettelytietokannat (SPD) ovat käsittellisiä tietorakenteita. Alan asiantuntijat tietävät, että varsinaisen toteutuksen ei välttämättä tarvitse sisältää kahta erillistä tietokantaa vaan ne voivat käyttää yhtä tietokantaa, jonka tietueet sisältävät esimerkiksi SPD-indeksikentän, joka osoittaa, kuuluuko tietue ensi- vai toissijaiseen SPD:hen. Tällainen toteutus voidaan yleistää tukemaan useampaa kuin kahta SPD:tä edellyttäen esimerkiksi, että indeksin arvot ovat muut kuin 1 ja 2. Lisäksi IPsec-toteutus voisi *rekursiivisesti soveltaa SPD-tietueita nousevalla indeksillä.*

Vaikka esillä olevaa keksintöä on kuvattu joiltakin osin viitaten sen tiettyyn suoritusmuotoon, alan asiantuntijat ymmärtävät siihen liittyvät variaatiot ja muunnelmat. Siksi seuraavien patenttivaatimusten tulkintaa ei tule rajoittaa, vaan niihin tulee lukea mukaan variaatiot ja muunnelmat, jotka on johdettu esillä olevasta keksinnön aiheesta.

PATENTTIVAATIMUKSET

1. Menetelmä, jossa paketit lähetetään ja vastaanotetaan turvallisessa yhteydessä ensimmäisen ja toisen verkkosolmun välillä. Menetelmän mukaisesti kyseisiä paketteja voidaan siirtää useissa itsenäisissä tietoverkoissa ensimmäisen ja toisen verkkosolmun välisellä polulla, ja ensimmäinen verkkosolmu ja kukin tietoverkko voivat noudattaa eri turvamenettelyjä, jotka määrittävät paketteihin sovellettavia tiettyjä muunnoksia; kyseinen menetelmä on **tunnettu siitä, että** ensimmäinen verkkosolmu pystyy dynaamisesti muuttamaan turvamenettelyään niin, että paketteihin sovelletaan sopivaa muunnosta turvallisen yhteyden ylläpitämiseksi.

2. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu siitä, että** ensimmäinen verkkosolmu on liikkuva verkkosolmu ja toinen verkkosolmu on lähtösolmu; menetelmässä liikkuva verkkosolmu sisältää SPD (Security Policy Database) - tietokannan, jonka käsittämiä erilaisia turvamenettelyjä voidaan dynamisesti soveltaa yhteyden kautta kulkeviin paketteihin.

3. Minkä tahansa edeltävän patenttivaatimuksen mukainen menetelmä, **tunnettu siitä, että** ensimmäisen verkkosolmun turvamenettely käsittää ensi- ja toissijaisen SPD:n; tällöin ensisijainen SPD sisältää tietueita ensisijaisen turvamenettelyn mukaisiin muunnoksiin ja toissijainen SPD sisältää tietueita toissijaisen turvamenettelyn mukaisiin muunnoksiin.

4. Minkä tahansa edeltävän patenttivaatimuksen mukainen menetelmä, **tunnettu siitä, että** ensisijaisen SPD:n tietueisiin lisätään attribuutti, joka osoittaa, että toissijaista turvamenettelyä on käytettävä, voidaan käyttää tai ei saa käyttää paketteihin.

5. Minkä tahansa edeltävän patenttivaatimuksen mukainen menetelmä, **tunnettu siitä, että** ensisijainen SPD sisältää tietueita "sisäisiä" muunnoksia (sisäisiä otsikoita) varten ja toissijainen SPD sisältää tietueita "ulkoisia" muunnoksia varten, ja lähteviin paketteihin suoritetaan sisäisiä muunnoksia ennen ulkoisia ja saapuvaan liikenteeseen päinvastoin.

6. Minkä tahansa edeltävän patenttivaatimuksen mukainen menetelmä, **tunnettu siitä, että** toissijainen menetelmä määrittää lisämuunnoksia, kun lähtevään liikenteeseen on sovellettu kaikkia ensisijaisen menettelyn muunnoksia.

7. Menetelmä, jossa saapuva liikenne käsitellään käänteisessä järjestyksessä vaatimukseen 6 verrattuna.

8. Minkä tahansa edeltävän patenttivaatimuksen mukainen menetelmä, **tunnettu siitä, että** ensi- ja toissijaiset menettelyt voidaan konfiguroida itsenäisesti ja yhtä aikaa, jolloin menettelyjen muokkaaminen voidaan rajoittaa vain toiseen tai molempiin.

