SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE VARAŽDIN

GORAN BOŽIĆ

PRIMJENA IPSEC-A U SPRJEČAVANJU UNUTARNJIH ZLONAMJERNIH POČINITELJA

VARAŽDIN, 2008

PODACI O ZAVRŠNOM RADU

I. Autor

Ime i prezime:	Goran Božić
Datum i mjesto rođenja:	17.07.1961., Virovitica
Naziv fakulteta i datum diplomiranja	Elektrotehnički fakultet Sveučilišta u Zagrebu, 1986.
Sadašnje zaposlenje	Franck d.d., Zagreb

II. Završni rad

Naslov:	Primjena IPsec-a u sprječavanju unutarnjih zlonamjernih počinitelja
Broj stranica, slika, tabela:	168 stranica, 88 slike, 29 tablica
Znanstveno područje, smjer i disciplina iz koje je postignut akademski stupanj:	Društvene znanosti, polje informacijskih znanosti
Mentor ili voditelj rada:	prof.dr.sc. Miroslav Bača
Fakultet na kojem je rad obranjen:	Fakultet organizacije i informatike Varaždin
Oznaka i redni broj rada:	

III. Ocjena i obrana

Datum prihvaćanja teme od Znanstveno-nastavnog vijeća:	18.ožujak 2008
Datum predaje rada:	10. travanj 2008
Datum sjednice ZNV-a na kojoj je prihvaćena pozitivna ocjena rada:	27. svibanj 2008
Sastav Povjerenstva koje je rad ocijenilo:	Dr.sc. Miroslav Bača, mentor i član, Dr.sc. Zdravko Krakar, član, Dr.sc. Željko Hutinski, član
Datum obrane rada:	17. lipanj 2008
Sastav Povjerenstva pred kojim je rad obranjen:	Dr.sc. Željko Hutinski, predsjednik Dr.sc. Miroslav Bača, mentor i član, Dr.sc. Zdravko Krakar, član,
Datum promocije:	

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE VARAŽDIN

GORAN BOŽIĆ

PRIMJENA IPSEC-A U SPRJEČAVANJU UNUTARNJIH ZLONAMJERNIH POČINITELJA

VARAŽDIN, 2008

Predgovor

Virtual Private Network (VPN) je tehnologija koja omogućava sigurno povezivanje računala u virtualne privatne mreže preko javne mrežne infrastrukture, a IPsec se vrlo često koristi kao 'protokol'. U posljednje vrijeme IPsec se sve više implementira i u mrežne operacijske sustave. Proizvođači mu primjenu vide u povećanju sigurnosti na mreži. Kolika je stvarna korist ove tehnike analizirano je na sustavu gdje je korišten Microsoft Windows operacijski sustav. Učinkovitost je analizirana kroz smanjivanje prijetnji unutrašnjih zlonamjernih korisnika ili unutrašnji počinitelj. Tijekom analize prijetnji i načina izvođenja došlo je do spoznaje da IPsec može biti iskorišten i od strane unutrašnji počinitelj, da se zaštiti od kontrole sadržaja. Da bi se potvrdila ispravnost konfiguracije IPsec-a, prema definiranim zahtjevima, korišten je alat za penetracijsko testiranje. Isti alat je iskorišten i za detekciju IPsec VPN sustava korištenih od strane. Različite implementacije IPsec-a se različito ponašaju za vrijeme penetracijskog testiranja tako da će se neki IPsec VPN sustave lakše detektirati, a druge teže. Standardi i preporuke neke 'opcije' nisu strogo definirali tako da su ih proizvođači implementirali prema svojim mišljenjima. Rezultati analize učinkovitosti IPsec-a na lokalnoj mreži pokazuju da se određene prijetnje smanjuju ili potpuno uklanjaju

SADRŽAJ

Popis slika

Popis tabela

1. UVOD

Sveopća umreženosti postala je stvarnost i računalni se sustavi koriste u svim sferama ljudske djelatnosti. Briga o informacijskoj sigurnosti postaje nužnost u poslovnoj politici svake organizacije. Informacija je imovina i kao takvu ju je potrebno prikladno zaštititi, kako bi se omogućilo normalno poslovanje organizacije [41]. Većina organizacija je već načinila prve korake u brizi o informacijskoj sigurnosti kroz implementiranje antivirusnih i vatrozidnih sustava, no to nije dovoljno. U ratu protiv zlonamjernih korisnik savjet iz knjige 'Umijeće ratovanja' Sun Tzu, može služiti kao smjernica kako povećati šanse za uspjeh. Citat glasi:

- Ako znaš druge i znaš sebe, nećeš biti u opasnosti u stotinama bitaka,
- Ako ne znaš druge, ali znaš sebe, možeš izgubiti, možeš dobiti,
- Ako ne znaš druge i ne znaš sebe, biti ćeš ugrožen u svakoj pojedinačnoj bitki.

Zlonamjerni korisnici svakodnevno nalaze nove metode kako kompromitirati sigurnost informacijskog sustava tako da se često nalazimo u situaciji koja ne daje mnogo izgleda za uspjeh. Da bi se ravnopravno borili moramo dobro upoznati neprijatelja kao i svoj sustav koji štitimo. Analiza potencijalnih zlonamjernih korisnika definirat će okvire u kojima treba tražiti metode za borbu protiv njih. Poznavanje sustava koji se treba zaštiti potrebno je iz najmanje dva razloga. Prvi je vezan uz poznavanje ranjivosti sustava i slabih točaka. Drugi je vezan uz poznavanje svih funkcionalnosti sustava koje mogu biti iskorištene u borbi protiv zlonamjernih korisnika. Jedna funkcionalnost koja se intenzivno koristi u zaštiti prometa od vanjskih zlonamjernih korisnika na javnim mrežama je IPsec (engl. Internet Protokol security). Do nedavno se mogao naći samo na aktivnim komunikacijskim uređajima koji su osiguravali siguran promet na javnim mrežama. Danas se IPsec implementira i u mrežne operacijske sustave, sa ciljem povećanja sigurnosti informacijskog sustava. Pitanje koje se nameće je na koga će se primijeniti ova tehnička metoda. Dosadašnja istraživanja ukazuju na podjednaku zastupljenost unutrašnjih i vanjskih

zlonamjernih korisnika u sigurnosnim incidentima. Trend ulaganja u sigurnost pokazuje da se na vanjske zlonamjerne korisnike koristi daleko više sredstava. U radu su analizirani unutrašnji zlonamjerni korisnici (u daljnjem tekstu unutrašnji počinitelji) jer su oni realna prijetnja sigurnosti informacijskog sustava. Zašto im se ne pridaje pažnja kao i vanjskim zlonamjernim korisnicima? Kako mogu provesti svoje prijetnje, samo su neka pitanja na koja će se u radu pokušati odgovoriti. Obje komponente o kojima je riječ nalaze se na sustavu. Treba ih samo dobro proučiti i analizirati da li je moguće povećati sigurnost informacijskog sustava ako je napadač unutrašnji počinitelj a alat sa kojim se protiv njega borimo IPsec. Dosadašnja praksa pokazala je veliku učinkovitost primjene IPsec-a u sprječavanju vanjskih počinitelja, međutim taj se alat do sada nije koristio u prevenciji unutarnjih počinitelja.

Iz navedenog se može izvesti slijedeća radna hipoteza:

H1:

Razvojem i upotrebom modela preveniranja sigurnosnih napada temeljenog na alatu IPSec povećava se razina sigurnosti informacijskog sustava.

Da bi se ova hipoteza potvrdila u radu će biti potrebno provesti slijedeće:

- Potvrditi postojanje realne opasnosti od unutrašnjih zlonamjernih korisnika.
- Analizirati module sustava kojima IPsec osigurava jednostavno definiranje granica štićenog područja informacijskog sustava (perimetar).
- Analizirati sigurnost IPsec-a kroz standarde i protokole koji ga definiraju.
- Analizirati učinkovitosti IPsec-a u smanjivanju i uklanjanju nekih prijetnji unutrašnjih zlonamjernih korisnika na testnom modelu.
- Analizirati eventualne probleme koji mogu proizaći iz upotrebe IPsec-a na lokalnoj mreži.

2. UNUTARNJI NAPADAČI INFORMACIJSKOG SUSTAVA

U godišnjem izvještaju '*E-Crime Watch Survey*' [1] za 2007 prikazani su rezultati istraživanja vezani uz prijetnje informacijskom sustavu. Na uzorku od 443 ispitanika neka od postavljenih pitanja su:

- Mišljenje o broj sigurnosnih incidenata u odnosu na prošlu godinu:
  - Povećao – 33%,
  - Smanjio – 19%,
  - Nije bilo promjene – 28%,
  - Ne zna – 20%.
- Zastupljenost izvor prijetnji:
  - 34% vanjski počinitelj[1],
  - 37% unutrašnji počinitelj,
  - 24% nepoznati.
- Ciljevi napada su bili slijedeći:
  - 27% neautoriziran pristup podacima, sistemskim resursima, mreži,
  - 24% krađa intelektualnog vlasništva,
  - 23% druge informacije kao što su financijske i privatne informacije,
  - 19% fraud[2] - prevare kroz poslovne procese, kreditne kartice i sl.
- Metode izvršenja napada su bile:
  - 45% socijalni inženjering (prošle godine 38%),
  - 39% kompromitiranje korisničkih računa,
  - 36% kopiranje informacija na mobilne uređaje (USB[3] memorija, foto aparati, mobiteli),
  - 35% korištenjem vlastitih korisničkih računa,
  - 31% korištenjem naprednih metoda probijanja zaporki, snifera[4] (17% prošle g.).

[1] Vanjski zlonamjerni korisnik
[2] Prevara
[3] Engl. Universal Serial Bus

- Rješavanje napada unutar organizacije bez uplitanja zakonodavstva:
    - 67% unutrašnji počinitelj,
    - 66% vanjski počinitelj.
- Razlozi zbog čega se stvar rješava interno:
    - 40% nivo štete premali za podizanje optužnice,
    - 34% manjak dokaza,
    - 28% nemogućnost identifikacije počinitelja.
- Praktična rješenja u borbi protiv napadača:
    - 82% statefull firewalls[5],
    - 79% kontrola pristupa,
    - 78% računalna kontrola pristupa,
    - 72% vatrozid na aplikacijskom nivou.
- Rješenja koje najmanje doprinose borbi protiv napadača:
    - Ručno pokretanje zakrpa,
    - Kompleksnost lozinke,
    - Nadzor,
    - Bedževi[6],
    - RBL[7] SPAM[8] filtriranje.

Rezultati pokazuju da je trend sigurnosnih incidenata u porastu te da tome porastu ravnomjerno doprinose vanjski počinitelji i unutrašnji počinitelji. Za primijetiti je da su ciljevi napada usmjereni na intelektualno vlasništvo te na prevare koje su moguće kroz poslovne procese. Metode izvršenja napada pokazuju da se više koriste jednostavne metode kao što je socijalni inženjering za razliku od tehničkih metoda

[4] Osluškivanje prometa po mreži
[5] *Stateful inspection* načinom provjere paketa moguće je utvrditi da li su paketi dijelovi neke uspostavljene veze ili ne. Za razliku od statičkog filtriranja paketa, koje analizira pakete samo na temelju njihovih zaglavlja, *stateful inspection* način rada registrira sve uspostavljene konekcije između pojedinih mrežnih sučelja te na temelju njihovih stanja obavlja provjere.
[6] Identifikacijska oznaka.
[7] Engl. Remote Blackhole List – popis IP adresa servera čiji vlasnici ne žele spriječiti raspačavanje *spama*
[8] neželjene reklamne poruke e-pošte

kao što je slušanje i analiza prometa po mreži. Razvoj informatičke tehnologije pogoduje unutrašnji počiniteljima jer željene podatke sad mogu iznesti na memorijskim karticama, fotoaparatima, mobitelima koji postaju sve manji a iskoristivi memorijski prostor sve veći. Rezultati ispitivanje ukazuju na zanimljivu činjenicu kad se radi o načinu otkrivenih i identificiranih napadača. Više od polovice svih napada rješava se unutar organizacije bez uplitanja zakonodavstva. Razloga za to ima više, no sigurno je da jedan i strah od lošeg publiciteta. U borbi protiv napada na informacijski sustav i dalje se više sredstava ulaže u sprečavanje napada vanjski počinitelja, tj. investira se u uređaje koji se implementiraju na sigurnosnom perimetru mreže. Sigurnosni perimetar (engl. security perimeter) predstavlja granicu koja odvaja dio sustava s jednim sigurnosnim postavkama od dijela sustava gdje važe neke druge postavke. Mora postojati i nerizičan put (engl. trusted path) koji osigurava korisniku da pristupi željenom sustavu tako da ga pri tome ne mogu kompromitirati drugi procesi i/ili korisnici. Sigurnosni uređaji se implementiraju na te putove. Kad govorimo o perimetrima treba reći da je njih danas sve teže definirati i trend je da se oni pomiču prema izvoru podataka bez obzira da li to znači server ili dio mreže

Zanimljivi su i odgovori koji su dati na pitanje o metodama koje najmanje doprinose u borbi protiv napadača. To ne znači da te metode ne treba primijeniti. Iskustvo ispitanika koji su sudjelovali u ispitivanju samo govori da su napadači našli načina da zaobiđu navedene metode i da one nisu predstavljali nepremostivu prepreku za izvršenje napada, posebno ako se radilo o visoko motiviranom unutrašnji počinitelj.

Rasprava o postotku napada koji može biti izveden od vanjski počinitelja ili unutrašnji počinitelj je možda nebitna ako na slijedeća pitanja odgovorimo pozitivno:

1. Da li napad može biti izveden izvana?
2. Da li tako izveden napad može nanijeti štetu poduzeću?
3. Da li napad izvana može zaustaviti poslovanje poduzeća?
4. Da li napad može biti izveden iznutra?
5. Da li tako izveden napad može nanijeti štetu poduzeću?

6. Da li napad iznutra može zaustaviti poslovanje poduzeća?

Ako je moguće zaustaviti poslovanje poduzeća onda su postoci tu manje bitni i važni. No činjenica je da se unutrašnji počinitelj već nalazi unutar perimetra mreže vodi na zaključak da je šteta koju on može izazvati daleko veća od štete koju može napraviti napadač izvana. Isto tako je i šansa da se detektira unutrašnji počinitelj puno manja od detekcije vanjski počinitelja koji mora probiti neki sigurnosni uređaj na perimetru mreže i tako ostaviti trag svoga djelovanja. Osnovna stvar koju treba imati na umu kad se govori o unutrašnji počiniteljima je da imaju pristup i da će iskoristiti ranjivost sustava što im daje velike šanse za uspjeh a istovremeno umanjuje šanse da budu otkriveni. Razlozi zbog kojih se prijetnje unutrašnji počinitelj ignoriraju možda treba tražiti u činjenicama da:

- Organizacija ne zna što se događa u informacijskom sustavu,
- Lakše je ignorirati, jer u protivnom moramo nešto poduzeti,
- Organizacija se boji javnog publiciteta koji bi joj mogao štetiti.

Zašto prijetnje unutrašnji počinitelj mogu biti opasnije od prijetnji vanjski počinitelja, iako i jedni i drugi mogu uzrokovati štetu poduzeću, su slijedeći:

- Lakše ih je izvesti,
- Trenutna sigurnosna rješenja nisu projektirana za unutrašnji počinitelje,
- Velika je šansa da uspiju,
- Mala šansa da budu otkriveni.

Očigledne posljedice napada unutrašnji počinitelj na poduzeće su:

- Financijski gubici,
- Financijska nestabilnost,
- Smanjenje prednosti u odnosu na konkurenciju,
- Gubitak korisnika,
- Smanjenje povjerenja korisnika.

Unutrašnji počinitelj je potrebno uzeti kao realnu prijetnju informacijskog sustava. Da se dobije jasnija slika o opasnosti koji oni predstavljaju potrebno je naći sve prijetnje

i načine na koje se prijetnje mogu provesti. Iz načina na koje se prijetnje mogu provesti može se odrediti kako se boriti za njihovo smanjivanje ili uklanjanje. Jedan od načina borbe sigurno je i korištenje tehničkih metoda.

Za unutrašnji počinitelj ili 'unutarnjeg' zlonamjernog korisnika možemo reći da je netko tko se nalazi unutar perimetra informacijskog sustava i ima određena prava koja su definirana poslovnim procesom koji obavlja. Komponenta 'zlonamjernog korisnika' znači da ima namjeru iskoristiti ranjivosti sustava i kao takav predstavlja prijetnju informacijskom sustavu. [2]

2.1. ANALIZA NAPADAČA

Kao uvod u problematiku unutrašnji počinitelj poslužiti će se još jednim istraživanjem 'Unutrašnji počinitelj Threat Study: Illicit Cyber Activity in Banking and Finanse Sector [10]' te dati nekoliko zanimljivih nalaza. Prije toga nekoliko primjera koji pokazuju kako to unutrašnji počinitelji djeluju.

Nezadovoljan sistem administrator postavio logičku bombu koja je nakon njegovog odlaska obrisala vrijedan softver zbog čega je tvrtka pretrpjela štetu od $10 milijun što je uzrokovalo da 80% zaposlenika ostane bez posla

Djelatnik koji je radio u razvoju aplikacija i zbog smanjenja broja ljudi izgubio je posao. Svoje nezadovoljstvo prvo je pokazao na način da je tri tjedna nakon otkaza, iskoristivši podatke od kolege, spoji se s udaljene lokacije i promjeni sadržaj Web stranice, te poslao mail svim kupcima u kome su se nalazili i korisnički podaci za pristup. Istraga ni uspjela identificirati počinitelja. Mjesec i pol kasnije isti djelatnik je pokrenuo skriptu koja je resetirala lozinke oko 4000 korisničkih računa. Osuđen je na zatvor, uvjetnu kaznu i novčanu kaznu.

Zaposlenik u državnoj upravi nije napredovao prema svojim očekivanjima i dan prije dolaska novog financijskog direktora obrisao je sve relevantne podatke sa svoga računala i računala kolega. Istraga je našla počinitelja, obrisani podaci su se uspjeli vratiti. Protiv počinitelja nije podignuta optužnica već mu je omogućeno da otkaz.

Primjeri su samo vrh brijega jer iz prije objavljene statistike je vidljivo da ~67% sigurnosnih incidenata nije rješavano korištenjem zakonodavstva, pa je za pretpostaviti da ih ima puno više.

Usporedba vanjski počinitelja i unutrašnji počinitelj ukazuje na potrebu promjene uobičajenog pristupa zaštite informacijskog sustava, tabela 2.1.

Vanjski počinitelj	**Unutrašnji počinitelj**
Visoki medijski publicitet	Neatraktivan za medije
Ograničeno poznavanje žrtve	Odlično poznavanje žrtve
Napadač ostavlja tragove	Napadač skriva tragove
Vrijeme ograničeno	Vrijeme nije ograničeno
Obrana usmjerene infrastrukturno	Obrana usmjerena prema podacima
Odgovornost IT odjela	Nedefinirana odgovornost

Tabela 2.1. Usporedba unutrašnji počinitelj i vanjski počinitelja (izvor: vlastiti rad)

Unutrašnji počinitelj ne treba biti tehnički obrazovan stručnjak jer ne treba zaobilaziti sve sigurnosne uređaje koje smo postavili na perimetar mreže i za koje svake godine ulažemo sve više novaca. Osim toga nema potrebe da troši vrijeme na proučavanje žrtve jer je jako dobro poznaje. Ima vremena na pretek da testira sustav za razliku od vanjski počinitelja koji možda odustane od napada ako se pokaže da eventualna žrtva nije vrijedan truda ili da informacije koje može dobiti nisu ekvivalentne uloženom trudu. Kad je u pitanju vanjski počinitelj obrana je usmjerena na infrastrukturu i za nju je odgovaran IT odjel. Za unutrašnji počinitelj obrana bi trebala biti usmjerena prema podacima i za nju u velikom broju informacijskih sustava nitko ne snosi formalnu odgovornost. Ovakvo stanje još više pogoduje unutrašnji počiniteljima u realizaciji njihovih ciljeva. Provedeno istraživanje bi trebalo dati bolji

sliku o unutrašnji počiniteljima. Odgovore na postavljena pitanja su dale organizacije koje su priznale da su imali problema s unutrašnji počinitelji i gdje su identificirani. Ako se uzme u obzir činjenica da mnogi ne žele priznati probleme s unutrašnji počiniteljima, neki ih ignoriraju, neki niti znaju da postoje, stanje je vjerojatno i lošije od prikazanog. Analiza nalazi je provedena da bi se objasnila potreba uključivanje unutrašnji počinitelj u sigurnosnih planova.

Nalaz 1. Znanje koje s raspolagalo za vrijeme izvođenja napada:

- U 87% slučajeva posjedovalo se osnovno znanje i koristile su legitimne akcije,
- U 9% slučajeva napadi su izvedeni skriptama ili programima,
- U 70% slučajeva iskorištene sistemske ili proceduralne manjkavosti,
- U 26% iskorištena su prava druge osobe,
- U 23% slučajeva počinitelj dolazi iz IT sektora.

Nalaz 2. Da li su napadi izvršeni slučajno ili su planirani:

- U 81% slučajeva napadi su unaprijed planirani, dok je u većem broju napada bilo informirano i više osoba,
- U 31% slučajeva postojali su vidljivi indikatori o nedozvoljenom ponašanju napadača.

Nalaz 3. Koji su motivi napadača (jedan ili više istovremeno):

- 81% - financijska dobit,
- 23% - osveta,
- 19% - krađa povjerljivih informacija,
- 15% - nezadovoljstvo rukovodstvom ili politikom poduzeća,
- 15% - potreba da se osoba uvažava.

