Uspostava i testiranje VPN tunela

Štefanec, Ivan

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni studij

USPOSTAVA I TESTIRANJE VPN TUNELA

Diplomski rad

Ivan Štefanec

Osijek, 2024.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

Obrazac D1: Obrazac za ocjenu diplomskog rada na sveučilišnom diplomskom studiju

Ocjena diplomskog rada na sveučilišnom diplomskom studiju

Ime i prezime pristupnika:	Ivan Štefanec
Studij, smjer:	Sveučilišni diplomski studij Elektrotehnika, smjer Komunikacije i
Mat. br. pristupnika, god.	D-563, 29.10.2012.
JMBAG:	0165036914
Mentor:	prof. dr. sc. Krešimir Grgić
Sumentor:	
Sumentor iz tvrtke:	
Predsjednik Povjerenstva:	izv. prof. dr. sc. Višnja Križanović
Član Povjerenstva 1:	prof. dr. sc. Krešimir Grgić
Član Povjerenstva 2:	mr. sc. Anđelko Lišnjić
Naslov diplomskog rada:	Uspostava i testiranje VPN tunela
Znanstvena grana diplomskog rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak diplomskog rada:	Virtualne privatne mreže (VPN) i mehanizam tuneliranja predstavljaju temelj za uspostavu sigurne kriptirane komunikacije kroz nesigurno okruženje. U radu je potrebno analizirati i objasniti mehanizme VPN tuneliranja, te uspostaviti VPN tunele unutar testnog okruženja, te provesti njihovu detaljnu analizu i testiranje.

Datum ocjene pismenog dijela diplomskog rada od strane mentora:	17.09.2024.
Ocjena pismenog dijela diplomskog rada od strane mentora:	Izvrstan (5)
Datum obrane diplomskog rada:	8.10.2024.
Ocjena usmenog dijela diplomskog rada (obrane):	Izvrstan (5)
Ukupna ocjena diplomskog rada:	Izvrstan (5)
Datum potvrde mentora o predaji konačne verzije diplomskog rada čime je pristupnik završio sveučilišni diplomski studij:	08.10.2024.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O IZVORNOSTI RADA

Osijek, 08.10.2024.

Ime i prezime Pristupnika:	Ivan Štefanec
Studij:	Sveučilišni diplomski studij Elektrotehnika, smjer Komunikacije i informatika
Mat. br. Pristupnika, godina upisa:	D-563, 29.10.2012.
Turnitin podudaranje [%]:	4

Ovom izjavom izjavljujem da je rad pod nazivom**: Uspostava i testiranje VPN tunela**

izrađen pod vodstvom mentora prof. dr. sc. Krešimir Grgić

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis pristupnika:

SADRŽAJ

1. UVOD **1**

1.1 Zadatak diplomskog rada ..... Error! Bookmark not defined.

2. TEORIJA VPN-a ..... Error! Bookmark not defined.

2.1 Najčešći VPN protokoli **3**

2.2 IPsec protokol **5**

2.2.1 Autentifikacijsko zaglavlje (AH) 7

2.2.2 ESP protokol 9

2.2.3 Sigurnosne asocijacije (SA) 10

2.3 IPsec načini rada **12**

2.3.1 Transportni način 12

2.3.2 Tunelski način 14

2.4 Parametri IPsec-a **15**

2.4.1 Scenarij 15

2.4.2 Osnovna konfiguracija 16

2.4.3 Protok podataka 16

2.4.4 IKE/IPsec prijedlog 16

3. KREIRANJE I KONFIGURACIJA VPS **18**

3.1 Popis alata i programa **18**

3.2 Kreiranje VPS **19**

3.2.1 Odabir operativnog sustava i verzije 19

3.2.2 Regija 20

3.2.3 Linode plan 20

3.2.4 Detalji 22

3.2.5 Kreiranje administrativne *(engl. Root)* lozinke 23

3.2.6 Detalji VPS-a 23

3.3 Podešavanje VPS-a putem SSH terminala i komadni **24**

3.4 Instalacija i konfiguracija IPsec-a na VPS-u **30**

4. KONFIGURACIJA I TEST VPN NA HUAWEI VPN UREĐAJU **32**

4.1 Dogovor IPsec postavki **32**

4.2 Konfiguracija VPN-a **33**

4.3 Mapiranje izvorne i odredišne adrese **36**

4.4 Dodavanje sigurnosne politike vatrozida **37**

4.5 Dodavanje NAT pravila i mapiranje rute na NTH serveru **38**

4.6 Testiranje VPN-a 39
5. ZAKLJUČAK 42
SAŽETAK 43
ABSTRACT 44
ŽIVOTOPIS 45
LITERATURA 46

1. UVOD

Zaštita informacija postala je sve kritičnija u digitalnom dobu, jer su informacije postale ključna sredstva u poslovanju i svakodnevnom životu. Korištenje virtualne privatne mreže jedan je od najučinkovitijih načina za zaštitu podataka tijekom prijenosa. VPN (engl. *Virtual Private Network*) uspostavlja kriptirane tunele za prijenos podataka, omogućujući sigurne veze između udaljenih korisnika ili mreža putem interneta, čime osigurava privatnost i sigurnost. Proces obuhvaća odabir odgovarajućeg VPN protokola i njegovu konfiguraciju te implementaciju sigurnosnih mjera, uključujući enkripciju i autentifikaciju. Unutar rada će se objasniti i opisati uspostavljanje VPN tunela te njegovo testiranje i proći detaljno kroz sve aspekte vezane uz uspostavu VPN kao i sve dijelove koje utječu na rad VPN. Naposljetku je na primjeru pokazan postupak uspostavljanja VPN tunela.

Rad je podijeljen u pet poglavlja, a ona su *Uvod*, *Virtualne Privatne Mreže, Kreiranje i konfiguracija VPS*, *Konfiguracija i test VPN na Huawei VPN uređaju* i *Zaključak.*

U drugom poglavlju opisane su virtualne privatne mreže, najčešći VPN protokoli te značajke i rad IPsec-a (engl. *Internet Protocol Security*). IPsec kao skup protokola je bitan pojam koji je razrađen u detalje te su se objasnili načini rada i parametri potrebni za njihovu konfiguraciju.

Poglavlje *Kreiranje i Konfiguracija VPS-a* sadrži detaljne upute i savjete kako od početka do kraja postaviti VPS, te kako instalirati, postaviti i konfigurirati IPsec-a na virtualnom uređaju.

U poglavlju *Konfiguracija i test VPN-a na Huawei uređaju* opisuje se kako kreirati IPsec na fizičkom uređaju i način odrade testiranja nakon što su dvije strane postavile IPsec i pokušali se povezati.

2. VIRTUALNE PRIVATNE MREŽE

Virtualne privatne mreže (engl. *Virtual Private Network, VPN*) omogućuju proširenje privatnih mreža i resursa koji su ograničeni unutar mreže te njihovo slanje preko javnih mreža poput interneta. Navedeno omogućuje centralnom računalu slanje i primanje podataka preko mreže koja je zajednička ili dostupna javnosti, dok se čini kao da je u pitanju privatna mreža. Posjeduje sve značajke, sigurnosne mjere i politike upravljanja mrežom koje su česte u privatnim mrežama. To se postiže stvaranjem virtualne veze između dva mjesta korištenjem namjenskih veza, enkripcije ili njihove kombinacije. VPN je tehnička veza između dvije lokacije širokopojasne mreže WAN (engl. *Wide Area Network*) preko interneta. Međutim, korisniku se čini kao da se radi o vezi privatne mreže, zbog čega se naziva virtualna privatna mreža ili VPN.

Pojam "virtualna" implicira da fizička arhitektura mreže treba biti neprimjetna za svaku VPN vezu. Obično to također znači da korisnik VPN-a ne posjeduje fizičku mrežu, već koristi javnu mrežu koju dijeli s više drugih korisnika. Protokoli za tuneliranje koriste se kako bi se osigurala potrebna transparentnost višim slojevima. Da bi se riješile posljedice nepostojanja fizičke mreže, ključno je pregovarati o sporazumu o razini usluge s pružateljem mrežnih usluga. Ovaj sporazum jamčit će dostupnost i performanse mreže potrebne za rad VPN-a.

U okviru VPN-a, pojam "privatna" odnosi se na osiguranje tajnosti podataka koji će se prenositi preko VPN-a. Promet VPN-a često prolazi kroz javnu mrežu, što zahtijeva primjenu sigurnosnih mjera za zaštitu svih vrsta prometa koji se prenose putem VPN veze. Sigurnosni zahtjevi uključuju:

- šifriranje podataka
- autentifikaciju izvora podataka
- sigurno stvaranje i redovito ažuriranje kriptografskih ključeva koji se koriste za šifriranje i autentifikaciju.

Izraz "mreža", iako fizički ne postoji, treba se prepoznati i tretirati kao produžetak infrastrukture privatne mreže. Virtualna privatna mreža (VPN) mora biti dostupna ostatku mreže, svim uređajima i aplikacijama ili određenoj grupi, korištenjem uobičajenih tehnika mrežne arhitekture poput usmjeravanja i adresiranja. VPN-ovi su ključni u području kibernetičke sigurnosti i mrežne komunikacije. Uspostavom sigurnih i šifriranih veza, VPN-ovi omogućuju korisnicima privatno prenošenje podatke preko javnih mreža, čime štite osjetljive informacije od potencijalnih prijetnji. Bilo da se koriste za udaljeni pristup ili povezivanje između lokacija, VPN-ovi pružaju fleksibilno rješenje organizacijama i pojedincima koji žele poboljšati svoju privatnost, sigurnost i učinkovitost

mreže. Kroz enkripciju, mehanizme autentifikacije i strategijsku alokaciju resursa, VPN-ovi imaju ključnu ulogu u osiguravanju sigurne komunikacije i prijenosa podataka [1].

2.1. Najčešći VPN protokoli

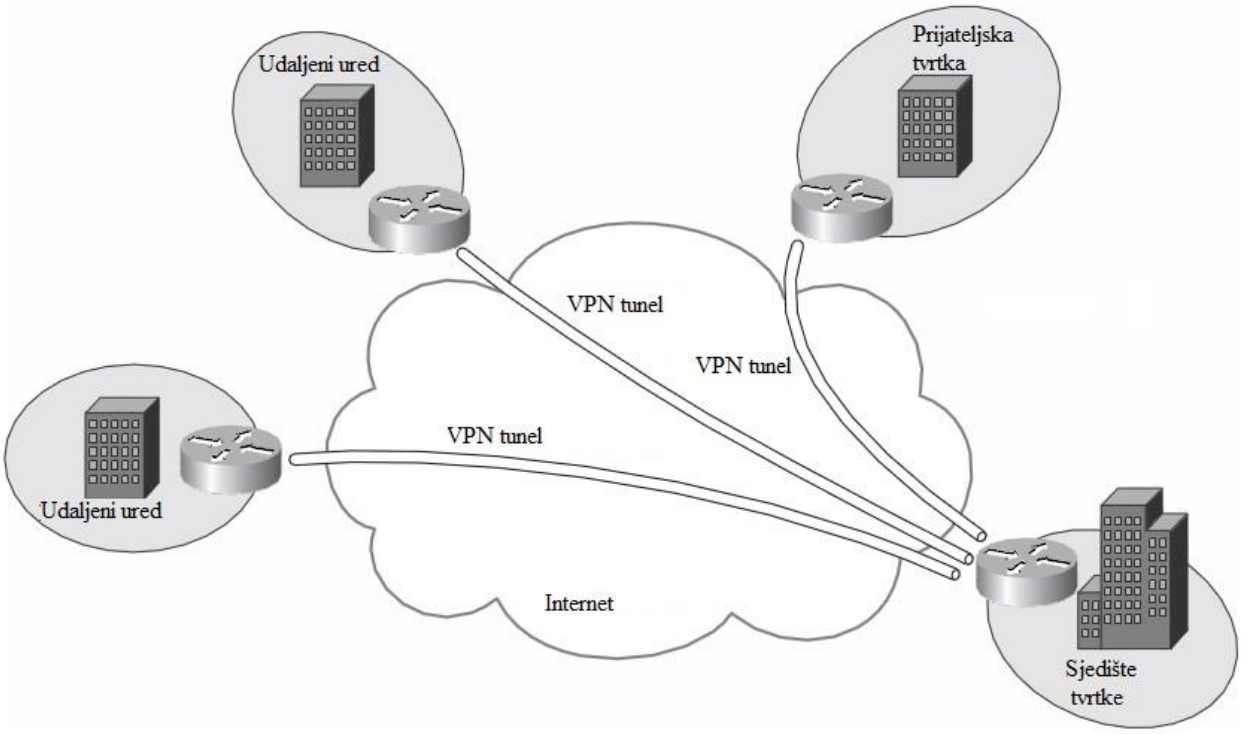
Za uspješnu komunikaciju VPN tunela ključno je da obje strane koriste iste protokole. Među najpoznatijim protokolima su:

- OpenVPN: Poznat po svojoj fleksibilnosti, *open-source* prirodi i snažnim sigurnosnim značajkama. OpenVPN podržava različite algoritme enkripcije i metode autentifikacije, što ga čini široko prihvaćenim za osobnu i poslovnu upotrebu.
- IPsec (engl. *Internet Protocol Security*): Predstavlja skup protokola koji se koristi za osiguravanje internet komunikacija enkripcijom i autentifikacijom svakog paketa podataka tijekom prijenosa. Često se koristi za „*site-to-site*“ VPN-ove i udaljeni pristup VPN-ovima zbog svojih snažnih sigurnosnih značajki.
- L2TP/IPsec (engl. *Layer 2 Tunneling Protocol / IPsec*): Pruža mehanizam tuneliranja, dok IPsec pruža sigurnosne značajke, kombinirajući najbolje od oba protokola za poboljšanu sigurnost i kompatibilnost s različitim uređajima i operacijskim sustavima.
- SSTP (engl. *Secure Socket Tunneling Protocol*): Razvijen od strane Microsofta, SSTP koristi SSL/TLS enkripciju preko TCP porta 443, što olakšava prolazak kroz vatrozidove i *proxy* poslužitelje. Primarno se koristi u Windows okruženjima i poznat je po svojoj snažnoj sigurnosti.
- PPTP (engl. *Point-to-Point Tunneling Protocol*): Iako manje siguran u usporedbi s novijim protokolima, PPTP je jednostavan za postavljanje i široko podržan. Radi na sloju veze podataka i pruža enkripciju putem MPPE (engl. *Microsoft Point-to-Point Encryption).*
- WireGuard: Relativno novi VPN protokol dizajniran za jednostavnost i poboljšane performanse. WireGuard teži biti brži i sigurniji od tradicionalnih VPN protokola poput OpenVPN-a i IPsec-a, nudeći pojednostavljenu bazu koda i efikasni kriptografski dizajn.

Ovi protokoli se razlikuju po sigurnosti, performansama i jednostavnosti postavljanja pa izbor često ovisi o specifičnim slučajevima korištenja, zahtjevima kompatibilnosti i sigurnosnim razmatranjima pri implementaciji VPN-a [2].

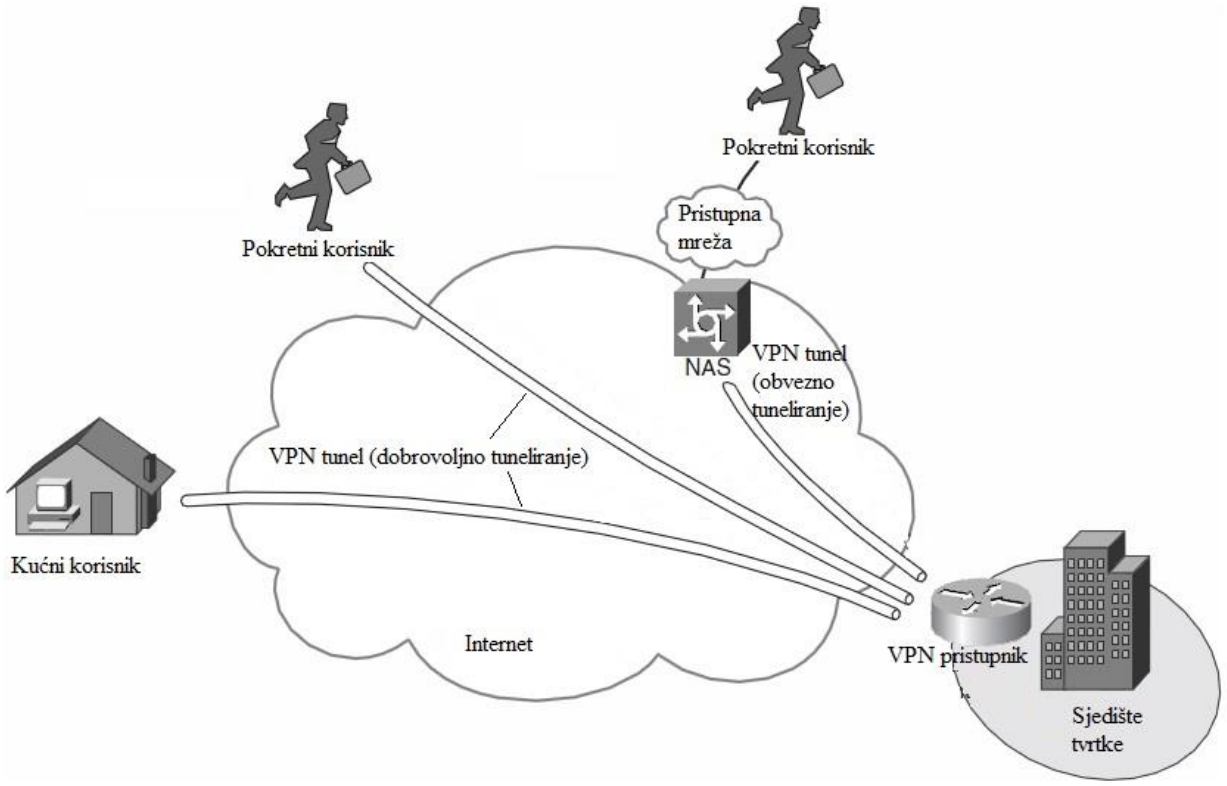
Prema mogućnostima primjene VPN-a rješenja mogu se podijeliti na dva dijela: mjesto do mjesta (engl. *site-to-site*) prikazano na slici 2.1 i udaljeni pristup (*eng. remote access*) prikazano na slici 2.2. Mjesto do mjesta omogućava vezu između različitih organizacija koje se nalaze na udaljenim lokacijama ili unutar jedne organizacije koja ima međusobno udaljene urede. Postoje dvije vrste

mjesto do mjesta VPN-a to su intranet i ekstranet. Intranet se koristi za spajanje lokalnih mreža udaljenih podružnica jednog poduzeća u jedinstvenu privatnu mrežu upotrebom Internet infrastrukture. Ekstranet se koristi za povezivanje različitih organizacija kako bi mogle razmjenjivati podatke i zajedničke resurse na siguran način.



