Nezdružljivost tehnologij pri virtualnih zasebnih omrežjih: protokol IPsec in preslikovanje IP naslovov (NAT)

Povzetek

Namesto najetih vodov kot infrastrukturo za zasebne povezave lahko uporabljamo kar Internet. Skozi Internet naredimo virtualne povezave s tuneliranjem, nalaganjem več protokolnih skladov enega vrh drugega. Največkrat uporabljen in najbolj univerzalen protokol za virtualna zasebna omrežja, ki zagotavlja tudi zasebnost s šifriranjem, je IPsec.

Druga, danes zelo razširjena tehnologija pri povezavah v Internet je preslikovanje IP naslovov (NAT – network address translation). Glavna razloga za uporabo preslikovanja IP naslovov sta: varnost z uporabo zasebnih IP naslovov in požarnih zidov ter pomanjkanje IPv4 naslovov.

Ker sta se protokol IPsec in preslikovanje IP naslovov razvijala istočasno in povsem neodvisno, je prišlo do hudih nezdružljivosti. Obstaja celo precej razširjeno prepričanje, da sta to dve popolnoma nezdružljivi tehnologiji.

Običajni IPsec v tunelskem načinu uporablja dva protokola: kontrolni IKE protokol preko vrat 500 UDP transportnega protokola in ESP protokol za šifriran prenos uporabniških podatkov. Predvsem ESP protokol je težaven pri prehajanju preko NAT naprav, ker ne vsebuje številke vrat, zaradi aplikativne vsebine pa tudi kontrolni protokol IKE ni čisto brez težav.

S skrbnim načrtovanjem in upoštevanjem omejitev je mogoče doseči delujoče stanje v enostavnejših okoljih. Za bolj splošno rabo je bil razvit novejši tip IPsec protokola, ki ESP promet še enkrat inkapsulira v UDP pakete. To je IPsec NAT–T (NAT traversal). Za združljivost s starejšo različico IPsec protokola je poskrbljeno tako, da se o uporabljeni različici partnerja dogovorita s kontrolnim IKE protokolom v času vzpostavljanja povezave.

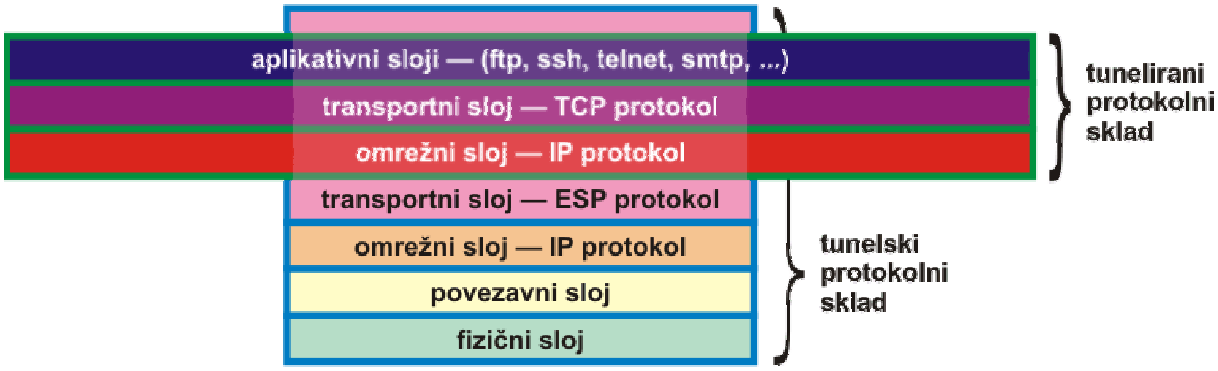
1. Uvod

Zaradi splošne dostopnosti in nizke cene širokopasovnih povezav v svetovno omrežje Internet se je že pred časom porodila ideja, da bi uporabljali Internet tudi kot infrastrukturo za zasebne povezave. Pred tem so za zasebne povezave običajno služili dražji in praviloma počasnejši najeti vodi. Prva ideja je bila, da bi tako povezali cela omrežja, kasneje pa tudi za oddaljeno delo posameznikov – odjemalcev. Na ta način zgradimo tako imenovana virtualna zasebna omrežja (VPN – virtual private network).