9. Minkä tahansa edeltävän patenttivaatimuksen mukainen menetelmä, **tunnettu siitä, että** ensisijainen turvamenettely pysyy muuttumattomana ja toissijainen turvamenettely konfiguroidaan niin, että sitä sovelletaan valikoiden tiettyihin paketteihin.

10. Minkä tahansa edeltävän patenttivaatimuksen mukainen menetelmä, **tunnettu siitä, että** muunnostoiminnot sisältävät paketin muunnoksia, esimerkiksi protokollaotsikoiden tai vaihtoehtojen lisäämistä ja poistamista, pakettien kapselointia ja kapseloinnin purkamista uusien pakettien sisällä, pakettien tai niiden osien salausta ja salauksen purkamista tai pakettien tai niiden osien pakkaamista ja pakkauksen purkamista.

11. Patenttivaatimuksen 10 mukainen menetelmä, **tunnettu siitä, että** muunnostoiminnot sisältävät siirtotilamuunnoksia, joissa käytetään AH (Authentication Header) -tunnistusotsikkoa ja ESP (Encapsulating Security Payload) -hyötykuormaa, sekä IP-in-IP-tunneleiden, AH-tunneleiden ja ESP-tunneleiden kapselointia ja kapseloinnin purkamista.

12. Patenttivaatimuksen 2 mukainen menetelmä, **tunnettu siitä, että** liikkuva verkkosolmu muodostaa verkkoyhteyden käyttämällä esimerkiksi Mobile IP:tä paikallisesti määritellyn Access Zone -vyöhykkeen kanssa muodostettavan

yhteyden kautta; tällöin Access Zone -vyöhyke tukee verkkovierailua vaihtamalla yhteyden toiseen Access Zone -vyöhykkeeseen.

13. Minkä tahansa edeltävän patenttivaatimuksen mukainen menetelmä, **tunnettu siitä, että** itsenäisiin verkkoihin sisältyy Internet, paikalliset Intranetit, kotiverkot, paikalliset Access Zone -vyöhykkeet ja tietoliikenneverkot, esimerkiksi langattomat ja ei-langattomat verkot.

14. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu siitä, että** verkkojen (tai solmujen) turvamenettelyt koskevat paketteihin tehtäviä erityisiä muunnoksia, kun paketit siirretään verkojen (tai solmujen) läpi; menetelmässä paketteihin sovellettavat sopivat muunnokset perustuvat kyseisiin muunnoksiin, joita on sovellettu niin, että kyseiset muunnokset käännetään käytännössä niin, että paketin hyötykuormatiedot voidaan elvyttää.

15. Matkaviestinlaite, joka pystyy muodostamaan yhteyden verkon kanssa ja jossa on tiedonsiirtoa koskeva turvamenettely, jonka mukaan paketteja siirretään matkaviestinlaitteeseen sekä siitä pois. Tiedonsiirron turvamenettely käsittää:

ensimmäisen muunnossarjan, joka liittyy ensisijaiseen turvamenettelyyn, jotka sovelletaan siirrettyihin paketteihin

toisen muunnossarjan, joka liittyy toissijaiseen turvamenettelyyn, jota sovelletaan sopivalla tavalla ja valikoiden tiettyihin paketteihin.

16. Patenttivaatimuksen 15 mukainen matkaviestinlaite, jossa ensisijainen turvamenettely on sellainen, joka määrittää tiettyjen pakettien käsittelyn, ja toissijainen turvamenetely on sellainen, joka määrittää tiettyjen muiden pakettien käsittelyn.

17. Patenttivaatimuksen 15 mukainen matkaviestinlaite, jossa ensisijaisen turvamenettelyn muunnostietueet sisältävät attribuutin, esimerkiksi, mutta siihen rajoittumatta, lippuosan, joka osoittaa, että toissijaista turvamenettelyä on käytettävä, voidaan käyttää tai ei saa käyttää paketteihin.

18. Patenttivaatimuksen 15 mukainen matkaviestinlaite, jossa matkaviestinlaitteen yhteys Internetiin siirtää paketit siirtokerroksen, esimerkiksi TCP:n tai UDP:n päällä.

PATENTKRAV

1. Metod med vilken paket sänds och mottas i en säker förbindelse mellan första och andra nätnoden. I enlighet med metoden kan ifrågavarande paket överföras genom flera självständiga informationsnät på vägen mellan den första och den andra nätnoden, och första nätnoden och vart och ett informationsnät kan följa olika säkerhetsförfaranden, vilka bestämmer vissa förändringar för tillämpande på paketerna; den ifrågavarande metoden är **kännetecknad därav att** den första nätnoden kan dynamiskt ändra sitt säkerhetsförfarandet så att en lämplig förändring tillämpas paketerna för upprätthållande av en säker förbindelse.