Slika 2.1. VPN od mjesta do mjesta [9]

Udaljeni pristup omogućava korisnicima koji trebaju pristupiti privatnoj mreži povezivanje s bilo koje lokacije radi korištenja resursa ili podataka organizacije. Ovi vanjski korisnici, bilo da rade od kuće ili su na terenu, koriste VPN klijentski program za pristup mreži na daljinu.



Slika 2.2. VPN udaljeni pristup [9]

2.2. IPsec protokol

IPsec je standard i skup protokola koji se koristi u računarstvu kako bi osigurao sigurnu komunikaciju između dvije komponente preko internetske mreže. Navedeno se postiže autentifikacijom i enkripcijom podatkovnih paketa, pružajući siguran i šifriran kanal.

Obuhvaća protokole koji olakšavaju proces provjere identiteta agenata uključenih u sjednicu (*eng. session*) i određivanja kriptografskih ključeva koji će se koristiti tijekom sesije te pruža zaštitu podataka za komunikaciju između:

- dva računala (računalo-računalo)
- dva sigurnosna pristupnika (mreža-mreža)
- sigurnosnog pristupnika i računala (mreža-računalo).

IPsec koristi kriptografske mehanizme sigurnosti kako bi zaštitio komunikaciju preko mreže Internetskog protokola. Sustav omogućuje autentifikaciju vršnog čvora na razini mreže, autentifikaciju podrijetla podataka, integritet podataka, tajnost podataka putem šifriranja i zaštitu od napada ponovnog izvođenja. Opcionalan je za IPv4, a obvezan za IPv6 koji obuhvaća mehanizme za zaštitu prometa [4].

Nudi sljedeće značajke:

- autentifikaciju, šifriranje, integritet podataka te zaštitu od ponovljenih napada
- sustav nudi sigurnu generaciju i automatsko obnavljanje kriptografskih ključeva
- snažne kriptografske algoritme za jamstvo sigurnosti,
- podržava autentifikaciju temeljenu na certifikatima
- ima sposobnost integracije budućih kriptografskih algoritama i protokola razmjene ključeva
- omogućava sigurnost za L2TP i PPTP tunelne protokole za udaljeni pristup.

IPsec je posebno namijenjen osiguravanju kompatibilnosti i besprijekorne komunikacije između različitih sustava i mreža. Kada se pravilno konfigurira, ne utječe na mreže i korisnike koji ih ne podržavaju.

IPsec protokoli uključuju:

- Autentifikacijska zaglavlja AH (engl. *Authentication Headers*) pružaju integritet i autentifikaciju izvora podataka za IP datagrame i pruža zaštitu protiv napada ponavljanjem.
- ESP (engl. *Encapsulating Security Payloads*) protokol osigurava tajnost podataka, autentifikaciju izvora, integritet, uslugu protiv ponavljanja (oblik integriteta djelomične sekvence) i ograničenu tajnost prometnog toka.
- Sigurnosne asocijacije SA (engl. *Security associations*) nude paket algoritama i podataka koji pružaju parametre potrebne za AH i/ili ESP operacije. ISAKMP (engl. *Internet Security Association and Key Management Protocol*) pruža okvir za provjeru autentičnosti i razmjenu ključa, sa stvarno ovjerenim materijalom za izradu ključa dobivenim ručnom konfiguracijom s unaprijed dijeljenim ključevima IKE (engl. *Internet Key Exchange*)[4].

Postoje dvije verzije IKE s pripadajućim karakteristikama:
IKEv1 (Internet Key Exchange verzija 1):

- razvijen krajem 1990-ih
- definiran u RFC 2409 [10]
- široko korišten u ranim IPsec implementacijama
- pruža okvir za autentifikaciju i razmjenu ključeva.

IKEv2 (Internet Key Exchange verzija 2):

- nasljednik IKEv1
- definiran u RFC 7296 [8]
- donosi poboljšanja u odnosu na IKEv1, uključujući bolji prolazak kroz NAT (engl. *Network Address Translation*), smanjeno vrijeme postavljanja veze i poboljšane sigurnosne postavke.

IKEv2 je dizajniran tako da bude efikasniji i fleksibilniji za mobilne i udaljene pristupne VPN scenarije. Svaka verzija IKE-a je evoluirala kako bi adresirala sigurnosne probleme, poboljšala performanse i prilagodila se promjenama u mrežnim okruženjima, čineći IKEv2 preferiranim izborom u modernim implementacijama VPN-a zbog poboljšanih mogućnosti i funkcionalnosti [7].

2.2.1. Autentifikacijsko zaglavlje (AH)

IPsec AH je ključna komponenta IPsec protokolskog skupa, uz ESP protokol. Dok se ESP fokusira na pružanje povjerljivosti podataka, AH je posebno dizajniran da ponudi usluge autentičnosti i integriteta za IP pakete.

AH postiže svoje ciljeve uključivanjem hash-baziranog koda autentifikacije poruke MAC (engl. *Message Authentication Code*) u naslov IP paketa, koji se izračunava nad sadržajem paketa, uključujući odabrane dijelove IP zaglavlja. Ovaj MAC omogućava primatelju IPsec-om zaštićene komunikacije provjeru da paket nije bio izmijenjen tijekom prijenosa i da dolazi od očekivanog pošiljatelja. Dodatno, AH pruža zaštitu protiv napada ponavljanja uključivanjem mehanizma koji detektira i odbacuje duplicirane ili zastarjele pakete.

Autentifikacija koju pruža IPsec AH ključna je za verifikaciju identiteta pošiljatelja i osiguravanje da podaci nisu izmijenjeni tijekom prijenosa. Uključivanjem AH u IP pakete, organizacije mogu uspostaviti visok stupanj povjerenja u integritet svojih mrežnih komunikacija, posebno u scenarijima gdje je sigurnost podataka od izuzetne važnosti. Ovaj mehanizam autentifikacije dodaje sloj sigurnosti koji osigurava da su podaci koji se prenose autentični i da ih nisu izmijenile neovlaštene strane.

Nadalje, AH protokol je instrumental u poboljšanju cjelokupnog sigurnosnog stanja IPsec implementacija. Korištenjem AH uz ESP, organizacije mogu postići sveobuhvatan sigurnosni okvir koji rješava kako povjerljivost podataka, tako i probleme integriteta podataka. Kombinacija AH i ESP omogućava robusnu sigurnosnu arhitekturu koja štiti osjetljive informacije i istovremeno provjerava autentičnost komunikacijskih krajnjih točaka.

U praktičnom smislu, AH protokol djeluje izračunavanjem *hash-a* nad sadržajem IP paketa i dodavanjem tih informacija o autentifikaciji u zaglavlje paketa. *Hash* služi kao digitalni potpis koji primatelj može verificirati kako bi potvrdio integritet i autentičnost paketa.

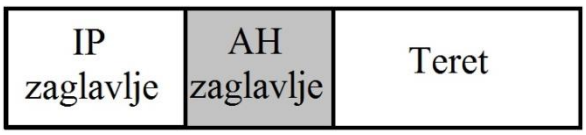
IPsec AH (Slika 2.3) je temeljna komponenta IPsec protokolskog skupa, pružajući ključne usluge autentičnosti i integriteta za IP pakete. Uključivanjem AH u IPsec implementacije, organizacije mogu uspostaviti sigurne komunikacijske kanale koji štite od izmjene podataka i neovlaštenog pristupa, čime se poboljšava ukupna sigurnost njihovih mrežnih infrastruktura [5].

Tablica 2.1. Format paketa autentifikacijskog zaglavlja

AH paket				
Oktet	**0**	**1**	**2**	**3**
Bit	**0-7**	**8-15**	**16-23**	**24-31**
0	Sljedeće zaglavlje	Dužina tereta	Rezervirano	
32	Indeks sigurnosnih parametara (engl. *Security Parameters Index – SPI*)			
64	Redni broj paketa			
96	Vrijednost za provjeru integriteta (engl. *Integrity Check Value – ICV*)			
...	...			

Tablica 2.1. prikazuje format autentifikacijskog zaglavlja, a njegovi dijelovi su:

- sljedeće zaglavlje (8 bita) – označava vrstu sljedećeg zaglavlja, čime govori koji je protokol iz gornjih slojeva zaštićen. Vrijednost se uzima iz popisa brojeva IP protokola
- dužina tereta (8 bita)
- rezervirano (16 bita) – rezervirano za buduću uporabu, do tada su svi bitovi 0
- indeks sigurnosnih parametara (32 bita) – proizvoljna vrijednost koja se koristi (skupa s odredišnom IP adresom) radi identificiranja sigurnosne asocijacije prijemne strane
- redni broj paketa (32 bita) – monotono strogo rastući redni broj (povećan za 1 za svaki poslani paket) koji se koristi za sprečavanje napada ponavljanjem. Kada je otkrivanje ponavljanja omogućeno, redni brojevi se nikada ne koriste ponovno, zato što se mora dogovoriti nova sigurnosna asocijacija prije pokušaja povećavanja rednog broja preko njegove maksimalne vrijednosti
- vrijednost za provjeru integriteta (*n* puta po 32 bita) – vrijednost za provjeru promjenjive dužine. Može sadržavati dopunu radi poravnavanja polja s 8-oktetnim granicama za IPv6 ili 4-oktetnim granicama za IPv4.



Slika 2.3. IP paket s AH zaglavljem [1]

2.2.2. ESP protokol

ESP (engl. *Encapsulating Security Payload*) unutar IPsec-a pruža autentifikaciju izvora, integritet i povjerljivost paketa. ESP također podržava konfiguracije samo s enkripcijom ili samo s autentifikacijom, iako je korištenje samo enkripcije bez autentifikacije nepreporučljivo zato što je nesigurno. Za razliku od autentifikacijskog zaglavlja ESP u transportnom načinu rada ne pruža autentifikaciju i integritet za cijeli IP paket. Međutim, u tunelirajućem načinu rada, gdje je cijeli originalni IP paket enkapsuliran i dodano mu je novo zaglavlje, ESP zaštita je omogućena cijelom unutarnjem IP paketu (uključujući i unutarnja zaglavlja) dok vanjska zaglavlja (uključujući vanjska zaglavlja IPv4 opcija i IPv6 proširenja) ostaju nezaštićena [4].

Tablica 2.3. Format ESP paketa

<table>
<tr><th colspan="5">ESP paket</th></tr>
<tr><td>Oktet</td><td>0</td><td>1</td><td>2</td><td>3</td></tr>
<tr><td>Bit</td><td>0-7</td><td>8-15</td><td>16-23</td><td>24-31</td></tr>
<tr><td>0</td><td colspan="4">Indeks sigurnosnih parametara (engl. Security Parameters Index – SPI)</td></tr>
<tr><td>32</td><td colspan="4">Redni broj paketa</td></tr>
<tr><td>64</td><td colspan="4" rowspan="3">Teret
(zaštićeni podatci)</td></tr>
<tr><td>...</td></tr>
<tr><td>...</td></tr>
<tr><td>...</td><td colspan="4" rowspan="3">Dopuna (0-255 okteta)</td></tr>
<tr><td>...</td><td colspan="2">Duljina dopune</td><td>Sljedeće zaglavlje</td></tr>
<tr><td>...</td><td colspan="4" rowspan="2">Vrijednost za provjeru integriteta (engl. Integrity Check Value – ICV)
...</td></tr>
<tr><td>...</td></tr>
</table>

Tablica 2.3. prikazuje ESP format:

- indeks sigurnosnih parametara (32 bita) - proizvoljna vrijednost koja se koristi (skupa s odredišnom IP adresom) radi identificiranja sigurnosne asocijacije prijemne strane
- redni broj paketa (32 bita) – monotono strogo rastući redni broj (povećan za 1 za svaki poslani paket) koji se koristi za sprječavanje napada ponavljanjem. Postoji poseban brojač za svaku sigurnosnu asocijaciju
- teret (promjenjiva dužina) – zaštićeni sadržaj originalnog IP paketa, uključujući bilo koje podatke korištene radi zaštite sadržaja (npr. inicijalizacijski vektor za kriptografski algoritam). Vrsta zaštićenog sadržaja je označena s poljem *Sljedeće zaglavlje*
- dopuna (0-255 okteta) – dodatak za enkripciju, radi povećanja tereta do veličine koja odgovara veličini bloka enkripcije
- duljina dopune (8 bita) – veličina dopune u oktetima
- vrijednost za provjeru integriteta (*n* puta po 32 bita) – vrijednost za provjeru promjenjive dužine. Može sadržavati dopunu radi poravnavanja polja s 8-oktetnim granicama za IPv6 ili 4-oktetnim granicama za IPv4.

2.2.3. Sigurnosne asocijacije (SA)

IPsec koristi koncept sigurnosne asocijacije kao temelj za izgradnju sigurnosnih funkcija unutar IP-a. Sigurnosna asocijacija je, jednostavno rečeno, skup algoritama i parametara (kao što su ključevi) koji se koriste za enkripciju i autentifikaciju određenog toka podataka u jednom smjeru. Stoga su u normalnoj, dvosmjernoj komunikaciji, tokovi podataka osigurani s parom sigurnosnih asocijacija.

Sigurnosna asocijacija je jednosmjerna (simplex) logička veza između dvaju IPSec sustava, koju jedinstveno identificira sljedeća trojka:

- indeks sigurnosnih parametara
- IP adresa odredišta
- sigurnosni protokol.

Indeks sigurnosnih parametara SPI (engl. *Security Parameters Index*) je 32 -bitna vrijednost kojom se razlikuju sigurnosne asocijacije s istom adresom odredišta i sigurnosnim protokolom. Prenosi se u zaglavlju sigurnosnog protokola (AH ili ESP). SPI ima samo lokalni značaj. SPI vrijednosti u rasponu 1-255 su rezervirane od strane IANA-e (engl. *Internet Assigned Numbers Authority*). SPI vrijednost 0 se mora koristiti za lokalne implementacije, u specifične svrhe. SPI je izabran od strane odredišnog sustava tijekom ustanovljavanja sigurnosne asocijacije [1].

IP adresa odredišta može biti *unicast*, *broadcast* ili *multicast* adresa. Međutim, trenutni mehanizmi upravljanja sigurnosnim asocijacijama su definirani samo za *unicast* adrese. Sigurnosni protokol može biti AH ili ESP. Sigurnosna asocijacija pruža sigurnosne usluge prometu prenošenog bilo pomoću AH ili ESP-a, ali ne oba. Drugim riječima, za vezu koja bi trebala biti zaštićena s AH i ESP, dvije sigurnosne asocijacije moraju biti definirane za svaki smjer. U ovom slučaju, niz sigurnosnih asocijacija koji definira vezu naziva se snop sigurnosnih asocijacija. Sigurnosne asocijacije unutar snopa ne moraju se prekinuti u istoj krajnjoj točki.

Sigurnosna asocijacije se ustanovljavaju pomoću ISAKMP (engl. *Internet Security Association and Key Management Protocol*) protokola. Kako bi odlučio koju zaštitu treba pružiti odlaznom paketu, IPsec koristi indeks SPI, indeks u bazi podataka SAD (engl. *Security Association Database*), zajedno s adresom odredišta u zaglavlju paketa, koji zajedno jedinstveno identificiraju sigurnosnu asocijaciju za taj paket. Sličan se postupak obavlja kod dolaznih paketa, gdje IPsec skuplja ključeve za dešifriranje i autentifikaciju iz baze podataka sigurnosnih asocijacija. Za multicast, sigurnosna asocijacija provodi se za grupu i duplicira se za sve autentificirane primatelje unutar grupe.

Može postojati više od jedne sigurnosne asocijacije za grupu, korištenjem različitih indeksa sigurnosnih parametara, a time se omogućava više razina sigurnosti unutar skupine [1].

