HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

IPSec NAT traversal

CCERT-PUBDOC-2005-07-127

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

IPSec je protokol kojim se osigurava sigurnost IP komunikacije. Korištenjem IPSec-a sigurnost se implementira na trećem, mrežnom sloju ISO/OSI referentnog modela. Detaljni opis samog protokola može se pronaći u dokumentu *IPSec protokol* [1], objavljenom na CARNet CERT-ovim stranicama. Standard je postao vrlo popularan, no također u sebi sadrži određene nedostatke koji ograničavaju mogućnosti njegove uporabe. Najveći nedostatak protokola jest nemogućnost uspostave komunikacije između entiteta od kojih se jedan ili oba nalaze iza uređaja koji provode NAT (eng. *network address translation*), odnosno NAPT (eng. *network address port translation*) translaciju (u nastavku dokumenta oba ova pojma označavat će se jedinstveno kao NAT).

Obzirom na poznata ograničenja adresiranja kod IPv4 protokola, ali i zbog podizanja razine sigurnosti, u korporativnim okruženjima, ali i malim uredima (eng. *SOHO – small office, home office*) široko je prihvaćeno interno privatno adresiranje, a pristup Internet-u se osigurava upravo korištenjem NAT-a (npr. na *gateway* uređaju ili vatrozidu). Na taj način efikasno se rješavaju problemi u IP adresiranju i podiže razina sigurnosti internih mreža.

Nažalost, zbog same implementacije IPSec protokola, ali i IKE protokola koji se koristi za uspostavu SA skupa sigurnosnih parametara u IPSec komunikaciji, korištenje NAT-a u komunikacijskom kanalu između entiteta onemogućava uspostavu IPSec komunikacije. Razlog tome su promjene u IP (promjena adrese) te TCP i UDP zaglavljima (promjena porta), što u većini slučajeva narušava kontrolne sume (eng. *checksum*), odnosno integritet paketa, o čemu će više riječi biti u nastavku dokumenta.

IPSec NAT-T (eng. *NAT traversal*) tehnologija definirana u RFC dokumentima 3947 "*Negotiation of NAT-Traversal in the IKE*" [2] i 3948 "*UDP Encapsulation of IPsec ESP Packets*"[3] unapređuje IPSec tako da, uz određena ograničenja, omogućava uspostavu IPSec komunikacije i između entiteta koji se nalaze iza NAT uređaja.

U nastavku dokumenta su opisana ograničenja IPSec protokola, obzirom na NAT translaciju, te je dan prikaz IPSec NAT-T tehnologije sa svojim mogućnostima i nedostacima.

2. NAT ograničenja IPSec protokola

NAT translacija ograničava korištenje IPSec protokola na više načina. Ograničenja proizlaze iz samog načina oblikovanja AH i ESP IPSec paketa, ali i zbog svojstava IKE protokola za razmjenu SA skupa sigurnosnih parametara [1].

U nastavku poglavlja opisana su najvažnija ograničenja IPSec protokola prilikom NAT translacije, dok se popis svih problema u uspostavi i održavanju IPSec komunikacije koji mogu nastati kao posljedica NAT translacije može pronaći u RFC dokumentu 3715 "*IPsec-Network Address Translation (NAT) Compatibility Requirements*" [6].

2.1. IKE ograničenja

Bez obzira provodi li se IKE komunikacija korištenjem glavnog (eng. *main mode*) ili agresivnog (eng. *aggressive mode*) moda, entiteti se između ostalog identificiraju prema IP adresi i portu, odnosno provjerom *hash* vrijednosti tih parametara [1]. Primjenom NAT translacije dolazi do promjene IP adrese i porta pošiljatelja. Primatelj IKE paketa provjerava iste te podatke prilikom primanja te ga, zbog neispravnih (promijenjenih) vrijednosti odbacuje.

Nadalje, neke implementacije IKE protokola dozvoljavaju isključivo IKE promet s UDP porta 500, te odbacuju sve pakete koji dolaze s drugih izvorišnih portova, uzrokujući na taj način momentalno odbacivanje paketa koji su NAT translatirani bez ikakvih dodatnih provjera [4].

Treći problem kod NAT translacije IKE paketa predstavlja to što NAT mapiranja UDP prometa imaju vrlo kratki period valjanosti. Ukoliko primatelj IKE poruke ne odgovori na vrijeme dolazi do brisanja postojećeg UDP mapiranja u NAT tablici, čime je onemogućena dostava IKE paketa pošiljatelju. Ovo je problem kod uspostave IKE komunikacije, ali i kod održavanja IKE SA skupa sigurnosnih parametara [4].