2. Tuneliranje

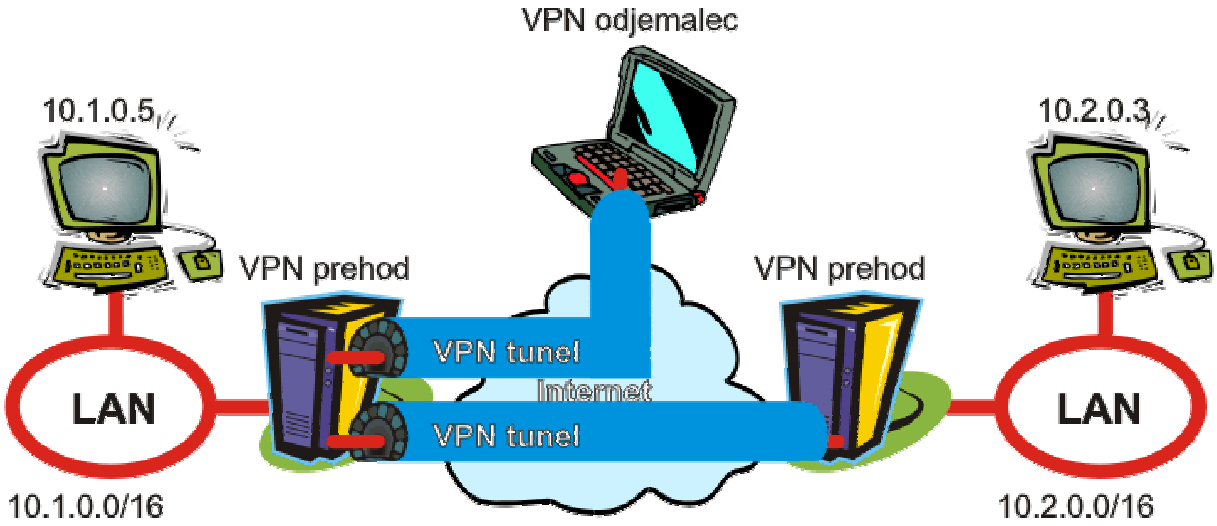
Pri izgradnji virtualne zasebne povezave preko Interneta izkoriščamo princip tuneliranja. To pomeni, da dva ali celo več protokolnih skladov naložimo enega na drugega. Nižji tunelski protokolni sklad služi kot infrastruktura, nadomestek za fizični kanal, za prenos protokolov višjega tuneliranega sklada.

Protokolni sklad pri IPsec tuneliranju



Na tak način lahko povezujemo celo izolirana zasebna omrežja med seboj, tudi če med njimi ni ustrezne protokolne povezave. Npr. povezava dveh DECnet omrežij preko IP omrežja. Drugi, danes bolj običajen razlog je medsebojna povezava zasebnih IP omrežij, ko želimo ohraniti visok nivo zasebnosti z uporabo šifriranja.

Komunikacija preko tunelskih povezav



Poznamo veliko vrst tunelskih povezav – protokolov v IP omrežju: PPTP, L2TP, GRE tunel, SSH tunel, SSL tunel, IPsec. Nekateri zagotavljajo visok nivo zasebnosti s šifriranjem, medtem ko drugi le vzpostavljajo tunel med omrežji. Mi smo za večino povezav izbrali IPsec tunelski način, ker je standarden, vsebuje zelo dodelane mehanizme za zagotavljanje zasebnosti s šifriranjem in je že dobro preizkušen skozi vrsto let. Najvažnejše pa je, da ne pogojuje vrste opreme, operacijskih sistemov in drugih programskih rešitev. Podprt je skoraj na vseh platformah.

2.1 IPsec

IPsec povezava v osnovi uporablja dve vrsti protokolov:

- UDP protokol na vratih 500 za kontrolni promet IKE: za dogovarjanje o parametrih povezave, šifrirnih algoritmih, izmenjavi šifrirnih ključev, vzdrževanje IPsec povezave.
- ESP protokol – IP transportni protokol št. 50, za šifriran prenos uporabniških podatkov