2. Metod enligt patentkrav 1, **kännetecknad därav att** den första nätnoden är en rörlig nätnod och den andra nätnoden är en startnod; i metoden innehåller den rörliga nätnoden en SPD (Security Policy Database) –databas, vilken innefattar olika säkerhetsförfaranden som kan dynamiskt tillämpas på paketen som löper via förbindelsen.

3. Metod enligt något av de föregående patentkraven, **kännetecknad därav att** den första nätnodens säkerhetsförfarande innefattar en primär och en sekundär SPD; varvid den primära SPD:n innehåller post för förändringar i enlighet med det primära säkerhetsförfarandet och den sekundära SPD:n innehåller post för förändringar i enlighet med det sekundära säkerhetsförfarandet.

4. Metod enligt något av de föregående patentkraven, **kännetecknad därav att** till den primära SPD:s post tilläggs ett attribut, vilket påvisar att det sekundära säkerhetsförfarandet bör användas, kan användas eller får inte användas på paketerna.

5. Metod enligt något av de föregående patentkraven, **kännetecknad därav att** den primära SPD:n innehåller post för "inre" förändringar (inre rubriker) och den sekundära SPD:n innehåller post för "yttre" förändringar, och på de avgående paketerna utförs inre förändringar före yttre och på inkommande trafik tvärtom.

6. Metod enligt något av de föregående patentkraven, **kännetecknad därav att** det sekundära förfarandet bestämmer tilläggsförändringar, efter att alla primära förfarandets förändringar tillämpats på den avgående trafiken.

7. Metod med vilken den inkommande trafiken behandlas i omvänd ordningsföljd jämfört med patentkrav 6.

8. Metod enligt något av de föregående patentkraven, **kännetecknad därav att** de primära och sekundära förfaranden kan konfigureras självständigt och samtidigt, varvid redigerandet av förfaranden kan begränsas till bara den ena eller till båda.

9. Metod enligt något av de föregående patentkraven, **kännetecknad därav att** det primära säkerhetsförfarandet förblir oförändrat och det sekundära säkerhetsförfarandet konfigureras så att det tillämpas selektivt på vissa paket.

10. Metod enligt något av de föregående patentkraven, **kännetecknad därav att** förändringsfunktionerna innehåller paketens förändringar, till exempel tilläggande och avlägsnande av protokollrubriker eller alternativ, kapslande och hävande av kapslande av paket inom nya paket, kryptering och hävande av kryptering av paket eller delar av dessa eller packande och hävande av packande av paket eller delar av dessa.

11. Metod enligt patentkrav 10, **kännetecknad därav att** förändringsfunktionerna innehåller överföringstillståndsförändringar, i vilka AH (Authentication Header) – identifieringsrubriken och ESP (Encapsulating Security Payload) –nyttolast, samt kapslande och hävande av kapslande av IP-in-IP-tunnlarna, AH-tunnlarna och ESP-tunnlarna används.

12. Metod enligt patentkrav 2, **kännetecknad därav att** den rörliga nätnoden bildar en nätförbindelse genom användande av till exempel Mobile IP i förbindelse med den lokalt bestämda Access Zone –zonen, varvid Access Zone –zonen stöder nätbesökandet genom att byta förbindelsen till en annan Access Zone –zon.

13. Metod enligt något av de föregående patentkraven, **kännetecknad därav att** de självständiga näten innefattar Internet, lokala Intranät, hemnäten, lokala Access Zone –zoner och datakommunikationsnäten, till exempel trådlösa och icke-trådlösa nät.

14. Metod enligt patentkrav 1, **kännetecknad därav att** nätens (eller nodernas) säkerhetsförfaranden gäller speciella förändringar som görs på paketen, då paketen överförs genom näten (eller nodarna); i metoden grundar sig de på paketerna tillämpbara lämpliga förändringarna på de ifrågavarande förändringarna, vilka är tillämpade så att de ifrågavarande förändringarna inverteras i praktiken så, att paketernas nyttolastinformation kan upplivas.

15. En mobilterminal, vilken kan bilda en förbindelse med nätet och vari det finns ett säkerhetsförfarande gällande dataöverföring, enligt vilket paket överförs till mobilterminalen och därifrån bort. Dataöverföringens säkerhetsförfarande innefattar:

en första förändringsserie, vilken anknyter sig till det primära säkerhetsförfarandet, vilken tillämpas på de överförda paketen

en andra förändringsserie, vilken anknyter sig till det sekundära säkerhetsförfarandet, vilken på ett lämpligt sätt och selektivt tillämpas på vissa paket.