2.2. IPSec AH ograničenja

Obzirom da AH protokol, bez obzira radi li se o transportnom ili tunelskom načinu rada autenticira čitav IP paket, bilo kakva promjena paketa, a u konkretnom slučaju NAT translacija IP adrese i TCP/UDP porta (implicitno to podrazumijeva i promjenu kontrolnih suma TCP i UDP zaglavlja), rezultira narušavanjem integriteta paketa i njegovim odbacivanjem na strani primatelja.

2.3. IPSec ESP ograničenja

Za razliku od AH protokola koji ni u kojem slučaju ne može funkcionirati ukoliko se negdje na komunikacijskom kanalu provodi NAT translacija, ESP u bi teoretski mogao funkcionirati u tunelskom načinu, pod uvjetom da se provodi isključivo translacija IP adrese (čisti NAT), bez translacije porta. U praksi je takav slučaj nije previše vjerojatan.

Problem ESP protokola kod NAT translacije je taj što ESP paketi ne sadrže vidljiva TCP ili UDP zaglavlja, a iza IP zaglavlja slijedi ESP zaglavlje. NAT uređaji ne sadrže mehanizam kojim bi mogli multipleksirati različite IPSec ESP spojeve koji prolaze kroz isti uređaj. Teoretski bi se za to moglo koristiti SPI polje (skup sigurnosnih parametara) ESP zaglavlja [1], pošto je vjerojatnost da to (32-bitno) polje bude isto za dva IPSec ESP spoja izrazito mala, no problem u tom slučaju predstavlja nemogućnost određivanja koji odlazni IPSec ESP promet odgovara kojem dolaznom IPSec prometu, odnosno koji SPI u odlaznim paketima odgovara SPI polju u dolaznim paketima. Mapiranje SPI polja nije moguće, pošto ESP protokol digitalno potpisuje i ESP zaglavlje, pa bi promjena SPI polja uzrokovala narušavanje integriteta ESP paketa [4].

3. IPSec NAT traversal

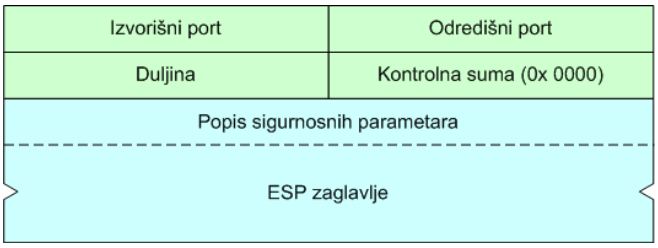
Osnovna ideja IPSec NAT traversal (u nastavku dokumenta NAT-T) tehnologije je korištenje UDP paketa za enkapsulaciju IPSec ESP i IKE paketa. IPSec AH paketi ne mogu se enkapsulirati korištenjem NAT-T tehnologije. Standardni port za IPSec NAT-T komunikaciju je UDP port 4500.

Korištenje istog UDP porta za NAT-T enkapsulaciju pojednostavljuje konkretnu implementaciju i konfiguraciju (npr. vatrozidnih pravila), no isto tako to znači da NAT-T interno mora razlikovati IPSec

ESP promet, IKE promet, te kontrolni promet za održavanje UDP kanala. Da bi to bilo moguće NAT-T definira tri vrste enkapsuliranih zaglavlja.

IPSec ESP zaglavlje enkapsulira se u standardno UDP zaglavlje koje se sastoji od izvorišnog i odredišnog porta, duljine paketa i kontrolne sume. Kontrolna suma UDP zaglavlja trebala bi biti nul vrijednost, a primatelj je ne bi trebao interpretirati.

Nakon tako oblikovanog UDP zaglavlja slijedi standardno ESP zaglavlje, uz uvjet da prvo polje zaglavlja (SPI) koje označava skup sigurnosnih parametara ne smije imati nul vrijednost. 32-bitna nul vrijednost koja slijedi neposredno nakon UDP zaglavlja rezervirana je isključivo za IKE pakete (Slika 1).