2.1.1 ESP (Encapsulated Security Payload) protokol

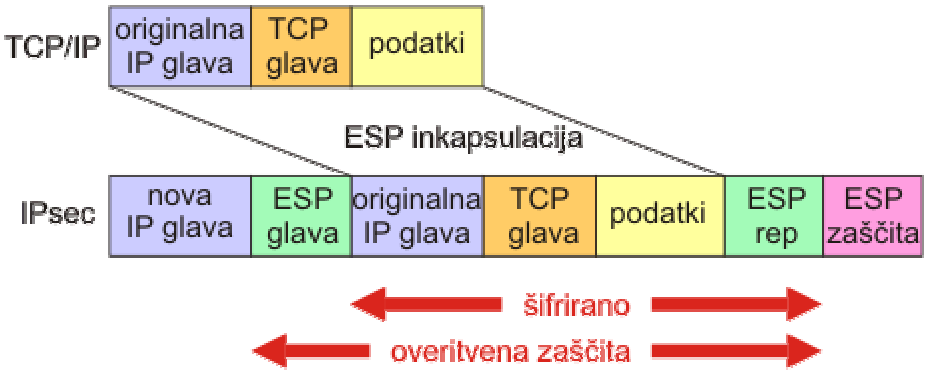
ESP je namenski transportni protokol v IP omrežjih namenjen izključno IPsec povezavam. Omogoča zaupnost s pomočjo šifriranja. Uporablja simetrične šifrirne algoritme. Ker lahko IP paketi prihajajo k cilju v zamešanem vrstnem redu, mora biti vsak ESP paket posebej zaključena šifrirana enota.

ESP protokol zagotavlja avtentikacijo izvora podatkov. Zagotovljena je tudi integriteta podatkov ter sekvenčna integriteta, ki zagotavlja, da noben paket ne manjka ali da kateri ni podvojen. Sekvenčna integriteta je zagotovljena s sekvenčnimi števili, ki se pri ESP protokolu praviloma nikoli ne smejo ponoviti. Po izteku 32 bitnih sekvenčnih številk se povezava ponovno uskladi z novimi parametri.

ESP protokol omogoča celo zaupnost samega toka podatkov, saj je v tunelskem načinu šifriran celoten originalni protokol skupaj z originalnima IP naslovoma izvora in cilja.

Protokol je opisan v IETF standardu RFC 2406.

Format paketa ESP protokola



Vsebina ESP protokola

ESP glava:

- SPI (Security Parameters Index) – številka, ki označuje pakete posamezne povezave (32 bit)
- sekvenca – štetje paketov po modulu 32 (32 bit)

ESP podatki:

- podatki ESP sloja – vsebujejo inkapsuliran višji protokolni sklad (variabilna dolžina):
  - originalna IP glava;
  - originalni transportni protokol (npr. TCP ali UDP);
  - originalni podatki.

ESP rep:

- polnilo – do večkratnika celega šifrirnega bloka (0–255 oktetov, odvisno od uporabljenega šifrirnega algoritma)
- dolžina polnila (8 bit)
- naslednja glava – označuje naslednji protokol višjega sloja (8 bit)
- overitveni podatki – integritetna zaščita (variabilna dolžina – odvisno od uporabljenega overitvenega algoritma)

Vidimo lahko, da ESP protokol ne vsebuje številke vrat za diferenciranje storitev kot jih imata TCP in UDP protokola. Uporaba številke vrat kljub temu, da gre za transportni protokol, ni smiselna, saj se ESP protokol uporablja izključno za prenos podatkov v IPsec.

ESP sloj v skladu leži prenizko, da bi že določal aplikativno storitev, vedno šele nad ESP protokolom nastopa pravi transportni protokol, ki nosi informacijo o storitvi. To nam že najavlja dva problema:

- problem s preslikovanjem IP naslovov (NAT) opisan v nadaljevanju,
- problem z zagotavljanjem kvalitete storitev (QoS).

ESP protokol ne predvideva potrditev (ACK). Potrditve lahko zahtevajo višji sloji, npr. TCP, ki so inkapsulirani v ESP protokolu. Vendar pa ESP sloj tak potrditveni paket ne razlikuje od običajnih podatkovnih paketov. Na ESP nivoju ni razvidno, da gre za potrditveni paket. Enako velja za ponovitve TCP paketov, kjer gre s stališča ESP protokola za nov omrežni promet, saj se sekvenčna številka pri ESP ne sme ponoviti.

Kljub temu da ESP protokol izgleda kot nepovezavni protokol, v resnici ni čisto tako. Vzpostavitev povezave in uskladitev parametrov poteka z vzporednim kontrolnim IKE protokolom preko vrat 500 UDP protokola. Pri tem se poleg šifrirnih in overitvenih parametrov dogovori za vrednost SPI indeksa, ki ga v glavi privzame ESP protokol. Povezava

in vrednost SPI indeksa sta dogovorjena za vsako stran komuniciranja posebej. Dohodni in odhodni ESP paketi imajo različno in med seboj neodvisno vrednost SPI indeksa.