Implementacija IPsec-a održava dvije baze podataka vezane za sigurnosne asocijacije:

- baza podataka sigurnosnih politika SPD (engl. *Security Policy Database*) određuje koje sigurnosne usluge će biti ponuđene IP prometu, ovisno o raznim čimbenicima kao što su izvor, odredište, ulazni ili izlazni promet itd. Sadrži organizirani popis unosa polica, odvojeno za ulazni i/ili izlazni promet. Ovi unosi mogu navesti da neki promet ne smije proći kroz IPsec obradu, neki mora biti odbačen, a ostatak mora biti obrađen od strane IPsec modula. Upisi u ovoj bazi podataka su slični pravilima vatrozida ili filtrima paketa
- baza podataka sigurnosnih asocijacija ili SAD (engl. *Security Associations Database*) sadrži informacije o parametrima svake sigurnosne asocijacije, poput AH ili ESP algoritama i ključeva, rednih brojeva, načinu rada protokola i vremenu života sigurnosne asocijacije. Za obradu izlaznog prometa, SPD unos pokazuje na SAD unos. To jest, SPD određuje koju sigurnosnu asocijaciju treba koristiti za dani paket. Za obradu ulaznog prometa SAD se konzultira kako bi se utvrdilo kako se paket treba obraditi.

2.3. IPsec načini rada

Postoje dva različita načina prema kojima IPsec može raditi:

- transportni način
- tunelski način.

Odabir između tunelskog načina i transportnog načina u IPsec implementacijama ovisi o specifičnim sigurnosnim zahtjevima i mrežnoj arhitekturi implementacije. Odabir odgovarajućeg načina u IPsec konfiguracijama također uzima u obzir čimbenike kao što su performanse, skalabilnost i upravljivost. Tunelski način, iako pruža robusnu sigurnost na razini mreže, može unijeti dodatno opterećenje zbog procesa enkapsulacije i dekripcije na mrežnim granicama. Nasuprot tome, transportni način, fokusirajući se na enkripciju od kraja do kraja, može ponuditi manju latenciju i bolje performanse za pojedinačne komunikacije domaćina unutar mreže.

Zaključno, razumijevanje razlika između IPsec tunelskog načina i transportnog načina ključno je za dizajniranje sigurnih komunikacijskih infrastruktura. Korištenjem tunelskog načina za sigurnost na razini mreže i transportnog načina za sigurnost na razini domaćina, organizacije mogu prilagoditi svoje IPsec implementacije kako bi učinkovito zadovoljile specifične sigurnosne i operativne zahtjeve [6].

2.3.1. Transportni način

Transportni način ima svoju svrhu, način funkcioniranja, upotrebu te prednosti i nedostatke.

Svrha:

- Osigurava komunikaciju između dva uređaja od kraja do kraja (engl. *end-to-end*).

Način funkcioniranja:

- Samo je sadržaj IP paketa (dio s podacima) enkriptiran i/ili autentificiran.
- Originalno IP zaglavlje ostaje netaknuto i koristi se za usmjeravanje paketa kroz mrežu.
- Tipično se koristi za komunikaciju između dva domaćina (engl. *host-to-host*).

Upotreba:

- Sigurna komunikacija između dva domaćina (npr. klijent i poslužitelj).
- Zaštita podatkovnog prometa na internim mrežama.

Prednosti:

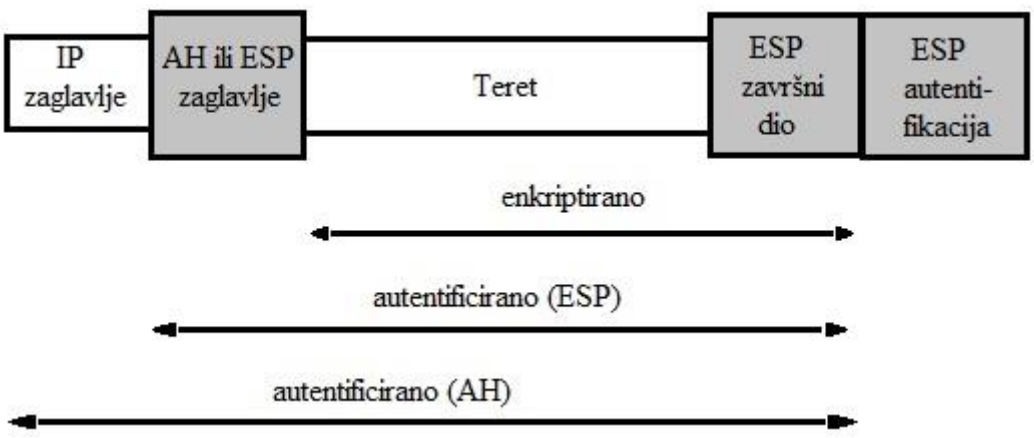
- Manji trošak u usporedbi s tunelskim načinom jer je enkriptiran samo korisni dio.
- Očuvanje originalnog IP zaglavlja omogućava učinkovitije usmjeravanje.

Nedostaci:

- Manje siguran od tunelskog načina jer originalni IP naslov, koji sadrži informacije kao što su adrese izvora i odredišta, nije enkriptiran.

Transportni način: Enkriptira samo korisni dio, zadržava originalni IP naslov, najbolji za komunikaciju između pojedinačnih domaćina.

Slika 2.4. Originalni IP datagram [1]



Slika 2.5. IP datagram u IPsec transportnom načinu rada [1]

2.3.2. Tunelski način

Tunelski način isto kao i transportni način ima svoju svrhu, način funkcioniranja, upotrebu te prednosti i nedostatke (Slika 2.6).

Svrha:

- Osigurava komunikaciju između dvije mreže ili između udaljenog korisnika i mreže.

Način funkcioniranja:

- Cijeli IP paket (naslov i sadržaj) je enkriptiran i/ili autentificiran.
- Novo IP zaglavlje je dodano enkriptiranom paketu i koristi se za usmjeravanje.
- Tipično se koristi za komunikaciju mreža s mrežom ili za VPN-ove za udaljeni pristup.

Upotreba:

- VPN-ovi između lokacija, gdje su dvije mreže sigurno povezane preko interneta.
- VPN-ovi za udaljeni pristup, gdje se pojedinačni korisnici sigurno povezuju s mrežom.

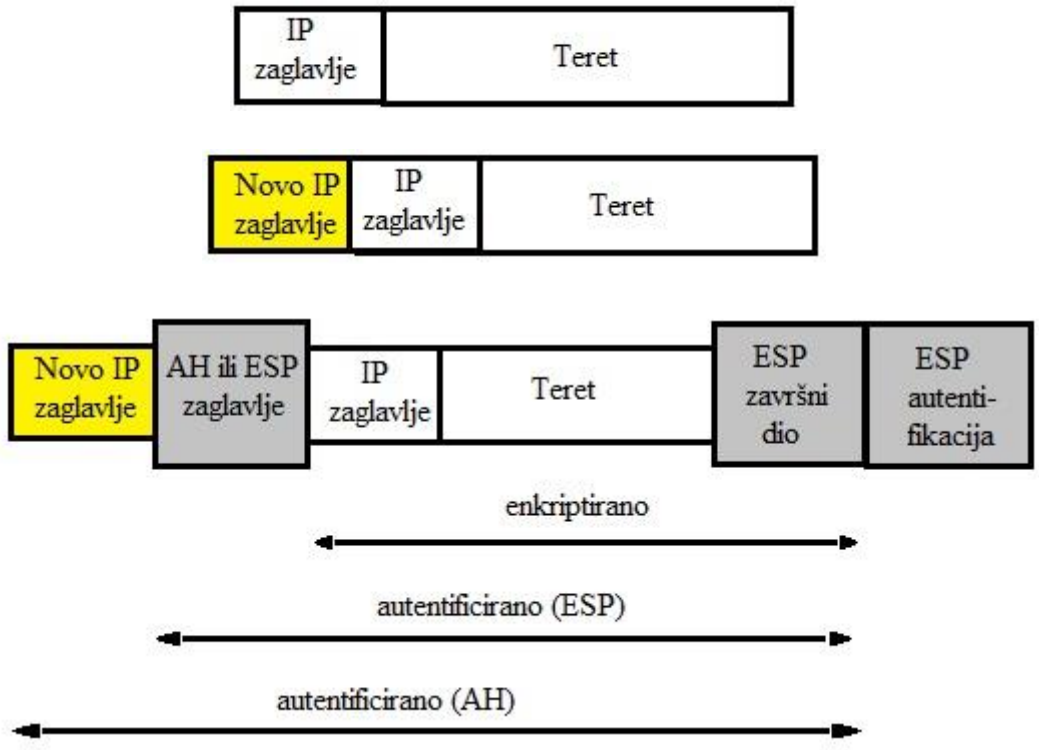
Prednosti:

- Pruža veću sigurnost jer je cijeli originalni IP paket enkriptiran.
- Vanjski IP naslov može se koristiti za skrivanje originalnih IP adresa, pružajući dodatnu sigurnost i anonimnost.

Nedostaci:

- Veći trošak zbog dodavanja novog IP naslova i enkripcije cijelog paketa.
- Može rezultirati većim veličinama paketa, što može utjecati na performanse.

Tunelski način: Enkriptira cijeli IP paket, dodaje novo IP zaglavlje, najbolji za komunikaciju mreža s mrežom ili VPN-ove za udaljeni pristup.



Slika 2.6. IP datagram u IPsec tunelirajućem načinu rada [1]

2.4. Parametri IPsec-a

IPsec se sastoji od više dijelova koji će se objasniti u nastavku te se mogu svrstati u 4 skupine:

1. Scenarij
2. Osnovna konfiguracija
3. Protok podataka
4. IKE/IPsec prijedlog.

2.4.1 Scenarij

Pod scenarijem na VPN uređaju poduzeća postoje dvije opcije, a to su:

- Mjesto do mjesta - ovaj način se koristi u scenariju gdje je *peer* uređaj jedan jedini *gateway*. Lokalni uređaj je *gateway* grananja u topologiji zvijezde, ili *gateway* na jednom od krajeva tunela. *Peer* uređaj ima fiksnu IP adresu ili naziv domene.
- Mjesto do više mjesta (engl. *site-to-multisite*) - ovaj način se koristi kada je lokalni uređaj glavni *gateway*, a *peer* uređaji su višestruki *gateway*-i. Također se koristi s L2TP preko IPsec-a, IKEv1 i IKEv2 pristupom putem biranja. *Peer* uređaj može biti *gateway* grananja, PC, iOS uređaj, Android uređaj ili bežična bazna stanica.

2.4.2. Osnovna konfiguracija

Kada se govori o osnovnoj konfiguraciji pod time se misli na sljedeće podatke:

- Ime VPN tunela
- Peer IP adresa – odredišna IP adresa VPN uređaja
- Peer IP adresa od klijenta – odredišna IP adresa klijentovog uređaja (VPS).
- Vrsta autentifikacije – PSK (engl. *pre-shared key*) ili RSA potpis (engl. *Rivest-Shamir-Adleman signature*). PSK je lozinka za koju se dvije strane odluče podijeliti sigurnosnim putem. RSA potpis uključuje generiranje para kriptografskih ključeva, a to je javni ključ koji se koristi za enkripciju i verifikaciju te se slobodno distribuira i poznat je svima. Privatni ključ se čuva tajno i koristi se za dekripciju i potpisivanje.

Peer IP adrese odnose se na specifične IP adrese dodijeljene pojedinačnim VPN krajnjim točkama ili uređajima koji sudjeluju u VPN vezi.

2.4.3. Protok podataka

Pod postavkama protoka podataka mora/ju se mapirati izvorna/u IP domenu/e i odredišnu/e IP domenu/e. IP domena obično se odnosi na raspon ili podmrežu IP adresa koje se koriste unutar VPN mreže. IP domena upravlja se i dodjeljuje od strane administratora VPN-a ili pružatelja usluga i koristi se za olakšavanje komunikacije i usmjeravanja između različitih uređaja i krajnjih točaka unutar VPN-a.

2.4.4. IKE/IPsec prijedlog

IKE/IPsec prijedlog se dijeli u dvije faze: Faza 1 (IKE prijedlog) i faza 2 (IPsec prijedlog) IKE prijedlog je odgovoran za pregovaranje, uspostavljanje, modificiranje i brisanje sigurnosnih udruženja (SA) i kriptografskih ključeva. Uključuje sljedeće komponente:

- Odabir IKE verzije: Odabire se između IKEv1 i IKEv2.
- Algoritam za šifriranje: Specificira algoritam koji se koristi za šifriranje podataka. Česti algoritmi uključuju AES (engl. *Advanced Encryption Standard*), DES (engl. *Data Encryption Standard*) i 3DES (engl. *Triple Data Encryption Standard*).
- Algoritam za integritet: Specificira algoritam koji se koristi za osiguravanje integriteta podataka. Česti algoritmi uključuju SHA1 (engl. *Secure Hash Algorithm 1*), SHA2 (engl.

Secure Hash Algorithm 2), MD5 (engl. *Message Digest Algorithm 5)* i AES (engl. *Advanced Encryption Standard*).

- DH (engl. *Diffie-Hellman*) grupa: Specificira grupu koja se koristi za DH razmjenu ključeva, što osigurava sigurnu razmjenu kriptografskih ključeva.
- PRF ili pseudo-slučajna funkcija (engl. *Pseudo-Random Function*): Specificira algoritam koji se koristi za generiranje pseudo-slučajnih vrijednosti, koje su ključne za generiranje ključeva. Česti PRF-ovi se temelje na algoritmima SHA1, SHA2, MD5 i AES.
- Trajanje: Specificira koliko dugo će sigurnosno udruženje SA koje je stvorio IKE ostati valjano prije potrebe za ponovnim pregovaranjem.

Tijekom pregovaranja IKE-a, svaki uređaj šalje svoj prijedlog drugome te se dogovaraju o zajedničkom skupu parametara na temelju vlastitih mogućnosti i sigurnosnih politika. IKE prijedlozi osiguravaju da se oba kraja VPN tunela slažu oko načina sigurne razmjene ključeva i uspostave šifrirane komunikacije. IKE prijedlozi se konfiguriraju u postavkama VPN uređaja i moraju se podudarati na oba kraja kako bi se VPN tunel uspješno uspostavio.

IPsec prijedlog se pokreće tek kada je IKE prijedlog uspješno završen. IPsec prijedlog, može se reći, nadograđuje IKE prijedlog, a odnosi se na dio pregovaračkog procesa u kojem se stvaraju stvarna sigurnosna udruženja (SA) između dva kraja veze kako bi se osiguralo da se obje strane slažu o algoritmima šifriranja, integriteta i razmjene ključeva za zaštitu prometa koji će biti poslan preko VPN-a.

IPsec prijedlog uključuje sljedeće komponente:

- Način enkapsulacije: Odnosi se na metodu koja se koristi za enkapsulaciju IP paketa dodatnim zaglavljima i završetcima. Pod zadano se koristi transportni način rada osim ako se ne definira drugačije.
- Sigurnosni protokol: Bira se između jednog od navedenih protokola: ESP, AH, ESP-AH. AH-ESP protokol u IPsec-u koristi i AH i ESP kako bi pružio sveobuhvatne sigurnosne usluge, uključujući integritet podataka, autentifikaciju izvora podataka, povjerljivost podataka i zaštitu od ponavljanja napada.
- ESP enkripcija: Algoritam koji se koristi za šifriranje sadržaja IP paketa. Česti algoritmi uključuju GCM, AES, 3DES i DES.
- ESP autentifikacija: algoritam koji se koristi za autentifikaciju sadržaja IP paketa. Koriste se SHA2 ili SHA1 algoritmi.

- PFS (engl. *Perfect Forward Security*): Iako izravno nije povezano s autentifikacijom, PFS se često razmatra u IPsec prijedlozima radi poboljšane sigurnosti. PFS osigurava da kompromitacija dugoročnog ključa ne kompromitira ključeve prethodnih sesija, čime se pruža dodatna zaštita od kriptografskih napada.
- SA trajanje: Specificira koliko dugo će prijedlog biti validan prije ponovnog pokretanja prijedloga zbog sigurnosti prometa. Postavlja se u sekundama i kilobajtima ili samo u sekundama.

3. KREIRANJE I KONFIGURACIJA VPS

U ovom poglavlju je opisan postupak konfiguracije i uspostave VPN tunela između NTH-ovog fizičkog servera (simtest-mtt), VPN uređaja i VPS (engl. *Virtual Private Server*) od poslužitelja Linode. U okviru ovog poglavlja prikazani su i pojašnjeni primijenjeni alati i programi, proces kreiranja VPS-a, njihovog podešavanja, instalacija i konfiguracije.