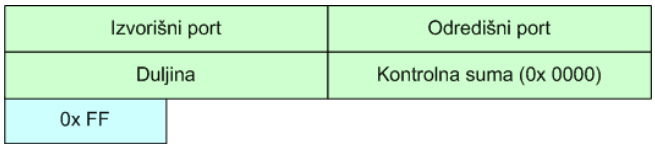


Slika 1: NAT-T enkapsulacija IPSec ESP paketa

Enkapsulacija **IKE zaglavlja** provodi se tako da, nakon standardnog UDP zaglavlja, kod kojeg se, za razliku od IPSec ESP enkapsulacije, ne postavljaju nikakvi dodatni zahtjevi na kontrolnu sumu, slijedi 32-bitna nul vrijednost (eng. *non-ESP marker*) koja označava da se radi o IKE paketu. Nakon toga slijedi standardno IKE zaglavlje (Slika 2).

Slika 2: NAT-T enkapsulacija IKE paketa

Zbog karakteristika UDP protokola koji nije konekcijski orijentiran (eng. *connectionless*) i ne sadrži nikakve mehanizme za održavanje komunikacijskog kanala, što je bitno kod NAT translacije, odnosno održavanja NAT mapiranja, potrebno je redovitim slanjem paketa održavati uspostavljenu UDP vezu aktivnom. Zbog toga NAT-T, osim enkapsulacije IPSec ESP zaglavlja i IKE zaglavlja, definira i treću vrstu paketa tzv. **NAT-*keepalive***. NAT-*keepalive* paket sastoji se od standardnog UDP zaglavlja kod kojeg, isto kao i kod IPSec ESP enkapsulacije, kontrolnu sumu primatelj ne treba interpretirati, te 8-bitnog polja koje slijedi UDP zaglavlje i koje sadrži `0xFF` vrijednost (Slika 3). Ovaj paket služi isključivo za održavanje NAT mapiranja i primatelj bi ga trebao zanemarivati.



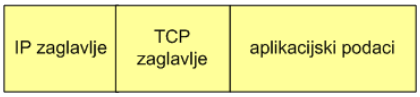
Slika 3: NAT-T enkapsulacija paketa za održavanje UDP kanala

U NAT-T IPSec komunikaciji između dva entiteta izvorišni i odredišni portovi UDP zaglavlja moraju imati iste vrijednosti za sve tri vrste ranije opisanih paketa.

3.1. Enkapsulacija i dekapsulacija IPSec ESP paketa

Postupak enkapsulacije i dekapsulacije IPSec ESP paketa definiran je RFC dokumentom 3248 " UDP Encapsulation of IPsec ESP Packets" [3]. NAT-T UDP enkapsulacija IPSec ESP paketa ovisi o načinu rada, tako da se za transportni i tunelski način rada provode različiti postupci enkapsulacije i dekapsulacije kako je u nastavku opisano. Slike u nastavku zbog jednostavnosti odnose se na

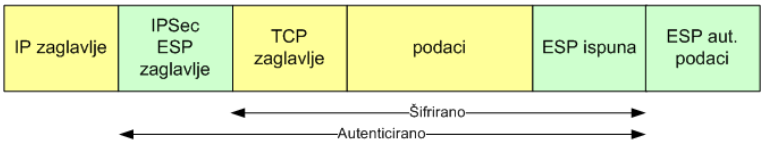
enkapsulaciju TCP paketa, iako se na isti način provodi i enkapsulacija UDP paketa. Na sljedećoj slici (Slika 4) prikazan je standardni IPv4 TCP paket, a postupci NAT-T enkapsulacije takvog paketa u transportnom i tunelskom načinu rada dani su u nastavku.



Slika 4: Standardni TCP paket

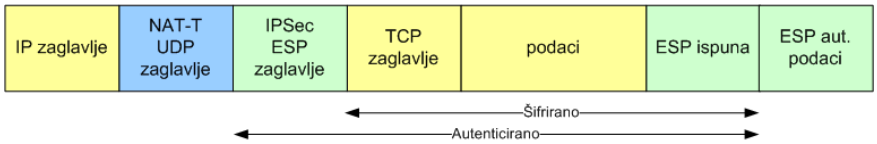
3.1.1. Transportni način rada

Slika 5 prikazuje standardno oblikovani IPSec ESP paket u IPSec transportnom načinu rada [1].



Slika 5: Standardno oblikovani ESP paket u transportnom načinu rada

Za razliku od tako oblikovanog ESP paketa, NAT-T enkapsulacija IPSec ESP paketa u transportnom načinu rada provodi se kako je prikazano na slici (Slika 6).



Slika 6: Enkapsulacija ESP paketa u transportnom načinu rada

NAT-T enkapsulacija se provodi se u sljedećim koracima [3]:

1. Provodi standardna transportna ESP enkapsulacija [1].
2. Oblikuju se UDP [9] i IP zaglavlja [7], s izračunatim kontrolnim sumama i ispravno podešenim poljima duljine i protokola (IP protokol 17 – UDP).