3. Preslikovanje IP naslovov (NAT)

Preslikovanje IP naslovov (NAT – network address translation) je metoda, ki preslika IP naslove omrežnih paketov iz ene množice IP naslovov v drugo na način, ki je običajno transparenten za izvor in cilj. Največkrat se preslika cela skupina zasebnih notranjih IP naslovov v en sam zunanji javni IP naslov, ki nam ga dodeli ponudnik internetnega dostopa. Na ta način zagotovimo vsem uporabnikom v zasebnem delu omrežja transparenten dostop do javnega omrežja. Omejitev je le, da se vsa komunikacija začenja v zasebnem omrežju. Za nasprotne zahteve, ki izvirajo iz javnega omrežja, moramo na NAT napravi urediti statične preslikovalne izjeme.

Preslikovanje IP naslovov se danes zelo množično uporablja iz predvsem dveh razlogov:

- v požarnih zidovih zaradi varnosti.
  Notranjim zasebnim omrežjem dodelimo zasebne IP naslove. S tem računalnike »skrijemo« pred javnim omrežjem. Pri izhodu v javno omrežje požarni zid ali robni usmerjevalnik pretvarja zasebne IP naslove v javne.
- zaradi pomanjkanja IPv4 naslovov.
  IPv4 naslovi so 32 bitni, kar pomeni, da je vseh možnih IP naslovov nekaj več kot štiri milijarde. Zaradi posebnosti, kot so: grupiranje v razrede zaradi lažjega usmerjanja, zasebni IP naslovi, namensko rezervirani IP naslovi, jih je dejansko uporabnih še precej manj. Zaradi širokega razmaha Interneta in ker se danes IP protokol uporablja tudi izven računalniškega okolja (telefonija, razne namenske naprave) je dejansko začelo primanjkovati IP naslovov.

Za preslikovanje IP naslovov obstajajo še drugi redkeje zastopani razlogi: zagotavljanje transparentnosti pri spremembah mrežne topologije, menjava internetnega ponudnika, posebnosti pri usmerjanju prometa, podvojeni IP naslovi …

Preslikovanje IP naslovov srečamo tudi doma, v hotelskih omrežjih ter celo v nekaterih javnih omrežjih, pri nas npr. omrežje IP preko Mobitel GSM, GPRS in NeoWLAN omrežij.

Preslikovanje IP naslovov najbolj poenostavljeno pomeni, da se omrežnim paketom, ki potujejo preko NAT naprave spremeni IP naslov. Običajno se spremeni izvorni IP naslov,

lahko pa tudi ciljni ali celo oba IP naslova. V resnici je postopek precej bolj zapleten. Poleg IP naslova se običajno pri TCP in UDP transportnih protokolih spremeni tudi številka vrat in zaradi protokolnih pravil še kontrolna vsota.

Pomembno je, da gre ves promet ene seje skozi isto NAT napravo. Če tega ne zagotovimo si morajo NAT naprave deliti iste nastavitve in med sabo izmenjevati stanja trenutnih povezav – preslikovalnih sej.

Preslikovanje IP naslovov mora biti transparentno za aplikacije. Pogosto je zato potrebno na NAT napravi za posamezne posebne aplikacije uporabiti poseben program – aplikacijski prehod, ki preverja in preslikuje tudi vsebino višje ležečih aplikativnih protokolov. FTP je najbolj popularen aplikativni protokol, ki rabi tak aplikacijski prehod. Da programski aplikacijski prehod lahko opravlja svojo nalogo, protokol ne sme biti šifriran, razen če tudi programski aplikacijski prehod vsebuje ustrezne šifrirne algoritme in pozna šifrirni ključ.

3.1 Primer preslikovanja IP naslovov

Neka organizacija ima notranje zasebno IP omrežje in povezavo v Internet preko ponudnika internetnih storitev. Robni usmerjevalnik zasebnega IP omrežja ima globalno veljaven IP naslov na zunanji povezavi, ostali notranji sistemi imajo le lokalne zasebne IP naslove. Pri komuniciranju s svetom lahko lokalni sistemi hkrati uporabljajo isti javni IP naslov z metodo preslikovanja svojih IP naslovov. Niz lokalni IP naslov, lokalna številka izvornih vrat se preslika v javni IP naslov in dodeljeno številko izvornih vrat.