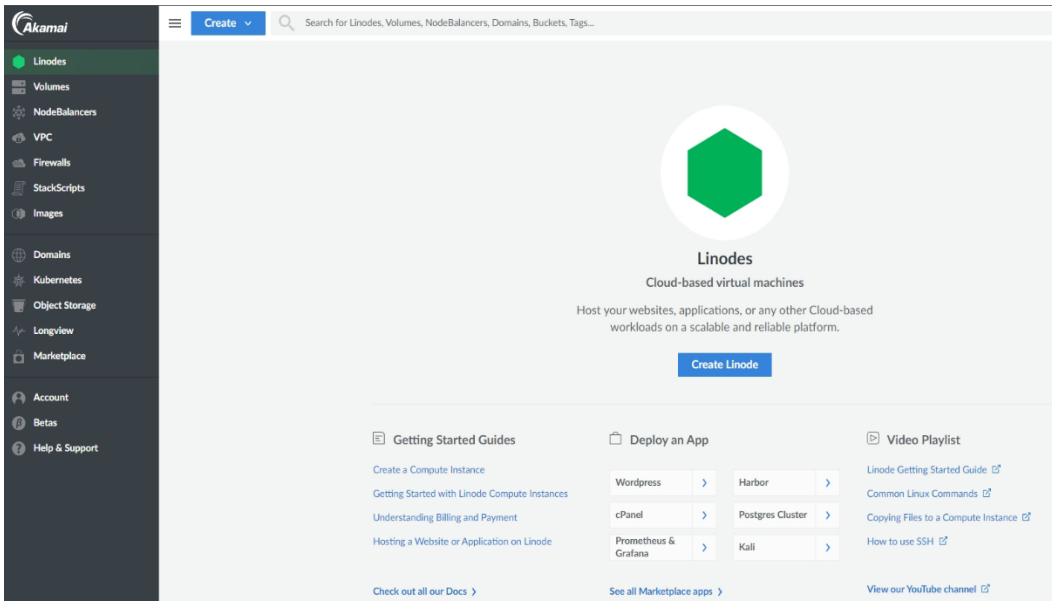
3.1. Popis alata i programa

Za uspostavu i testiranje VPN tunela u ovom radu mora se imati:

1. Registrirani račun na stranici https://cloud.linode.com/ koja omogućuje kreiranje VPS.
2. Pristup na Huawei *gateway* korisničko sučelje koje odobrava odgovorna osoba IT odjela u poduzeću.
3. Instaliran programski paket MTPuTTY (besplatno se može preuzeti na mrežnoj stranici: https://www.putty.org/). MTPuTTY se obično koristi za sigurno povezivanje s udaljenim poslužiteljima i spajanja na terminal, prvenstveno Linux ili Unix sustavima. SSH (engl. *Secure Shell*) šifrira vezu, osiguravajući da su preneseni podaci između klijenta i poslužitelja sigurni.
4. Korištenje PING ili TELNET komande u UNIX-u.

3.2. Kreiranje VPS

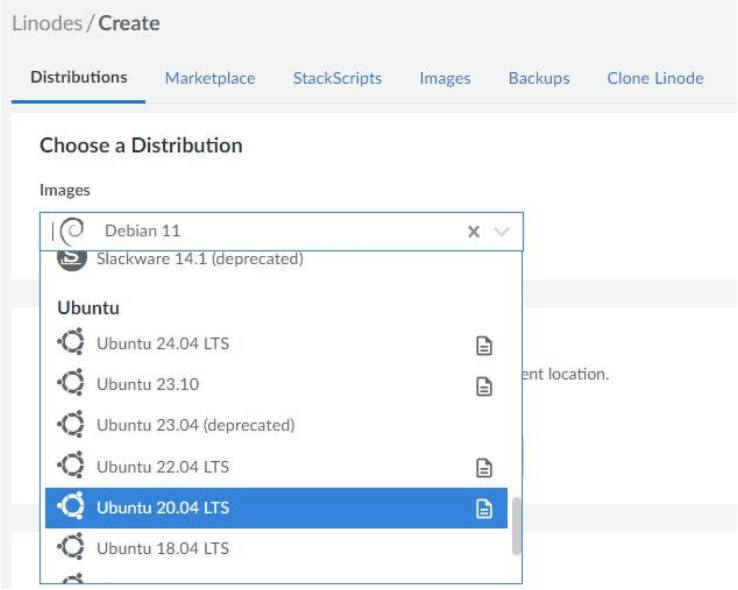
Nakon kreiranja računa i logiranja na stranicu odabire se „Create Linode“. Nakon toga otvara se novi prozor gdje se odabiru postavke VPS-a kao što je prikazano na slici 3.1.



Slika 3.1. Početno korisničko sučelje Linode

3.2.1. Odabir operativnog sustava i verzije

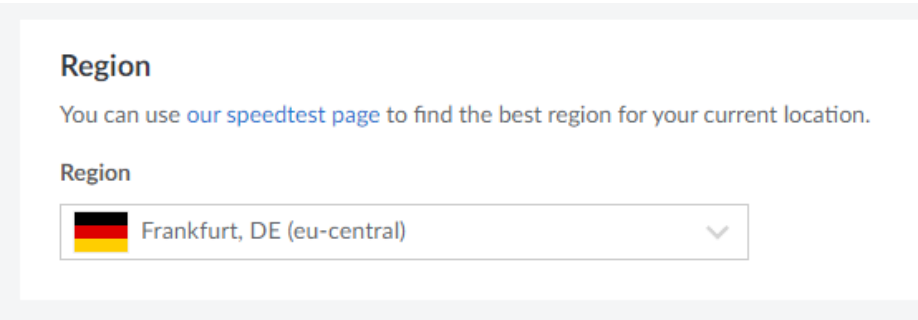
Opcija prikazana slikom 3.2. omogućuje početak sa stabilnim Linux operativnim sustavom i izgradnju vlastitog softverskog stoga (engl. *Software Stack*). Popularne distribucije uključuju najnovija LTS (engl. *Long Term Support*) izdanja Ubuntu-a, Debian-a, CentOS Stream-a, RHEL-derivata (kao što su AlmaLinux i Rocky Linux) i mnoge druge. Svaka distribucija dolazi s vlastitim setom predinstaliranog softvera i naredbi. U osnovi se odabire operativni sustav i verzija koja je najpoznatija korisniku VPS-a.



Slika 3.2. Početno korisničko sučelje Linode

3.2.2. Regija

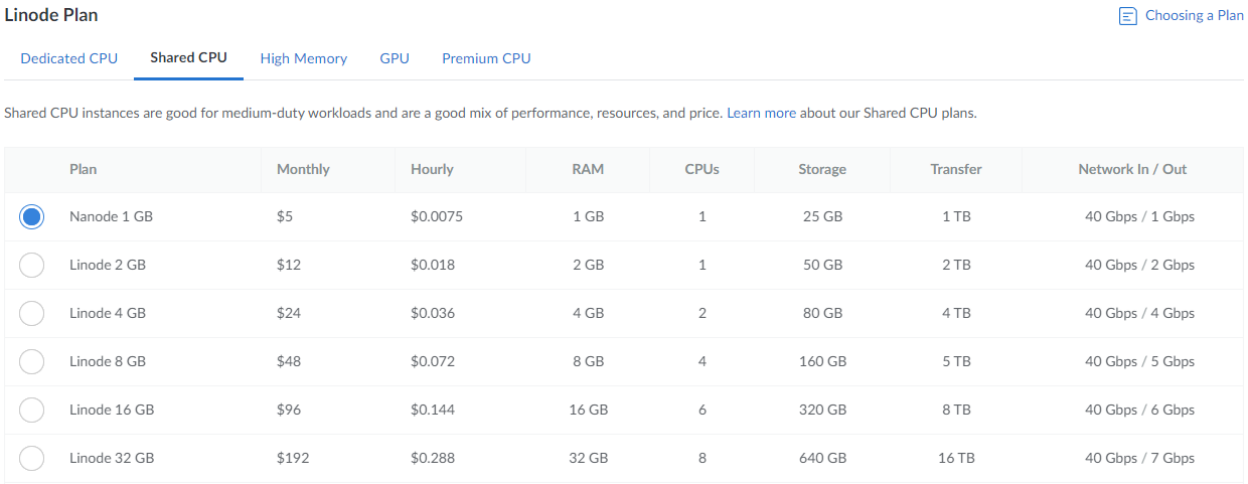
Mora se odabrati regija u kojoj će se smjestiti VPS (Slika 3.3). Regije odgovaraju pojedinačnim DC-ovima (engl. *Data Center*), svaki smješten u drugom geografskom području. Preporučljivo je odabrati regiju koja je najbliža klijentu s kojim se želi uspostaviti VPN. Navedeno pomaže u smanjenju latencije i može znatno utjecati na brzinu i kvalitetu veze. Pošto se od poduzeća VPN *gateway* nalazi u Švicarskoj odabrana je Njemačka pošto se Švicarska ne nalazi na popisu zemalja.



Slika 3.3 Odabir regije gdje će nam se nalaziti VPS

3.2.3. Linode plan

Linode nudi nekoliko različitih vrsta instanci i veličine planova, svaka s unaprijed određenim resursima hardvera (kao što su vCPU jezgre, memorija i prostor za pohranu). U nastavku će se objasniti popis vrsta instanci zajedno s njihovim veličinama planova i primjerima upotrebe. Za potrebe ovog rada kao primjer odabrat će se najjeftiniji plan (Slika 3.4).



Slika 3.4. Odabir konfiguracije VPS-a

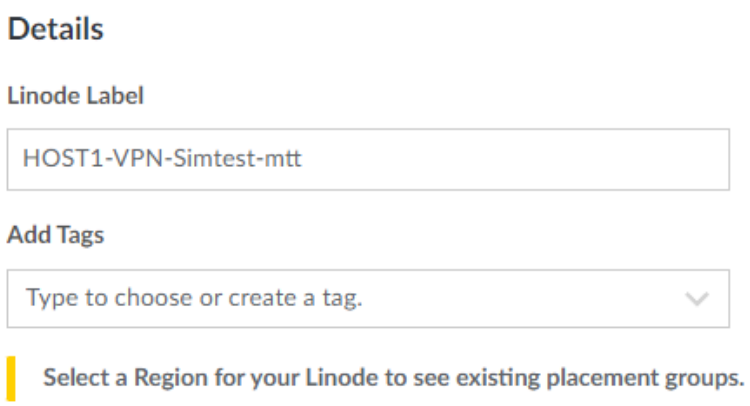
Cijena ovisi o odabiru komponenti ispod:

- Dedicirani ili dijeljeni CPU (engl. *Central Processing Unit*): Dijeljeni CPU-ovi su povoljniji i stoga mogu pružiti veću vrijednost u usporedbi s cijenom, posebno za radna opterećenja koja nisu zahtjevna za CPU i kada visoke CPU performanse nisu potrebne. Radna opterećenja prikladna za dijeljene CPU instance uključuju razvojne servere, *staging* servere, *web* stranice s malim prometom, osobne blogove te produkcijske aplikacije koje možda neće biti pogođene zbog sukoba resursa. Dedicirani CPU-ovi preporučuju se za većinu produkcijskih aplikacija i svaku aplikaciju koja zahtijeva 100 % kontinuirane upotrebe. Navedeno uključuje eCommerce web stranice, poslovne aplikacije, servere za igrice, CI/CD (engl. *Continuous Integration/Continuous Deployment*) alate, transkodiranje audio i video zapisa, strojno učenje, znanstveno računanje, baze podataka s visokim prometom i mnogo više.
- RAM (engl. *Random Access Memory*): Radna memorija dostupna za procese poslužitelja. Poslužitelj pohranjuje informacije u memoriji potrebne za obavljanje svojih funkcija. Također, podatke pohranjuje u memoriju kako bi se brzo dohvatili u budućnosti ako je vjerojatno da će biti potrebni. Podacima pohranjenima u RAM-u pristupa se brže nego podacima pohranjenima na disku Linodea, ali nije riječ o trajnom skladištenju.
- CPUs: Broj vCPU-a (engl. *Virtual Central Processing Unit*). Što je veći broj vCPUs, to se više posla može obaviti istovremeno. Planovi također dolaze s dijeljenim CPU jezgrama ili s posvećenim CPU jezgrama. Posvećene CPU jezgre omogućuju sustavu korištenje 100 % resursa CPU-a u svakom trenutku, dok dijeljene CPU jezgre zahtijevaju nižu kontinuiranu upotrebu i mogu biti pogođene sukobom resursa.

- Skladište (engl. *Storage*): Trajno pohranjivanje ugrađeno u VPS. Velike baze podataka, medijske datoteke i druga skladišta ili datoteke zahtijevaju više prostora za pohranu. Skladište VPS-a održava se na SSD-ovima visokih performansi za brzi pristup.
- Prijenos (engl. *Transfer*): Ukupna količina prometa koju VPS može poslati tijekom mjeseca. Ulazni promet poslan VPS-u ne računa se u kvotu prijenosa. Ako se premaši kvota, usluga se neće isključiti već će se umjesto toga obračunati dodatni troškovi.
- *Network In:* Maksimalna propusnost za ulazni promet poslan prema VPS-u. Koja će biti propusnost također ovisi o drugim čimbenicima, poput geografske udaljenosti između klijenta i VPS-a te propusnosti lokalnog ISP-a (engl. *Internet Service Provider*). Brzina se računa u Gb/s (gigabiti u sekundi).
- *Network Out:* Maksimalna propusnost za odlazni promet poslan iz VPS-a. Propusnost kao i kod *Network In-a* ovisi o drugim čimbenicima, poput geografske udaljenosti između klijenta i VPS-a te propusnosti lokalnog ISP-a (engl. *Internet Service Provider*). Brzina se također računa u Gb/s.

3.2.4. Detalji

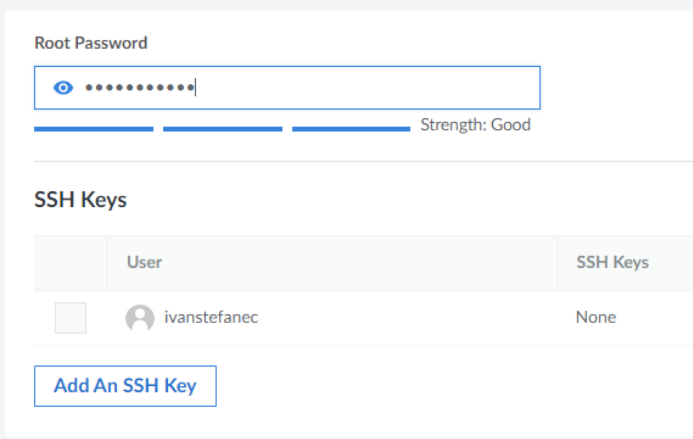
U izborniku (Slika 3.5) postavlja se ime VPS-a i moguća oznaka koja je opcionalna. Ime treba služiti da bi se prikazao pokazatelj za što se VPS koristi. Ime može sadržavati samo slova, brojeve, podvlake, crtice i točke. Oznake (engl. *Tags*): Dodavanje oznaka omogućuje kategorizaciju Linode usluge prema vlastitim željama. Na primjer, web razvojna agencija može dodati oznaku za svakog klijenta koje poduzeće ima. Također se mogu staviti oznake koje označavaju koje usluge su za razvoj, testno ili produkcijsko okruženje.



Slika 3.5. VPS Detalji

3.2.5. Kreiranje administrativne *(engl. Root)* lozinke

Izraz "*root*" obično se odnosi na račun ili lozinku povezanu s administrativnim računom na Unix operativnim sustavima.



Slika 3.6. Postavljanje lozinke i SSH key-a

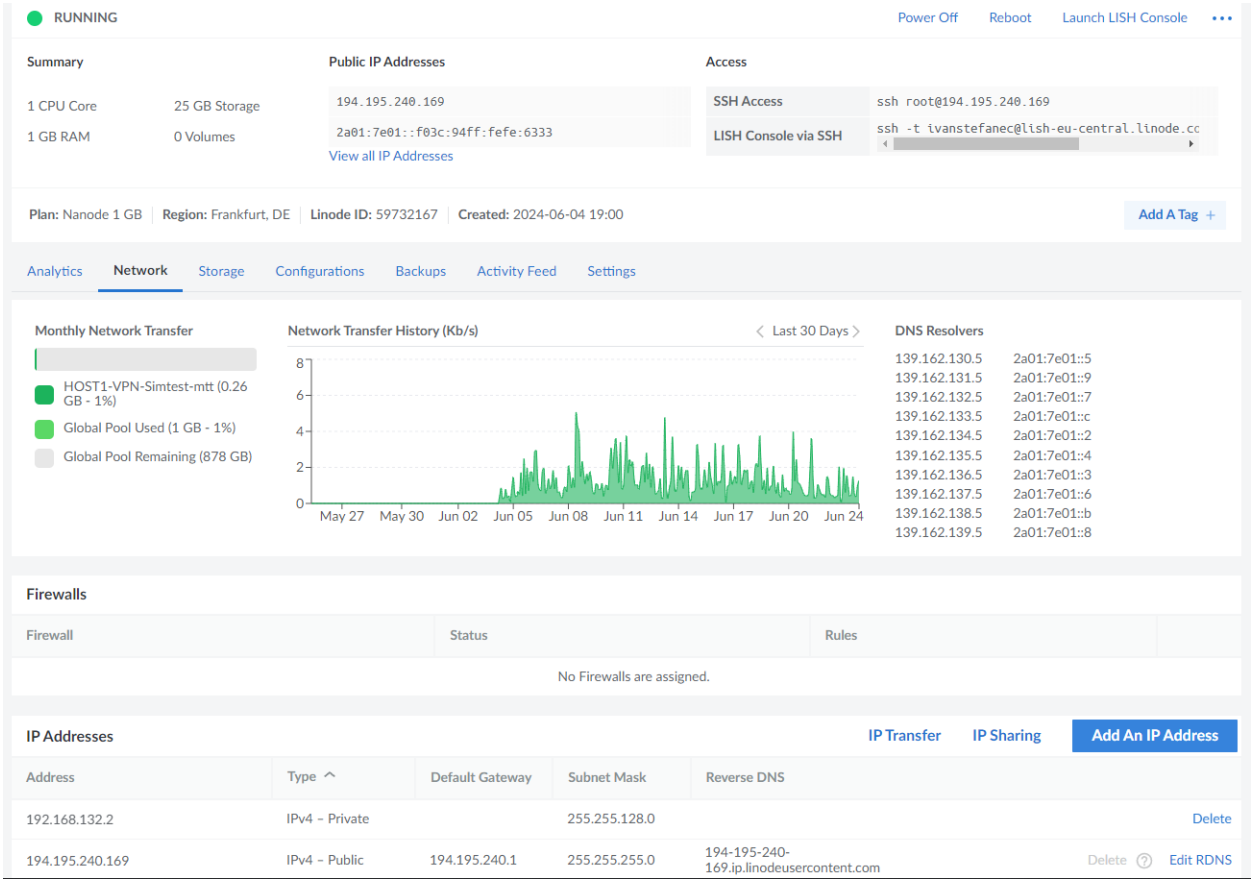
Lozinka se može postaviti prema slobodnom izboru, ali je izrazito važno da bude što kompleksnija zbog sigurnosti sustava (Slika 3.6). SSH ključevi omogućuju prijavu putem SSH-a bez potrebe za lozinkom. SSH ključevi se stvaraju kao par: privatni ključ koji je pohranjen na lokalnom računalu i javni ključ koji se može prenijeti na udaljene sustave i usluge. Budući da se dijeli samo javni ključ, privatni ključ je siguran i zaštićen, ovo je mnogo sigurnija metoda autentifikacije od lozinki.