Nalaz 4. Profil napadača

- Dob – od 18 do 59 godina,
- Spol – 58% muškarci,
- Različita rasna, etnička i socijalna okruženja,
- Radno mjesto napadača:

    - 31% servisno,
    - 23% službenik,
    - 19% profesionalno,
    - 23% tehničko.
- 17% napadača imalo 'admin' ovlasti,
- 15% napadača već prije okarakterizirano kao 'teški karakter',
- 4% prije smatrani kao 'nepouzdani',
- 19% napadača svrstano u nezadovoljne.

Nalaz 5. Metode utvrđivanja sigurnosnih incidenata

- 61% incidenata otkriveno od osoba izvan sigurnosne službe,
- Incidenti većinom otkriveni neautomatiziranim putem,
- 22% incidenata otkriveno kroz reviziju ili nadzorne procedure,
- U 74% slučajeva do identiteta počinitelja došlo se kroz logove,
- U 30% slučajeva provedena forenzička istraga.

Nalaz 6. Gubici nastali sigurnosnim incidentima

- U 91% slučajeva financijski gubici (od $168.000 do $691.000.000),
- U 30% slučajeva financijski gubici prelaze $500.000.

Nalaz 7. Vrijeme i mjesto izvršavanja napada

- U 83% slučaja napad je fizički izvršen s lokacije žrtve,
- U 70% slučaja za vrijeme radnog vremena,
- U 30% slučajeva napadi izvršeni od kuće napadača.

Iz nalaza proizlazi da unutrašnji počinitelju nisu potrebna stručna znanja da izvede napad. Napad je planirao i nije izazvana slučajnim djelovanjem. Motiv je u velikoj većini financijske prirode što može upućivati na načine otkrivanja unutrašnji počinitelj. Posao otežava i činjenica što za unutrašnji počinitelj ne možemo napraviti neki profil jer se nalazi u svim godištima, oba spola i može se nalaziti na svakom radnom mjestu. Metode da se otkriju treba tražiti u multidisciplinarnom pristupu tj. zajedničkom djelovanju sigurnosne službe, revizije, informatičke službe i samih

djelatnika. Vrijeme napada nije ograničeno na radno vrijeme već se odvija tijekom cijelog dana.

Upravama nije drago čuti a sami zaposlenici to ne žele priznati da velika prijetnja poduzeću dolazi od njezinih zaposlenika. Bez obzira na ovu činjenicu poduzeće i dalje veću pažnju posvećuje vanjski počiniteljima. Razlozi su u činjenici da je vanjski počinitelja lakše vidjeti i definirati obranu protiv njega. Ako zbog djelovanja vanjski počinitelja bude oštećen Web site to ćemo primijetiti a i drugi korisnici će nas obavijestiti. Za razliku od ovoga unutrašnji počinitelj može godinama kopirati povjerljiv sadržaj na USB i odnositi ga izvan poduzeća. Ovo je ne samo teško otkriti već je i teško definirati učinkovitu obranu.

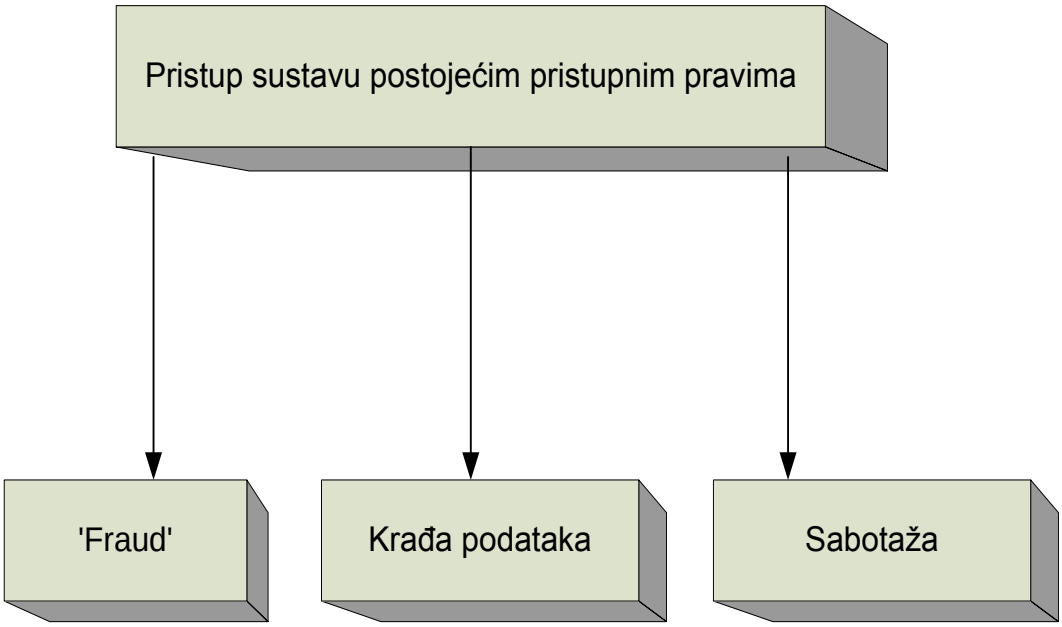
U osnovi svih napada je pokušaj pribavljanja nekih pristupnih prava, zatim njihovo povećanje što se više može da bi mogao ostvariti cilj napada i kompromitirao sustav. Problem koji imamo ovdje je da unutrašnji počinitelj već ima određena prava i za njih ne treba ništa potrošiti. Pogledajmo kako se može izvesti napad ovisno o tome da li imamo prava dovoljna za izvršenje napada ili ih moramo povećati.

2.2. IZVOĐENJE NAPADA

Cilj napada koji se izvodi kad se koriste već postojeća prava prikazan je na slici 2.1. Tijek napada kad korisnik koristi svoja postojeća prava pokazuje da tu nema nekih posebnih akcija koje korisnik mora napraviti da bi recimo ukrao podatke. To može raditi kroz dugi period vremena i ako neke druge metode ne detektiraju ovaj problem tehnička rješenja tu neće biti od pomoći. Ako unutrašnji počinitelj iskoristi svoja prava i napravi sabotažu to svakako nije dobro no sreća je u tome što je to jednokratna akcija i nakon što se provede sigurno će biti detektirana. Provođenje napada s ovim ciljem ukazuje na propuste i omogućava poboljšanje zaštite.

Fraud je napad koji unutrašnji počinitelj provede kroz poslovni proces koji obavlja. Primjer može biti nezadovoljni službenik na blagajni koji će iskoristiti manjkavosti aplikacije, poslovnog procesa ili nadzora te osigurati sebi materijalnu korist. Metode

revizije, nadzora nadređenih više će biti učinkovite nego neka tehnička rješenja i za ovu vrstu napada.

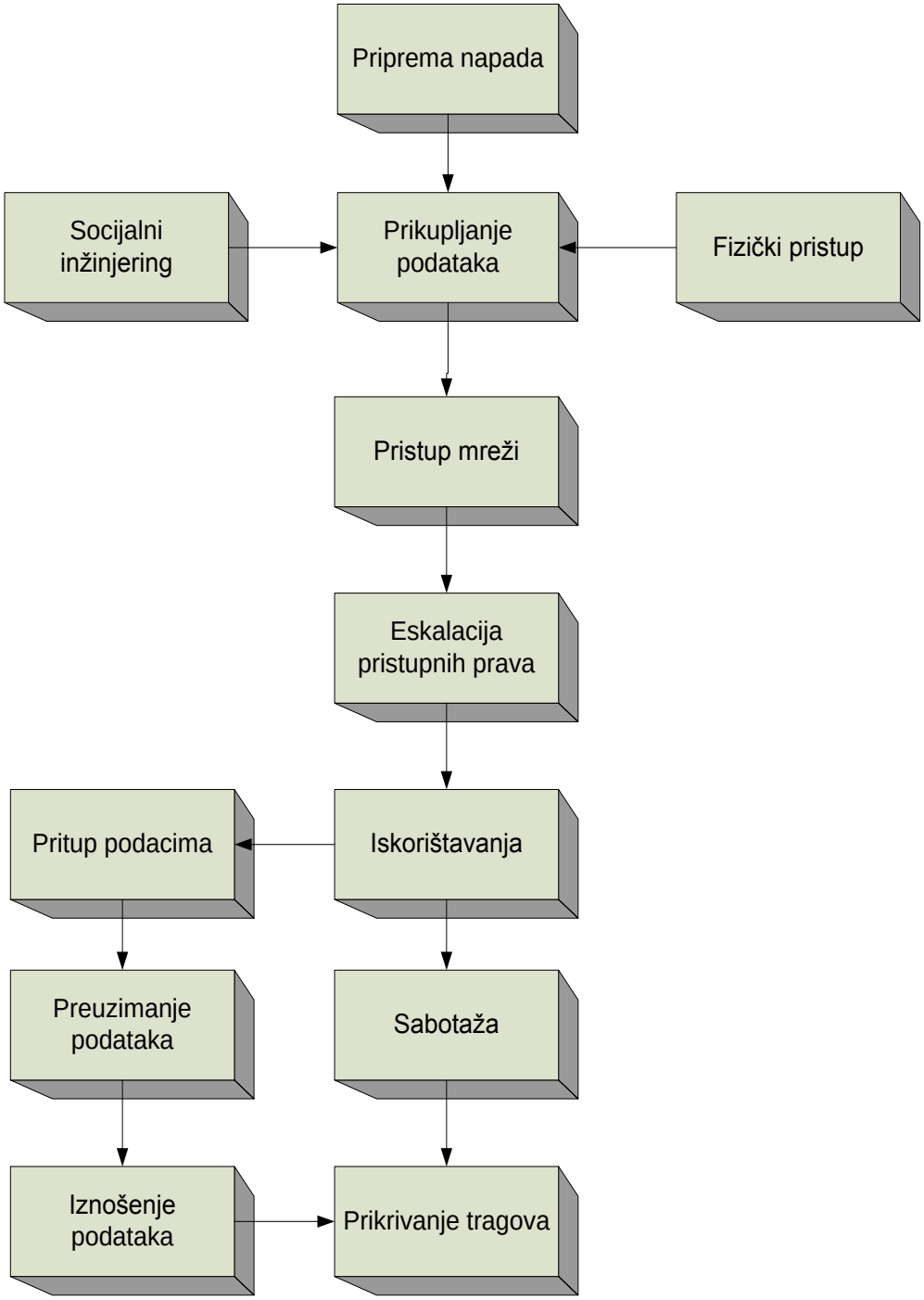


Slika 2.1. Tijek napada s postojećim pravima (izvor: vlastiti rad)

Ako je unutrašnji počinitelj netko tko ima određena prava pristupa onda je napad unutrašnji počinitelj iskorištenje dobivenih prava u svrhu napada. Pitanje koje se nameće je 'Zašto ta osoba ima ta prava i kako ih je dobila?' Problem više manje svih organizacija je da korisnici dobivaju više prava nego im treba za obavljanje svojih zadataka. Treba razlikovati kako je napadač došao do prava koja su mu omogućila napad, da li je iskoristio dobivena ili ih je pribavio na neki neregularan način.

Tijek napada kad je potrebno pribaviti prava koja osiguravaju iste prije spomenute ciljeve napada prikazan je na slici 2.2. Da se pribave odgovarajuća prava potrebno je provesti neke akcije koje se mogu detektirati a korištenjem nekih tehničkih rješenja smanjiti ili onemogućiti. Analizom tijeka ove vrste napada mogu nam pomoći u pristupu borbe protiv unutrašnji počinitelj. Sa slike je vidljivo da napadač mora na neki način doći do potrebnih prava koja će mu osigurati uvijete da izvede neki od napada. Kako to nije slučajno izvedena akcija kojom se kompromitira sigurnost

informacijskog sustava, prvo je donesena odluka da se izvrši napad. Priprema za napad možemo promatrati kao početak izvođenja nekog napada s ciljem stjecanja dodatnih prava. Da bi se na primjer došlo do korisničkog računa i lozinke, može se poslužiti tehnikom socijalnog inženjeringa (kao jednom od zatupljenijih metoda) ili fizičkim pristupom. Iskorištavanjem tih podataka unutrašnji počinitelj se prijavljuje na mrežu čime dobiva dodatna prava. Iskorištavajući nove veće ovlasti može pristupiti podacima i preuzeti ih na neki od medija (USB memorija, USB disk, fotoaparat, mobitel) i nakon iznošenja prikriti tragove. Ako je plan dugoročan onda će biti potrebno prikrivanje eventualnih tragova, no ako je cilj jednokratan kao i kod sabotaže onda je odnošenjem ili uništavanjem podataka ostvaren cilj.



Slika 2.2. Tijek napad kad se pribave druga prava (izvor: vlastiti rad)

Ako govorimo o mogućim motivima unutrašnji počinitelj onda su tu svakako slijedeći razlozi:

- Doći do nedozvoljenih informacija,
- Steći financijsku dobit,

- Nezadovoljstvo i osveta,
- Dokazati vlastitu sposobnost,
- Industrijska špijunaža,
- Ideološke razlike i/ili patriotizam,
- Emocionalni problemi.

Nabrojani motivi upućuju na ljudske slabosti ili probleme koje unutrašnji počinitelj rješava na radnom mjestu.

2.3. KATEGORIJE PRIJETNJI UNUTRAŠNJIH POČINITELJA

Treba napomenuti da unutrašnji počinitelj ne mora biti samo zaposlenik poduzeća. To može biti osoba koja ima neke veze s poduzećem ili s nekim od zaposlenika. Ovisno o nivou pristupa tj. na koji način je unutrašnji počinitelj došao do pristupnih prava možemo ih podijeliti u četiri grupe. O ovome treba voditi računa kad se planira sustav za upravljanje informacijskog sustava. Jer ako ne postoji kompletno rješenje koje povezuje sve resurse poduzeće moguće je da neke od slijedećih kategorija unutrašnji počinitelj obave svoje nakane:

- Pravi unutrašnji počinitelj,
- Pridruženi unutrašnji počinitelj,
- Unutrašnji počinitelj s posuđenim pravima,
- Vanjski počinitelj s posuđenim pravima.

2.3.1. PRAVI UNUTRAŠNJI POČINITELJI

Pravi unutrašnji počinitelj je zaposlenik poduzeća s svim svojim pravima i ovlastima koje je dobio. Tipičan primjer je zaposlenik koji posjeduje 'bedž' koji mu osigurava pravo pristupa resursima poduzeća te korisničke podatke na mreži koji mu osiguravaju pristup do podataka. Ovaj tip unutrašnji počinitelj obično čini najveću štetu jer ima sva prava potrebna za to. Eskalacija prava obično se odnosi na dodatna prava kolega ili sistemska prava administratora sustava. Princip 'najmanjih privilegija' koji treba primijeniti ide za tim da se korisniku osiguraju najmanja prava koja će mu

osiguravati obavljanje posla. Načini borbe protiv ovih unutrašnji počinitelj zasniva se na:

- Ograničenja i kontrola prava pristupa,
- Ponašanje – ove vrste unutrašnji počinitelj uklapa se u predvidljiv obrazac. Djelatnik obično iskazuje nezadovoljstvo, nije sretan i ljuti se na neposredne rukovodioce, upravu ili politiku poduzeća,
- Novac – je jedan od faktora koji može ukazati na unutrašnji počinitelj koji u jednom trenutku ima financijskih problema dok i drugom tih problema nema.

2.3.2. PRIDRUŽENI UNUTRAŠNJI POČINITELJ

Pridruženi unutrašnji počinitelji su osobe s ograničenim pravima pristupa. Radi se obično o ljudima koji rade kroz ugovor, službama za čuvanje i čišćenje prostora. Ovo nisu zaposlenici poduzeća ali u sklopu obavljanja određenih poslova imaju određena prava pristupa i ovlasti. Problemi s ovim unutrašnji počiniteljima je u tome što njima neke fizičke zaštite ne predstavljaju neku prepreku jer u obavljanju svoga posla imaju prava pristupa svim resursima. Primjer je zaključavanje prostorija nakon odlaska s posla gdje povjerljive informaciju ostaju na radnim stolovima. Zaključana vrata i nisu neka zaštita jer čuvarska služba ili služba za čišćenje nemaju problema s ulaskom u prostorije.

Zaštita se provodi povećanjem znanja i svjesnosti o ovim sigurnosnim problema. Spremanje stola prije odlaska s radnog mjesta, zaključavanje PC nakon dizanja s radnog mjesta smanjuje mogućnost pristupa povjerljivim informacijama.

Način borbe zasniva se na povećanju svjesnosti koji ima za cilj promijeniti obrasce ponašanja kod radnika. Druga metoda je kontrola pristupa ovim službama koje bi svoje poslove morali obavljati uz prisustvo zaposlenika poduzeća.

2.3.3. UNUTRAŠNJI POČINITELJ S POSUĐENIM PRAVIMA

Prve dvije grupe unutrašnji počinitelj imale su legitimno pravo pristupa resursima informacijskog sustava. Ova grupa to nema jer se radi o poslovnim partnerima, prijateljima ili znancima koji iskorištavaju prava zaposlenika poduzeća za pristup

sustavu. Primjer je prijatelj kojega ostavljate samog u sobi s mogućnošću pristupa računalu i podacima na stolu. Veći problem je kad netko izvana preuzme prava radnika i pristupi sustavu s udaljene lokacije. Načini na koji je došao do podataka može biti na legalan način, tj. da mu ih je radnik svojevoljno dao s nekom namjerom ili su ukradena.

Način borbe protiv ovih unutrašnji počinitelj je propisivanje strogih procedura i uputa koje radnici moraju potpisati čime preuzimaju odgovornost za svoje ponašanje.

2.3.4. VANJSKI POČINITELJ S POSUĐENIM PRAVIMA

Vanjski počinitelj s posuđenim pravima su osobe koji nemaju nikakva prava na sustavu, njima se ne vjeruje ali im se ostavi otvoren pristup resursima informacijskog sustava. Dobar primjer danas imamo u bežičnim mrežama. Ako poduzeće uspostavi bežičnu mrežu bez zaštite pristupnim točkama, što priječi pristup Vanjski počinitelj da se spoju na sustav? Ništa. Isto je da se ostavi otvorena vrata poduzeća bez kontrole, pitanje je vremena kad će netko ući da vidi o čemu se tu radi. Iako je ovo očiti sigurnosni problem, on se često zanemaruje. Kontrola pristupa mora se provoditi na isti način u 'virtualnom' svijetu kao što se provodi u fizičkom.

2.4. VRSTA PRIJETNJI I NAČINI IZVOĐENJA NAPADA

Prije nego nabrojimo prijetnje potrebno je jednoznačno definirati što se podrazumijeva pod prijetnjama i kakve će posljedice biti za informacijski sustav.[2]

Prijetnja je svaki neželjeni događaj koji može poništiti ili smanjiti učinkovitost sustava, odnosno ograničiti ili onemogućiti ispunjenje cilja sustava ili procesa.

Sigurnosni rizik definira se kao mogućnost realizacije nekog neželjenog događaja. Neželjeni događaj može utjecati na :

- povjerljivost (*eng. confidentiality*),
- integriteta (*eng. integrity*),
- raspoloživost (*eng. availability*) informacijskih resursa.

Povjerljivost se odnosi na zaštitu određenih sadržaja, odnosno informacija od bilo kakvog namjernog ili nenamjernog otkrivanja neovlaštenim osobama. *Integritet* mora

osigurati konzistentnost informacija i onemogućiti bilo kakve neovlaštene promjene sadržaja. *Raspoloživosti* podrazumijeva da su sve relevantne informacije, u za to vremenski prihvatljivom terminu, raspoložive odgovarajućim subjektima. Bilo koji od ovih zahtjeva može biti kompromitiran na razne načine: bilo namjernom ili nenamjernom ljudskom pogreškom, bilo zbog nedostataka i kvarova opreme i aplikacija ili zbog drugih izvanrednih događaja.

To znači da je sigurnosna prijetnja (*eng. threat*) neželjeni događaji koji se može negativno odraziti na integritet, povjerljivost i raspoloživost resursa.

U nastavku će se identificirati prijetnji koji se mogu primijeniti na postojeći IT sustav i time ugroziti poslovanje organizacije. Izvor prijetnji se definira kao okolnosti ili događaji koji mogu prouzrokovati štetu u IT sustavu. Izvore prijetnje koje ćemo ovdje promatrati su namjerni, a to su oni izvori koji ciljano iskorištavaju nedostatke u sustavu u svrhu neovlaštenog pristupa povjerljivim podacima. U ovu skupinu najčešće spadaju ljudi te razni štetni programi (crvi, virusi...) i sl.

Pod pojmom ranjivosti (*eng.Vulnerability*), smatraju se svi propusti i slabosti u sustavu sigurnosti koji omogućuje provođenje neovlaštenih aktivnosti. Ranjivost se najčešće povezuje s propustima u programskom kodu, no mogući su i mnogi drugi primjeri, kao što su površno implementirana fizička sigurnost, nedovoljno poznavanje i neprikladan izbor tehnologija i alata, propusti u dizajnu sustava, propusti u implementaciji i održavanju sustava i sl.

Sad kad su definirani osnovni pojmovi treba odrediti kako unutrašnji počinitelj prijeti informacijskom sustavu.

2.4.1. PRIJEVARE U PROVEDBI POSLOVNIH PROCESA

Ova vrsta prijetnje je poznata i pod imenom ‘Fraud'. Korisnik u obavljanju svoga posla upoznat je sa svim ranjivostima poslovne aplikacije i poslovnog procesa u kojem sudjeluje. Rezultat ovoga su slijedeći načini na koji se vrše prijevare u provedbi poslovnog procesa:

- Zloupotreba principa „nužnih ovlasti“,

- Zloupotreba nedosljedno provedenog pravila o odvajanju nadležnosti,
- Iskorištavanje nedostataka pravila o prisutnosti dviju osoba,
- Poricanje transakcija.