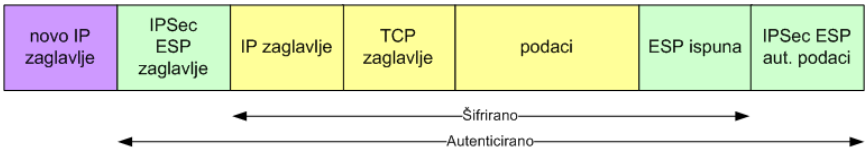
Dekapsulacija paketa provodi se u sljedećim koracima [3]:

1. UDP zaglavlje se uklanja.
2. Ponovno se računaju i umeću sljedeća polja IP zaglavlja: kontrolna suma, duljina paketa i protokol (IP protokol 50 – ESP).
3. Provodi se standardna dekapsulacija ESP paketa [1].

Obzirom da nakon tako provedene dekapsulacije IP adresa izvora i odredišta poruke ne moraju odgovarati originalnim (zbog provođenja NAT-a), kontrolna suma unutrašnjeg TCP [8] ili UDP zaglavlja [9] neće biti ispravna, te je kontrolnu sumu potrebno ponovno izračunati, s time da se prethodno umetnu odgovarajuće adrese koje su prethodno razmijenjene u IKE komunikaciji (poglavlje 3.2.4).

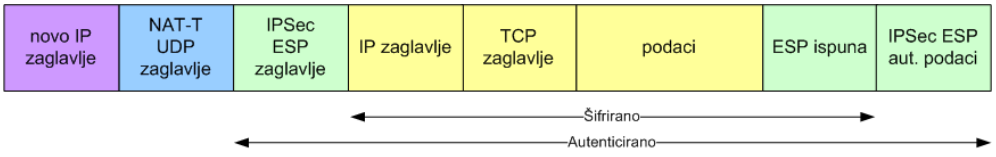
3.1.2. Tunelski način rada

Slika 7 prikazuje standardno oblikovani IPSec ESP paket u IPSec tunelskom načinu rada [1].



Slika 7: Standardno oblikovani ESP paket u tunelskom načinu rada

Za razliku od tako oblikovanog ESP paketa, NAT-T enkapsulacija IPSec ESP paketa u tunelskom načinu rada provodi se kako je prikazano na slici (Slika 8).



Slika 8: Enkapsulacija ESP paketa u tunelskom načinu rada

NAT-T enkapsulacija se provodi se u sljedećim koracima [3]:

3. Provodi standardna tunelska ESP enkapsulacija [1].
4. Oblikuju se UDP [9] i IP zaglavlja [7], s izračunatim kontrolnim sumama i ispravno podešenim poljima duljine i protokola (IP protokol 17 - UDP).

Dekapsulacija paketa provodi se u sljedećim koracima [3]:

4. UDP zaglavlje se uklanja.
5. Ponovno se računaju i umeću sljedeća polja IP zaglavlja: kontrolna suma, duljina paketa i protokol (IP protokol 50 – ESP).
6. Provodi se standardna dekapsulacija ESP paketa [1].

Ovisno o načinu rada, odnosno politici uređaja na krajnjoj točki IPSec tunela, provjeravaju se enkapsulirana IP zaglavlja ili po potrebi provodi NAT translacija da bi se paket prilagodio transportu u lokalnoj mreži.

3.2. Uspostava IPSec komunikacije kroz NAT-T korištenjem IKE-a

IKE protokol služi za uspostavu IPSec komunikacijskog kanala između dvaju entiteta. Više o standardnom načinu uspostave IKE, i kasnije IPSec komunikacije moguće je pronaći u dokumentu IPSec protokol [1], dok je detaljna specifikacija protokola definirana u RFC dokumentu 2409 "*The Internet Key Exchange (IKE)*" [10].

Uz nužne promjene, IKE se koristi i kod uspostave NAT-T IPSec komunikacije. Da bi se NAT-T komunikacija uopće mogla uspostaviti potrebno je ustanoviti NAT-T kompatibilnost entiteta i moći detektirati postojanje NAT translacije u komunikacijskom kanalu između dvaju entiteta koji žele uspostaviti IKE (i IPSec) komunikaciju.

3.2.1. Detekcija NAT-T kompatibilnosti entiteta

Utvrđivanje kompatibilnosti entiteta i detekcija NAT translacije provode se u prvoj fazi uspostave (uspostava IKE SA) IKE komunikacije koja se može provesti na glavni ili agresivni način [1].