3.2.6. Detalji VPS-a

Ostale opcije nakon ove su opcionalne i ovise o pristupu i vrsti korištenja VPS-a. Nakon postavljanja svih opcionalnih parametra i obveznih detalja potrebno je kliknuti na gumb „Create Linode“ koji se nalazi na dnu stranice. Nakon 1-2 minute VPS je aktivan i spreman za dodatnu konfiguraciju i korištenje. Nakon što status prijeđe u „*Running*“ vidljivo je mnogo detalja VPS-a uključujući osnovne podatke VPS-a, statistike korištenja procesora, detalji i analiza mreže, upravljanje SSD diska, provjera i izmjena konfiguracije, dnevnik aktivnosti i promjene postavki VPS-a vidljivo na slici 3.7. Najvažniji podaci VPS-a za konfiguraciju IPsec-a su:

- javna IP adresa (*engl. Public IP*): Radi se o odredišnoj IP adresi VPS-a koja je 194.195.240.169
- privatna IP adresa (*engl. Private IP*): Radi se o izvornoj IP adresi VPS-a koja je 192.168.132.2.
- SSH pristup (engl. *SSH Access*): Korisničko ime za spajanje na terminal putem SSH.

- Podmrežna maska (engl. *Subnet mask*): Riječ je o 32-bitnom broju koji se koristi zajedno s IP adresom kako bi se odredilo koji dio te adrese pripada mreži, a koji dio pripada uređaju unutar te mreže. Ovaj broj je potreban da bi se dodala ruta na krajnjem fizičkom serveru *simtest-mtt*.

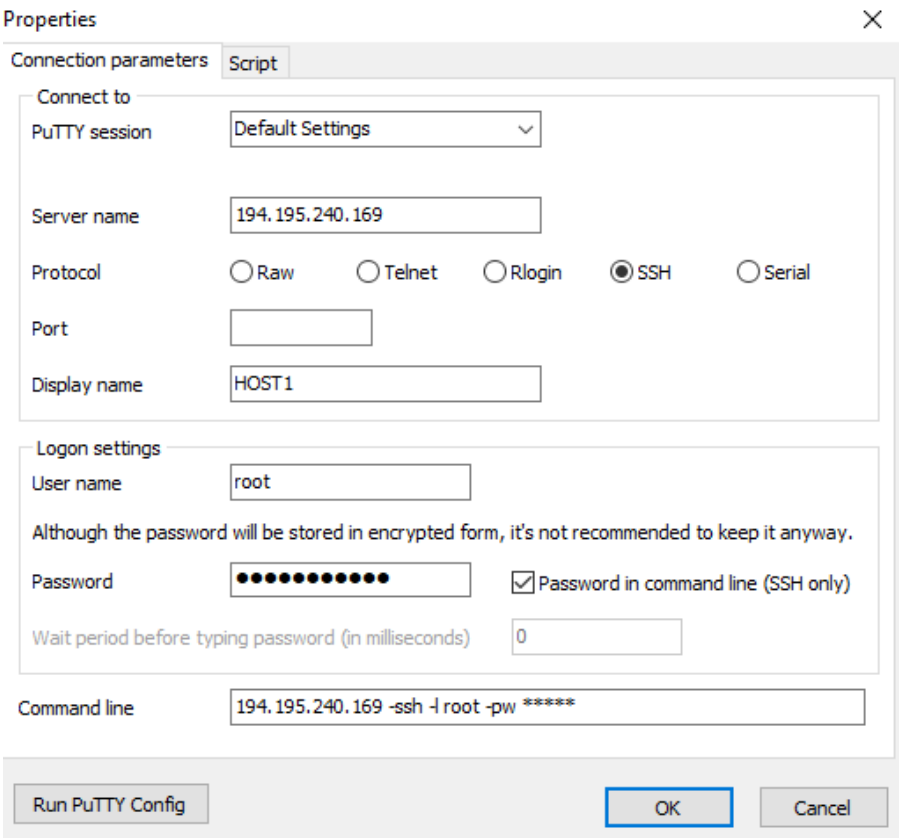


Slika 3.7. Detalji VPS-a na Linode-u

3.3. Podešavanje VPS-a putem SSH terminala i komandi

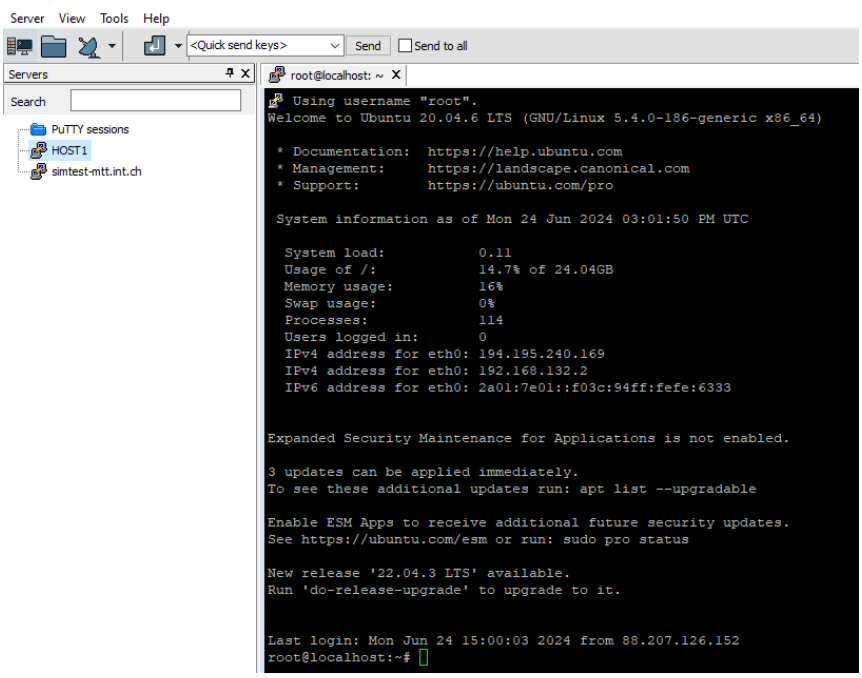
Podešavanje VPS-a vršit će se putem terminala (Slika 3.8) na koji se spaja korištenjem ranije spomenutog programa MTPuTTY. Odabire se kreiranje novog servera za povezivanje te upisujemo obvezne podatke:

- javna adresa IP servera
- protokol spajanja na terminal
- naziv servera
- korisničko ime
- lozinka.



Slika 3.8. Konfiguracija za spajanje na VPS putem terminala

Nakon što se terminal logira izgleda kao na slici 3.9.

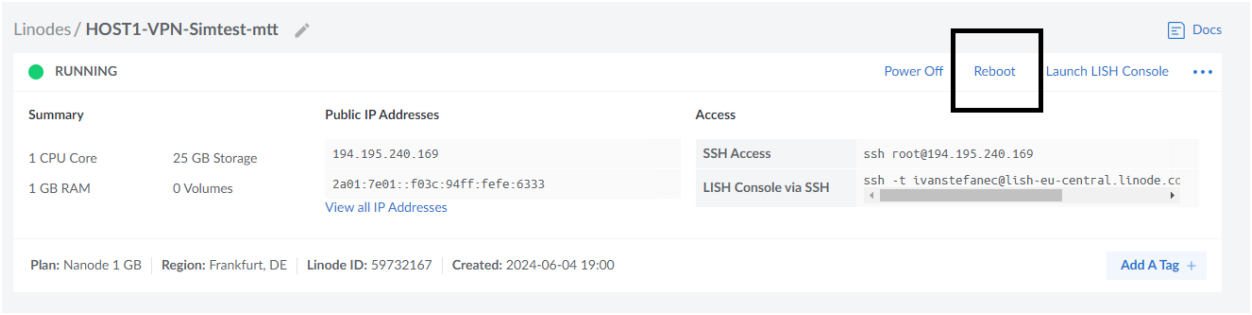


Slika 3.9. SSH terminal nakon uspješnog logiranja

Prije svega moraju se odraditi dvije komande:

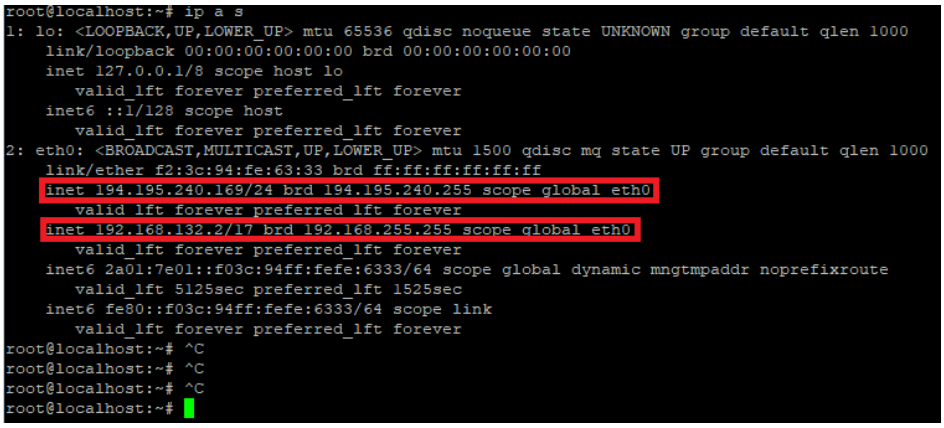
- *„apt update“*: Koristi se kako bi se osvježio lokalni indeks paketa. Kada se pokrene, komanda kontaktira konfigurirane repozitorije (definirane u */etc/apt/sources.list* i */etc/apt/sources.list.d/)* i preuzima listu paketa iz tih repozitorija. Ove liste sadrže informacije o najnovijim verzijama paketa koje su dostupne za instalaciju. Osigurava da upravitelj paketa *apt* bude svjestan najnovijih verzija paketa koje pružaju repozitoriji.
- *„apt upgrade“*: Koristi se za nadogradnju instaliranih paketa na najnovije verzije dostupne u repozitorijima. Ako su dostupne nove verzije paketa, *apt upgrade* će ih preuzeti s repozitorija i instalirati na sustavu. Isto tako instalira sigurnosne nadogradnje, ako su dostupne, čime osigurava da sustav bude ažuran i siguran.

Nakon izvršenja ovih dviju komandi potrebno je resetirati VPS kako bi se pohranile izmjene odrađene nakon pokretanja komandi. Navedeno se jednostavno odradi tako da se ode na Linode i klikne na *Reboot* (Slika 3.10). ili komandom u terminalu „*reboot“*.



Slika 3.10. Linode reboot opcija

Korištenjem komande „*ip a s*“ u terminalu može se vidjeti odredišna i izvorna adresa kao što je prikazano na slici 3.11.



Slika 3.11. Lista odredišne i izvorne IP adrese u terminalu

Linija „*inet 192.168.132.2/17 brd 192.168.255.255 scope global eth0*“ opisuje mrežnu konfiguraciju mrežnog sučelja *eth0* s IPv4 (engl. *Internet Protocol version 4*) adresom 192.168.132.2/17

Sastoji se od:

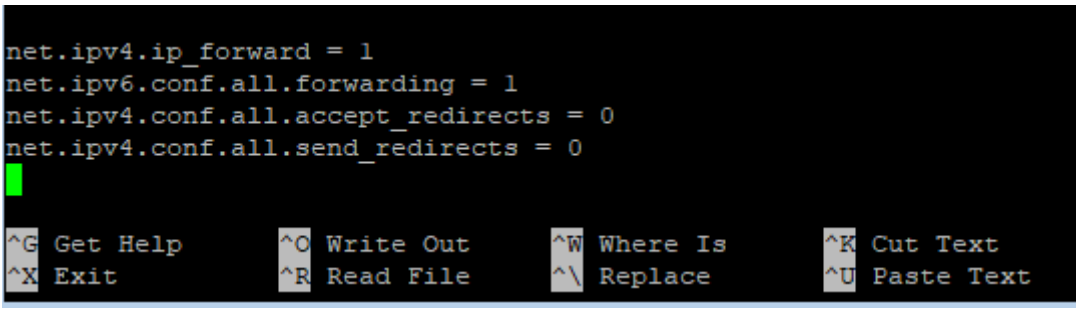
- *inet 192.168.132.2/17*: Ovo označava da sučelje eth0 ima IPv4 adresu 192.168.132.2 s podmrežnom maskom /17. Maska podmreže /17 znači da se prvih 17 bitova IP adrese koristi za mrežni dio, dok se preostalih 15 bitova koristi za adrese hostova unutar te mreže. Navedeno rezultira podmrežnom maskom 255.255.128.0.
- *brd 192.168.255.255*: Ovo specificira broadcast adresu za podmrežu, koja je 192.168.255.255. Broadcast adrese koriste se za slanje podatkovnih paketa svim uređajima unutar određene podmreže.
- *scope global*: Ovo označava da je IP adresa 192.168.132.2 globalno dostupna, što znači da se može koristiti za komunikaciju s uređajima izvan njene podmreže.
- *eth0*: Ovo je naziv mrežnog sučelja kojem je dodijeljena IP adresa.

Sljedeći korak je omogućavanje IP prosljeđivanja pošto pod normalno ta opcija nije uključena. Da bi se to odradilo mora se koristiti komanda „*nano*“ za konfiguracijsku datoteku „*sysctl.conf*“. Komanda „*nano*“ pokreće jednostavan tekstualni urednik koji se često koristi u Unix operacijskim sustavima, a konfiguracijska datoteka „*sysctl.conf*“ se koristi za konfiguriranje kernelnih parametara tijekom izvršavanja.

Ovi parametri kontroliraju različite aspekte ponašanja, performansi i sigurnosti sustava među kojima su najčešći:

- Konfiguracija mreže: Prilagodba parametara vezanih uz mrežu, poput omogućavanja prosljeđivanja IP paketa za rutiranje paketa između mrežnih sučelja.
- Prilagođavanje performansi: Konfiguriranje postavki za upravljanje memorijom, I/O operacije i raspoređivanje CPU-a radi optimizacije performansi sustava.
- Postavke sigurnosti: Postavljanje sigurnosno vezanih parametara za kontrolu ponašanja kernela i smanjenje određenih vrsta napada ili ranjivosti.

U svrhu omogućavanja IP prosljeđivanja potrebno je dodati 4 linije ispod na kraj datoteke kao što je vidljivo na slici 3.12.



Slika 3.12. Editiranje datoteke *sysctl.conf*

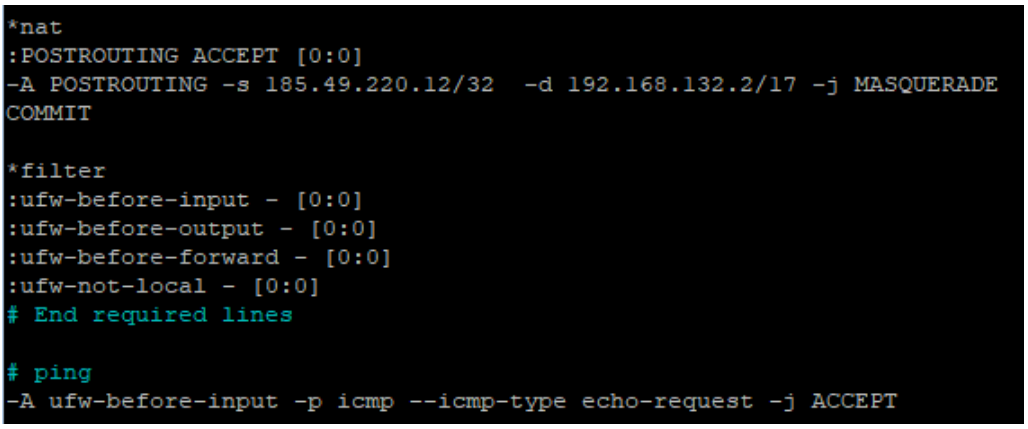
Izmjene se spremaju sa „Ctrl + O“ i zatvaranje urednika sa „ Ctrl + X“.

Nakon izmjene datoteke „*sysctl.conf*“ potrebno je odraditi komandu „*sysctl -p*. Navedena komanda ponovno učitava datoteku „sysctl.conf“ i ažurira kernelne parametre prema novim postavkama navedenima u datoteci.