Oblici zloupotreba u gore navedenim slučajevima mogu biti slijedeći:

- Korupcija i ucjena,
- Sukob interesa,
- Fiktivni prihodi,
- Neprijavljene obveze,
- Pretjerana procjena vrijednosti,
- Nedosljedna objava informacija,
- Nefinancijske prijevare,
- Novčane pronevjere,
- Krađa novca (prije unošenja),
- Zloupotreba ili krađa inventara,
- Manipulacija s fakturama,
- Manipulacija s plaćama,
- Manipulacija s materijalnim troškovima,
- Manipulacija s nalozima za plaćanje,
- Prijevare s isplatama iz blagajne.

2.4.2. NEOVLAŠTEN FIZIČKI PRISTUP

Kritična i osjetljiva informacijski resurs trebaju biti smještena u sigurnim područjima, zaštićena prikladnim sigurnosnim barijerama i kontrolama ulaza. Trebaju biti fizički zaštićena od neautoriziranog pristupa. No kako to u većini poduzeća nije slučaj onda unutrašnji počinitelj iskorištava ovo da bi:

- Neovlašteno pristupio aktivnim računalnim resursima,
- Neovlašteno pristupio opremi kod koje se ne nalaze operateri,
- Neovlašteno pristupio u zaštićene prostore.

2.4.3. SOCIJALNI INŽENJERING

Socijalni inženjering[9] je umjetnost i znanost nagovaranja ljudi da ispune zahtjeve napadača. Radi se o načinu stjecanja informacija i podataka do kojih napadač legitimnim putem ne bi mogao doći. Pri tome se ne iskorištavaju propusti implementacija operacijskih sustava, protokola i aplikacija, nego se napad usmjerava na najslabiju kariku cjelokupnog lanca – ljudski faktor.

Filozofija - Pristup informacijama koje čuvaju ljudi mnogo je jednostavniji od pristupa zaporkom zaštićenim informacijama. Napadači iskorištavaju ljudsku psihologiju i na taj način uspijevaju u navođenju žrtava na ispunjavanje njihovih zahtjeva bez izazivanja nepotrebnih sumnji. Napadač koji provodi napad zasnovan na socijalnom inženjeringu mora posjedovati osobine poput dobrog pamćenja, snalaženja u razgovorima, odgovarajućeg načina razmišljanja i slično, jer mu one donose prednost prilikom izvođenja napada.

Uvjeravanje - Nagovaranje ili uvjeravanje je akcija poduzeta od strane napadača kojoj je konačan cilj potaknuti žrtvu na izvršavanje željenih postupaka.

Lažno predstavljanje - Ovisno o situaciji, napadač se mora maskirati odnosno pretvarati da je netko tko nije kako bi prikupio željene informacije od žrtve. *Ovo je najčešće korištena metoda napada*. Odabir lažne uloge ovisi o konkretnoj situaciji i željenom cilju.

Stvaranje odgovarajuće situacije - Ovdje se radi o sposobnosti stvaranja situacije u kojoj je žrtva primorana donositi brze i važne odluke pod velikim psihološkim pritiskom s jedne strane, i brojnim zahtjevima napadača s druge. Usprkos brojnim pokušajima suzbijanja ovog problema korištenjem različitih alata, tehnologija i

[9] Link; http://www.cert.hr/documents.php?id=264 (5.11.2007)

zakona, neželjena elektronička pošta još je uvijek veliki problem gotovo svih informacijskih sustava.

Moralna odgovornost - Radi se o ljudskom ponašanju u kojem žrtve pokušavaju pomoći napadaču jer osjećaju da je to njihova moralna obveza. Dobar primjer ovakvog ponašanja je slučaj u kome je napadač iz iste zemlje kao i neki inozemni zaposlenik te on, koristeći osjećaj moralne dužnosti zaposlenika, dolazi do potencijalno osjetljivih informacija. Napadači koji se koriste opisanom tehnikom najčešće su vrlo bistre osobe, a svoje žrtve promatraju i upoznaju kroz dulje vrijeme te s njima uspostavljaju blizak osoban odnos.

Želja za pomaganjem - Čest je ljudski osjećaj želje za nesebičnom pomoći drugima. Kao jednostavan primjer može poslužiti situacija u kojoj napadač zatraži pomoć od žrtve koja mu odbija pomoći jer traži neke nedostupne informacije. Međutim, lijepim razgovorom napadač pobudi osjećaj djelomične krivnje i potakne žrtvu na razmišljanje o tomu kako će i njoj vjerojatno zatrebati pomoć kada se nađe u jednakoj situaciji kao i on u tom trenutku. Žrtva najčešće pomisli kako se radi o sitnim informacijama i kako nikomu neće škoditi ukoliko pomogne čovjeku i izvan protokola. Tako otkriva potencijalno osjetljive informacije. Napadač odlazi zadovoljan jer je dobio što je htio, a žrtva ostaje relativno zadovoljna jer je pomogla nekomu.

Iskorištavanje starih veza i kooperacije - U ovom načinu socijalnog napadanja, napadač obnavlja stare ili stvara nove veze sa žrtvama. Napadač će stvoriti odnos koji je dovoljan za stjecanje povjerenja. Ovakav pristup kod socijalnog inženjeringa ima vrlo velik stupanj uspješnosti, što je posebno izraženo ukoliko je žrtva spremna za ostvarivanje suradnje s napadačem. Na taj način je prijeđena početna barijera i prikupljanje željenih informacija kreće lakšim tijekom.

2.4.4. NEOVLAŠTENO OTKRIVANJE LOZINKI DRUGIH OSOBA

Ako pristupna prava kojima raspolaže unutrašnji počinitelj nisu dovoljna ili ako ne želi da ga otkriju potrebno je nekako doći do njih. Neki od načina su:

- Dešifriranje lozinki s računalnih sustava,

- Uvid u nešifrirane lozinke,
- Pogađanje lozinki,
- Uvid u sadržaj prometa po mreži (engl. sniffing[10]).

2.4.5. NEOVLAŠTENO KORIŠTENJE SIGURNOSNIH ALATA

Ako ne postoji implementirana sigurnosna politika kroz koju su definirane razne politike, procedure i upute onda lokalnu mrežu može promatrati kao javnu. U takvoj mreži nemamo informaciju što je sve instalirano na računalo korisnika niti što se sve spaja na takvu opremu. Način na koji se može provesti ovaj napad je:

- Korištenje sigurnosnih alata u svrhu prikupljanja informacija o sustavu.

2.4.6. PRISLUŠKIVANJE KOMUNIKACIJSKOG TIJEKA

Još jedna posljedice, prije navedenog slučaja, kad ne postoji implementirana sigurnosna politika za informacijski sustava. Način na koji unutrašnji počinitelj može doći do željenih podataka je:

- Instalacija hardverskog 'keylogger[11]' alata,
- Instalacija softverskog 'keylogger',
- Korištenje 'sniffing' alata.

2.4.7. ISKORIŠTAVANJE PROGRAMSKIH RANJIVOSTI

Svaki je računalni sustav podložan programerskim pogreškama, a većina takvih grešaka imaju kritične posljedice. Ne treba zanemariti činjenicu da složeni sustavi zahtjevaju pažljivu konfiguraciju, a pogreške u jednom sustavu mogu se odraziti i na drugi sustav. Unutrašnji počinitelj može iskoristit slijedeće programske ranjivosti:

- Iskorištavanje grešaka u standardnim programskim paketima,
- Iskorištavanje grešaka u aplikativnim sustavima,
- Iskorištavanje ranjivosti web aplikacija.

2.4.8. POJAVA ILI UNOŠENJE MALICIOZNIH PROGRAMA

[10] Analiza mrežnih paketa
[11] Zapisuje svaki pritisak na tipkovnici

Malicioznih ili zlonamjerni programa je softver napravljen tako da se neprimjetno ubaci u sistem računara i načini neku vrstu štete. Zlonamjerni program može biti računarski virus[12], crv[13], trojanski konj[14], spyware[15], adware[16] ili neki drugi štetni program. Unutrašnji počinitelj za ostvarivanje svojih ciljeva može se koristiti slijedećim zlonamjernim programima ili metodama:

- Namjerno unošenje računalnog virusa,
- Namjerno unošenje Trojanaca ili Backdoor[17] programa,
- Izvođenje 'hackerskih' napada.

2.4.9. NEOVLAŠTENI LOGIČKI PRISTUP

Kad govorimo o logičkoj sigurnosti mislimo na sigurnosti resursa pohranjenih na računalima (baze podataka, datoteke, multimedijalni zapisi) i zaštitu takvih resursa. Iako na prvi pogled logička i fizička sigurnost nemaju puno dodirnih točaka, realnost je bitno različita. Bez organizacijske i tehnološke integracije ova dva segmenta korporacijske sigurnosti nemoguće je odgovoriti na pitanja poput: 'Tko ima prava pristupa kojim resursima?', 'Da li ta prava odgovaraju potrebama radnoga mjesta?', 'Da li osoba koja lokalno pristupa bazi podataka stvarno fizički i prisutna na poslu?'. Unutrašnji počinitelj koristi nedefiniranu situaciju za:

- Pristup pomoću lozinke otkrivene na nedozvoljeni način,
- Pristup dijeljenim pristupnim pravima,
- Pristup pomoću važećih ali nekonzistentnih prava,
- Pristup 'default' korisničkim pravima,

[12] Program koji se razmnožava kopirajući samoga sebe, bilo kao točnu kopiju ili kao promijenjeni oblik, u neki drugi dio izvršnoga koda.
[13] Crv je zapravo skup virusa koji ima sposobnost da se samostalno umnožava i nije mu potrebna datoteka-domaćin
[14] Program je koji naizgled radi jedno, ali ustvari radi nešto drugo. Iako nisu uvijek zlonamjerni ili ugrožavajući, često su korišteni za brisanje datoteka i tvrdih diskova, ili se koriste kako bi napadaču omogućili udaljeni pristup kompjuterskom sistemu.
[15] Kategorija malicioznog softvera sa namjenom da presreće ili preuzima djelomičnu kontrolu rada na računalu bez znanja ili dozvole
[16] adware – (engl. advertising, reklamiranje; software) aplikacija koja se koristi prikupljenim podacima kako bi bez korisnikovog pristanka, u što većem broju i što nametljivije prikazivala reklame vezane uz korisnikove interese
[17] Program koji otvara dodatni port za udaljeni pristup

- Pristup 'backdoor' korisničkim pravima,
- Pristup temeljem iskorištavanja sistemskih ranjivosti,
- Zloupotreba administratorskih prava.

2.4.10. NEOVLAŠTEN UVID U POVJERLJIVE PODATKE

Način da unutrašnji počinitelj dođe do željenih informacija je i:

- Uvid u sistemske podatke,
- Uvid u povjerljive podatke koji su u strukturiranom obliku,
- Uvid u povjerljive podatke koji su u nestrukturiranom obliku,
- Nestandardna pretraga podataka.

2.4.11. ODNOŠENJE POVJERLJIVIH PODATAKA

Razvoj tehnologije omogućio je unutrašnji počinitelju da koristi memorijske uređaje koji su svakodnevno sve manjih dimenzija i sve većeg kapaciteta. Osim toga otvorenost poduzeća nastaje kao rezultat zahtjeva uprave da korisnik ima pristup raznim izvorima informacija na razne načine. Ovo ide na ruku unutrašnji počinitelju da iskoristi:

- Pomoćne medija za pohranu (USB memorija, CD-ROM),
- Korištenjem tehnike stenografije,
- Prikriveno slanje podataka mail[18]-om, ftp[19] ili sličnim protokolima,
- Prikriveno slanje podataka wireless[20] komunikacijom,
- Odnošenje podataka po prestanku radnog odnosa.

2.4.12. JAVNA OBJAVA POVJERLJIVIH INFORMACIJA

Još jedna posljedice nedefinirane sigurnosne politike može rezultirati slijedećem:

- Nekontrolirana distribucija podataka elektroničkim putem,
- Iznošenje povjerljivih informacija verbalnom komunikacijom,
- Neadekvatan otpis računalne opreme,

[18] Elektronička pošta
[19] Engl. File Transfer Protocol - protokol za prijenos datoteka
[20] Bežična mreža

- Izlaganje povjerljivih informacija uslijed nesmotrenosti u radu.

2.4.13. NEOVLAŠTENI UVID U DOKUMENTE ILI EKRANSKE PRIKAZE

Fizička sigurnost koja se ne provodi adekvatno može omogućiti unutrašnji počinitelju da dođe do podataka i na slijedeće načine:

- Otkrivanje lozinke za rad na sustavu pregledom radnog prostora,
- Otkrivanje povjerljivih dokumenata u radnom prostoru.

2.4.14. KRAĐA RESURSA

Krađa resursa nije nešto što se ne događa ali se ne promatra sa stanovišta sigurnosti informacijskog sustava. Unutrašnji počinitelj koristi ovu metodu da bi ostvario neki od ciljeva i to kroz:

- Krađu prijenosnih računala,
- Krađu stolnih ili serverskih računala,
- Krađu papirnatih dokumenata,
- Krađu printerskih ispisa,
- Krađu podataka na medijima za pohranu.

2.4.15. VANDALIZAM

Vandalizam možemo promatrati kao vrstu napada na informacijske sustave s ciljem namjernog oštećivanja ili uništavanja resursa informacijskog sustava da bi se otežao ili onemogućilo daljnje korištenje ili rad napadnutog resursa.

2.4.16. SABOTAŽA

Pod sabotažom možemo svrstati vrsta napada kojemu je cilj onemogućavanje ovlaštenog korisnika da se koristi kompjutorskim ili mrežnim uslugama i servisima. Uskraćivanje usluga – DoS (eng. Denial Of Service) najčešće se izvodi putem istovremenog slanja velikog broja poruka ili tolike količine podataka da se resursi glavnog kompjutora u tolikoj mjeri iskoriste da više ne mogu raditi. Unutrašnji počinitelju kojemu je to cilj napada može do njega doći kroz:

- Unošenje destruktivnog programa,
- Narušavanje integriteta hardverskog okruženja,
- Narušavanje integriteta softverskog okruženja.

2.4.17. NEOVLAŠTENO KORIŠTENJE SISTEMSKIH RESURSA

Još jedan način na koji unutrašnji počinitelj koristeći se svojim ovlastima ili ovlastima drugih korisnika može doći do svog cilja kao što je:

- Prekomjerna upotreba sistemskih resursa,
- Manipulacija sistemskim programima ili konfiguracijskim parametrima,
- Instalacija i korištenje neodobrenih programskih paketa (mail, IM[21], P2P[22]…),
- Pokretanje računala s alternativnim operativnim sustavom.

2.4.18. POVREDA INTELEKTUALNOG VLASNIŠTVA TREĆE STRANE

U svim 'Odredbama i uvjetima korištenja' nekog proizvoda definira se što se smatra pod 'Intelektualno vlasništvom'. Kršenje tih odredbi poduzeće može imati problema. Unutrašnji počinitelj kome je cilj da poduzeće dovede u takvu situaciju može napraviti slijedeće:

- Neovlašteno preuzimanje, pohrana ili distribucija sadržaja s intelektualnim vlasništvom,
- Namjerno korištenje nelicenciranog softvera,
- Neovlašteno unošenje ili iznošenje softvera.

2.4.19. PRIKRIVANJE PODATAKA O NEDOZVOLJENIM AKTIVNOSTIMA

Ako je unutrašnji počinitelju cilj da svoje aktivnosti provodi u dužem vremenskom razdoblju mora se potruditi da prikrije tragove. To može izvesti na način izvede:

- Neovlašteni pristup i/ili izmjeni evidencijski zapis,
- Sigurno brisanje podataka s diskovnog prostora,
- Prikrivanje identiteta u komunikaciji.

[21] instant poruke - je servis za komuniciranje u realnom vremenu
[22] znači peer-to-peer, program kojim se spajaju razna računala i omogućava da međusobno izmjenjuju datoteke

2.4.20. NEOVLAŠTENA PROMJENA PROGRAMSKOG KODA

Još jedan način da unutrašnji počinitelj iskoristi propuste u poslovnim procesima je da:

- Namjerno ugradnji neprihvatljivog programskog koda tijekom razvojnog ciklusa,
- Neovlašteno promjeni programskog koda u produkcijskom radu.

Na sve ove prijetnje i načine na koji se oni mogu izvesti, vratit će se još jednom pri kraju kad se bude analizirala učinkovitost IPsec-a u smanjivanju prijetnji unutrašnji počinitelj i u kojoj mjeri.

2.5. PREVENCIJA I/ILI DETEKCIJA

U borbi protiv prijetnji unutrašnji počinitelj moguće je implementirati metode prevencije i detekcije. Uvijek je potrebno pokušati onemogućiti izvođenje napada. Kad to nije moguće potrebno je detektirati napadača i minimizirani štetu koja je nastala njegovim djelovanjem. Korištenje prevencije i detekcije treba biti izvedeno na optimalan način. Mjere prevencije koje implementiramo obično će odvratiti od napada običnog unutrašnji počinitelj ili unutrašnji počinitelj s prosječnim znanjem i motivom. Kad je u pitanju visoko motiviran unutrašnji počinitelj koji posjeduje i znanje, mjere prevencije na njega neće djelovati. Ovdje nam mogu koristiti mjere detekcije koje će nam koristiti u otkrivanju tragova. Mogu se koristiti za definiranje novih sigurnosnih metoda koje bi takvu vrstu napada mogla spriječiti. Iako izgleda da je jednostavnije implementirati samo mjere prevencije bez detekcije u nekim slučajevima neće se znati koje dodatne mjere treba implementirati. Balansiranje ovih dviju metoda dat će optimalan rezultat i zadovoljiti zahtjeve za kvalitetniju borbu protiv unutrašnji počinitelj.

2.5.1. METODE PREVENCIJE

Metode prevencije koje nam stoje na raspolaganju u borbi protiv prijetnji unutrašnji počinitelj su slijedeće:

- Podizanje svijesti o sigurnosnim problemima,

- Odvajanje dužnosti,
- Rotacija dužnosti,
- Princip 'najmanjih prava',
- Kontrola fizičkog i logičkog pristupa,
- Propisane politike za sve važne segmente informacijskog sustava,
- Obrana koja se provodi po nivoima,
- Tehnike obrane koje nisu tehničke prirode,
- Arhiviranje kritičnih podataka,
- Kompletna rješenja koja u sebi povezuju sve aspekte poduzeća, ljude, podatke, tehnologiju, procedure i politike.

2.6. TRENDOVI KOJI POGODUJU UNUTRAŠNJI POČINITELJIMA

Neki od trendova koji su prisutni u informatičkoj industriji a koji pogoduju unutrašnji počiniteljima su:

- Outsourcing[23] je sve raširenija pojava u industriji. Sve više vanjskih firmi obavlja specijalizirane djelatnosti u poduzeću, kao što je čišćenje, sigurnosna služba, vatrogasna služba i sl. Da se dođe do povjerljivih podataka ne treba postati zaposlenik poduzeća jer je možda jednostavnije postati zaposlenik u poduzećima koja pružaju prije navedene usluge,
- Minituarizacija – smanjivanje memorijskih uređaja sve se više nastavlja. Osim toga mobilni telefoni objedinjuju sve veći broj funkcija koje koriste unutrašnji počinitelji u ostvarivanju svojih ciljeva,
- Otvaranje mreže i sustava – nastaje kao zahtjev uprava za pristup sustava s raznih lokacija uz što jednostavniji rad. To usložnjava infrastrukturu i neminovno dovodi do otvaranja sve većeg broja servisa prema van. U sve složeniji sustav postaje i sve ranjiviji što unutrašnji počinitelj može iskoristiti u svojim namjerama,

[23] *Outsourcing*, odnosno eksternalizacija određenih područja poslovanja, bilo da se radi o operativnim ili strateškim funkcijama, može znatno rasteretiti kapacitete i pružiti mogućnost za veću fokusiranost na primarnu djelatnost

- Jednostavnost korištenja 'hackerskih' alata – alati koji se koriste za neke sigurnosne provjere te sve veći broj hakerskih alata sve je jednostavnija za upotrebu. Ovakvi alati i neobrazovanom unutrašnji počinitelju omogućava ostvarivanje cilja jer se nalazi unutar perimetra mreže,
- Socijalni inženjering – sve je raširenija metoda i sve se više koristi u napadu na najslabiju kariku. To proizlazi iz činjenice da se u poduzećima ne provodi i povećanje svijesti o sigurnosnim problemima,
- Planiranje – jedan od trendova koji unutrašnji počinitelji koriste jer imaju vremena a cilj im je djelovanje u dužem vremenskom periodu. Za to se u ostvarivanju ciljeva ne ide 'stihijski' već se sustav testira i plan se provodi kroz duži vremenski period,
- Povećanje tolerancije – još jedan trend koji ide na ruku insiredu a to je smanjenje senzibilnosti na sigurnosne incidente. Prije bi otkriveni unutrašnji počinitelji bili medijski eksponirani i pobudili bi određene reakcije javnosti što bi rezultiralo i promjena u poduzećima da se to ne dogodi kod njih. Danas to nije medijski interesantna tema što pogoduje unutrašnji počiniteljima ali i poduzećima jer na taj način ne trebaju ništa poduzeti,
- Krađa identiteta – još jedan trend koji unutrašnji počinitelji primjenjuju kako zbog tehnološke mogućnosti a s ciljem da sakriju svoje djelovanje i dugoročno ostvaruju svoje ciljeve,
- Krtica – kao posljedica sve veće konkurenciji među poduzećima ovo je logičko rješavanje problema. Da bi se došlo do povjerljivih informacija provodi se obuka unutrašnji počinitelj te mu se osigurava tehnološku pomoći pri realizacije napada.