Prvi uvjet koji se mora ispuniti da bi uspostava IKE komunikacije uopće bila moguća je da oba entiteta mogu odgovarati na IKE poruke koje dolaze s portova različitih od UDP 500.

Nadalje, potrebno je utvrditi NAT-T kompatibilnost entiteta u komunikaciji. Ispitivanje kompatibilnosti provodi se u prve dvije poruke koje razmjenjuju entiteti (bez obzira radi li se o glavnom ili agresivnom načinu), provjerom *Vendor ID* (MD5 *hash* vrijednost proizvoljnog tekstualnog niza koji definira proizvođač) polja ISKMP zaglavlja [1]. Entitet oglašava svoju NAT-T kompatibilnost ukoliko se u tom 128-bitnom polju nalazi vrijednost:

```
0x 4a13 1c81 0703 5845 5c57 28f2 0e95 452f
```

što odgovara MD5 *hash*-u teksta "RFC 3947".

3.2.2. Detekcija NAT translacije

Za detekciju NAT translacije uvodi se novo, NAT-D (eng. *NAT discovery*) polje . Korištenjem NAT-D polja osigurava se ne samo detekcija postojanja NAT translacije, već i mjesto(a) gdje se NAT translacija događa. To je bitno zbog kasnijeg slanja NAT-*keepalive* paketa za održavanje IKE kanala [2].

Slika 9: Format NAT-D polja

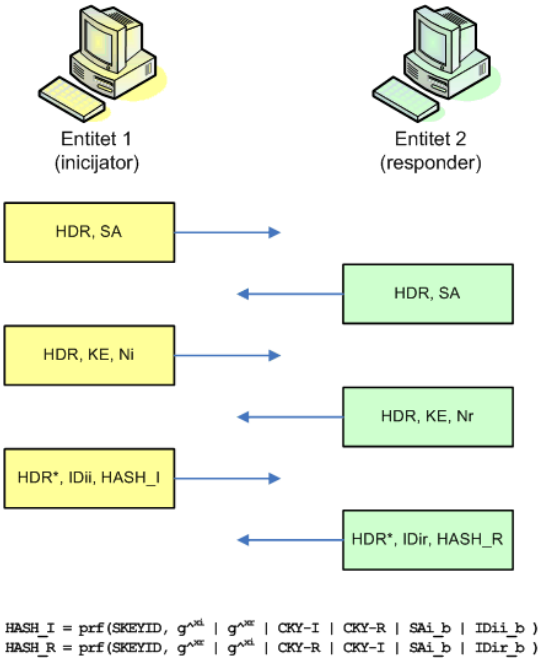
Slika 9 prikazuje format NAT-D polja ISAKMP zaglavlja. U nastavku su opisani elementi NAT-D polja.
Sljedeće zaglavlje (eng. *next payload*) – oznaka NAT-D polja ISAKMP zaglavlja (20).
Rezervirano (eng. reserved) – rezervirano.
Duljina zaglavlja (eng. *payload length*) – duljina NAT-D polja (ovisi o *hash* funkciji koja je dogovorena u IKE SA).
Hash – *hash* vrijednost koja se računa na sljedeći način:

```
HASH = HASH(CKY-I | CKY-R | IP | PORT)
```

gdje CKY-I i CKY-R označavaju kolačiće generirane od strane entiteta (eng. *initiator*, *responder*) koji sadrže *hash* vrijednost izračunate spajanjem (eng. *concatenation*) IP adrese, porta, protokola i slučajne vrijednosti generirane od strane oba entieta[1], dok IP i PORT označavaju IP adresu i port entiteta.