Nakon toga treba se odobriti da sustav prihvaća dolazne SSH konekcije kroz vatrozid Linux sustava koji koristi UFW (engl. *Uncomplicated Firewall*), a to se radi komandom „*ufw allow ssh“*. Objašnjenje komande:

- *ufw*: Ovo je naredbeni alat za upravljanje pravilima vatrozida UFW.
- *allow*: Ova podnaredba koristi se za dopuštanje dolaznog prometa za određenu uslugu ili port.
- *ssh*: Ovo je predefinirano ime usluge u UFW-u koje odgovara TCP portu 22, zadanim portom koji koristi SSH.

Nakon što se vatrozidu da dopuštenje za dolazne SSH konekcije onda se vatrozid upali komandom „*ufw enable*“. Dodatni potrebni korak je modificiranje UFW datoteke „*before.rules*“. sa „*nano*“ koja se nalazi na lokaciji “*/etc/ufw/before.rules*“. Potrebno je dodati linije ispod kao što je vidljivo na slici 3.13.



Slika 3.13. Uređivanje UFW-a

Objašnjenje linija:

- **nat*: Specificira da se sljedeća pravila moraju primijeniti na NAT (engl. *Network Address Translation*) tablicu. NAT tablica je temeljna komponenta usmjeravanja i sigurnosti mreže koja upravlja prijevodom IP adresa između različitih mreža.
- *:POSTROUTING ACCEPT [0:0]*: Inicijalizira POSTROUTING lanac u nat tablici s politikom prihvaćanja svih paketa ([0:0] predstavlja brojače paketa i bajtova).
- *-A POSTROUTING*: Dodaje (dodaje) pravilo u POSTROUTING lanac.
- *-s 185.49.220.12/32*: Specificira izvornu IP domenu (185.49.220.12/32 označava jednu IP adresu).
- *-d 192.168.132.2/17*: Specificira odredišnu IP domenu (192.168.132.2/17 označava IP adresu 192.168.132.2 s /17 mrežnom maskom).
- *-j MASQUERADE*: Radnja koja se izvodi ako paket odgovara pravilu, u ovom slučaju, maskiranje (promjena) izvorne IP adrese kako bi odgovarala IP adresi izlaznog sučelja.
- *COMMIT*: Označava kraj konfiguracije nat tablice.

Izmjene se spremaju s „Ctrl + O“ i zatvaranje urednika s „ Ctrl + X“. Nakon uređivanja postavki vatrozida potrebno je isti i resetirati s komandama „*ufw disable*“ te nakon toga s „*ufw enable*“.

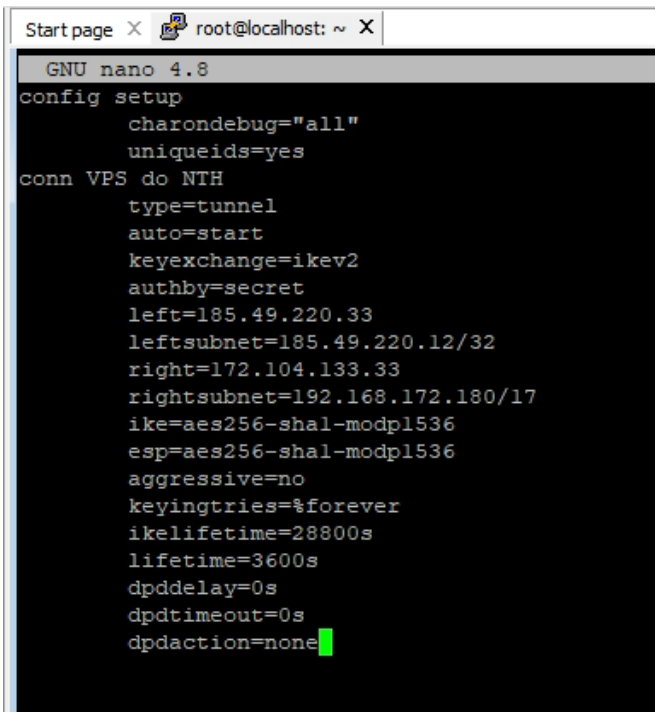
3.4. Instalacija i konfiguracija IPsec-a na VPS-u

Komanda „*apt install strongswan*“ koristi se za instalaciju paketa StrongSwan na Linux distribucijama temeljenima na Debianu, kao što je Ubuntu. StrongSwan je softver otvorenog koda koji pruža VPN rješenje temeljeno na IPsec-u. Pokretanje ove naredbe preuzet će i instalirati StrongSwan zajedno s njegovim dodacima na sustav, omogućujući postavljanje i upravljanje IPsec VPN-ovima.

Komanda sadrži:

- *apt*: Alat za upravljanje paketima koji se koristi u sustavima temeljenim na Debianu za instalaciju, ažuriranje i uklanjanje softverskih paketa.
- *install*: Ova podnaredba govori apt-u da instalira navedeni paket(e).
- *strongswan*: Ovo je naziv paketa koji se želi instalirati, a koji pruža StrongSwan VPN rješenje.

Nakon uspješne instalacije mora se odraditi postavljanje IPsec-a pomoću već spomenutog urednika s komandom „*nano /etc/ipsec.conf*“ prikazano na slici 3.14. U poslovnom svijetu jedna od dviju strana mora diktirati koje će se postavke koristiti pošto na obje strane postavke moraju biti identične. U većini slučajeva zahtjev diktira poduzeće, u ovom slučaju NTH.



Slika 3.14. Postavke IPsec-a na VPS-u

Objašnjenje konfiguracije:

config setup: Ova sekcija uključuje opće postavke za IPsec.

*charondebug="*all": Omogućava opsežne zapise za ispravljanje grešaka.

uniqueids=yes: Osigurava da duplikati jedinstvenih ID-ova nisu dopušteni.

conn VPS do NTH: Ova sekcija definira vezu pod nazivom "VPS do NTH".

type=tunnel: Specificira vrstu IPsec veze (tunel način).

auto=start: Automatski pokreće vezu kada se pokrene IPsec servis.

keyexchange=ikev2: Koristi IKEv2 za protokol razmjene ključeva.

authby=secret: Koristi unaprijed podijeljeni PSK za autentifikaciju.

left=185.49.220.33: Lijeva strana (udaljena) IP adresa. (*NTH peer IP*).

leftsubnet=185.49.220.12/32: Udaljena podmreža. (*NTH domain IP*).

right=194.195.240.169: Desna strana (lokalna) IP adresa. (*VPS peer IP*).

rightsubnet=192.168.132.2/17: Lokalna podmreža. (*VPS domain IP*)

ike=aes256-sha1-modp1536: Specificira algoritme za IKE (faza 1) enkripciju.

esp=aes256-sha1-modp1536: Specificira algoritme za ESP (faza 2) enkripciju.

aggressive=no: Onemogućava agresivni način za IKE.

keyingtries=%forever: Pokušava neograničeno uspostaviti vezu.

ikelifetime=28800s: Postavlja trajanje IKE sigurnosne asocijacije na 28800 sekundi.

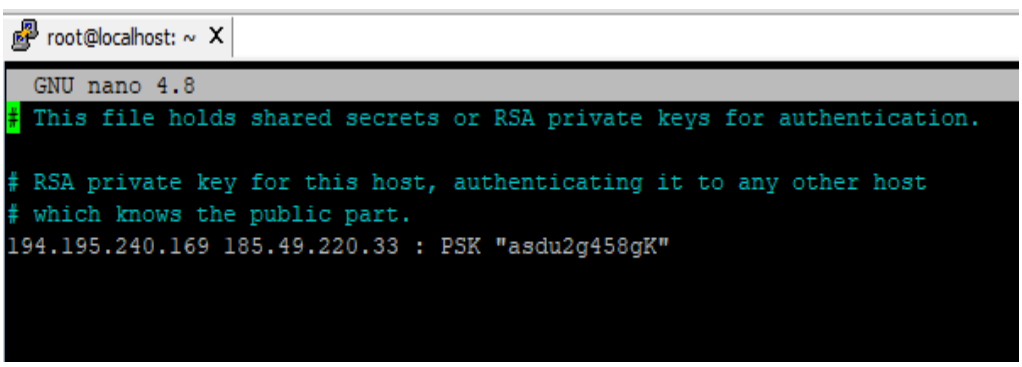
lifetime=3600s: Postavlja trajanje IPsec SA na 3600 sekundi.

dpddelay=0s: Onemogućava DPD (engl. *Dead Peer Detection*).

dpdtimeout=0s: Onemogućava DPD timeout.

dpdaction=none: Nema akcije u slučaju neuspjeha DPD-a.

Nakon postavki IPsec-a jedina stvar koja se još mora odraditi jest postavka PSK. Postavljanje PSK se radi editiranjem konfiguracijske datoteke s komandom „*nano /etc/ipsec.secrets*“ i konfigurira se kao što je prikazano na slici 3.15.



Slika 3.15. Postavljanje PSK za IPsec

4. KONFIGURACIJA I TEST VPN NA HUAWEI VPN UREĐAJU

U cilju postavljanja konfiguracije IPsec-a potrebno je ulogirati se na korisničko sučelje. Pristupne podatke daje odgovorna osoba IT odjela unutar poduzeća samo onim osobama koje su završile trening za korištenje uređaja.

4.1. Dogovor IPsec postavki

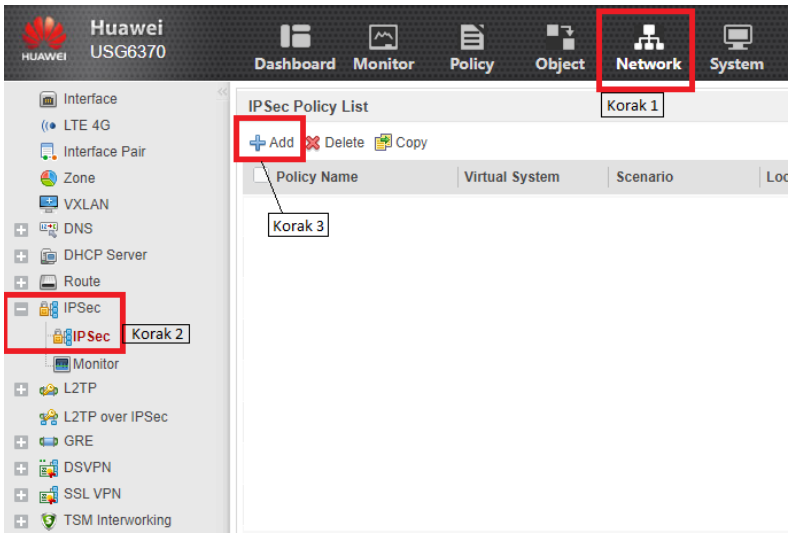
Prije kreiranja VPN tunela za klijenta mora se ispuniti excel tablica 4.1 gdje se definiraju parametri koji će se koristiti kako je prethodno spomenuto. BITNO: Ako klijent nije zadovoljan postavkama može se tražiti izmjena.

Tablica 4.1. Excel tablica za dogovor oko postavki i detalji za spajanje na VPN

NTH AG Site to Site VPN Details		
Date: 09.05.2018	**NTH AG**	**Customer**
Technical contact		
Name: Email: Phone number:	Ivan Stefanec	Linode client
Hardware VPN-Peers		
Hardware VPN-Peer	Huawei USG6300	Linode VPS
Software release VPN-Peer	V500R001C60SPC500	Ubuntu 20.04. LTS
IP-Address VPN-Peers		
Peer IP	185.49.220.33	
IKE Parameter		
Authentication Method	PSK	PSK
IKE Version	IKEv2	194.195.240.169
PSK	xxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxx
Key exchange encryption	AES-256	AES-256
Data integrity	SHA1	SHA1
Diffie-Hellman Group	5	5
Life Duration	3600 sec	3600 sec
Use aggressive mode	NO	NO
IPsec Parameter		
Data encryption	AES-256	AES-256
Data integrity	SHA1	SHA1
Use PFS	YES	YES
Diffie-Hellman Group	5	5
Life Duration	3600 sec	3600 sec
IP Policy		
VPN Domains	185.49.220.12	192.168.132.2

4.2. Konfiguracija VPN-a

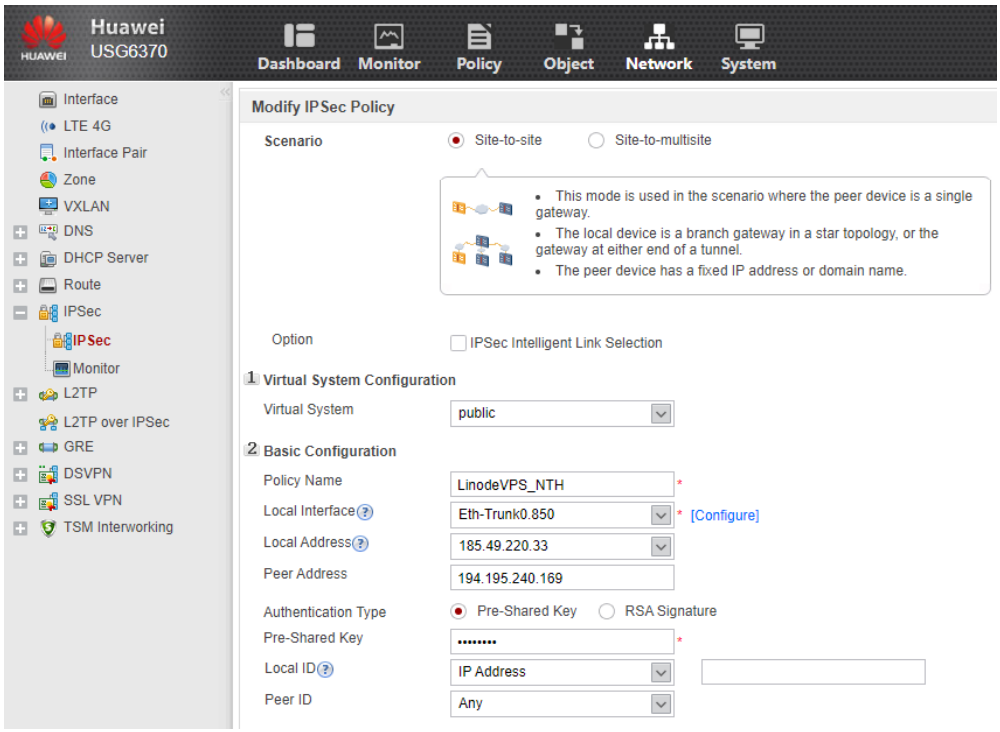
Nakon što je klijent potvrdio da su parametri u redu ili zatražio nove kreće se u kreiranje IPsec na NTH strani (Slika 4.1). Ulogira se na VPN korisničko sučelje te se u gornjem izborniku odabire *Network (Korak 1)*. Otvara se novi izbornik na lijevoj strani te se odabire *IPSec -> IPSec (Korak 2)*, nakon toga odabire se *ADD (Korak 3)*. Na ovom dijelu sučelja prije Koraka 3 može se vidjeti popis svih VPN tunela koji su prethodno kreirani.



Slika 4.1. Kreiranje IPSec-a

Zbog određenih pravila i postavki DC-a unutar poduzeća NTH neke opcije će ostati kao što su originalno postavljene. Nakon toga otvara se novi prozor prikazan slikom 4.2. gdje se postavljaju sljedeći podaci:

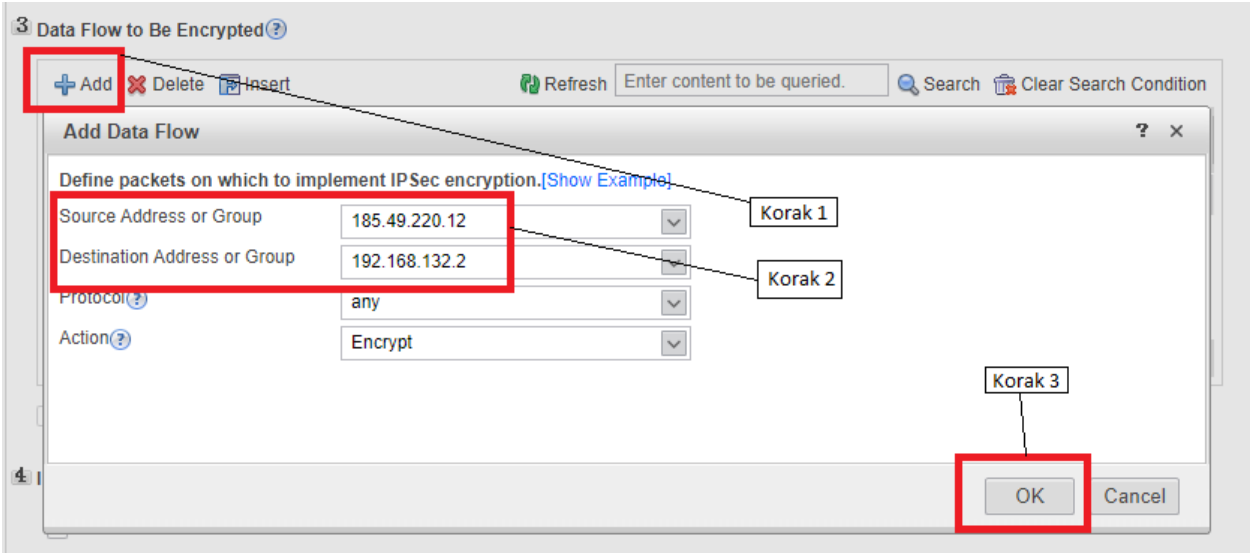
- *Scenario -> Site-to-site*: ostavlja se kao zadano.
- *Option -> IPsec inteligent Link Selection*: ostavlja se kao zadano.
- *Virtual System -> Public*: ostavlja se kao zadano.
- *Policy Name -> LinodeVPS_NTH*: postavlja se kao opis za što se tunel koristi zbog lakšeg pronalaženja prilikom mogućih izmjena postavki.
- *Local interface -> Eth-Trunk0.850*: ostavlja se kao zadano.
- *Local Address -> 185.49.220.33*: odredišna IP adresa VPN uređaja.
- *Peer Address -> 194.195.240.169*: odredišna IP adresa VPS-a.
- *Authentication Type -> Pre-Shared Key*: Vrsta autentifikacije za VPN.
- *Pre-Shared Key -> xxxxxxxxx*: PSK se najčešće dijeli putem SMS-a.
- *Local ID -> IP Address*: ostavlja se kao zadano.
- *Peer ID -> Any*: ostavlja se kao zadano.