Ovime su pokrivene moguće prijetnje unutrašnji počinitelj. Vidjeli smo da se u metodama prevencije ne spominju neka tehnička rješenja koja bi pomogla u smanjivanju ili uklanjanju pojedinih prijetnji.

Microsoft je u posljednjim verzijama operacijskih sustava implementirao i IPsec. Više o samom IPEsc-u će biti kasnije više riječi, sad samo to da je to proširenje IP protokola koje osigurava siguran prijenos podataka. Implementacija IPsec-a povećava sigurnost informacijskog sustava u suradnji sa sigurnosnim uređajima (vatrozidom, ruterom, proxy-em) tj. uvodi se još jedan sloj zaštite. U nalazi će se koristiti Windows 2003 Server kao mrežni operacijski sustav te Windows XP Profesional i Windows Vista Business klijentski operacijski sustav.

Implementacija IPsec-a u operacijski sustav omogućilo je pomicanje perimetra mreže bliže mjestu gdje se podaci nalaze. Kako IPsec povećava sigurnost informacijskog sustava kad se koristi u operacijskom sustavu od Microsoft-a ukratko će biti prikazano u slijedećem poglavlju.

3. PRIMJENA SERVISA/ALATA IPSEC-A U POVEĆANJU SIGURNOSTI

Microsoft implementacijom IPsec–a u operacijske sustave povećava sigurnost informacijskog sustava. Kako se mogu podešavati granice štićenog prostora (perimetar) te kako postaviti takve konfiguracije biti će prikazano u ovom poglavlju. Ukratko će se prikazati kako provesti implementaciju IPsec-a, da bi se dobio osjećaj o obimu posla. [3], [12],[13],[14],[15].

Organizaciji je potreban siguran mrežni promet iz slijedećih razloga:

- Zaštiti IT resursa,
    - Računala i podataka,
    - Zaštita sustava od malwera[24] (virusi, crvi, Trojanskih konja ..).
- Usklađenost za zakonskom regulativom,
    - Financijske ustanove,
    - Državna uprava,
    - Zdravstvo (Amerika – HIPAA[25]),
    - Ostale organizacije (propisane lokalne sigurnosne politike).
- Zaštita intelektualnog vlasništva,
- Poboljšati upravljanje informacijskog sustava.

Zahtjevi korisnika da mogu jednostavno pristupiti elektroničkoj pošti, datotekama, Web[26]-u bez obzira na koji način su ostvarili konekciju (Ethernet[27], wireless, remote access[28]) povećava složenost sustava. Kako raste složenost sudstva povećava se i rizik. Zadovoljenje zahtjeva da korisnik u bilo koje vrijeme može pristupiti željenom mrežnom resursu s bilo koje lokacije također omogućava i zlonamjernom kodu ili zlonamjernom korisniku da napadne računala bilo kada i s bilo koje lokacije. Pristup

[24] Softver napravljen tako da se neprimjetno ubaci u sistem računara i načini neku vrstu štete
[25] Engl. Healt Insurance Portability and Accountability Act
[26] Internetske stranice (točnije web stranice ili www stranice)
[27] Mrežna tehnologija za LAN mreže, temeljena na paketnom načinu rada
[28] Spajanje mobilnih korisnika na mržu poduzeča

resursima treba omogućiti samo autentificiranim i autoriziranim korisnicima i računalima. Mrežni resursi bi trebali biti izolirani, ne samo od Interneta već i od korisnika koji nisu autentificirani i od opreme koja nije pouzdana a nalazi se na lokalnoj mreži. Izolacija korisnika koji su prošli provjeru i oprema koja je pouzdana neovisna je od fizičke topologije mreže.

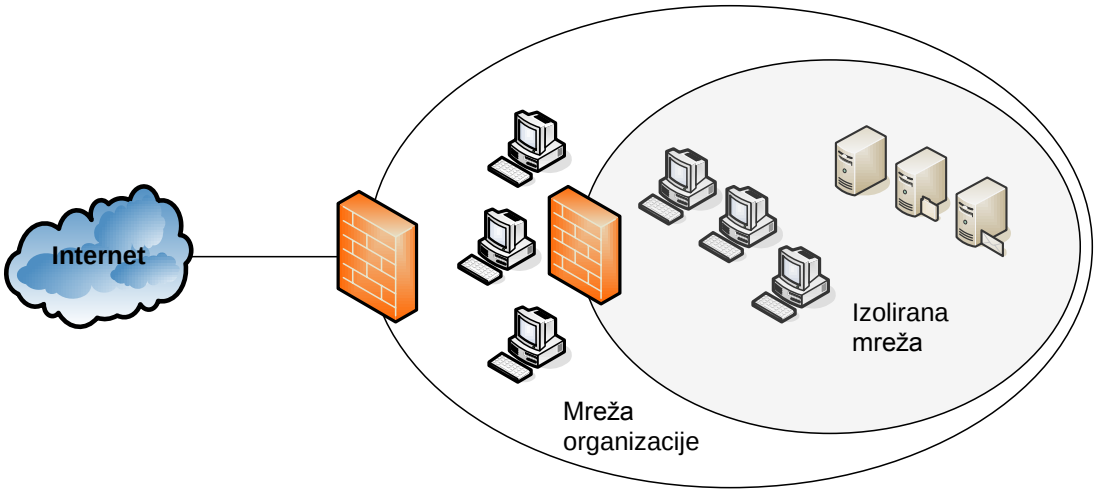
Do sada je izolacija pojedinih resursa provođeno na slijedeći nači:

- Fizički sloj OSI[29] modela – povlačimo dodatno kabliranje za pojedine grupe što je skupo i teško za održavanje za veće mreže,
- Podatkovni sloj OSI modela – Layer 2[30] switches[31], koji kreiraju VLAN[32] na osnovu fizičkog spoja na switchu,
- Mrežni sloj OSI modela – definiraju se logičke podmreže koji se spajaju preko rutera. Izolirane podmreže temeljene na VLAN zahtijevaju da svi switch-evi moraju podržavati VLAN-ove te je potrebno stalno održavanje topologije mreže zbog promjena lokacija pojedinih resursa,
- IPsec[33] i AD[34] u Windows mrežnom okruženju omogućava kreiranje logičke izolacije resursa temeljenu na ograničavanju pristupnih prava na osnovu autorizacije i autentifikacije. To znači da postoji logički segment mreže, u kome se nalaze računala koja dijele zajednički sigurnosni okvir gdje su definirani zahtjevi za sigurnu komunikaciju. Svaki član ove mreže provjerava identitet drugog računala prije nego s njime uspostavi komunikaciju. Zahtjevi za komunikaciju koji dođu izvan ove izolirane logičke grupe će biti ignorirani.

'Izolacija' kroz Windows mrežne operacijske sustave odvija se na mrežnom sloju OSI modela. Računala koji pripadaju izoliranoj grupi mogu biti spojeni na mrežu preko različitih mrežnih uređaja, hub[35]-ova, switche-va ili routera[36] i nalaziti se na različitim

[29] Engl. Open System Interconnection
[30] Podatkovni sloj je isto što i Layer 2
[31] Preklopnik
[32] Engl. Virtual LAN
[33] Engl. IP security protocol
[34] Eng. Active Directory
[35] Uređaj za povezivanje računala u zvijezdu

fizičkim lokacijama. Ovako kreirane izolirane grupe neovisne su o kabliranju, karakteristikama mrežnih uređaja, te ne zahtijevaju dodatna održavanja zbog promjena u topologiji mreže ili seljenju resursa.



Slika 3.1. Izolirana mreža u mreži organizacije (izvor: vlastiti rad)

Na slici 3.1. prikazana je izolirana mreža unutar organizacijske mreže. Izolacija je provedena vatrozidom, a može biti izvedena i s proxy[37] serverom ili ruterom. Resursi koji se nalaze unutra izolirane mreže zaštićeni su od ostatka resursa. Mnogi tipovi virusa i crva neće moći ući u izolirani dio mreže. Zlonamjerni korisnik i program izvan takve mreže neće moći jednostavno napasti resurse koji se nalaze unutra jer ne posjeduju autentifikacijske informacije koje su neophodne za uspostavljanje komunikacije. Dodatno podizanje sigurnosti izolirane mreže je u enkripciji prometa što istovremeno zadovoljava i zahtjeva zakonske regulative i preporuka standarda.

Mogući scenariji implementacija su:

- Packet filtering (propuštanje paketa kroz filtar radi identifikacije),
- Izolacija servera ili osiguranje servera,
- Izolacija domene i servera.

[36] Usmjerivača
[37] Uređaj koji stoji između klijeta i servra

3.1. PACKET FILTERING

U osnovi se radi o običnom filtriranju paketa koji se puštaju ili blokiraju, slično kao i kod vatrozida osim što nema naprednih opcija kao 'stateful filtering'. Koristimo ga za jednostavnije slučajeve.

Primjer za ovaj slučaj je servera koji se nalazi u DMZ[38] i na kojem blokiramo pristup svim portovima osim za TCP[39] protokol na portu 80. U tabeli 3.1. prikazan je način odvijanja prometa.

Sa IP	Prema IP	Protokol	Iz. Port	Od. Port	Akcija
Any	Lokalna IP	Any	n/a	n/a	Blokiraj
Any	Lokalna IP	TCP	Any	80	Pusti

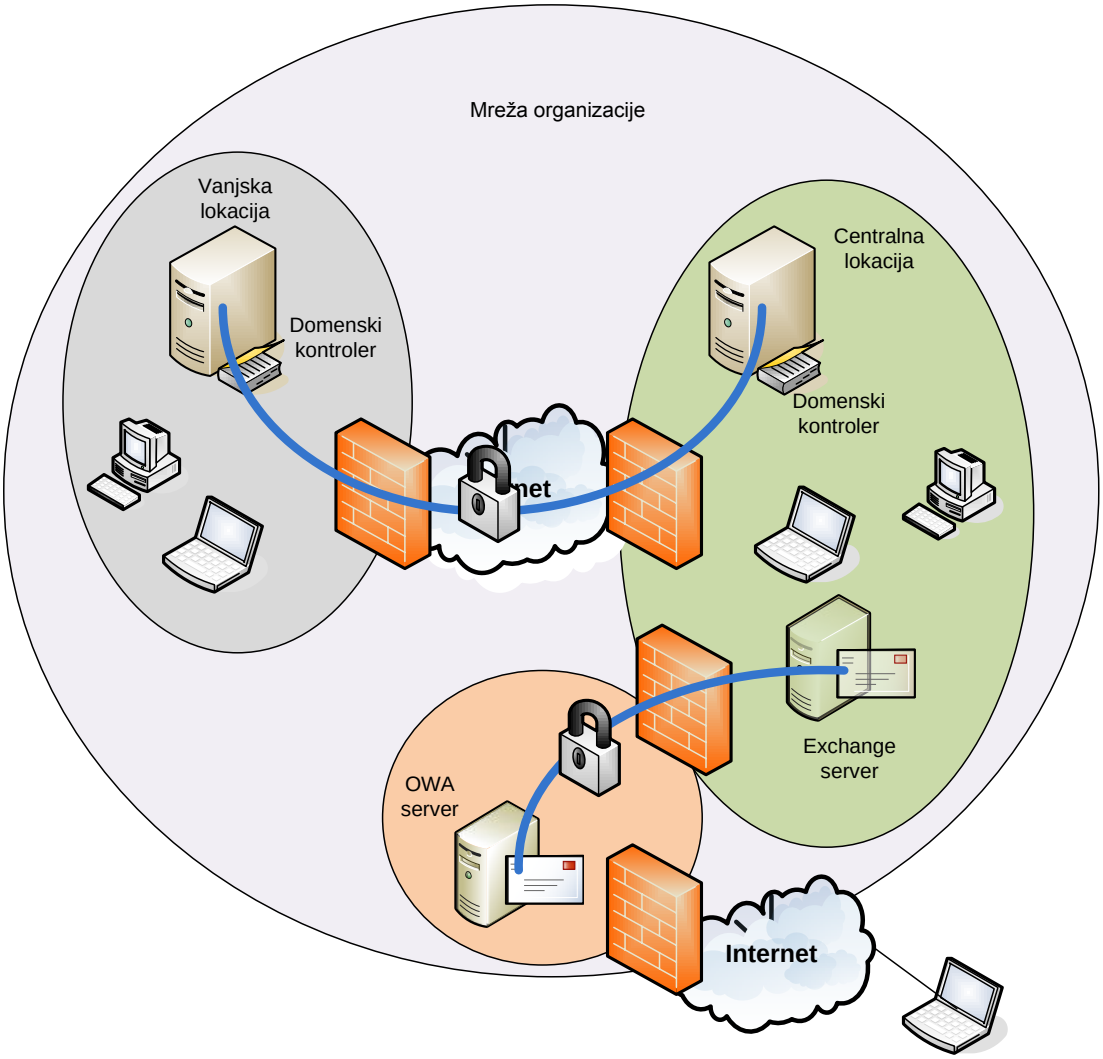
Tabela 3.1. Packet filetring (izvor: vlastiti rad)

3.2. IZOLACIJA SERVERA

Izolacija ili povećanje sigurnosti servera provodi se kroz autentifikaciju i kriptiranje prometa između željenih servera. Ovo rješenje može nadopuniti zaštitu koju provodimo s vatrozidom. Reduciraju se 'izuzeci' na vatrozidu i umjesto da otvaramo dodatne 'rupe' za sav željeni promet, otvorimo samo jednu za IPsec promet. Vatrozid radi na principu da pusti ili blokira paket. Izolacija servera pomoću IPseca će promet koji pusti i autentificirati.

Primjeri za ovaj scenarij su veza između frontend i backend Exchange servera,

[38] Engl. Demilitarized zone
[39] Engl Transmission Control Protocol



Slika 3.2. Izolacija servera (izvor: vlastiti rad)

kao i domenskih kontrolera među kojima se odvija replikacija a povezani su kroz Internet. Na slici 3.2. prikazani su ovi slučajevi i predstavljaju dobra rješenja za osiguravanje prometa između servera.

3.3. IZOLACIJA DOMENE I SERVERA

Kad se radi o izolaciji domene i servera postoje dva scenarija. Prvi je da se osigura siguran mrežni promet samo informatičkim resursima koji su članovi domene. Računala koja nisu u domeni ne mogu komunicirati s domenskim računalima. Drugi scenarij je da se reducira pristup kritičnim resursima unutar domene. Grupiranje računala u grupe odvija se prema zahtjevu o prometu koji želimo da se između računala odvija. Mogu se napraviti slijedeće grupe:

- Računala unutar izoliranog dijela mreže mogu inicirati komunikaciju sa svima računali unutar i izvan zaštićenih dijelova,
- Računala koja se ne nalaze unutar izolirane mreže mogu inicirati komunikaciju samo s računalima izvan izoliranog dijela.

Računala u izoliranom dijelu mreže ignoriraju zahtjeve za komunikacijom računala izvana. To može pomoći u zaštiti protiv zlonamjernog koda i korisnika izvana. Isto tako se smanjuje rizik od nekih napada s mreže kao što su skeniranje portova. Da bi ovakvo rješenje funkcioniralo potrebno je da na svakom resursu budu:

- Ispravni akreditivi – koristeći se tim akreditivima kod inicijalizacije komunikacije potvrđuje se identitet i autentificira se na drugom računalu,
- Mrežne postavke – postavke kojima se zahtjeva autentifikacija svih zahtjeva za komunikaciju, postavke za zaštitu komunikacije te kako provesti enkriptiranje.

Implementacija ovih zahtjeva na svakom pojedinom računalo nije jednostavna ni vremenski isplativa. U Windows okruženju uređivanje ovih postavki moguće je provesti s jednog mjesta. Sva računala koji se pridruže u Activ Directory tijekom prijave dobivaju određene akreditivi. Kroz Group Policy[40] dobiva ostale postavke u kojima se mogu definirati uvjeti uspostave komunikacije, autentifikacija, enkriptiranje prometa i sl. Koristeći prednosti koje proizlaze iz pripadnosti domeni (Group Policy) moguće je jednostavno izolirati željene resurse u zaštićeni logički dio mreže. Sve što je potrebno je provjeriti da li računalo pripada domeni i pravilno podesiti postavke u Group Policy gdje će se zahtijevati autentifikaciju za sav dolazni promet, zaštitu prometa te u nekim slučajevima i njegovu enkripciju.

Članovi domene mogu biti na mrežu organizacije spojeni na različite načine. Računala koja se ne nalaze u izoliranoj mreži uključuju 'stand-alone' računala i

[40] Centralna komponenta upravljačkog mehanizma Windows operacijskog sustava

računala koja ne podržavaju AD, UNIX[41], Linux[42], Apple[43]. Njihov pristup resursima u izoliranoj zoni omogućava se kroz ISA[44] server ili za to predviđeno računalo.

Dodatna zaštita koja se provodi izolacijom domene i servera smanjuje rizik od mnogih prijetnji i nadopunjava se na druge mrežne ili host orijentirane sigurnosne tehnologije, kao što je antivirusni , antispayware[45] produkti, IDS[46], vatrozidi. Za akreditaciju korisnika koristimo Kerberos ili certifikate (X.509[47]). Na ovaj način moguće je implementirati izolirane resurse domene s jednog mjesta bez potrebe intervencije na topologiji mreže, aktivnim komponentama mreže ili samim računalima.

3.3.1. IZOLACIJA DOMENE

Zaštita i izolacija domene provodi se u svrhu zaštite resursa. Kako se to provodi propisuje IEEE[48] standard 802.1X[49]. Svako se računalo identificira prije slanja paketa. Ovaj standard ne štiti promet nakon što se računalo identificira. SSL[50] osigurava autentifikaciju računala i tajnost podataka (enkripciju) za aplikacije koje mogu koristit ovaj protokol i klijenti kojim je omogućeno njegovo korištenje. Dok 802.1X radi na podatkovnom sloju OSI modela, SSL radi na aplikacijskom sloju što je relativno visoko u odnosu na mrežni sloj na kome se nalazi zaštita koja se ostvaruje IPsec-om

Da bi izolirali resurse domene koristimo se informacijom u AD o članovima domene i mrežnom politikom definiranu kroz postavke Group Policy u kojima zahtijevamo autentifikaciju i sigurnu komunikaciju drugih članova domene. Ovom politikom odvajamo članove domene od resursa koji ne pripadaju domeni. Inicijator komunikacije treba biti autentificiran kroz AD, član domene može inicirati promet prema resursima izvan izoliranog prometa. Prema potrebi može se definirati resursi

[41] Operativni sustav za računala
[42] Operativni sustav za računala
[43] Operativni sustav za računala
[44] Engl. Internet Security & Acceleration
[45] Alatkoji služi za uklanjanje svih spyware, keylogger, dialer i sličnih programa sa računala
[46] Engl. Intrusion Detection System
[47] Preporuka za digitalne certifikate
[48] Engl. Electrical and Electronic Engineers
[49] Standard za bežične mreže
[50] Engl. Secure Sockets Layer

koji ne pripadaju domeni a mogu inicirati nezaštićenu komunikaciju s nekim članovima domene.

Prednosti izolacije domene su slijedeći:

- Restrikcija dolazne komunikacije članova domene. Zahtjev za autentificiranje i zaštitu komunikacije smanjuje prijetnju od uređaja koji ne zadovoljavaju neke sigurnosne zahtjeve, nisu u nadležnosti organizacije te kao takvi mogu biti kompromitirani zlonamjernim programima kao što su virusi, crvi, spaywere[51]. Smanjuje se prijetnja i od DoS[52] napada jer računala koja ne posjeduju određene akreditive ne mogu uspostaviti komunikaciju,
- Nadopunjuje druge sigurnosne zaštitne mehanizme te štiti resurse u slučaju kompromitiranja resursa za zaštitu. Kompromitiranjem vatrozida neće biti moguće direktno pristupiti resursima domene,
- Pridruživanjem resursa domeni, dobiju se određeni akreditivi uz to da se zadovolje određeni uvjeti (određeni operacijski sustav, antivirusni program, zakrpe). Ovakvom proaktivnom mjerom povećava se sigurnost sustava i smanjuje rizik od napada,
- Osiguravanjem prometa među članovima domene umanjuje se mogućnost da paketi budu mijenjani i zna se od koga su paketi poslani. Dodatno se promet može enkriptirati čime se onemogućava zlonamjernom korisniku da dođe do sadržaja prometa.