3.2.3. NAT-T uspostava IKE SA

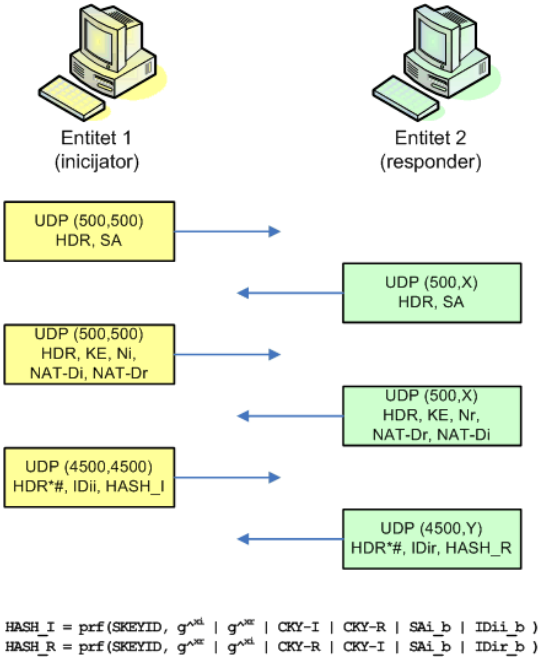
Uspostava IKE SA može se provesti u glavnom (6 koraka) i agresivnom načinu (3 koraka). Oba načina opisana su detaljnije u dokumentu "IPSec protokol". NAT-T uspostava IKE SA također se može provoditi na oba načina, s malim modifikacijama pojedinih poruka.
Kod NAT-T uspostave IKE SA, NAT-D polja uključuju se u treću i četvrtu razmjenu paketa kod glavnog načina ili drugu i treću razmjenu kod agresivnog načina uspostave IKE SA.
Oba entiteta u tim paketima osim uobičajenih parametara dodatno generiraju dva NAT-D zaglavlja (uz pretpostavku da oba entiteta koriste jednu IP adresu) u kojima, svaki zasebno računaju *hash* vrijednost na način opisan u poglavlju 3.2.1 Po zaprimanju paketa od druge strane, entiteti provjeravaju dobivene *hash* vrijednosti.
Ukoliko su tako izračunate NAT-D vrijednosti identične, između entiteta ne postoji NAT i IPSec kanal se može uspostaviti na uobičajeni način.
Slika 10 prikazuje standardni način uspostave IKE SA korištenjem glavnog načina, uz autentikaciju korištenjem tajnog ključa [1] koji se provodi razmjenom šest poruka između entiteta. Kompletna komunikacija odvija se preko UDP porta 500.



Slika 10: Standardna uspostava IKE SA (glavni način)

Ukoliko se pak *hash* vrijednosti iz NAT-D paketa ne podudaraju, to znači da se u komunikacijskom kanalu provodi NAT translacija, te da se sva nadolazeća IKE i IPSec komunikacija mora provoditi korištenjem NAT-T enkapsulacije. To podrazumijeva trenutnu promjenu IKE porta kod oba entiteta s UDP porta 500 na UDP port 4500.

Slika 11 prikazuje NAT-T uspostavu IKE SA korištenjem glavnog načina, uz autentikaciju korištenjem tajnog ključa. Inicijator po zaprimanju NAT-D zaglavlja od respondera (četvrti korak) zaključuje da u komunikacijskom kanalu provodi NAT translacija, te u petom koraku mijenja UDP port na 4500. Responder također u šestoj poruci odgovara s UDP porta 4500 na port određen tabelom NAT mapiranja.



Slika 11: NAT-T uspostava IKE SA(glavni način)

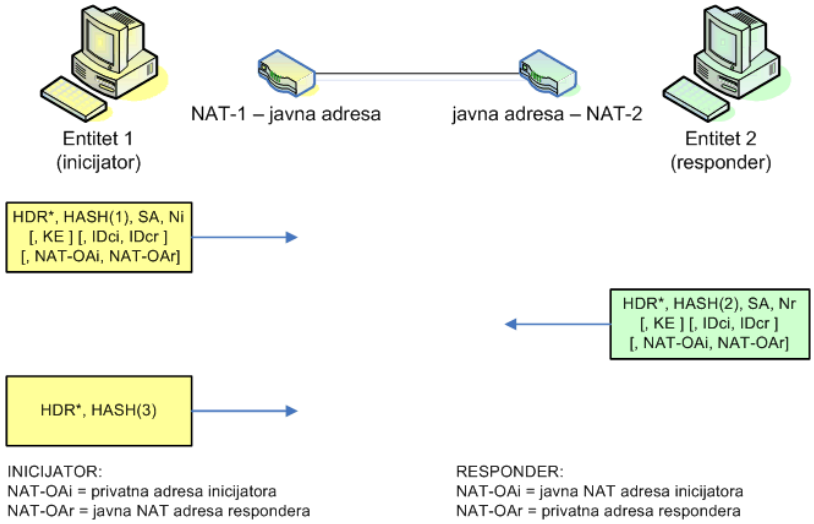
Na sličan način provodi se i uspostava IKE SA i u agresivnom načinu, te uz različite načine autentikacije klijenata.