16. En mobilterminal enligt patentkrav 15, vari det primära säkerhetsförfarandet är sådant som bestämmer behandlingen av vissa paket, och det sekundära säkerhetsförfarandet är sådant som bestämmer behandlingen av vissa andra paket.

17. En mobilterminal enligt patentkrav 15, vari det primära säkerhetsförfarandets förändringsposter innehåller ett attribut, till exempel, men inte begränsande till det, en flaggbit, vilket påvisar att det sekundära säkerhetsförfarandet bör användas, kan användas eller får inte användas på paketen.

18. En mobilterminal enligt patentkrav 15, vari mobilterminalens förbindelse med Internet överför paketerna på ett transportskikt, till exempel på TCP eller UDP.

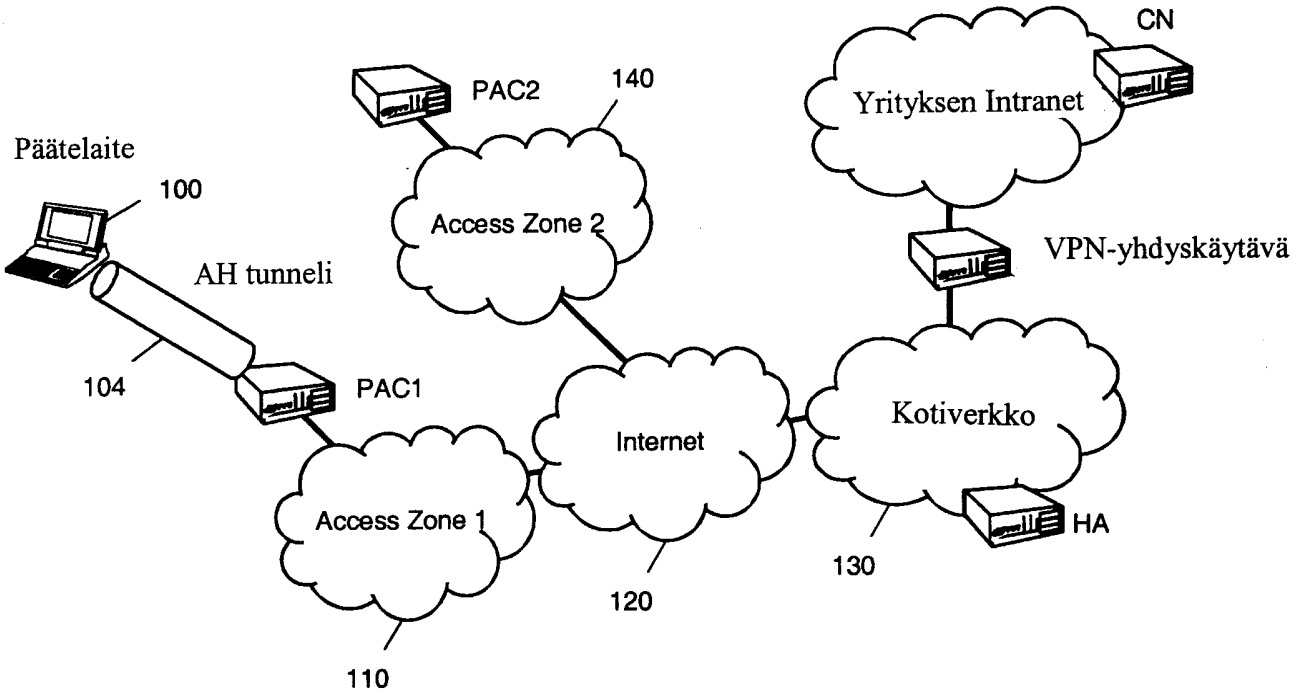
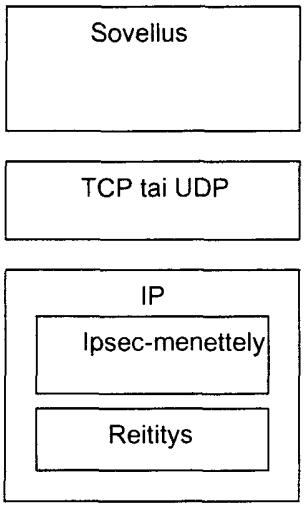
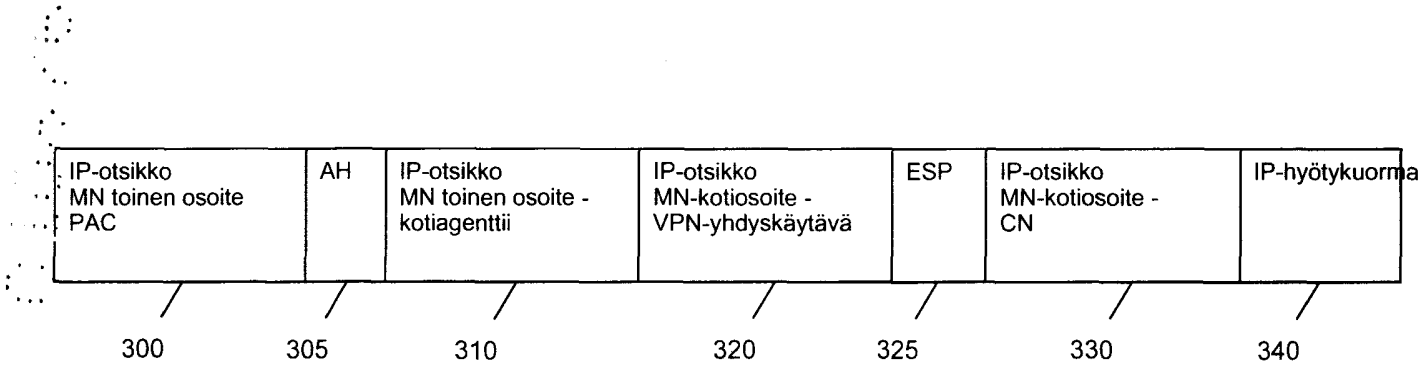