3.3.1.1. Proces komunikacije

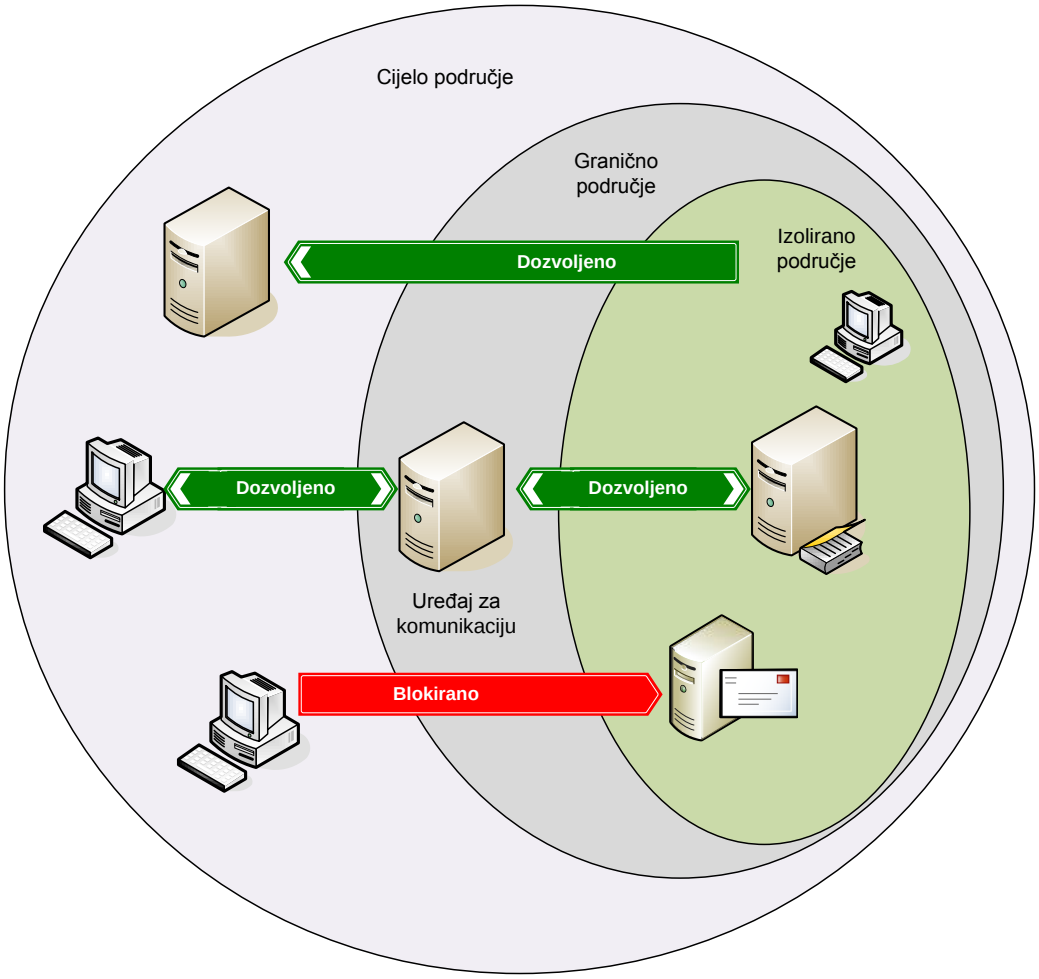
Na slici 3.3. prikazano ja kako se uspostavlja komunikacija izoliranog servera s okolinom. Postoje slijedeći slučajevi:

- Član domene inicira i ostvaruje komunikaciju s izoliranim serverom,
- Izolirano računalo inicira i ostvaruje komunikaciju s računalom u graničnom području a ono s članom domene,

[51] Široka kategorija malicioznog softwarea sa namjenom da presreće ili preuzima djelimično kontrolu rada na računalu bez znanja ili dozvole

[52] Engl. Denail-of-Service

- Svi ostali zahtjevi za komunikaciju se odbijaju.



Slika 3.3. Komunikacija u izoliranoj domeni (izvor: vlastiti rad)

3.3.2. IZOLACIJA SERVERA

Da bi zaštitili važan resurs, u ovom slučaju server, konfigurira se mrežna politika kroz Group Policy postavke u kojima zahtijevamo autentifikaciju i sigurnu komunikaciju između servera i određenih članova domene.

Standardan način kako se štite osjetljivi podaci na serveru je kroz prava pristupa na aplikacijskom sloju. Prije nego korisnik pristupi podatku potrebno je predočiti identifikacijske podatke koji kroz aplikacijski sloj (korištenjem ACLs[53]) omogućavaju korisniku pristup. Na ovaj način nije provedena zaštita od DoS napada, virusa ili crva pokrenutih s računala koji nisu članovi domene na lokalnoj mreži.

[53] Engl. Access Control Lists

Da dodamo još jedan sloj zaštite tako da ga izoliramo od računala koji nemaju prava pristupa (bili oni članovi domene ili ne) definiramo politiku koju implementiramo kroz Group Policy i primijenimo je na grupe u kojima se nalaze željeni resursi. Koristeći IPsec u izolaciji onemogućavamo ostvarivanje IP komunikacije bez zadovoljenja prije definiranih uvjeta. Izolacija servera osigurava slijedeće prednosti:

- Restrikcija dolaznih komunikacija koja se ograničava na članove domene,
- Dodatak drugim sigurnosnim mehanizmima u sprječavanju neželjenih komunikacija,
- Uvjetovanje članstvom u domeni za normalnu komunikaciju,
- Zaštita prometa s i od izoliranog servera,
- Zaštita aplikacija koje nemaju ugrađen sigurnosni mehanizam.

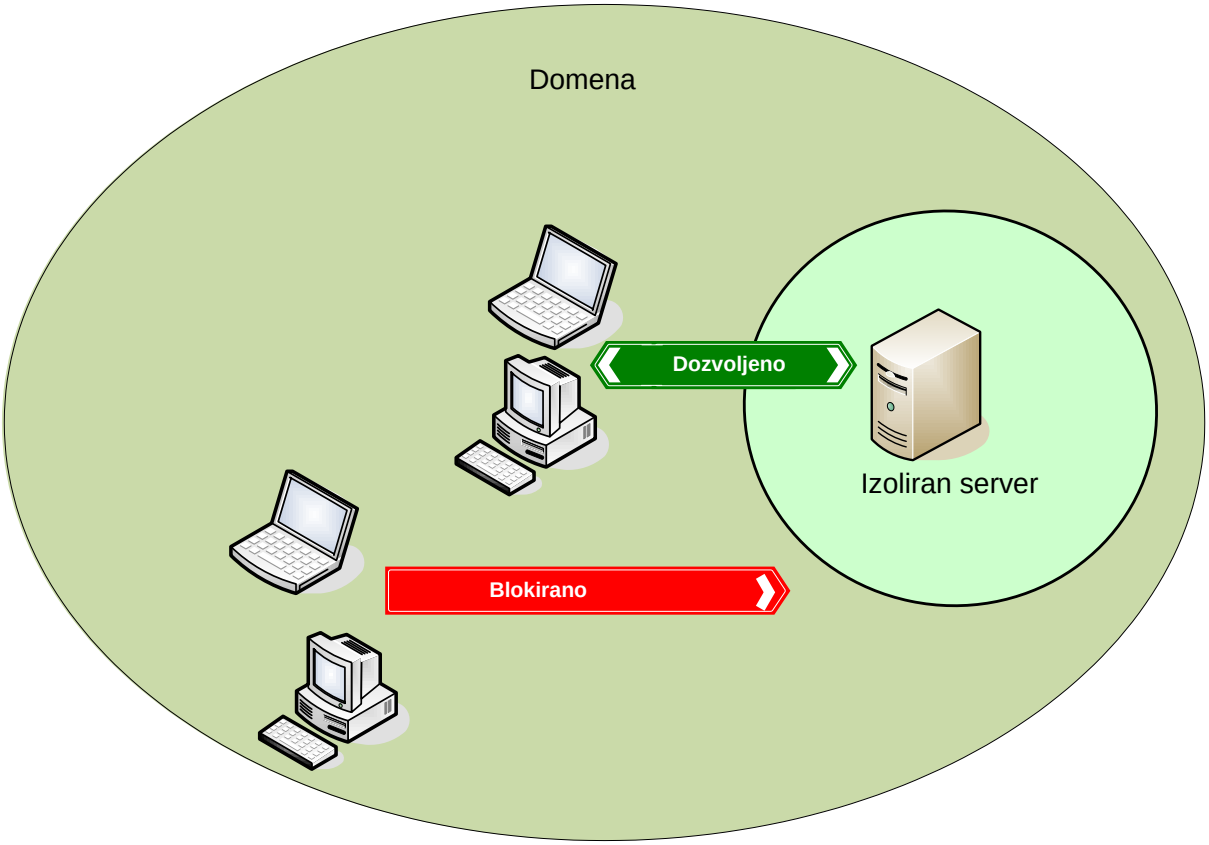
IPsec štiti promet od spoffing adresa[54], izmjena ili dodavanja podataka, krađe sesija i drugih napadima (replay attacks[55]). Osim postavki koje definiraju uvijete sigurne komunikacije mogu se definirati uvjeti kad se može ostvariti komunikaciju s računalima koji nisu članovi domene.

3.3.2.1. Proces komunikacije

Na slici 3.4. prikazano ja kako se uspostavlja komunikacija izoliranog servera s okolinom. Postoje slijedeći slučajevi:

- Član domene inicira i ostvaruje komunikaciju s izoliranim serverom,
- Izolirani server inicira i ostvaruje komunikaciju s računalom izvan domene,
- Svi ostali zahtjevi za komunikaciju se odbijaju.

[54] Krivotvorenje adrese
[55] Napad ponavljanjem inicijalizacijskog vektora



Slika 3.4. Komunikacija izoliranog servera (izvor: vlastiti rad)

Ukratko opisane konfiguracije mogu poslužiti u razumijevanju mogućnosti kako povećati sigurnost informacijskog sustava. Uz ovo potrebno je znati što sve donosi implementacija IPseca na mrežu, na što se mora paziti i kako pristupiti implementaciji. O svemu tome će biti više riječi u slijedećim poglavljima.

3.4. PREPORUKE ZA PROVOĐENJE IZOLACIJE DOMENE SA SIGURNOSNOG STANOVNIŠTVA

Cilj izolacije je izolirati opremu kojoj se vjeruje od one kojoj se ne vjeruje da bi se postigao dodatan nivo zaštite prometa na mreži. Koraci koji se predlažu pri provođenju izolacije upotrebom IPsec-a su slijedeći:

1. Odrediti trenutno stanje IT infrastrukture,
2. Odrediti grupe koje će se izolirati,
3. Razmotriti funkcionalnost kao posljedica IPsec prometa.

3.4.1. ODREĐIVANJE TRENUTNOG STANJA IT INFRASTRUKTURE

Prije početka planiranja izolacija potrebno je sakupiti i analizirati informacije o stanju IT infrastrukture, i to:

1. Mrežni segment,
2. Active Directory[56],
3. Konfiguracija klijenata.

3.4.1.1. Mrežni segment

Informacija koje su potrebne odnose se na izgled mreže, od kojih se segmenata sastoji i koje se komponente nalaze u pojedinim segmentima. U procjeni treba proći kroz sve mrežne uređaje, routere, switche-ve, vatrozide. Kroz ove uređaje prolazi IPsec promet tako da treba biti siguran da su sposobni ovaj promet obraditi tehnički i fizički.

Mrežna komunikacija

Analizirati promet po mreži u cilju dobivanja informacija:

- Koja komunikacija se odvija između grupe kojoj se vjeruje i grupi kojoj se ne vjeruje,
- Koja komunikacija bi mogla imati problema kad se implementira IPsec.

Kod analize tokova prometa treba voditi računa o slijedećem:

- Kako komuniciraju serveri i klijenti,
- Da li se planira ili implementira uređaj ili sustav koji bi mogli utjecati na izolirane grupe,
- Da li se koristi certifikat za proces autentifikacije,
- Da li postoji neki segment mreže s predefiniranim tipom prometa.

Struktura Active Directory

Druga važna komponenta u procjeni rizika i mogućnosti implementacije IPseca je Active Directory. Potrebno je doći do slijedećih informacija:

[56] Integracijska je točka za spajanje sustava, osiguranje mrežnih resursa i korisnika te konsolidiranje upravljačkih zadataka. Omogućuje učinkovito dijeljenje i upravljanje informacijama o mrežnim resursima i korisnicima

- Broj foresta[57],
- Broj i imena domena,
- Vrsta i broj uspostavljenih povjerenja,
- Imena i broj lokacija,
- OU[58] i Group Policy,
- Postojeća IPsec politika.

Konfiguracija klijenata

Zadnji skup informacija za mrežnu infrastrukturu su konfiguracije klijenata i servera. IPsec komunikacija ovisi o verzijama OS koja je implementirana na klijentima, tako da je s klijenata potrebno sakupiti slijedeće informacije:

- Operacijski sustav, SP, hotfix[59],
- Pripadnost domeni,
- Fizička lokacija,
- Hardver i pripadnost izolacijskim grupama.

3.5. PLANIRANJE IZOLACIJE DOMENE

Ako se dobro poznaje mrežna infrastruktura i konfiguracija klijenata može se krenuti s planiranjem izolacije. Dozvoliti ili blokirati komunikacije među klijentima odluka je koja se donosi na osnovu informacije o pouzdanosti ili povjerenja. Povjerenje klijenata zasniva se na informaciji o njegovom stanju o virusima, zakrpama i politici lozinki.

3.5.1. STANJA POVJERENJA

Povjerenje se definirana na slijedeći način:

Pouzdan – za klijenta koji zadovolji slijedeće kriterije:

- Operacijski sustav sposoban za IPsec komunikaciju (2k3[60], XP, 2k0[61] SP4),

[57] Šuma
[58] Engl. Organization Units, organizacijske jedinice
[59] Izmjena nakon zadnje verzije
[60] Operacijski sustav, Windows 2003 Server
[61] Opraciski sustav, Windows 2000 Server

- Pripadnost domeni (klijet mora pripadat domeni da bi mogao biti konfiguriran kroz GPO[62]).

Nepouzdan – za klijenta koji ne može zadovoljiti kriterije za pouzdanost i uključuje:

- 2k0, SP3,
- Nema windows OS,
- Ne pripada domeni,
- VPN[63] klijent.

3.5.2. ODREĐIVANJE IZOLACIJSKIH GRUPA

Kreiranje izolacijskih grupa temelji se na klijentima koji imaju isti ili sličan dolazni i odlazni mrežni promet. Grupe se osnivaju s ciljem restrikcije mrežnog prometa između pouzdanih i nepouzdanih klijenata. U Windows okruženju, izolacijske grupe se implementiraju kroz sigurnosne grupe Group Policy-a a izolacija grupa se provodi restrikcijom pristupnih prava kroz dozvolu/blokiranje mrežnog prometa pomoću IPsec-a. Neke standardne grupe koje se obično kreiraju su:

- Izolirana domena – najviše članova u kojoj su svi članovi pouzdani, pripadaju domeni. Sva komunikacija među njima je osigurana IPsec-om,
- Nepouzdan sustav – ova grupa sadrži klijente koji nisu sposobni komunicirati IPsec-om,
- Granična grupa – ova grupa je pouzdana ali joj je zadatak da komunicira s nepouzdanom grupom. Izložena visokom riziku,
- Grupa izuzetaka – sadrži klijente koji ne mogu biti osigurani IPsec-om ali su neophodni za funkcioniranje sustava, kao što su domenski kontroleri[64], DNS[65], WINS[66], DHCP[67].

[62] Engl. Group Policy Objects
[63] Engl. Virtual Private Network
[64] Serveri gdje se nalazi baza podataka o resursima domene
[65] Engl. Domain Name System
[66] Engl. Windows Internet Name Service
[67] Engl. Dynamic Host Configuration Protocol

3.6. RAZMOTRITI FUNKCIONALNOST KAO POSLJEDICU IPSEC PROMETA

IPsec povećava razinu sigurnosti no ima utjecaj na mrežni promet, karakteristike sustava kao što utječe na razne servise i alate.

3.6.1. UTJECAJ NA KARAKTERISTIKE MREŽE

IPsec troši određene resurse i procesnu snagu uređaja. Koliko je ona nije jednostavno odrediti jer ovisi o mnogo faktora, kao što je veličina prometa aplikacija, broj definiranih filtara. Slijedeće faktore treba uzeti u obzir:

- Karakteristike mreže - uspostava IKE[68] SA[69] usporava ostvarivanje konekcije i dolazi do kašnjenja. Vrijeme može varirati ali treba proći nekoliko sekundi da se izvrši ova faza. Nakon završetka dogovaranja parametara nema više kašnjenja u komunikaciji,
- Redundancija zbog ispuna - zbog dodatnih zaglavlja i ispuna korisnih podataka prije kriptiranja povećava se količina prometa po mreži te treba optimirani mrežne komponente prema očekivanom povećanju,
- Karakteristike procesora - zbog dodatnog poslova oko uspostavljanja konekcija te kreiranja dodatnih zaglavlja (AH[70] i ESP[71] protokoli) dolazi do dodatnih opterećenja procesora i memorije. Način autentifikacije također opterećuje sustav tako da autentifikacije certifikatom zahtjeva puno više memorije nego autentifikacija kroz Kerberos V5[72].

3.6.2. PROBLEMI S UREĐAJIMA NA GRANICAMA MREŽNIH SEGMENATA

Kod implementacije IPseca treba voditi računa o mrežnim uređajima koje koristimo za NAT[73]. Osim toga kroz vatrozid-ove treba dozvoliti ISAKMP[74], AH i ESP promet.

Kod autentifikacije treba paziti da različiti položaj klijenata zahtjeva i različiti način prijave. Vanjski korisnici moraju koristiti FQDN[75] domene za prijavu kroz Kerberos.

---

[68] Engl. Internet Key Exchange
[69] Engl. Security Association
[70] Engl. Authentication Header, sigurnosni protokol
[71] Engl. Encapsulating Security Payload, sigurnosni protokol
[72] Sustav za autentifikaciju, verzija 5
[73] Engl. Network Address Translation
[74] Engl. Internet Security Association and Key Management Protocol

3.6.3. FUNKCIONALNOST SUSTAVA

U sustavu koji funkcionira postoje mnogi uređaji koji nemaju mogućnosti komunikacije s IPsec-om. Takvi uređaji smatraju se nepouzdani i neće moći pristupit nekim resursima. Poslovni procesi možda zahtijevaju da i takvi uređaji imaju pristup do podataka koji se nalaze u izoliranim grupama. Za takve uređaje potrebno je osigurati pristup preko uređaja u grupi koji imaju pristup do željenih grupa.

3.6.4. ALATI ZA NADZOR MREŽE

Mnoge aplikacije za kontroli i nadzor mreže koriste informacije iz TCP/IP zaglavlja za analizu prometa. IPsec onemogućava pristup do tih informacija pa je potrebno voditi o tome računa kod planiranja da se nabave dodaci koji će omogućiti funkcionalnost uređaja.

Kad se zna na koji način IPsec može pomoći u izolaciji resursa u informacijskom sustavu, na što se mora paziti kod implementacije i kako se implementaciji treba pristupiti, ostaje još samo da se prikaže procedura podešavanja IPseca. Bez obzira da li se podešava na lokalnom resursu ili u kroz GPO koristi se grafička konzola. U nastavku je ukratko pokazano kako se provodi podešavanja IPsec-a. Uzet je primjer osiguranja promet prema bazi podataka.

3.7. KONFIGURIRANJE IPSEC

Konfiguriranje parametara IPsec-a u Windows implementacije provodi se kroz grafičku konzolu IPsec MMC[76] (dostupnu na verzijama Microsoft Windows XP i Microsoft Windows Server 2003, SP4). Kojim redom se podešavaju opcije i kako izgleda struktura IPsec prikazano je u nastavku, no prije toga su objašnjeni neki pojmovi, tabela 3.2.

Komponenta		Opis
Policy-wide	Opći podaci	Definira interval za provjeru eventualnih

[75] Engl. Fully Qualified Domain Name
[76] Engl. Microsoft Management Console

parameters			promjena u sigurnosnim postavkama
ISAKMP policy	ISAKMP postavke		Sadrži IKE[77] parametre, kao što je vrijeme trajanja ključa za kriptiranje i druge postavke. Također sadrži i listu sigurnosnih metoda zaštite identiteta za vrijeme autentifikacije IPsec para.
IPsec rule	IPsec pravila		Ova pravila definiraju određene akcije vezane uz listu filtra, metodu autentifikacije, IPsec mod i druge postavke. Tipično, IPsec pravilo se definira za specijalnu namjeru (na primjer, blokiraj sav dolazni promet s Interneta na TCP port 135). Mogu se definirati različita pravila u jednom IPsec policy-u. (Rules izbornik). IPsec pravila spaja IKE parametara za dogovaranje s jednim ili više IP filtra.
Filter List		Lista filtra	Filtar liste sadrže jednu ili više predefiniranih filtra kojima je opisan tip prometa te akciju koja će se na njega primijeniti ('permit', 'block' ili 'secure').
Filter Action		Akcija filtra	Akcije mogu biti definirane kao dozvola (permit) prometu, zabrana (block) prometa ili zahtjev za osiguranje sigurnog prometa (secure). Ako želimo da nam promet bude siguran potrebno je odrediti sigurnosne metode kao i njihov redoslijed. Pod ovime se misli da li će zahtjevi za komunikaciju koji nisu sigurni biti prihvaćeni, da li

[77] Engl. Internet Key Exchange

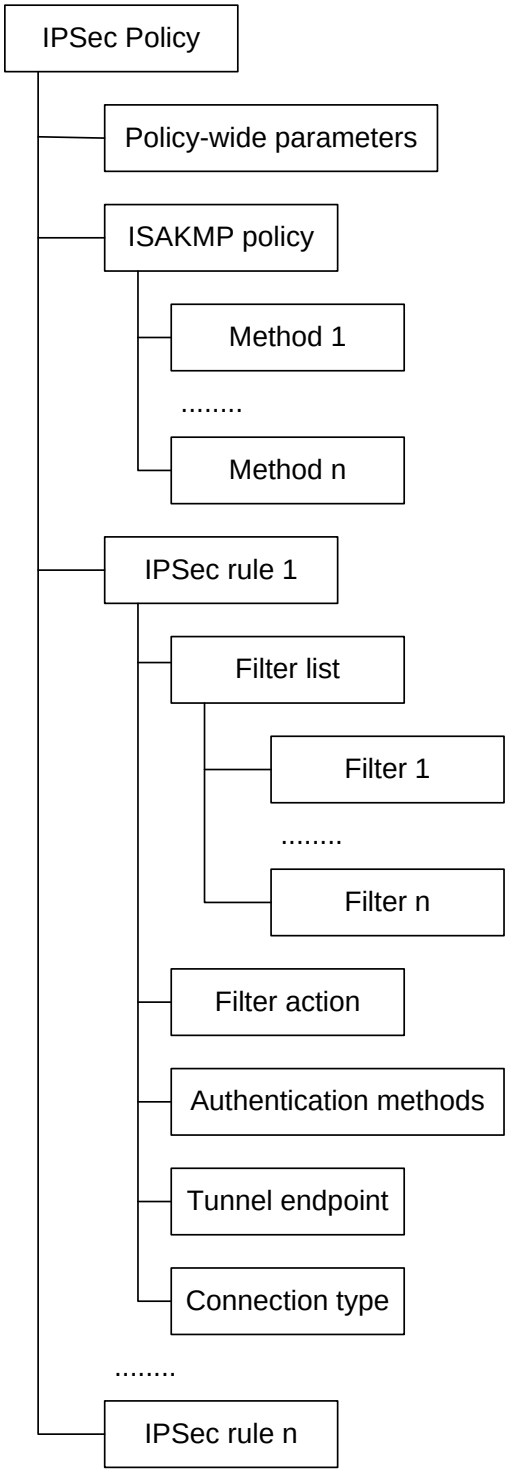
			će komunikacija s računalom koje ne podržava IPsec biti moguća i da li će biti korišten PFS[78]. PFS je mehanizam kojim se određuje da li se iz postojećeg materijal za ključ napraviti novi sesijski ključ ili će se pokrenuti novi Diffie-Hellman algoritam za izmjenu ključeva iz kojega će biti napravljen novi ključ za sesiju.
Authentication methods		Identifikacijska metoda	Postoji nekoliko metoda autentifikacije koje se koriste za zaštitu tijekom IKE dogovaranja. Dostupne metode su KerberosV5 protokol, certifikat i predefinirani ključ.
Tunnel endpoint		Drugi kraj tunela	Postavka definira potrebu da promet bude tuneliran i tko se nalazi na drugom kraju. Potrebno je definirati dva pravila za ovakvu komunikaciju. Prvo, za odlazni promet, završna točka je IP adresa ili dio mreže para na drugom kraju tunela. Drugo, za dolazni promet, završna točka je IP adresa lokalnog računala.
Connection type		Tip konekcije	Ovom opcijom određujemo da li će se pravilo primjenjivati na LAN konekciju, dial-up ili na oba tipa.