3.2.4. NAT-T uspostava IPSec SA

Uspostava IPSec SA standardno se provodi u brzom načinu (eng. *quick mode*), kompletno je šifrirana korištenjem parametara iz IKE SA i služi za definiranje IPSec SA skupa sigurnosnih parametara za daljnju IPSec komunikaciju.
Kod NAT-T uspostave IPSec SA, osim SA skupa sigurnosnih parametara, oba entiteta u komunikaciji razmjenjuju i način UDP enkapsulacije (UDP enkapsulacija u tunelskom ili transportnom načinu rada) te originalne IP adrese (isključivo kod korištenja IPSec NAT-T u ESP transportnom načinu rada).
Originalne adrese šalju se u NAT-OA polju ISAKMP zaglavlja.

Slika 12: Format NAT-OA polja

Slika 12 prikazuje format NAT-OA polja. U nastavku su opisani elementi NAT-OA polja.
Sljedeće zaglavlje (eng. *next payload*) – oznaka NAT-OA polja ISAKMP zaglavlja (21) duljine 1 okteta.
Rezervirano (eng. *reserved*) – 3 polja rezervirane namjene duljine 8, 8 i 16 okteta.
Duljina zaglavlja (eng. *payload length*) – 2 oktetna duljina NAT-D polja (ovisi o tipu IP adrese koji se koristi).
Identifikator tipa (eng. *ID type*) – tip IP adrese (IPv4 ili IPv6).
IP adresa – sadrži IP adresu (IPv4 – 4 okteta ili IPv6 – 16 okteta).
Slika 13 prikazuje NAT-T uspostavu IPSec SA za ESP transportni način rada. U primjeru na slici i inicijator i responder nalaze se iza NAT uređaja. Za razliku od uobičajene uspostave IPSec SA [1], u ovom slučaju ISAKMP zaglavlja poruka između inicijatora i respondera sadrže i dodatna NAT-OA polja ko ja označavaju originalne adrese entiteta kako ih svaki od njih vidi. Kako je i prikazano, inicijator kao originalne adrese vidi vlastitu privatnu adresu i javnu NAT adresu respondera, dok responder kao originalne adrese vidi vlastitu privatnu adresu, te javnu NAT adresu inicijatora. Te originalne adrese koriste se pri zamjeni IP adresa u enkapsuliranim ESP zaglavljima (poglavlje 3.1.1).

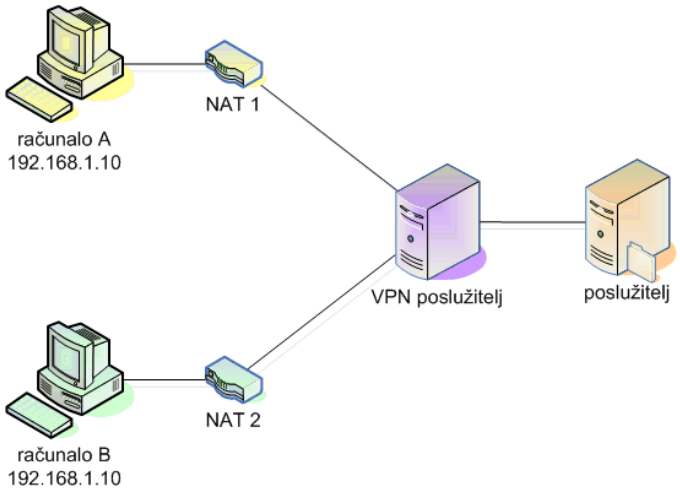


Slika 13: NAT-T uspostava IPSec SA u ESP transportnom načinu rada

4. Sigurnosna razmatranja

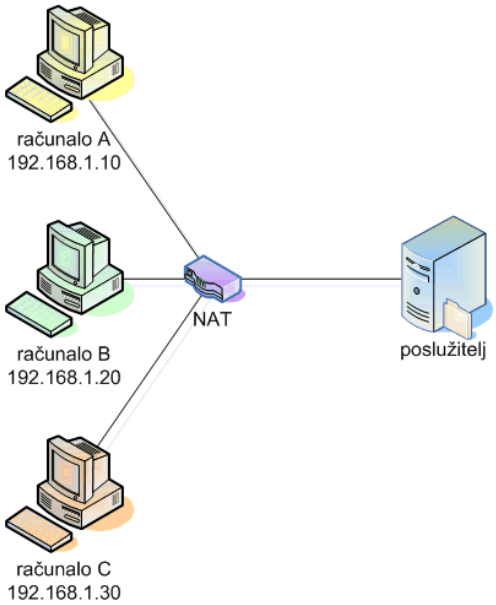
Kod IPSec NAT traversal tehnologije postoji nekoliko ograničenja koja proizlaze iz samog načina funkcioniranja IPSec NAT-T, tako da u posebnim slučajevima može doći do konflikta u tunelskom i transportnom načinu rada.