CN
PAC2
140
Yrityksen Intranet
Päätelaite
100
Access Zone 2
VPN-yhdyskäytävä
AH tunneli
104
PAC1
Internet
Kotiverkko
Access Zone 1
HA
130
120
110

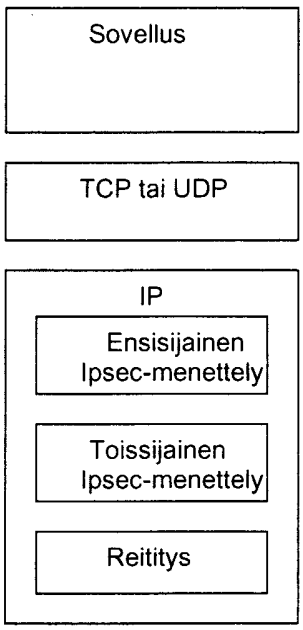
Figure 1



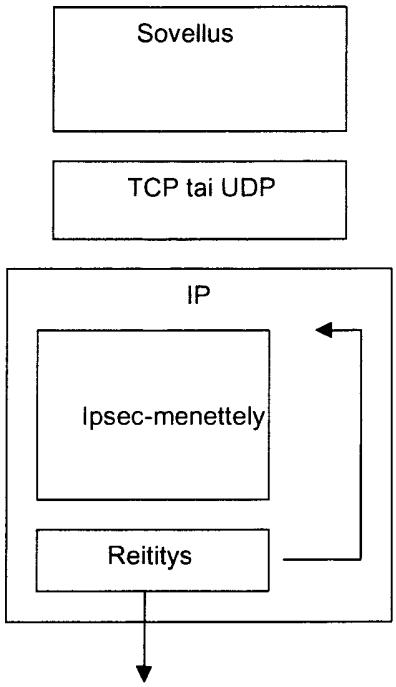
Kuvio 2



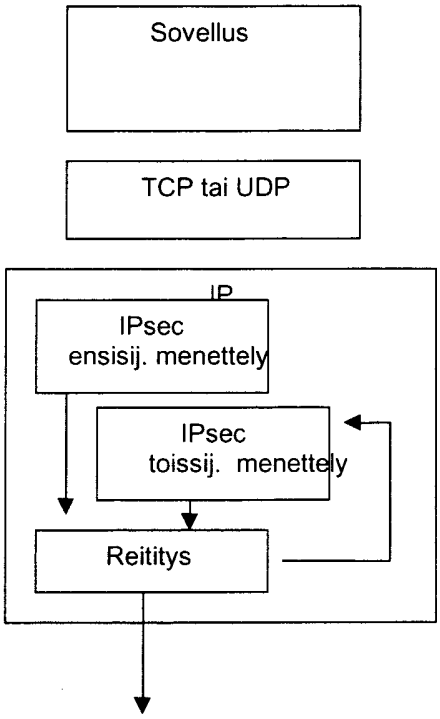
Kuvio 3


Sovellus
TCP tai UDP
IP
Ensisijainen Ipsec-menettely
Toissijainen Ipsec-menettely
Reititys