Tabela 3.2.Značenje pojedinih pojmova (izvor: vlastiti rad)

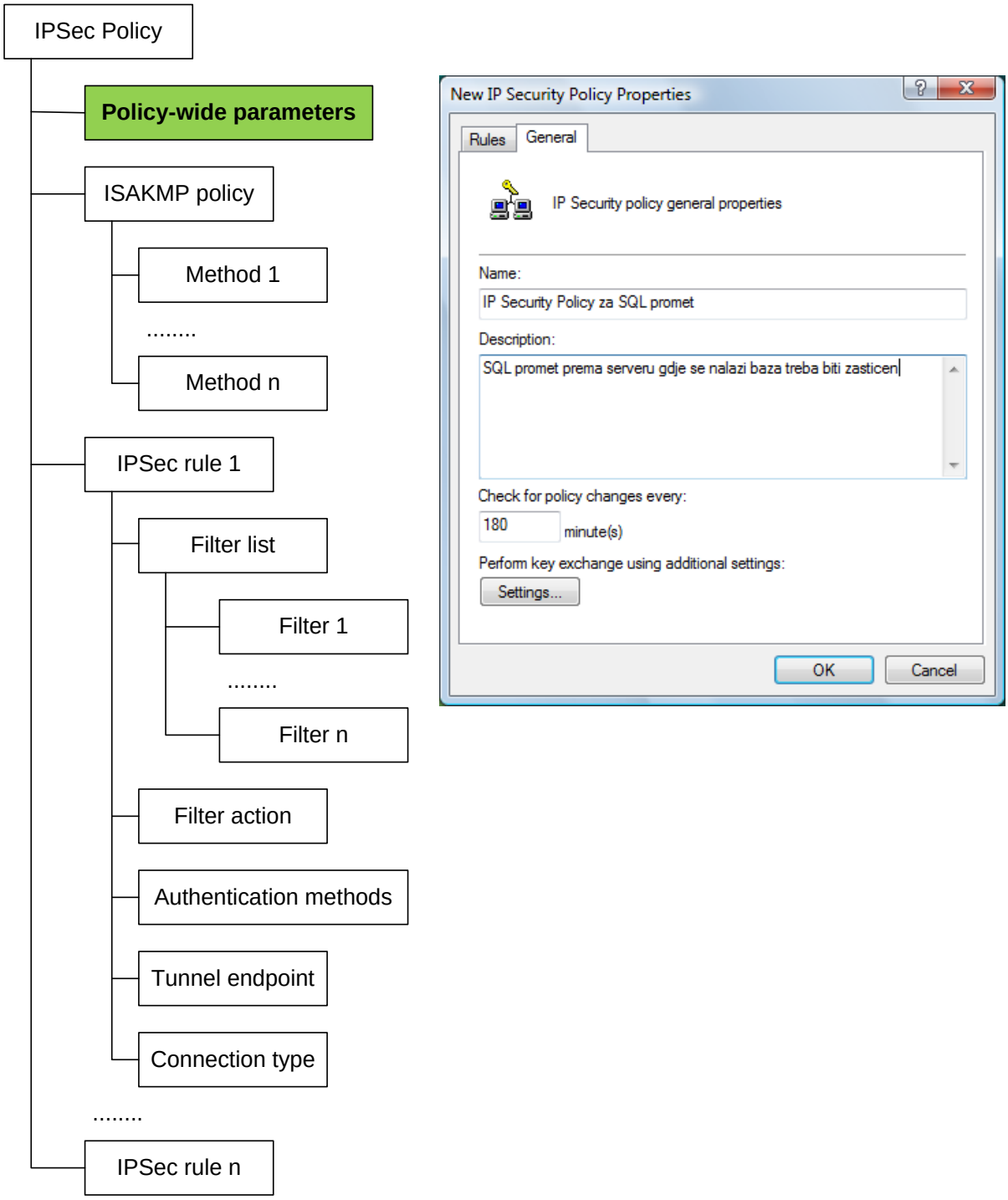
Na slici 3.5. Prikazana je IPsec struktura postavki. Sastavljena je od općih parametara i jednog ili više IPsec pravila. U općim podacima se nalazi ime koje smo dali i kako često će biti provjeravane promjene parametara. ISAKMP[79] postavke definiraju detalje metode dogovaranja koje će biti korištene u 'main' modu. Zatim

[78] Engl. Perfect Forward Secrecy
[79] Engl. Internet Security Association and Key Management Protocol

slijede pravila, koja sadrže liste jednog ili više filtra, akcije filtra i metodu autentifikacije. Osim toga tu je opcija za korištenje tunel moda i tip konekcije.

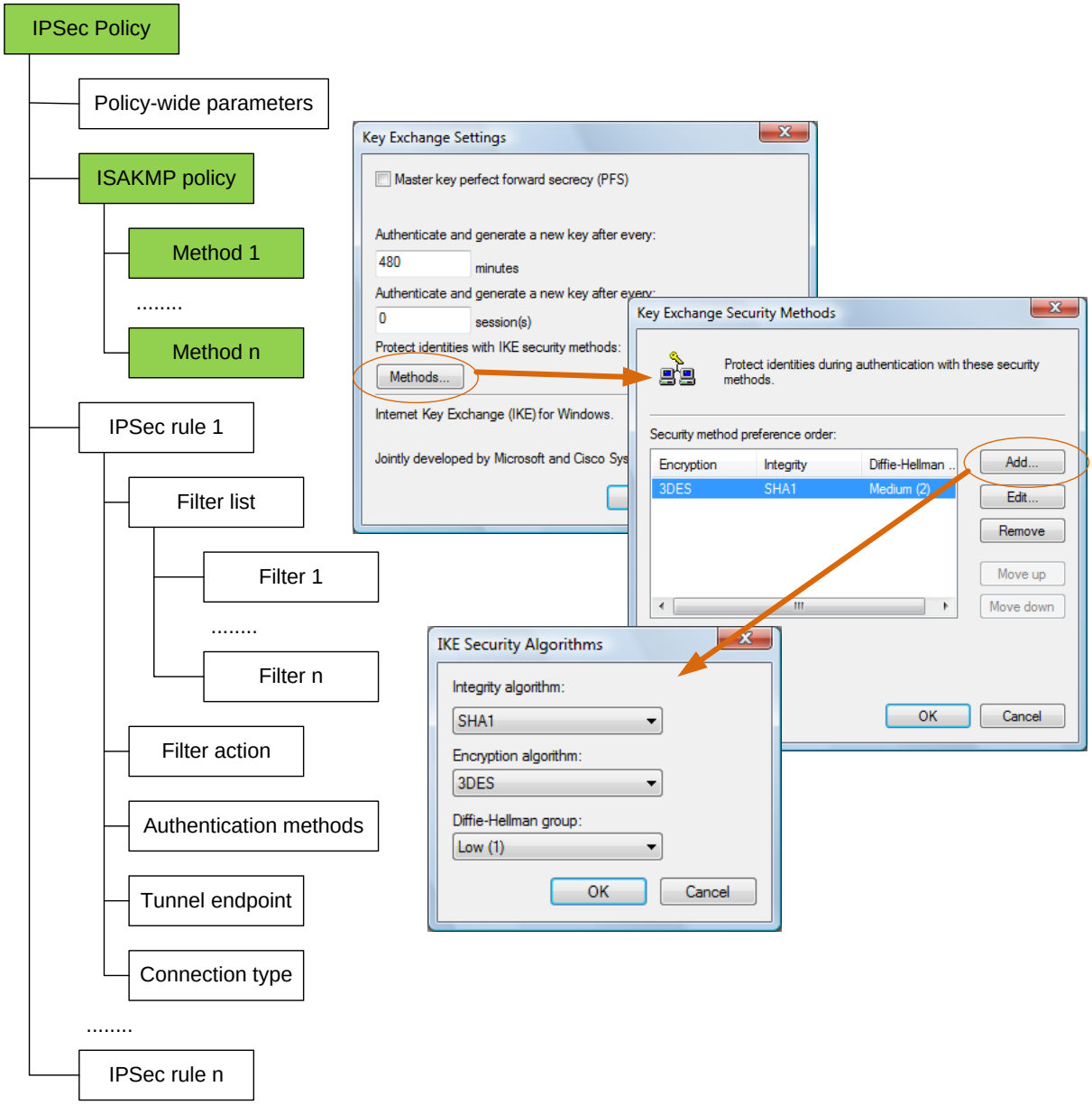


Slika 3.5. Struktura IPsec postavki (izvor: vlastiti rad)



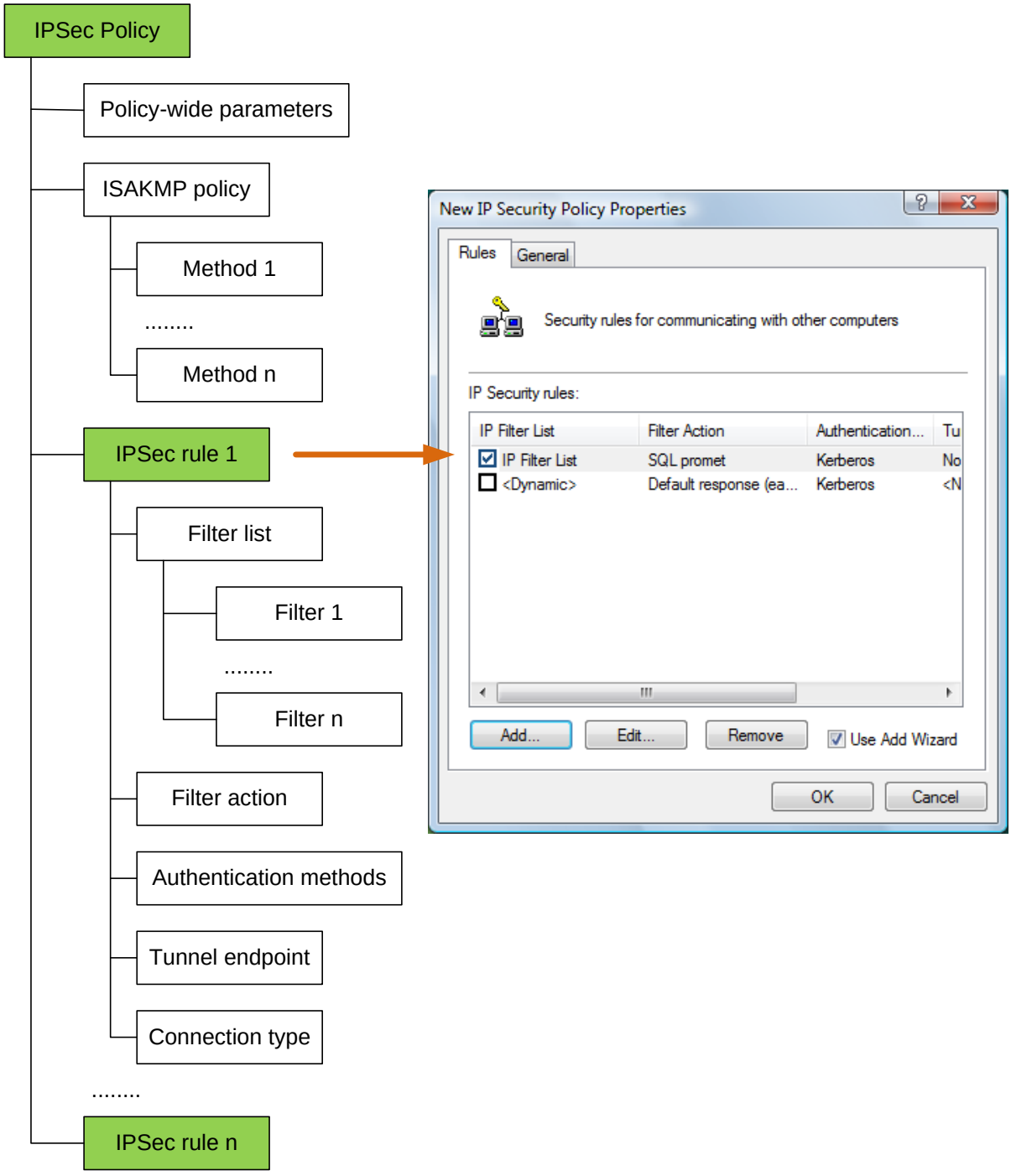
Slika 3.6. Početni ekran (izvor: vlastiti rad)

Nakon što se pokrene grafička konzolu dobijemo početni ekran, slika 3.6. Na njemu definiramo ime koje će postavke imati te objašnjenje za koju je namjenu kreirano. Osim toga ovdje se definira i vrijeme za koje će se provjeravati eventualna promjena u postavkama.



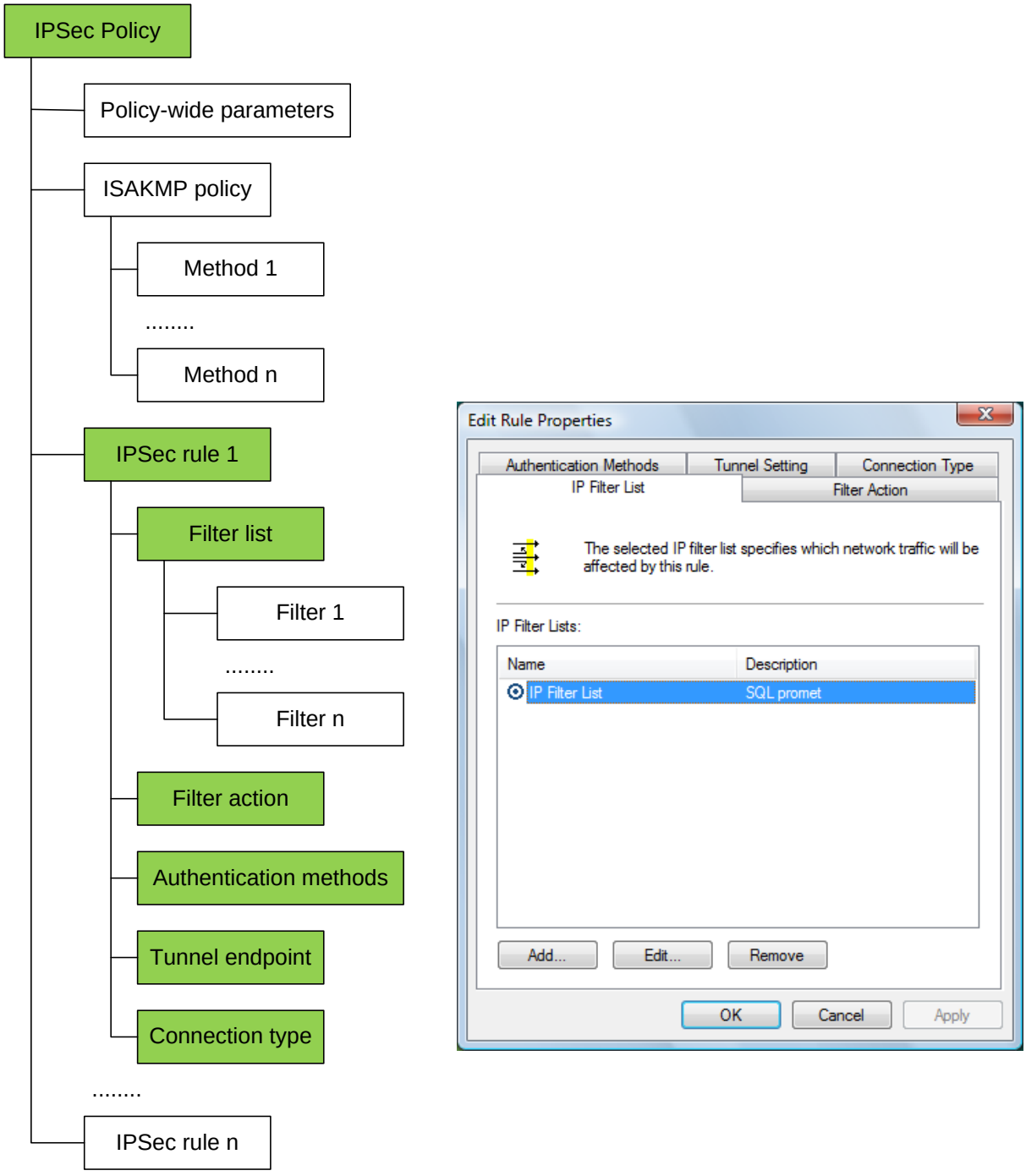
Slika 3.7. Definiranje sigurnosnog protokola (izvor: vlastiti rad)

Nakon upisa imena i opisa, selektiramo opciju 'Settings' koja omogućava definiranje sigurnosnog protokola koji će se koristit u komunikaciji, algoritam za integritet podataka te dužinu ključa koja će biti u 'Diffie-Hellman' algoritmu, slika 3.7.



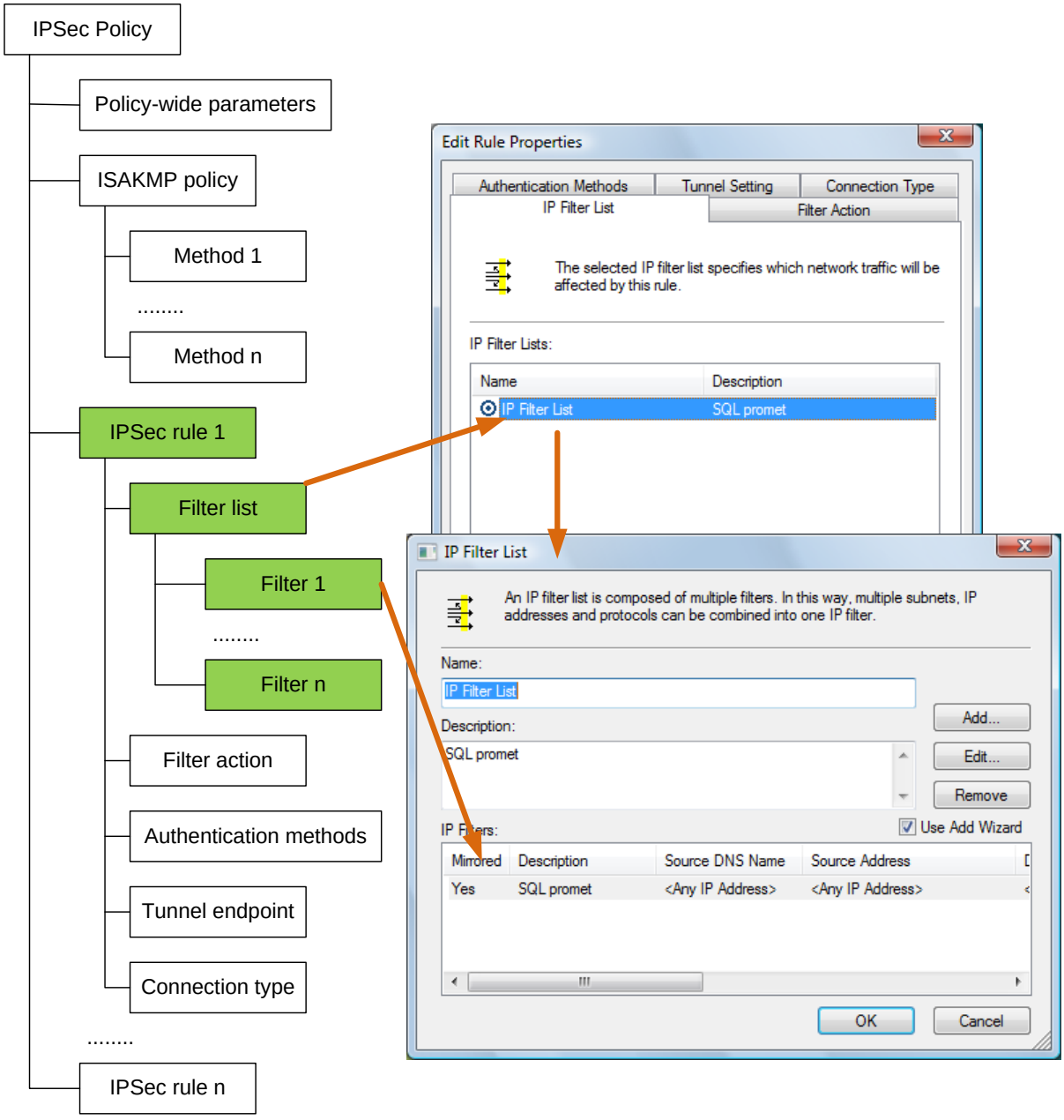
Slika 3.8. Definiranje pravila (izvor: vlastiti rad)

Kroz definiranje pravila, slika 3.8., određuje se koji promet će biti blokiran, koji propušten a za koji želimo da bude osiguran.