Slika 14 prikazuje situaciju u kojoj dolazi do konflikta u tunelskom načinu rada. Računalo A i računalo B nalaze se na privatnim mrežama koje su od javne mreže odvojene NAT1 i NAT2 uređajima. Oba računala koriste privatne IP adrese, koje su u ovom slučaju jednake. VPN poslužitelj u tom slučaju ima dva skupa sigurnosnih parametara SA koji se odnose na istu adresu [3][6], što može biti problem kad VPN poslužitelj mora usmjeravati pakete s poslužitelja nazad prema računalu A ili B.



Slika 14: Konflikt u tunelskom načinu rada

Ovaj problem moguće je riješiti tako da VPN poslužitelj dodjeljuje jedinstvene IP adrese udaljenim računalima, npr. korištenjem *DHCP over IPSec* tehnologije.



Slika 15: Konflikt u transportnom načinu rada

Slika 15 prikazuje konflikt u transportnom načinu rada. Računala A, B i C pristupaju poslužitelju u transportnom načinu rada, preko istog NAT uređaja. Moguća je situacija u kojoj poslužitelj ne može jednoznačno odrediti koji SA skup sigurnosnih parametara koristiti za komunikaciju s pojedinim računalom [3].

Osim opisanih mogućnosti konflikata, postoje još neki sigurnosni nedostaci koje NAT-T može unijeti. Kod IPSec NAT-T gubi se mogućnost autentikacije bazirana na IP adresama. To u načelu nije sigurnosni nedostatak, osim ukoliko se kao autentikacijski mehanizam koriste dijeljeni ključ koji dijeli više korisnika. U tom slučaju ne postoji mogućnost jednoznačne autentikacije korisnika, a također je moguće provođenje *Man-In-The-Middle* napada od strane nekog korisnika koji koristi dijeljeni ključ.
Također, napadač koji ima pristup komunikacijskom kanalu može modifikacijom paketa na razne načine uzrokovati DoS uvjete, odnosno nemogućnost uspostave komunikacije [2]. Postoje još neki inherentni nedostaci, no u praksi oni ne predstavljaju veći sigurnosni problem [2].

5. Zaključak

Obzirom da u današnje vrijeme većina korporativnih mreža koristi privatno IP adresiranje, a tu praksu koriste jednim dijelom i ISP-ovi prilikom prijave klijenata, mogućnost uspostave standardne IPSec komunikacije vrlo često je ograničena. S te strane, IPSec NAT traversal uvelike proširuje mogućnost uporabe IPSec, odnosno L2TP IPSec protokola.
Također, unatoč tome što IPSec NAT traversal tehnologija ne podržava korištenje AH u IPSec komunikaciji, pa čak i uz opisane, uvjetne sigurnosne nedostatke i dalje se može smatrati sigurnom za većinu primjena. Posebno se to odnosi na uspostavu VPN konekcija na Windows sustavima gdje je L2TP IPSec puno sigurnija metoda od korištenja PPTP protokola s MPPI enkripcijom.

6. Reference

[1] IPSec protokol,
http://www.cert.hr/filehandler.php?did=89
[2] Negotiation of NAT-Traversal in the IKE,
http://www.ietf.org/rfc/rfc3947.txt
[3] UDP Encapsulation of IPsec ESP Packets,
http://www.ietf.org/rfc/rfc3948.txt
[4] IPsec NAT Traversal Overview,
http://www.microsoft.com/technet/community/columns/cableguy/cg0802.mspx
[5] NAT Traversal (NAT-T) Security Issues,
http://www.windowsecurity.com/articles/NAT-Traversal-Security.html
[6] IPsec-Network Address Translation (NAT) Compatibility Requirements,
http://www.ietf.org/rfc/rfc3715.txt
[7] Internet Protocol
http://www.ietf.org/rfc/rfc0791.txt
[8] Transmission Control Protocol,
http://www.ietf.org/rfc/rfc0793.txt
[9] User Datagram Protocol,
http://www.ietf.org/rfc/rfc0768.txt
[10] The Internet Key Exchange (IKE),
http://www.ietf.org/rfc/rfc2409.txt
[11] Internet Security Association and Key Management Protocol (ISAKMP),
http://www.ietf.org/rfc/rfc2408.txt