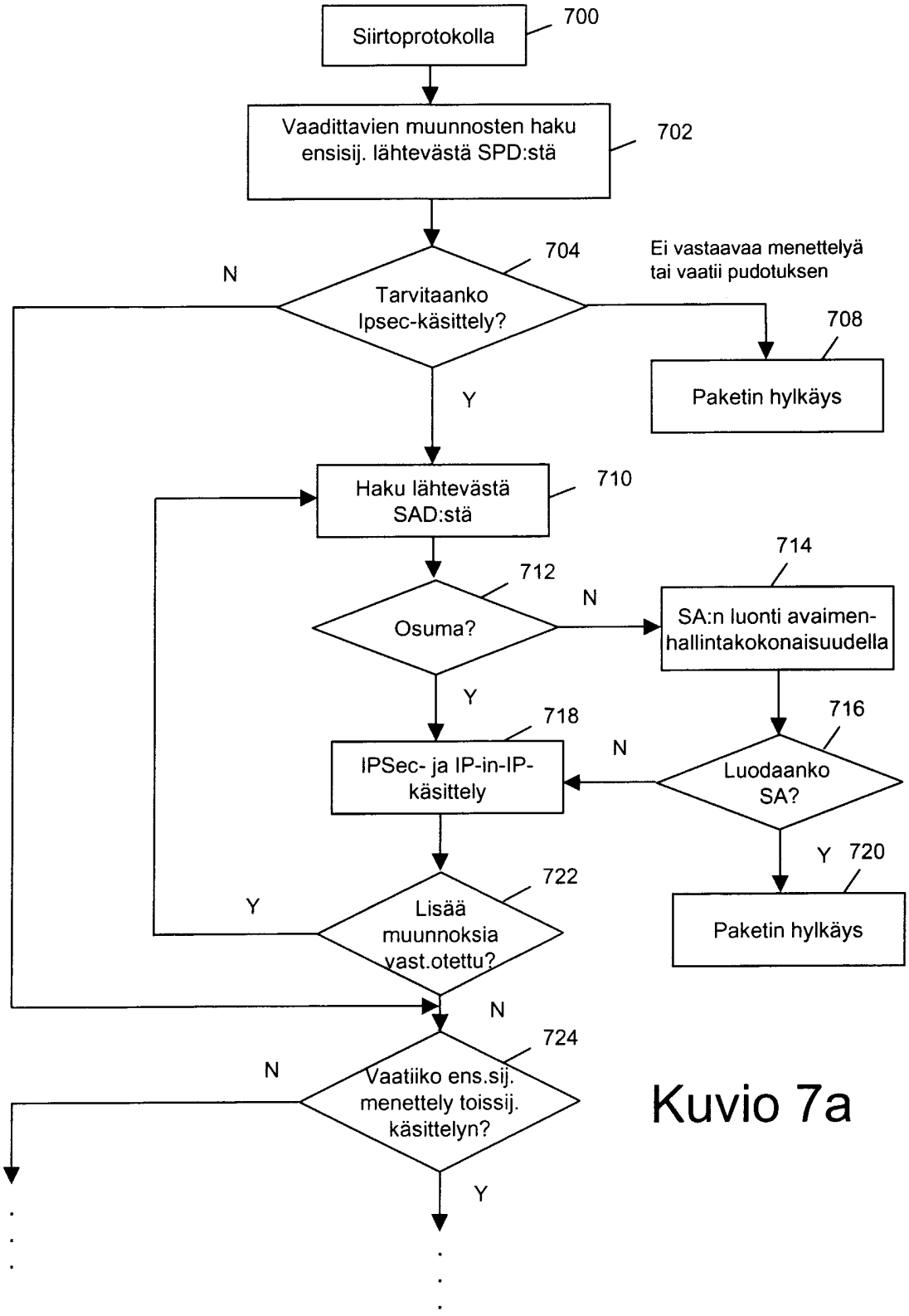
Kuvio 4



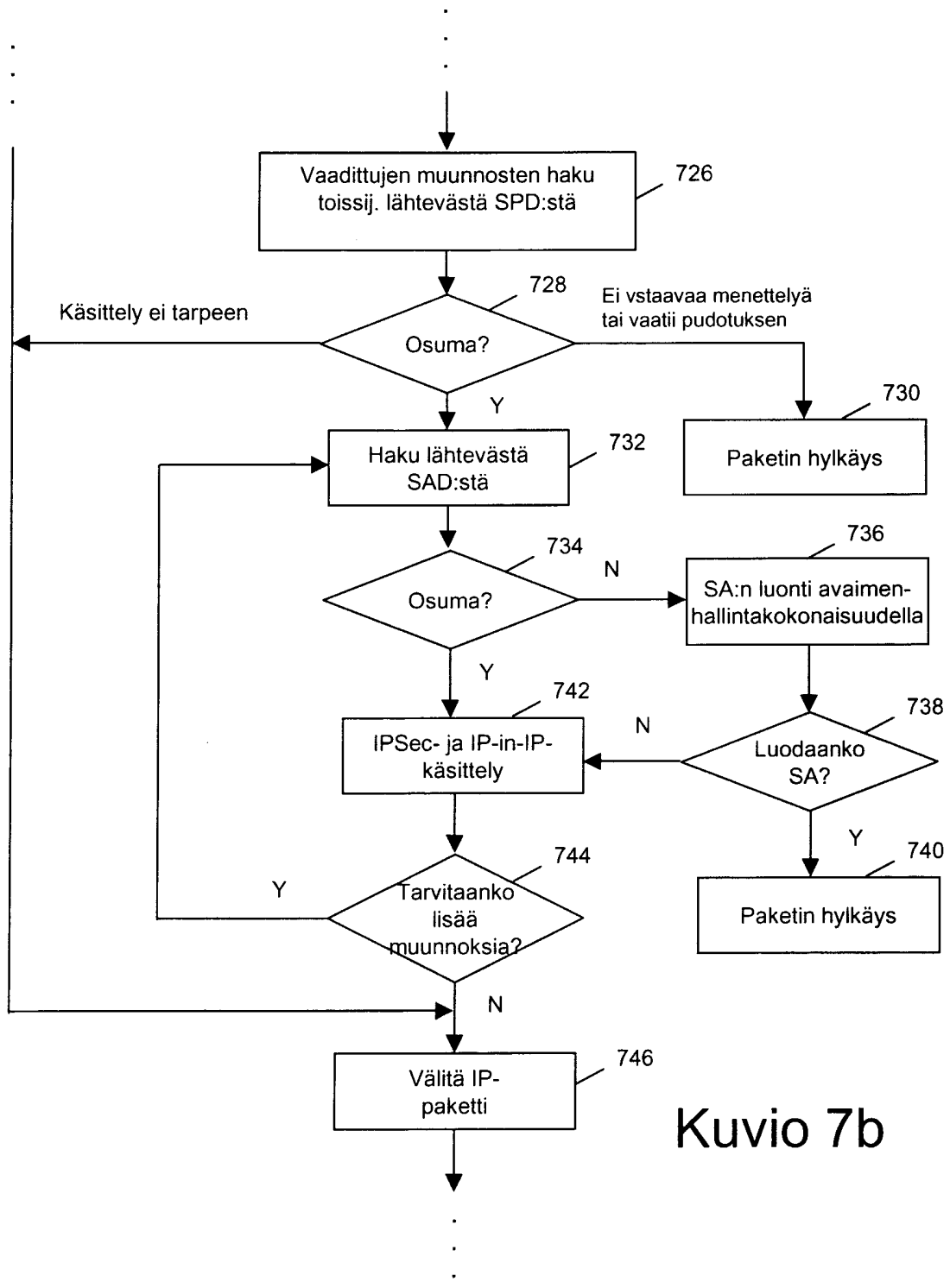
Kuvio 5


Sovellus
TCP tai UDP
IP
IPsec
ensisij. menettely
IPsec
toissij. menettely
Reititys