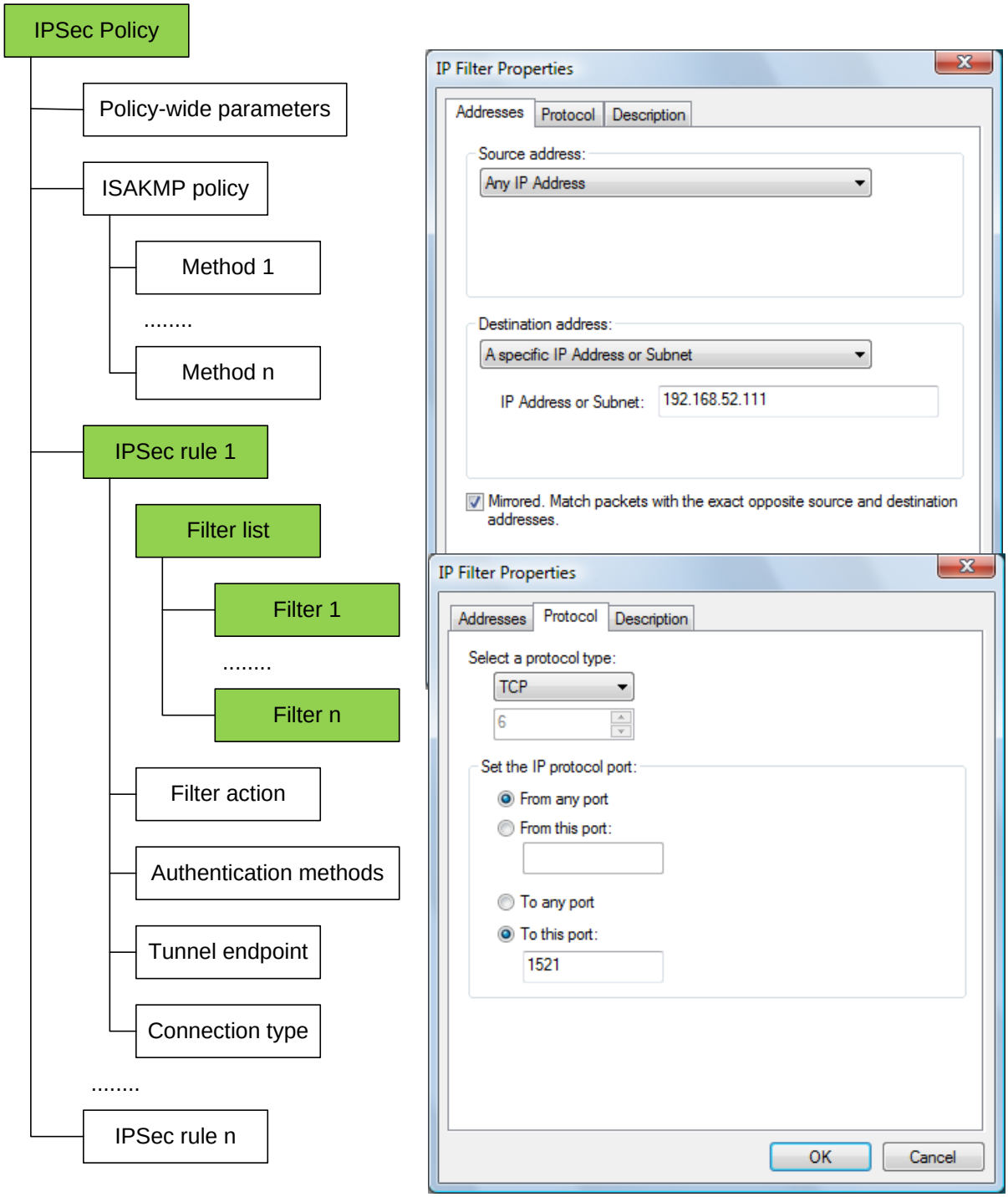
Slika 3.9. Lista filtra (izvor: vlastiti rad)

Na slici 3.9. prikazan je ekran kroz koji definiramo više parametara, kao što su akcije koje će biti poduzete, metoda autentifikacije, da li će biti korišten tunel mod između para koji komunicira kao i tip konekcije.



Slika 3.10. Definiranje liste fitera (izvor: vlastiti rad)

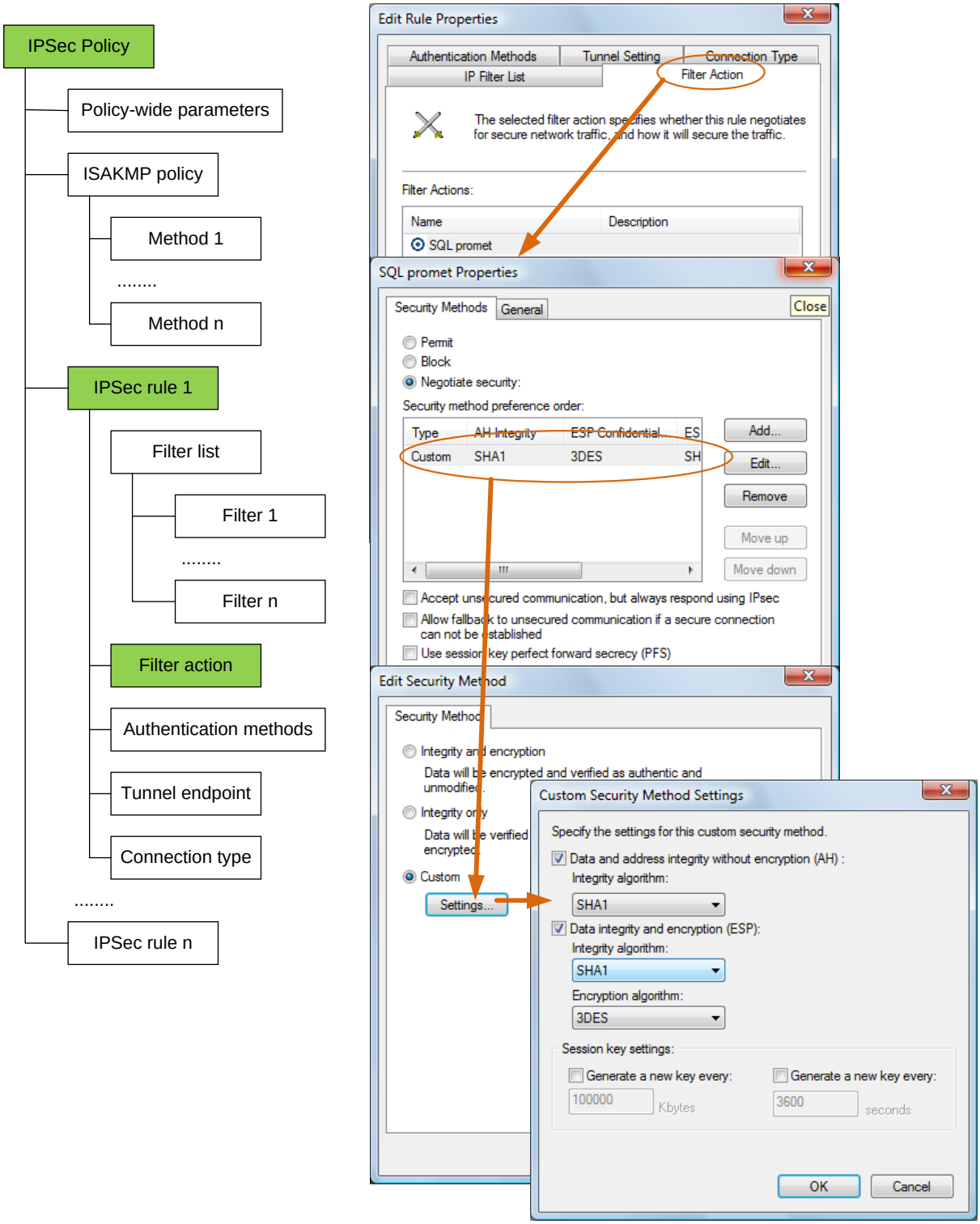
Na slici 3.10. prikazan je početak definiranje filtra. Nakon što se definira ime i opis potrebno je definirati parametre koji opisuju mrežni promet.



Slika 3.11. Definiranje filtra (izvor: vlastiti rad)

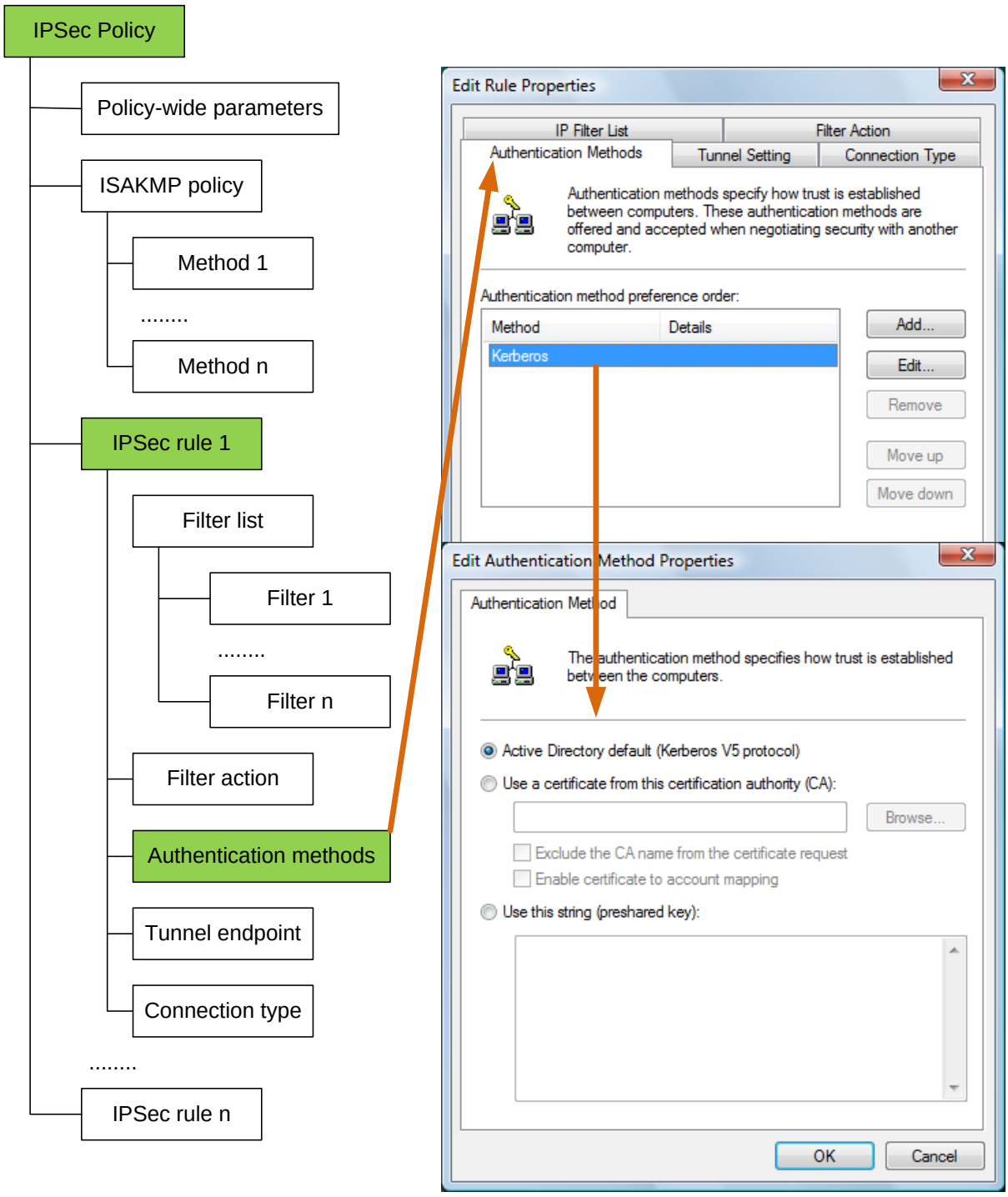
Na slici 3.11. prikazano je definiranje filtra za koji promet može biti iniciran s bilo kojeg klijenta i porta. Odredište mu je TCP port 1521 (port na kojem sluša Oracle[80] baza podataka)

[80] Oracle je ime za Oracle Corporation poduzeće koje sa bavi bazama podataka



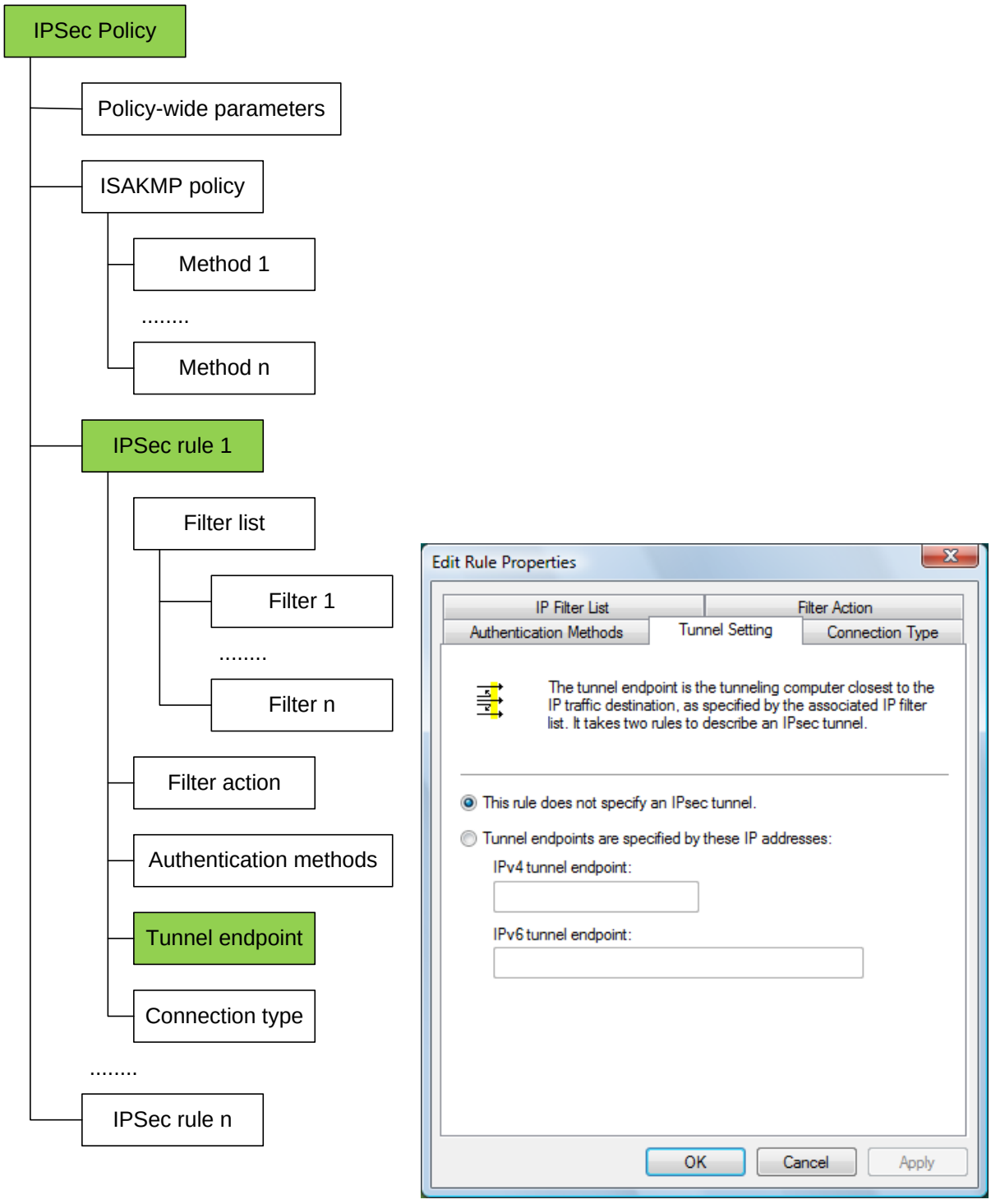
Slika 3.12. Određivanje akcije fitera (izvor: vlastiti rad)

Za definirani promet kroz filtar potrebno je odrediti kako će taj promet biti obrađen, slika 3.12. U ovo slučaju ne prihvaća se nekriptirani promet i određuju se sigurnosni parametri za siguran promet.



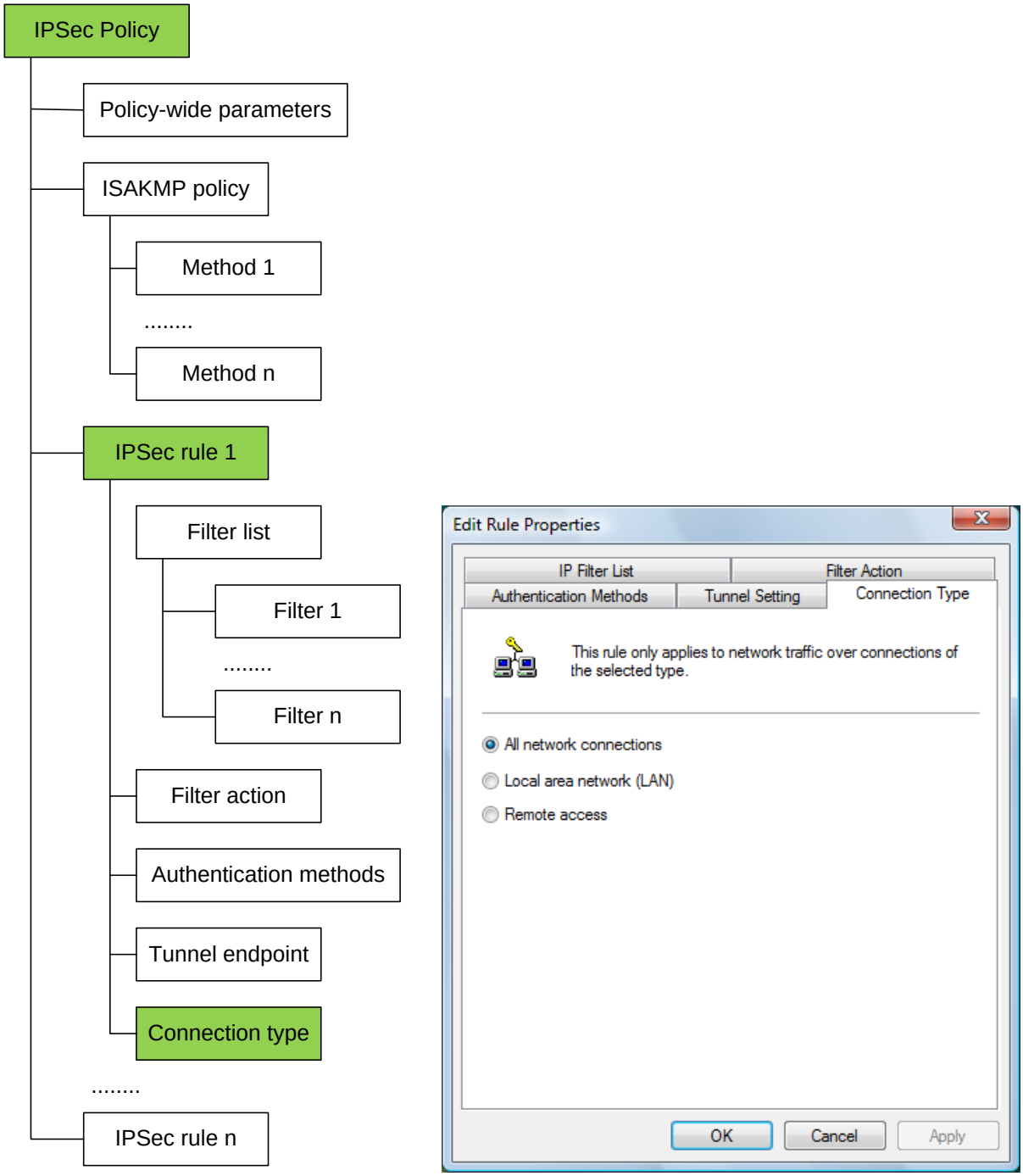
Slika 3.13. Metoda autentifikacije (izvor: vlastiti rad)

Na koji način se može izvršiti autentifikacija prikazano je na slici 3.14., gdje je definirano da će se iskoristiti Kerberos.