Slika 4.2. Osnovna konfiguracija

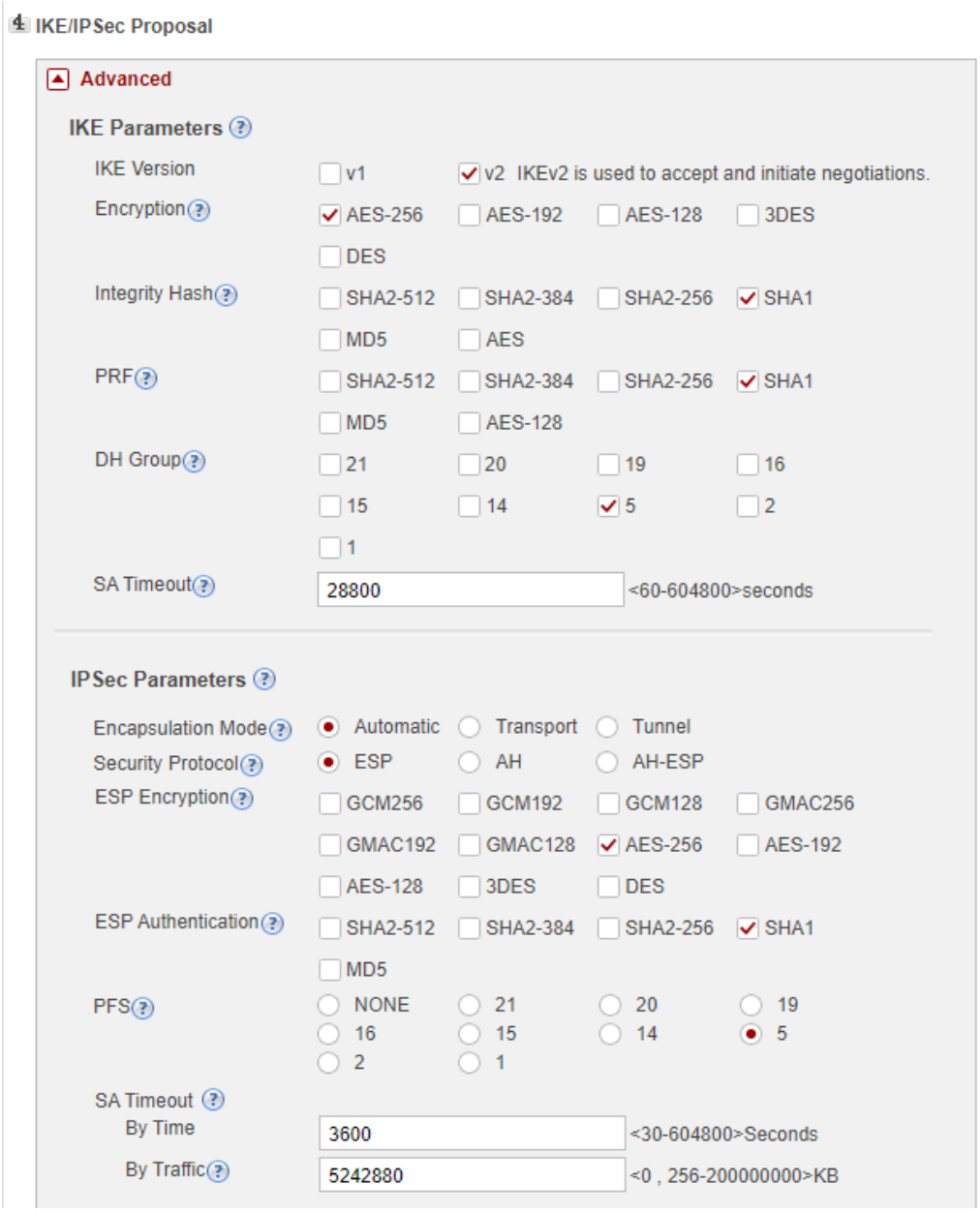
Pod dijelom *Data Flow to Be Encrypted* (Slika 4.3.) odabire se *ADD (Korak 1)* te se tu postavlja izvorna adresu od NTH i VPS-a *(Korak 2)*. Nakon postavljanja odabire se *OK (Korak 3)*. Postavljaju se podaci:

- *Source Address or Group -> 185.49.220.12*: izvorna IP adresa VPN uređaja.
- *Destination Address or Group -> 192.168.132.2*: izvorna IP adresa VPS-a.
- *Protocol -> any*
- *Action -> Encrypt*



Slika 4.3. Postavljanje izvornih adresa NTH i VPS-a

Zadnji korak kod konfiguracije IPsec-a obuhvaća postavljanje parametara kako je zadano u tablici 4.1 i prikazano na slici 4.4. Ovi parametri su ranije objašnjeni u poglavlju 2.4.4.

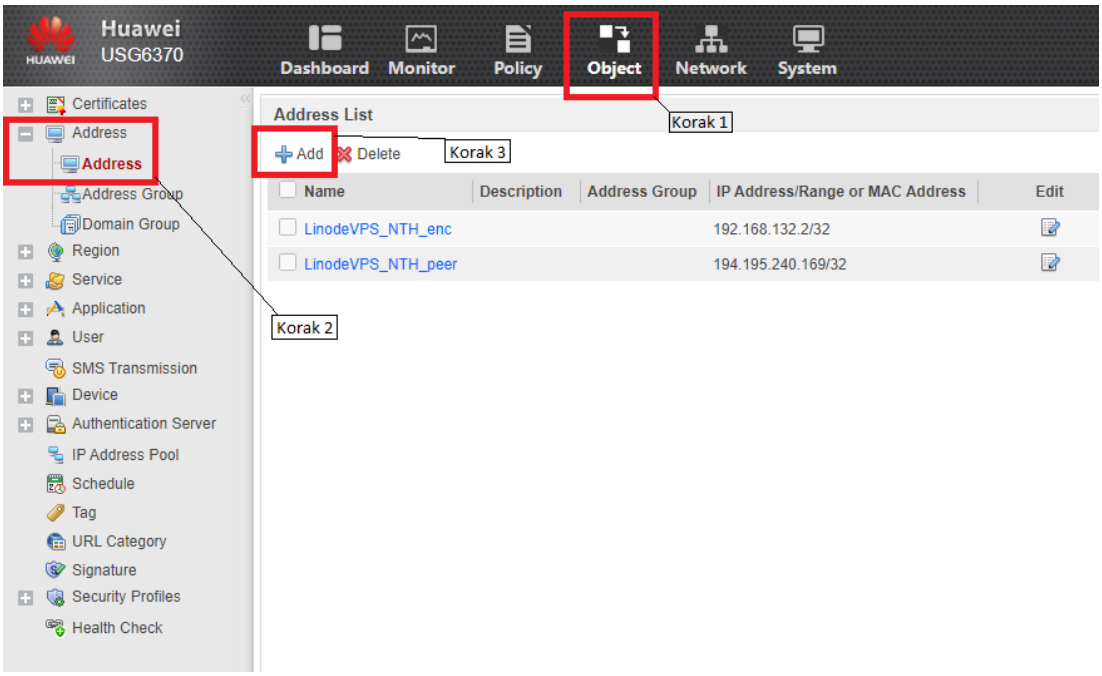


Slika 4.4. Postavke IKE i IPsec dijela

Nakon postavljanja svih obveznih opcija/parametara odabire se *Apply* na dnu prozora da se opcije/parametri spreme i da se kreira VPN tunel. Potrebno je još napraviti mapiranje IP adresa od VPS-a, dodavanje sigurnosne politike i postavljanje NAT pravila za VPN tunel.

4.3. Mapiranje izvorne i odredišne adrese

U gornjem izborniku odabire se *Object (Korak 1)* te na lijevoj strani *Address -> Address (Korak 2)* i na kraju *Add (Korak 3)* prikazano na slici 4.5.

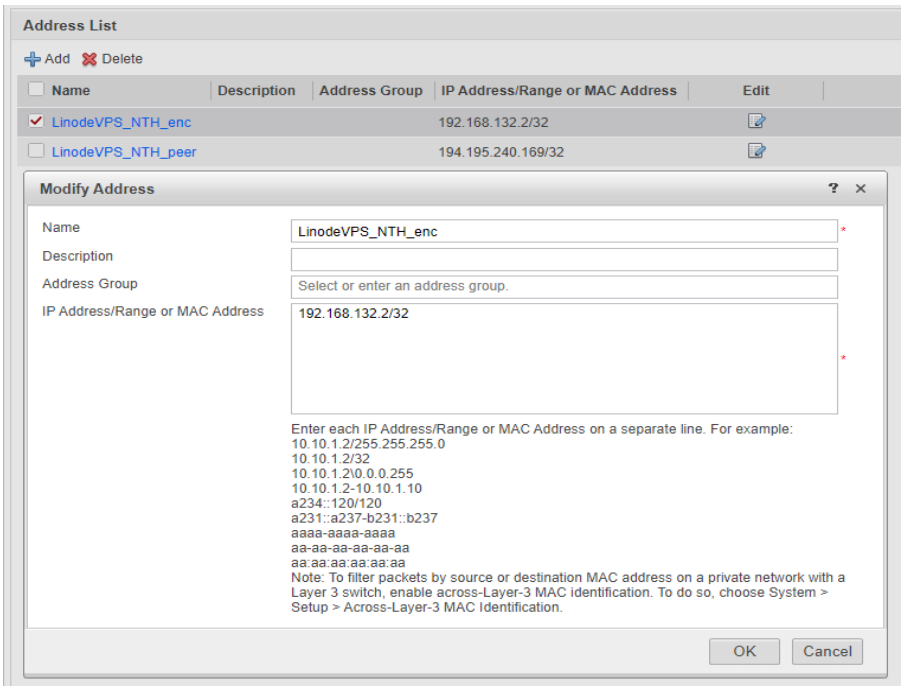


Slika 4.5. Sučelje za mapiranje IP adresa

Otvara se prozor za unos podataka i upisuju se podaci ispod. Postupak se mora ponoviti dva puta jer se mora mapirati izvorna IP adresa (na slici 4.6. mapirano kao *LinodeVPS_NTH_enc*) i odredišna adresa (na slici 4.6. mapirano kao *LinodeVPS_NTH_peer*). Postavljaju se podaci:

- *Name -> LinodeVPS_NTH_enc/LinodeVPS_NTH_peer*: Postavlja se kao opis za koji tunel se koristi mapiranje.
- *IP Address/Range or MAC Address ->194.195.240.169/32 & 192.168.132.2/32*: IP adresa od izvorne ili odredišne adrese s mrežnom maskom /32.

Nakon postavljanja svih podataka odabire se *OK* u otvorenom prozoru.



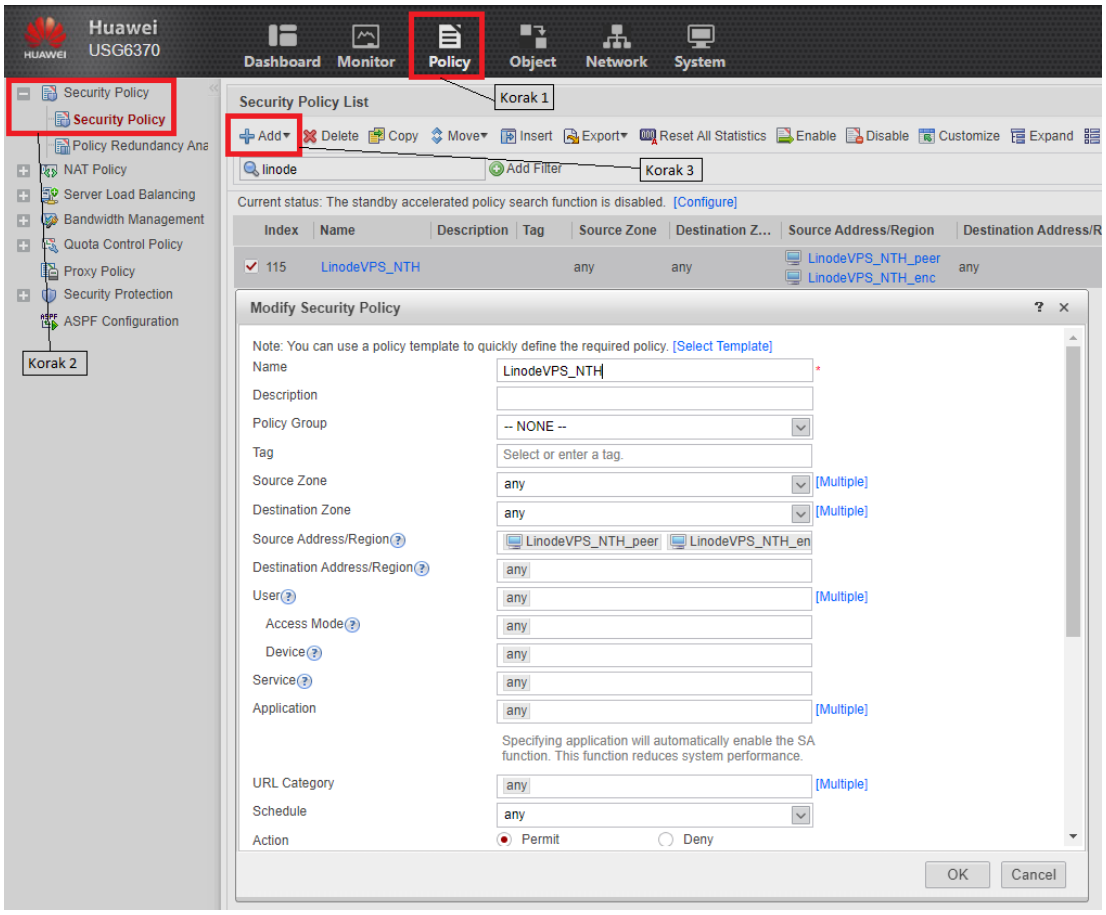
Slika 4.6. Mapiranje izvorne i odredišne IP adrese

4.4. Dodavanje sigurnosne politike vatrozida

Potrebno je dodati adrese izvorne i odredišne adrese na bijelu listu (engl. *whitelist*) putem stvaranja sigurnosne politike, inače će promet biti blokiran. Na slici 4.7. u gornjem izborniku odabire se *Policy (Korak 1)* te na lijevoj strani *Security policy -> Security policy (Korak 2)* i na kraju *Add (Korak 3)*. Otvara se novi prozor te se postavljaju podaci:

- *Name -> LinodeVPS_NTH*
- *Source Zone ->: Any*
- *Destination Zone -> Any*
- *Source Address/region -> LinodeVPS_NTH_peer & LinodeVPS_NTH_enc*: prethodno mapirana izvorna i odredišna IP adresa
- Sve ostale opcije ostaju kao zadane

Nakon postavljanja svih podataka odabire se OK u otvorenom prozoru.