3.2 Preslikovalna seja

V primeru, ko je več zasebnih IP naslovov preslikano v manj ali le en javni IP naslov, se ob prvem izhodnem paketu v NAT napravi vzpostavi preslikovalna seja, ki je v preslikovalni tabeli določena z nizom: originalni IP naslov, originalna izvorna številka vrat in dodeljeni IP naslov, dodeljena izvorna številka vrat. Vsi nadaljnji paketi te preslikovalne seje se potem preslikajo po istem pravilu. Zadnji paket, ki zaključuje povezavo, tudi zbriše zapis v preslikovalni tabeli in s tem zaključi preslikovalno sejo. Preslikovalna seja se lahko zaključi tudi z iztekom časovnika, če že dalj časa ni bilo nobene komunikacije.

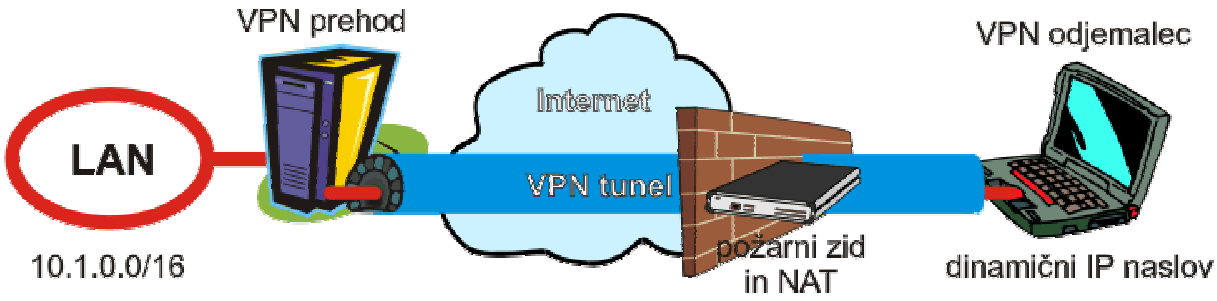
Preslikovanje IP naslovov zagotavlja zasebnost, ker se vse seje začenjajo enosmerno iz smeri zasebnega omrežja, vsi povratni paketi morajo imeti že vzpostavljeno preslikovalno

sejo. Po preslikavi dejanski zasebni IP naslovi izvornih sistemov niso več vidni zunanjemu svetu.

Težava nastopi pri preslikovanju IP fragmentov. Razlog je v tem, da le prvi fragment vsebuje TCP ali UDP glavo, ki je potrebna za preslikovanje. Ostali fragmenti ne vsebujejo številke TCP ali UDP vrat in zato NAT naprava ne ve, kateri preslikovalni seji pripadajo in jih ne zna pravilno preslikati. NAT naprava mora pred preslikovanjem izvesti združevanje fragmentov in ponovno fragmentacijo po preslikovanju.

4. Nezdružljivost protokola IPsec in preslikovanja IP naslovov

Danes zelo običajen način povezovanja in dela na daljavo shematično prikazuje spodnja slika.



Z oddaljenim odjemalcem želimo komunicirati skozi Internet z npr. službenim omrežjem. V ta namen vzpostavimo IPsec VPN tunel od odjemalca skozi Internet do robnega usmerjevalnika – VPN prehoda v podjetju. Zaradi varnosti imamo pred vstopom v Internet na svoji strani nameščen usmerjevalnik – požarni zid, ki opravlja tudi funkcijo preslikovanja IP naslovov.

V odvisnosti od izbire opreme in izvedbe zelo hitro naletimo na precej verjetne težave zaradi nezdružljivosti tehnologij. IPsec protokol in preslikovanje IP naslovov sta nastala približno v istem času in se razvijala povsem neodvisno. Tako nastala nezdružljivost IPsec protokola in preslikovanja IP naslovov je vedno pogostejša težava pri širšem uveljavljanju.

Nezdružljivosti IPsec protokola in preslikovanja IP naslovov lahko delimo v tri skupine:

- vgrajene nezdružljivosti, izhajajo iz samega principa delovanja;
- izvedbene nezdružljivosti;
- nezdružljivosti zaradi namensko vgrajenih IPsec funkcij v NAT napravah.