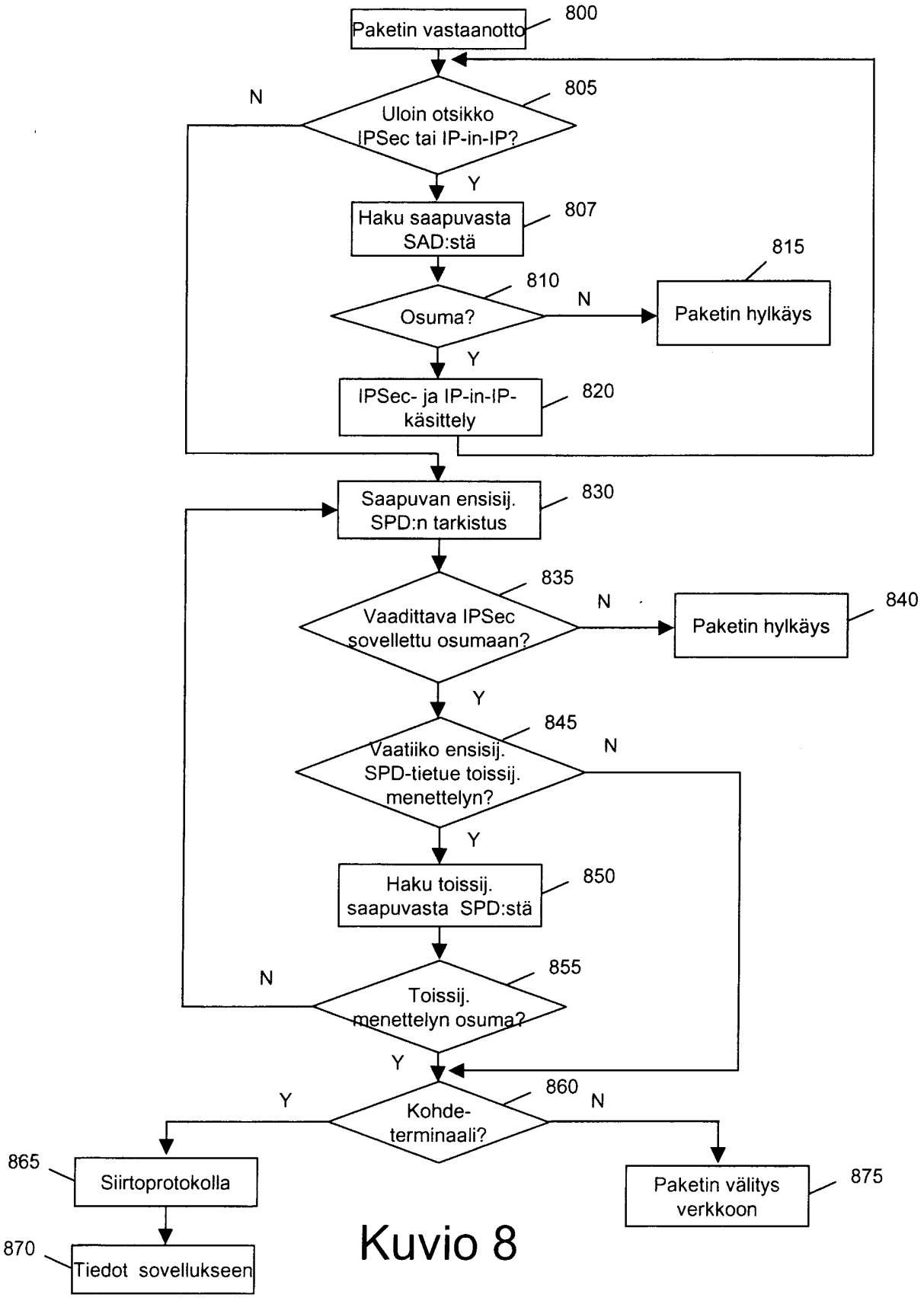
Kuvio 6


Siirtoprotokolla
700
Vaadittavien muunnosten haku ensisij. lähtevästä SPD:stä
702
Tarvitaanko Ipsec-käsittely?
704
Ei vastaavaa menettelyä tai vaatii pudotuksen
N
Y
Paketin hylkäys
708
Haku lähtevästä SAD:stä
710
Osuma?
712
N
Y
SA:n luonti avaimen-hallintakokonaisuudella
714
Luodaanko SA?
716
N
Y
Paketin hylkäys
720
IPSec- ja IP-in-IP-käsittely
718
Lisää muunnoksia vast.otettu?
722
Y
N
Vaatiiko ens.sij. menettely toissij. käsittelyn?
724
N
Y

Kuvio 7a


Vaadittujen muunnosten haku toissij. lähtevästä SPD:stä
726
728
Osuma?
Käsittely ei tarpeen
Ei vstaavaa menettelyä tai vaatii pudotuksen
Y
730
Paketin hylkäys
Haku lähtevästä SAD:stä
732
734
Osuma?
N
736
SA:n luonti avaimen-hallintakokonaisuudella
Y
742
IPSec- ja IP-in-IP-käsittely
N
738
Luodaanko SA?
Y
740
Paketin hylkäys
744
Tarvitaanko lisää muunnoksia?
Y
N
746
Välitä IP-paketti

Kuvio 7b


Paketin vastaanotto
800
Uloin otsikko IPSec tai IP-in-IP?
805
N
Y
Haku saapuvasta SAD:stä
807
Osuma?
810
N
Paketin hylkäys
815
Y
IPSec- ja IP-in-IP-käsittely
820
Saapuvan ensisij. SPD:n tarkistus
830
Vaadittava IPSec sovellettu osumaan?
835
N
Paketin hylkäys
840
Y
Vaatiiko ensisij. SPD-tietue toissij. menettelyn?
845
N
Y
Haku toissij. saapuvasta SPD:stä
850
Toissij. menettelyn osuma?
855
N
Y
Kohde-terminaali?
860
Y
N
Siirtoprotokolla
865
Paketin välitys verkkoon
875
Tiedot sovellukseen
870

Kuvio 8