Slika 4.7. Postavljanje sigurnosne politike vatrozida (engl. *firewall*)

4.5. Dodavanje NAT pravila i mapiranje rute na NTH serveru

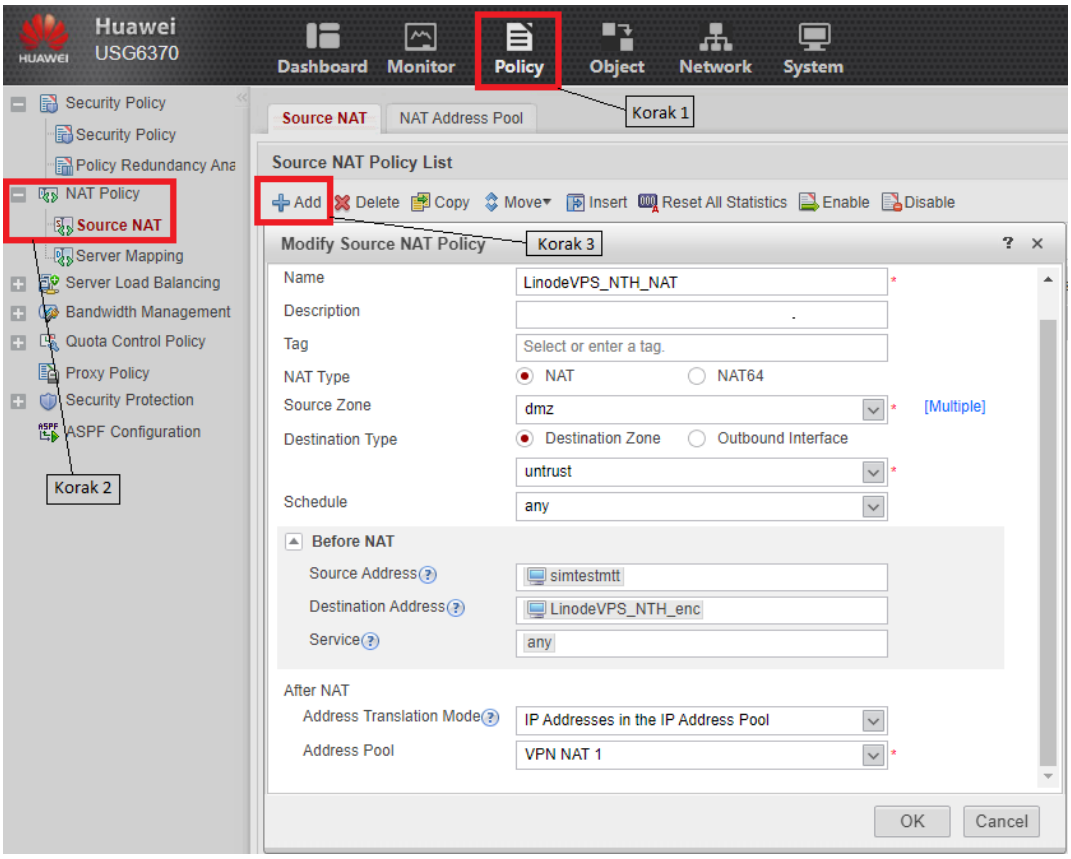
Potrebno je zamaskirati interne IP adrese NTH servera s izvornom adresom VPN te se zbog toga dodaje NAT pravilo. Na slici 4.8. u gornjem izborniku odabire se *Policy (Korak 1)* te na lijevoj strani *NAT Policy -> Source NAT (Korak 2)* i na kraju *Add (Korak 3)*. Otvara se novi prozor te se postavljaju podaci:

- *Name -> LinodeVPS_NTH_NAT*
- *Source Zone -> dmz*
- *Destination Type -> Destination Zone/untrust*

Parametri na slici 4.8. koji se nalaze pod opcijom *Before NAT*:

- *Source Address ->simtestmtt:* mapirana izvorna adresa NTH servera kojeg spajamo s VPS-om, u našem slučaju server *simtest-mtt*
- *Destination Address ->LinodeVPS_NTH_enc:* mapirana izvorna adresa VPS

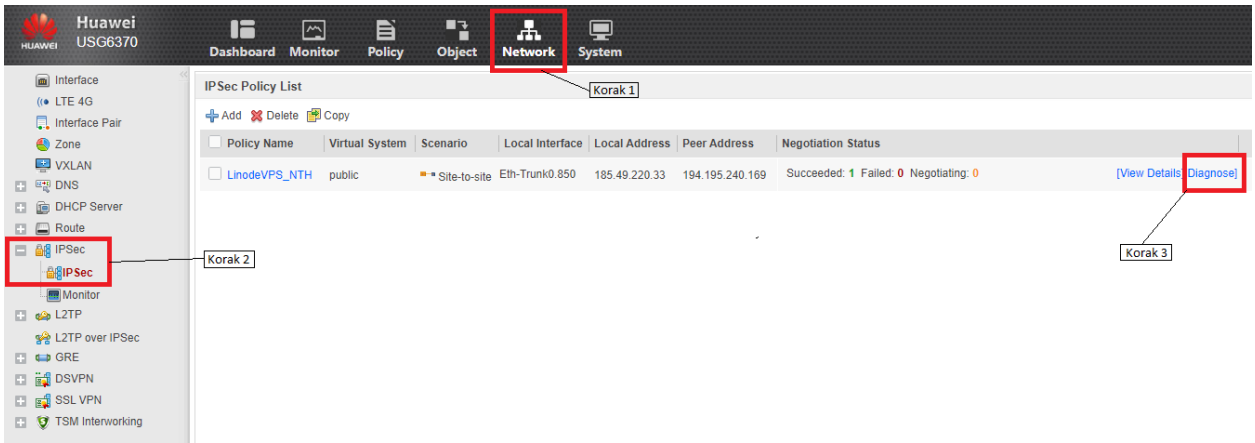
Nakon postavljanja svih podataka odabire se OK u otvorenom prozoru.



Slika 4.8. Postavljanje NAT pravila

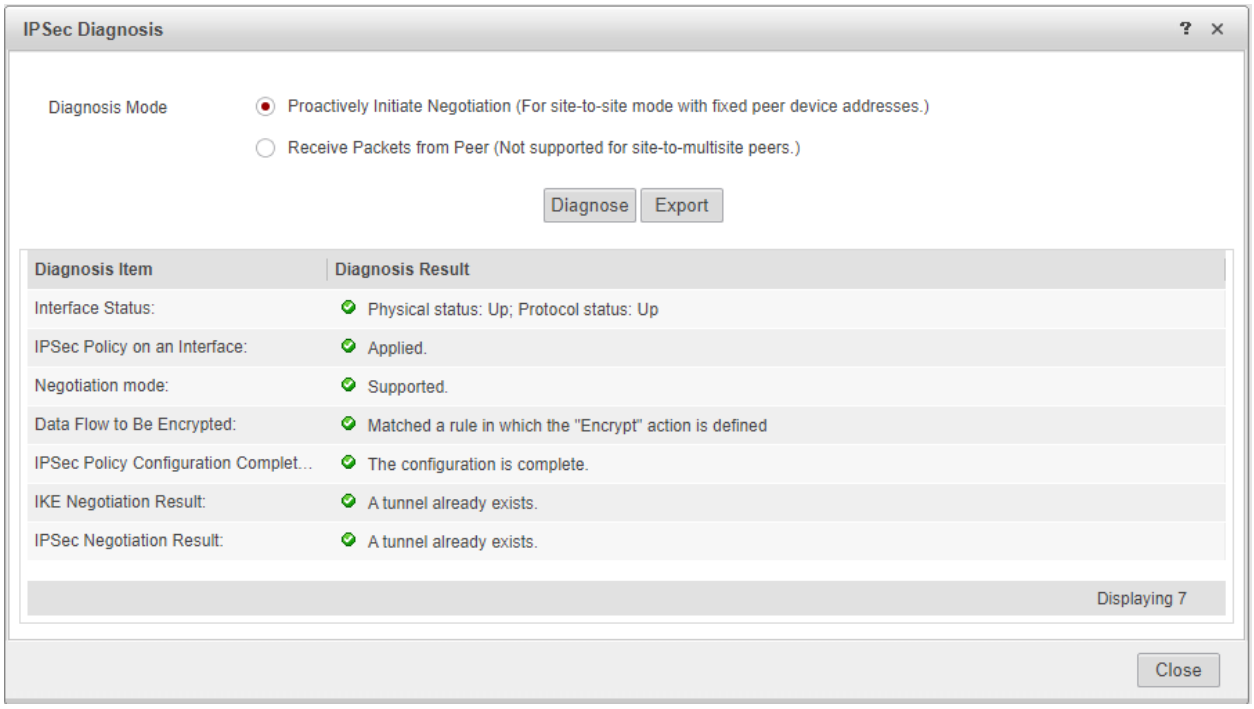
4.6 Testiranje VPN-a

Testiranje VPN se radi putem automatskog dijagnostičkog alata na Huawei uređaju (Slika 4.9). U gornjem izborniku odabire *Network (Korak 1)*. Otvara se novi izbornik na lijevoj strani te se odabire *IPSec -> IPSec (Korak 2)*, nakon toga odabire se *Diagnose (Korak 3)*.



Slika 4.9. Pokretanje dijagnostičkog alata

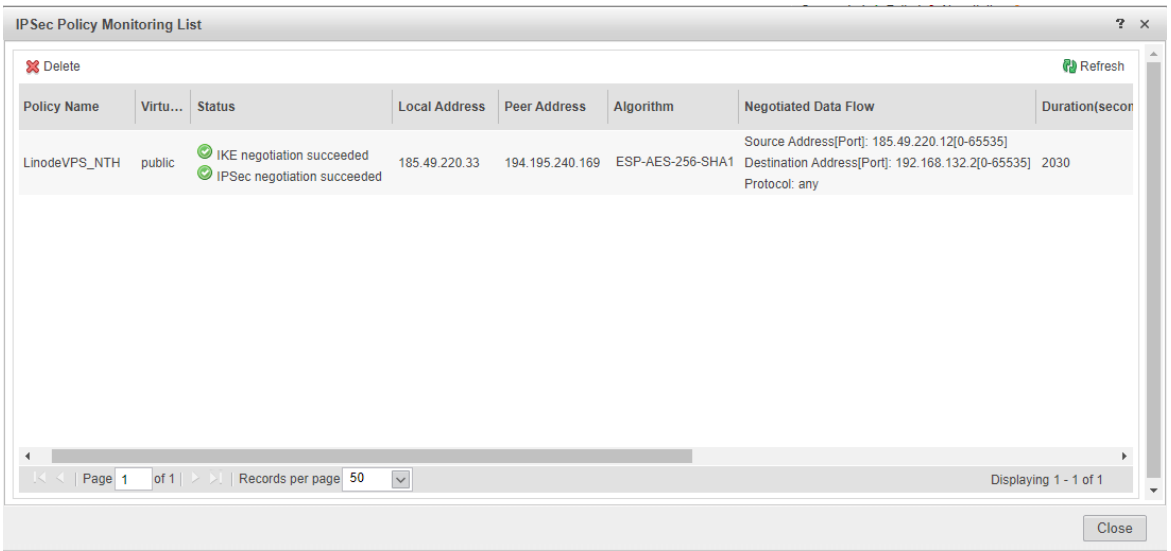
Otvara se novi prozor vidljiv na slici 4.10. gdje se odabire *Diagnose*. Ako je sve uredno postavljeno alat će ispisati detalje, ako su svi markirani sa zelenom kvačicom znači da je VPN tunel uspostavljen.



Slika 4.10. Testiranje VPN-a

Na slici 4.9. pored *Diagnose* opcije nalazi se i opciju *View Details*. Odabirom navedene opcije vidljivi su detalji prikazani na slici 4.11.

- Naziv VPN-a.
- Status IKE i IPsec pregovora.
- Odredišna IP adresu Huawei uređaja.
- Odredišna IP adresu VPS-a.
- Algoritam koji se koristi za enkripciju.
- Izvorne IP adrese Huawei uređaja i VPS-a.
- Koliko je dugo VPN tunel povezan u sekundama.



Slika 4.11. Detalji VPN-a

5. ZAKLJUČAK

Zadatak ovog diplomskog rada bio je opisati proces uspostave i testiranja VPN tunela koristeći primjere iz prakse. Rad je obuhvatio postavljanje VPN-a između fizičkog NTH servera simtest-mtt i virtualnog privatnog servera (VPS) s ulogom IPsec poslužitelja, uz korištenje Huawei VPN uređaja koji služi kao središnja točka za povezivanje i osiguranje podataka između različitih sustava. U okviru rada detaljno su opisane osnovne karakteristike i principi funkcioniranja VPN tehnologija, s posebnim naglaskom na IPsec protokol. IPsec je ključan za osiguranje integriteta i povjerljivosti podataka prilikom njihove razmjene preko nesigurnih mreža, kao što je internet. U radu su također obrađeni različiti VPN protokoli, njihova primjena, te prednosti i nedostaci, što je omogućuje dublje razumijevanje tehničkih aspekata VPN implementacija.

Jedan od ključnih elemenata rada bio je postupak postavljanja IPsec tunela, koji je izveden u nekoliko koraka, uključujući konfiguraciju IKE i IPsec prijedloga. Ovi prijedlozi definiraju sigurnosne parametre koji su potrebni za uspostavljanje sigurne veze, kao što su algoritmi za šifriranje i autentifikaciju, te trajanje sigurnosnih asocijacija. Također, rad je naglasio važnost odabira odgovarajućih parametara u odnosu na specifične potrebe sustava i razinu sigurnosti koja je potrebna. Dodatno, kroz praktičan primjer pokazana je važnost pravilne konfiguracije VPN-a za osiguranje sigurnosti komunikacije. Demonstrirano je kako korištenje naprednih sigurnosnih postavki, kao što su snažni algoritmi za šifriranje i autentifikaciju, može značajno smanjiti rizik od neovlaštenog pristupa osjetljivim podacima. Također, obrađena je uloga i važnost konfiguracije sigurnosnih politika i NAT pravila, koja su neophodna za pravilno funkcioniranje i zaštitu VPN tunela.

Provedena analiza i testiranje VPN veze između NTH servera i VPS-a omogućili su validaciju postavki i potvrdu da implementirani sustav ispravno funkcionira, osiguravajući potrebnu razinu sigurnosti i stabilnosti. Time je pokazano da VPN, kada je pravilno postavljen i konfiguriran, može pružiti visok stupanj zaštite za osjetljive podatke koji se prenose preko nesigurnih mreža.

Zaključno, ovaj rad ističe važnost pravilne implementacije i konfiguracije VPN-a kao ključnog elementa u zaštiti podataka i sigurnosti mrežne komunikacije u suvremenom poslovanju. Primjena naprednih tehnologija poput IPsec-a i pažljiva konfiguracija svih elemenata VPN-a od presudne su važnosti za zaštitu podataka od neovlaštenog pristupa i potencijalnih sigurnosnih prijetnji. Rezultati ovog rada mogu poslužiti kao vodič za buduće implementacije VPN-a u različitim okruženjima, osiguravajući da sustavi budu otporni na sve veće izazove u području kibernetičke sigurnosti.

Uspostava i testiranje VPN tunela

SAŽETAK

U diplomskom radu glavni zadatak je objasniti VPN mreže te protokole potrebne za njihovu uspostavu. Koristi se najčešći način rada VPN-a, a to je *site-to-site.* IPsec i IKE parametri te konfiguracije detaljno su prikazane i objašnjene jer je riječ o ključnim parametrima koji su neophodni za rad na VPN-u. Na praktičnom primjeru prikazali smo uspostavu između dviju strana, NTH koja koristi fizičke uređaje te strana klijenta koji koristi virtualne sustave VPS. Nakon konfiguracije i uspostave VPN-a prikazao se način testiranja VPN-a. Kreiranje, postavljanje i testiranje virtualnih privatnih mreža postalo je jedno od najtraženijih znanja u današnje vrijeme gdje je sve više informatičkih poduzeća podložno *cyber* napadima.

Ključne riječi: VPN, VPS, IPsec, IKE, IP

Establishment and testing of VPN tunnels

ABSTRACT

The main task of the master thesis is to explain VPN networks and the protocols necessary for their establishment. The most common mode of VPN operation, site-to-site, was used. IPsec and IKE parameters and configurations were detailed and explained as they are essential parameters necessary for VPN operation. A practical example demonstrated the establishment of a VPN connection between two parties: NTH, which uses physical devices, and the client side, which uses virtual VPS systems. After the configuration and establishment of the VPN, the method of testing the VPN was also presented. Creating, setting up, and testing virtual private networks has become one of the most sought-after skills in today's time, where an increasing number of IT companies are susceptible to cyber attacks.

Key words: VPN, VPS, IPsec, IKE, IP

ŽIVOTOPIS

Ivan Štefanec rođen je 27. prosinca 1989. u Virovitici. Nakon završene osnovne škole (OŠ Vladimira Nazora) Virovitica, 2004. godine upisao je Tehničku školu smjer Elektrotehničar u Virovitici. Maturirao je 2008. godine s vrlo dobrim uspjehom. Nakon završetka srednje škole upisao je preddiplomski studij na Elektrotehničkom fakultetu u Osijeku smjer *Komunikacije i informatika* koji završava 2012. godine. Unutar perioda preddiplomskog studija jedan semestar radio je kao demonstrator na predmetu Elektronika I. Nastavlja studirati isti smjer na diplomskom studiju na istom fakultetu. Od 2014. godine zapošljava se u NTH AG poduzeću gdje radi kao tehničar za VPN, isporuku servisa i osoba za održavanje određenih servera.

Potpis

_____

LITERATURA

[1] Martin W. Murhammer, Orcun Atakan, Zikrun Badri, Beomjun Cho Hyun Jeong Lee, Alexander Schmid; A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management; International Technical Support Organization, 1999.

[2] VPN Protocols Explained and Compared, dostupno na: https://www.avast.com/c-vpn-protocols

[3] HAYALE, Wassan Saad; JEBUR, Elaf Ayyed. Implementing Virtual Private Network using Ipsec Framework. International Journal Of Engineering Research & Technology, 2014.

[4] SNADER, Jon C. VPNs Illustrated: Tunnels, VPNs, and IPsec. Addison-Wesley Professional, 2015.

[5] P. Muñoz-Merino, A. García-Martínez, M. Muñoz-Organero, & C. Kloos, "Enabling practical ipsec authentication for the internet", On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, p. 392-403, 2006. https://doi.org/10.1007/11915034_63

[6] J. Kovács, L. Bokor, Z. Kanizsai, & S. Imre, "Review of advanced mobility solutions for multimedia networking in ipv6", Intelligent Multimedia Technologies for Networking Applications, p. 25-47, 2013. https://doi.org/10.4018/978-1-4666-2833-5.ch002

[7] C. Cremers, "Key exchange in ipsec revisited: formal analysis of ikev1 and ikev2",, p. 315-334, 2011. https://doi.org/10.1007/978-3-642-23822-2_18

[8] RFC 7296: https://datatracker.ietf.org/doc/html/rfc7296

[9] https://flylib.com/books/en/2.650.1/vpn_devices.html

[10] RFC 2409: https://datatracker.ietf.org/doc/html/rfc2409