4.1 Vgrajene nezdružljivosti

- Za identifikacijo pri overjanju koncev VPN tunela je po standardu mogoče uporabiti IP naslova VPN prehodov. Za to skrbi IKE kontrolni protokol. Če se IP naslov spremeni pride do težave pri identifikaciji partnerja povezave. Paketi, katerim ni mogoče določiti identifikacije se zavržejo. Temu se z ustrezno izvedbo lahko izognemo, če za identifikacijo ne uporabimo IP naslovov, marveč uporabniško določeno oznako, npr. ime računalnika.
- Če je za NAT napravo več sistemov, ki želijo vzpostaviti IPsec VPN tunel do istega cilja, nastopi težava pri vzpostavljanju povezave. Kontrolni IKE protokol uporablja protokol UDP z izvornimi in ciljnimi vrati št. 500. NAT naprava izvorna vrata zamenja, da lahko multipleksira več povezav z istim izvornim in ciljnim IP naslovom. Ciljni sistem mora dopuščati uporabo drugih izvornih vrat za IKE kontrolni protokol, kar ni običajno.
- Ciljni VPN prehod ne more ločiti dveh sistemov izza NAT naprave, ki uporabljata ločena IPsec VPN tunela. Zato je mogoče, da se že dogovorjene povezave med sabo zamešajo in podatki pošljejo napačnemu izvoru.
- Ker v ESP protokolu ni vrat, mora NAT naprava ločiti povezave na podlagi IP in ESP glave. V ESP glavi je polje SPI indeks, katerega vrednost določa pripadnost povezavi. Ker pa dvosmerni ESP promet uporablja za vsako smer svojo vrednost SPI indeksa, ki med sabo nista odvisni, ni možno ugotoviti, kateri povratni ESP promet pripada posamezni povezavi. NAT naprava bi za kreiranje preslikovalne seje morala pregledovati tudi vsebino kontrolnega IKE prometa in iz njega razbrati vrednost SPI indeksa ustreznega ESP prometa. Za to je potreben poseben program – aplikacijski prehod.
- Če je IPsec povezav preko NAT naprave do istega cilja več, je mogoče, da NAT naprava povratni promet narobe usmeri, med seboj zamenja. Ker ni pravila pri izbiri vrednosti SPI indeksa v ESP glavi, je mogoče celo, da si različni izvori izberejo enako vrednost SPI indeksa. Tako imamo lahko npr. promet z internega IP naslova 192.168.0.4 z SPI 470 in drugi promet z internega IP naslova 192.168.0.5 z istim SPI 470. Po prehodu skozi NAT napravo oba toka dobita isti izvorni IP naslov in imata isto SPI vrednost.
- Povezava mora biti vedno pričeta s strani za NAT napravo, saj mora v NAT napravi že obstajati vzpostavljena preslikovalna seja, da je promet mogoč tudi v obratni smeri.

4.2 Izvedbene nezdružljivosti

- Nekatere NAT naprave poznajo le UDP in TCP protokol. Pri drugih je mogoče namestiti za NAT napravo le en sistem, ki komunicira po protokolu brez vrat, pri katerem se preslika le IP naslov.
- Nekatere NAT naprave imajo prekratek čas pomnjenja UDP povezav – preslikovalnih sej. UDP protokol je v uporabi pri IKE kontrolnem protokolu in promet poteka le občasno, npr. pri usklajevanju novih ključev, izteku sekvenčnih števil ipd. Če NAT napravi poteče preslikovalna seja, je promet z zunanje strani onemogočen, z notranje strani pa je lahko ponovno vzpostavljena preslikovalna seja z drugačnimi parametri kot prejšnja.
- Nekatere NAT naprave ne znajo pravilno procesirati fragmentov, čeprav same pravilno fragmentirajo pakete. Najkrajši fragment ima lahko le 68 oktetov in prvi fragment ne vsebuje niti celotne glave npr. TCP protokola. Da je še težje, lahko prihajajo fragmenti v pomešanem vrstnem redu. Preslikovanje IP naslovov nad tem je zelo težavno, zato je najpreprostejše, da NAT naprava paket sestavi, preslika in potem ponovno fragmentira.

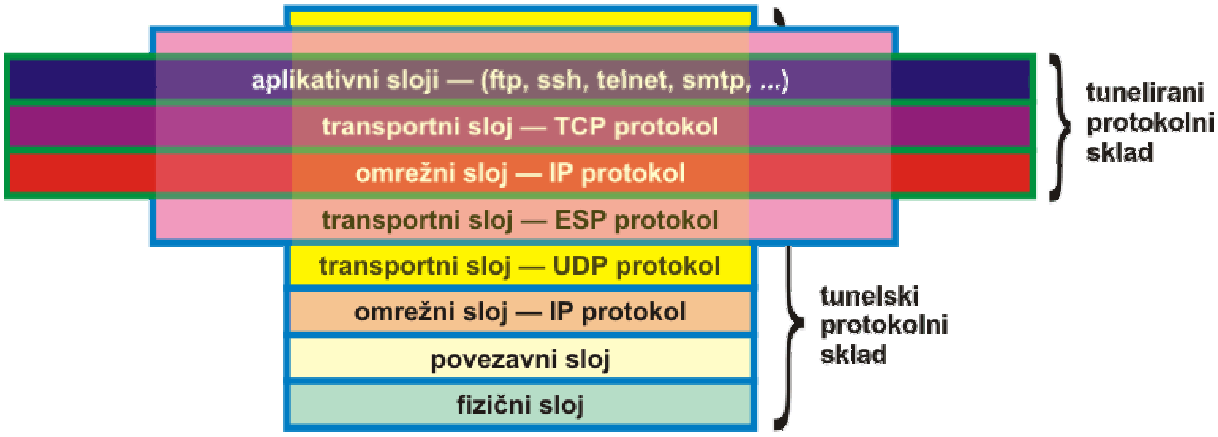
4.3 Nezdružljivosti zaradi namensko vgrajenih IPsec funkcij v NAT napravah

- Nekatere NAT naprave obravnavajo vrata 500 pri protokolu UDP na poseben način. Ker veliko IPsec implementacij zahteva za kontrolni IKE protokol uporabo obojih, izvornih in ciljnih vrat št. 500, NAT naprava ne spreminja številke izvornih vrat. To po drugi strani pomeni, da je mogoč izza NAT naprave le en sistem na posamezen cilj.
- Nekatere NAT naprave pregledajo vsebino kontrolnega IKE protokola, da potem aktivno obravnavajo celoten IPsec promet. Izkazalo se je, da vsebina IKE protokola ni standardizirana do zadnje podrobnosti in obstajajo manjše razlike glede na izvedbo, ki povzročajo težave.

5. Rešitev – IPsec NAT–T (NAT traversal)

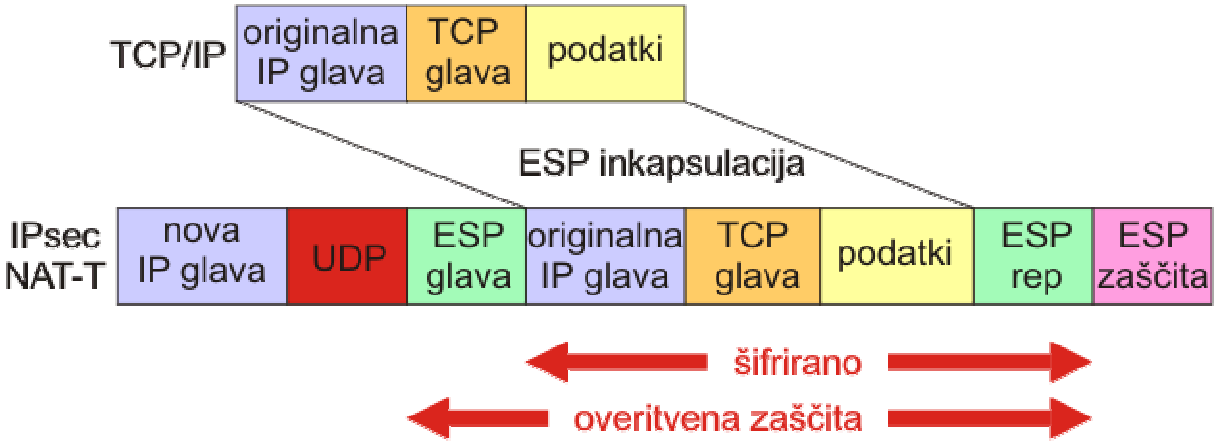
To je novejši tip IPsec protokola, ki je predviden za prehode skozi NAT naprave. Gre za dvojno inkapsulacijo. ESP protokol je še enkrat inkapsuliran v UDP protokol. Da je še manj težav pri prehodih skozi požarne pregrade, uporabljata usklajevalni IKE protokol in podatkovni promet isto številko UDP vrat – 4500.

Protokolni sklad IPsec NAT–T



NAT naprava se pri preslikovanju IP naslovov sploh ne zaveda prisotnosti ESP protokola, saj obdeluje le IP in UDP glavi.

Format paketa



Zasnovano je bilo, da vse deluje čimbolj transparentno glede na običajen IPsec protokol. Novejše naprave poznajo obe izvedbi IPsec protokola in se v času vzpostavljanja posamezne povezave s pomočjo kontrolnega IKE protokola dogovorijo, katera različica bo uporabljena. Dogovorjena različica je odvisna od prisotnosti preslikovanja IP naslovov.

Način inkapsulacije in dekapsulacije je enak kot pri običajnem IPsec protokolu z dodatnim korakom vrivanja in odstranjevanja UDP glave.

6. Zaključek

Preslikovanje IP naslovov je glavni razlog za počasnejše uveljavljenje varnega IPsec protokola. Kot lahko vidimo, je s skrbnim načrtovanjem in določenimi omejitvami IPsec promet v tunelskem načinu delovanja kljub vsemu mogoče voditi skozi požarni zid ali drugo NAT napravo. Danes to ponuja že večina cenenih usmerjevalnikov za domačo rabo.

To je lažje izvedljivo v manj zahtevnih okoljih, ko je za NAT napravo en sam ali manjše število sistemov, ki ne komunicirajo z istim ciljem. To so predvsem domača okolja.

Za večja omrežja se je bolje poslužiti novejše različice protokola IPsec NAT–T, ki z opisano funkcionalnostjo nima večjih težav. Nekatere NAT naprave imajo še vedno težave pri procesiranju fragmentov, kontrolni IKE protokol pa pogosto vsebuje velike pakete, ki jih je potrebno fragmentirati.

Tudi IPsec NAT-T ima slabosti: v starejših IPsec izvedbah še ni podprt in v nekaterih novejših ne povsem v skladu s standardom, saj gre za nov standard (RFC 3947 in 3948, januar 2005), zaradi dodatnega sloja rabi več procesiranja, dodatna glava v paketu pomeni manj uporabniških podatkov – slabši izkoristek protokola.

Za konec naj omenimo, da IPsec protokol poleg tunelskega načina pozna še drugi, transportni način delovanja. Že naziv pove, da v tem primeru ne gre za tuneliranje – nalaganje enega protokolnega sklada na drugega, ampak le za vrivanje dodatne ESP plasti v obstoječi protokolni sklad, podobno kot pri bolj poznanem TLS (SSL) protokolu. Pri tem ostane v paketu IP glava nespremenjena, za njo se med IP in transportni TCP ali UDP vrine glava ESP protokola, na koncu se doda obstoječi transportni del TCP ali UDP v šifrirani obliki. V tem primeru kakršnokoli preslikovanje IP naslovov ni dopustno in ne deluje, ker NAT naprava ne more popraviti kontrolne vsote v TCP ali UDP protokolu, saj je ta šifrirana skupaj z ostalo vsebino.

7. Viri:

- D. Hercog; predloge predavanj predmeta Protokoli v sodobnih telekomunikacijskih omrežjih; http://www.fe.uni-lj.si/~hercog/SodobniProtokoli/PSTKO_HP.htm
- T. Vidmar; Informacijsko komunikacijski sistem; Pasadena, Ljubljana: 2002
- A. J. Menzes, P. C. van Oorschot, S. A. Vanstone; Handbook of Applied Cryptography; CRC Press,1996

- Dokumentacija produkta FreeS/WAN – IPsec implementaciji v GNU/linux operacijskem sistemu, http://www.freeswan.org/
- Dokumentacija produkta StrongSWAN – IPsec NAT–T implementaciji v GNU/linuxu operacijskem sistemu http://www.strongswan.org/
- IETF standardi http://www.ietf.org/:
    - RFC 2406, IP Encapsulating Security Payload (ESP), november 1998
    - RFC 3715, IPsec-Network Address Translation (NAT) Compatibility Requirements, marec 2004
    - RFC 2401, Security Architecture for the Internet Protocol, november 1998
    - RFC 3022, Traditional IP Network Address Translator (Traditional NAT), januar 2001
    - RFC 2663, IP Network Address Translator (NAT) Terminology and Considerations, avgust 1999
    - RFC 2409, The Internet Key Exchange (IKE), november 1998
    - RFC 3947, Negotiation of NAT-Traversal in the IKE, januar 2005
    - RFC 3948, UDP Encapsulation of IPsec ESP Packets, januar 2005