Slika 3.14. Tunel mod (izvor: vlastiti rad)

Ako je potrebno da se komunikacija odvija u tunel modu u ovom ekranu se definiraju parametri, slika 3.14.

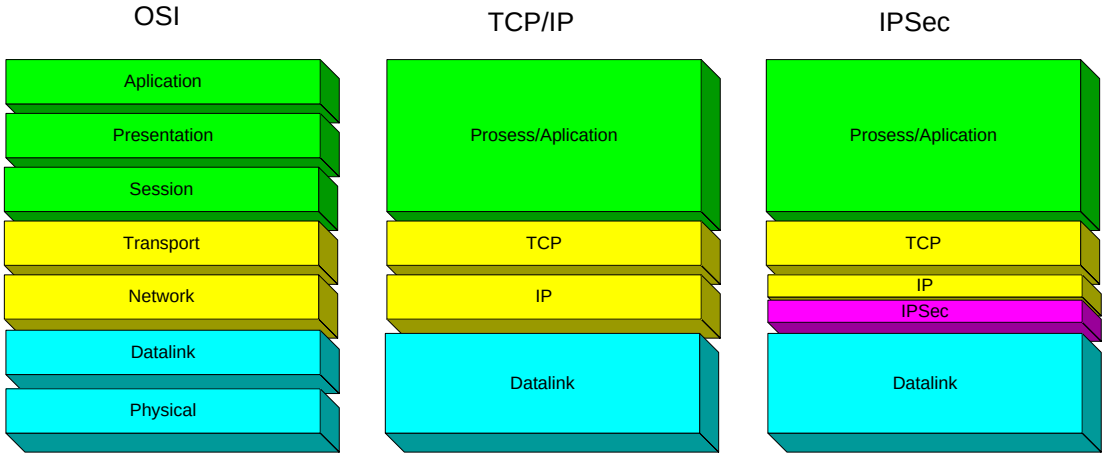


Slika 3.15. Tip konekcije (izvor: vlastiti rad)

Za koji tip konekcije će biti primijenjena ova politika definiramo na ekranu prikazanom na slici 3.15.

4. OSNOVE IPSEC-A

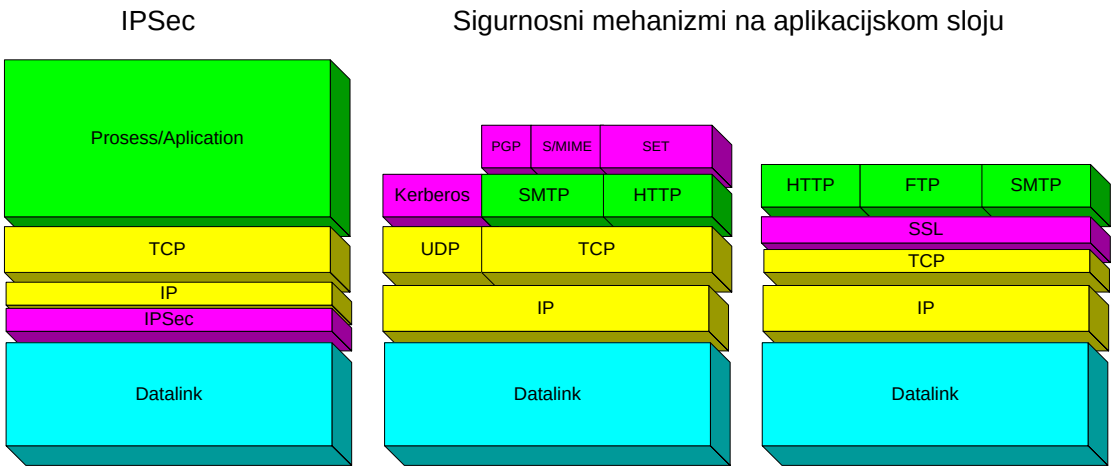
Jedan od osnovnih nedostataka TCP/IP stoga protokola u svom izvornom obliku jest nepostojanje nikakvih mehanizama kojima bi se osigurala zaštita i integritet podataka u prijenosu te izvršila autentifikacija strana u komunikaciji [7],[8]. IP protokol je proširen s IPsec-om. IPsec implementira sigurnu mrežnu komunikaciju na trećem, odnosno mrežnom sloju (engl. *Network layer)* ISO OSI[81] stoga protokola, tj. u internet sloju, ukoliko se promatra TCP/IP stog, slika 4.1.



Slika 4.1. OSI, TCP/IP stog i smještaj IPsec-a (izvor: vlastiti rad)

Naravno, sigurnost je moguće implementirati i u drugim slojevima, slika 4.2. Postoji čitav raspon sigurnosnih mehanizama na aplikacijskoj razini, PGP[82], S/MIME[83], Kerberos, SSL[84]/HTTPS[85], SSH[86]. Svaka od implementacija ima svoje prednosti i nedostatke, no detaljnija usporedba izlazi iz okvira ovog rada.

[81] Engl. International Standard Organization's Open System Interconnect
[82] Engl. Pretty Good Privacy
[83] Engl. Secure/Multipurpose Internet Mail Extensions
[84] Engl. Secure Sockets Layer
[85] Engl. Hypertext Transfer Protocol Secure
[86] Engl. Secure Shell

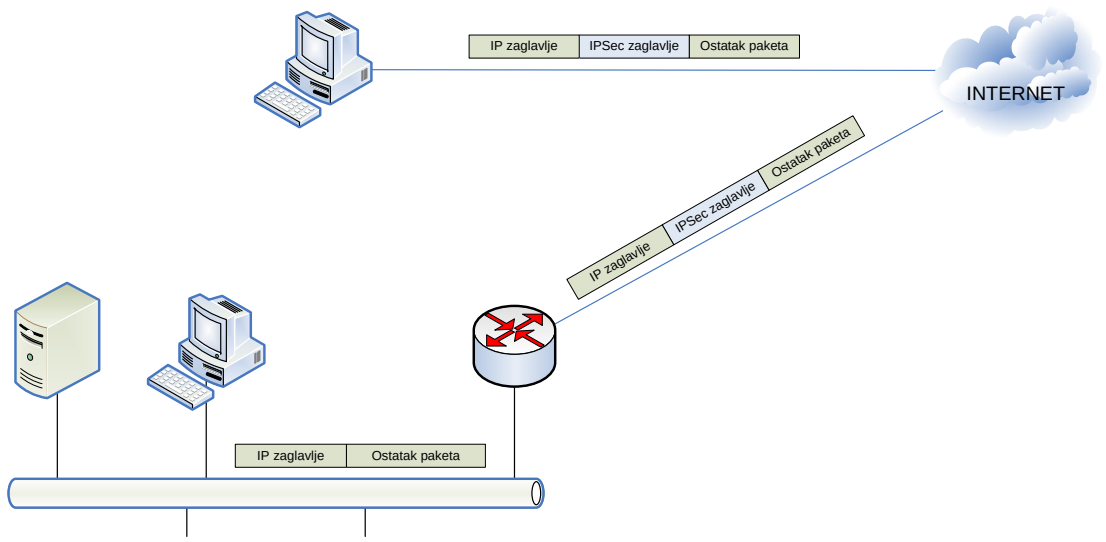


Slika 4.2. IPsec i drugi sigurnosni mehanizmi (izvor: vlastiti rad)

Pošto IP protokol osigurava uslugu komunikacijskog kanala od kraja do kraja (engl. *end-to-end),* zaštita kanala na istoj razini korištenjem IPsec-a omogućava mu neovisnost obzirom na niže slojeve. To znači da komunikacijski uređaji na putu između dvaju entiteta ne moraju podržavati IPsec, što omogućava korištenje IPsec-a bez obzira na način implementacije fizičkog sloja (engl. *Physical layer)* i sloja prijenosa podataka (engl. *Datalink layer).*

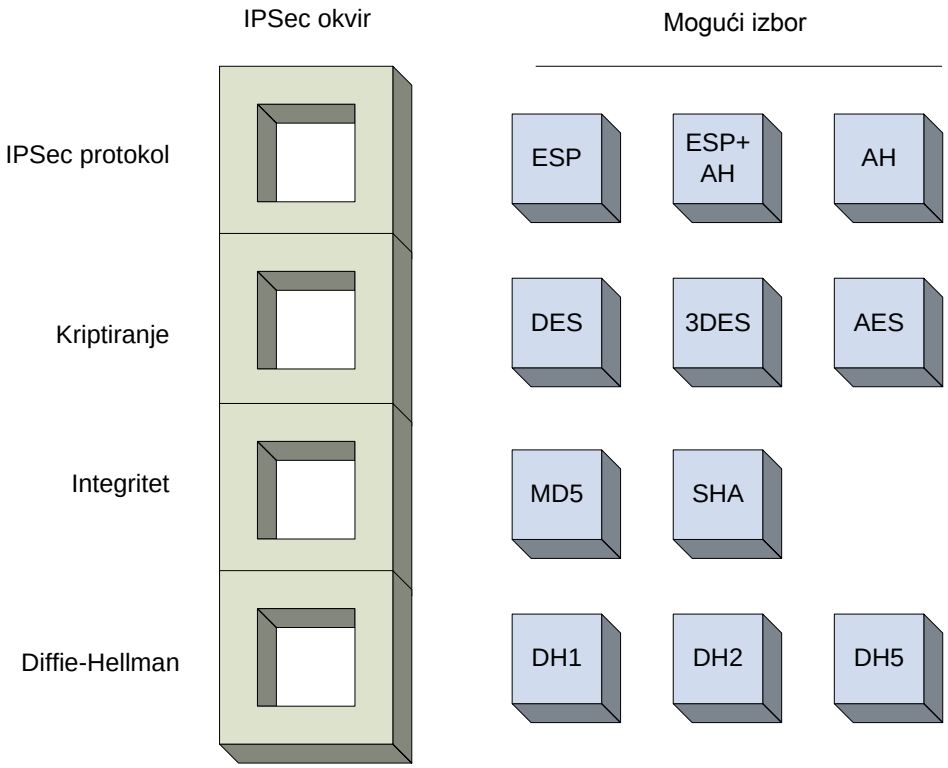
S druge strane, ukoliko dva krajnja entiteta podržavaju IPsec, njegova uporaba je transparentna obzirom na više slojeve protokolnog stoga. Aplikacije mogu koristiti sigurnu komunikaciju koju pruža IPsec, bez obzira na vlastitu funkcionalnost. Isto se odnosi i na protokole koji su implementirani u transportnom sloju (engl. *Transport layer),* što znači da svi podaci koji se prenose korištenjem TCP i UDP[87] protokola, isto kao i ICMP[88] poruke, mogu koristiti sigurni komunikacijski kanal koji pruža IPsec. Primjer komunikacije je prikazan na slici 4.3.

[87] Engl. User Datagram Protocol
[88] Engl. Internet Control Message Protocol



Slika 4.3. Primjer IPsec prometa (izvor: vlastiti rad)

IPsec možemo promatrati kao okvir (*engl. Framework*) servisa i protokola koji treba osigurati da IPsec zadovolji sigurnosne aspekte u mrežnoj komunikaciji, slika 4.4.



Slika 4.4. IPsec okvir (izvor: vlastiti rad)

Kako se iz slike vidi postoji više različitih protokola i algoritama koji mogu biti iskorišteni. Izbor ovisi o zahtjevima koji su postavljeni pred komunikaciju. Koje zahtjeve IPsec treba zadovoljiti kao servis pokazano je u nastavku.

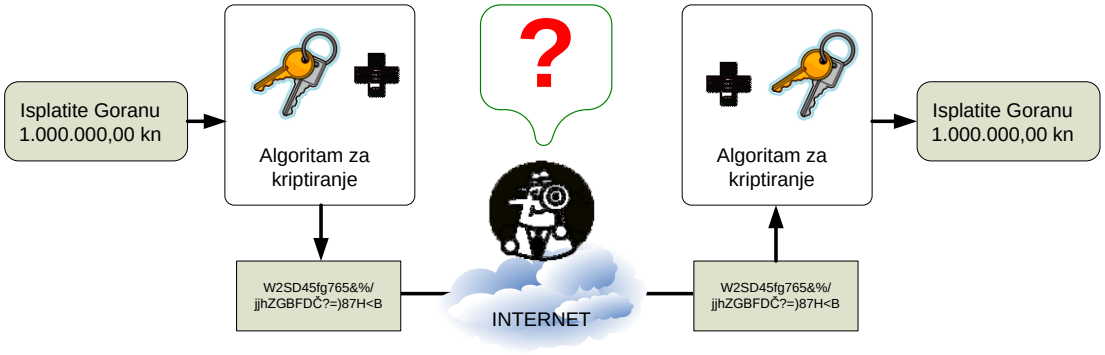
4.1. IPSEC KAO SERVIS

Pred IPsec kao servis postavljeni su zahtjevi da osigura osnovne sigurnosne aspekte mrežne komunikacije, a to su:

- Tajnost,
- Integritet,
- Autentifikacija.

4.1.1. TAJNOST

Kad smo prije govorili o Internetu rekli smo da imamo jednu dobru i jednu lošu vijest. Dobra vijest je da je Internet javna mreža. Loša vijest je da je Internet javna mreža. U uvjetima koji vladaju na lokalnim mrežama možemo primijeniti analogiju i reći da je dobra vijest da lokalna mreža funkcionira kao javna mreža. Loša vijest je ta da lokalna mreža poprima sigurnosni karakter javne mreže. Slanje podataka u sirovom obliku kroz bilo koju mrežu omogućavamo njihovo čitanje. Ako ih želimo zaštiti potrebno ih je kriptirati. Kod kriptiranja obje strane, pošiljalac i primalac moraju znati neka pravila koja se koriste kod transformacije originalne poruke. Pravila se odnose na algoritam i ključ. Algoritam je matematička funkcija koja kombinira poruku, tekst, karaktere ili sve troje sa stringom kojega nazivamo ključ. Izlaz je nečitljivi tekst i teško ga je dekriptirati bez poznavanje ključa. Jednostavan primjer kriptiranja nekog financijskog dokumenta prikazan je na slici 4.5.



Slika 4.5. Kriptiranje (izvor: vlastiti rad)

4.1.1.1. Algoritmi za kriptiranje

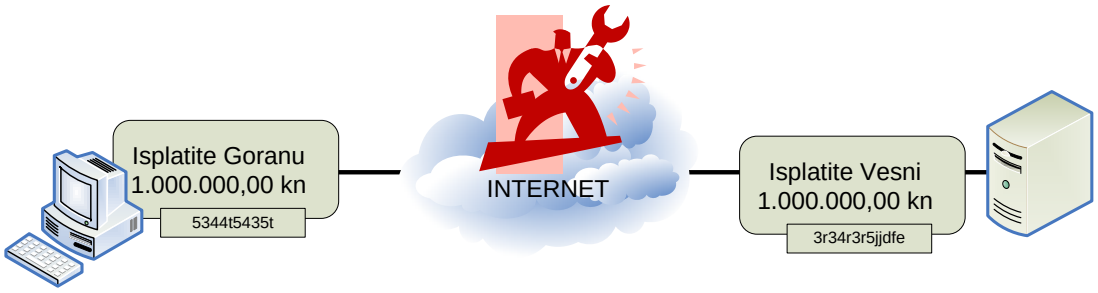
Stupanj sigurnosti ovisi o dužini ključa. Ako netko želi pogoditi ključ koristeći se nasilnom metodom pogađanja (engl. brute-force), broj mogućih kombinacija funkcija je dužine ključa [6]. Vrijeme potrebno da se dobiju sve kombinacije funkcija je procesorske snage računala. Neki od algoritama koje koristimo u kriptiranju su:

- DES – Data Encryption Standard je razvio IBM[89]. Koristi 56-bitni ključ i koristi simetrične ključeve,
- 3DES –3DES varijacija 56-bitnog DES-a. 3DES radi slično kao i DES, blok od 64-bita tri puta kriptira s tri različita ključa. 3DES efektivno je dvostruko jači od 56-bitnog DES,
- AES – Advanced Encryption Standard The National Institute of Standards and Tehnology (NIST) predložio novi standard za zamjenu DES-a. AES osigurava puno jaču sigurnost od DES i brzinu od 3DES-a. AES nudi tri različite dužine ključeva (128-bita,192-bita i 256-bita),
- RSA – Rivest, Shamir i Adleman[90] - koristi asimetrične ključeve. Svaka strane generira dva para ključeva, privatni i javni. Javi ključevi se izmjene međusobno i služe za kriptiranje poruka.

4.1.2. INTEGRITET

Integritet podatak je slijedeća kritična funkcija koju IPsec mora zadovoljiti, slika 4.6.

[89] Ime za poduzeće International Business Machines Corporation
[90] Autori algoritma



Slika 4.6. Integritet (izvor: vlastiti rad)

U svijetu računala i komunikacija nužno je osigurati integritet informacija prenošenih ili pohranjenih s nesigurnim medijem. Mehanizmi koji to omogućuju temeljeni na tajnom ključu zovu se *Message Authentication Codes* (MAC). U pravilu se MAC koristi između dvije strane koje dijele tajni ključ radi provjere informacija prenesenih između njih. MAC je djelić informacije koji koristimo za autentifikaciju poruke. MAC algoritam koristi tajni ključ i poruku da bi izračunao MAC oznaku (MAC sažetak). MAC osigurava integritet poruke (ukoliko se izvorna poruka izmjeni generirat će se različita MAC oznaka) i njezinu autentičnost (samo jedan tajni ključ generira ispravnu MAC oznaku) [18]. Za razliku od digitalnog potpisa, MAC oznaka izračunava se i provjerava istim ključem, tako da ju može provjeriti samo primatelj za kojeg je namijenjena. Postoje četiri vrste MAC-ova [19]:

1. Bezuvjetno siguran MAC temeljen na kriptiranju jednostrukim podloškom,
2. MAC temeljen na *hash* funkcijama (HMAC) koristi jedan ili više ključeva u spoju s *hash* funkcijom da bi generirao sažetak koji se dodaje na kraj poruke,
3. MAC temeljen na algoritmima za kriptiranje toka,
4. MAC izgrađen oko algoritma za kriptiranje. DES-CBC[91] MAC je u najširoj upotrebi. Osnovna ideja je u tome da se kao MAC sažetak koristi zadnji kriptirani blok poruke.

HMAC algoritam objavili su 1997. godine Mihir Bellare, Ran Canetti i Hugo Krawczyk (koji je napisao i RFC 2104). FIPS PUB[92] 198 generalizira i standardizira upotrebu

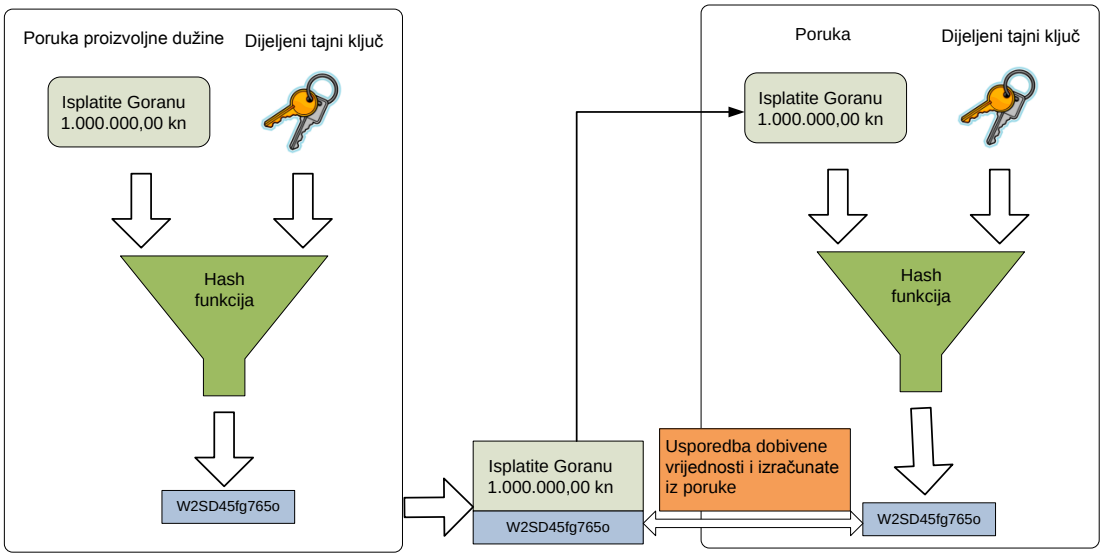
[91] Engl. Cipher-Block Chaining
[92] Engl. Federal Information Processing Standard Publication

HMAC [20]. HMAC algoritam izgrađen je oko algoritma za izračunavanje sažetka poruke (oko *hash* algoritma). Kao i svaki drugi MAC algoritam koristi se istodobno za provjeru integriteta podataka i autentičnost poruke. Svaka iterativna *hash* funkcija (npr. SHA-1[93]) može se koristiti za izračunavanje HMAC oznake. Otpornost HMAC algoritma ovisi o otpornosti *hash* funkcije oko koje je izgrađen kao i o veličini i kvaliteti tajnog ključa.

4.1.2.1. Algoritmi za Hash

Dva najčešće korištena algoritma u IPsec okviru su MD5[94] i SHA-1, [22], [23]. HMAC-om se garantira integritet podatka na način da se poruka i dijeljeni tajni ključ obrade s hash algoritmom kojemu za rezultat ima hash vrijednost. U osnovi, Hash funkcije računaju sažetke fiksne duljine iz ulaznog niza podataka proizvoljne duljine. Iz poruke se dobije fiksna vrijednost (obično 128-bitn) no iz hash-a ne možemo dobiti poruku i ova je jednosmjerni algoritam. Proces je prikazan na slici 4.7. Na strani primaoca poruke odvijaju se dva procesa. Prvo se primljena poruka i dijeljeni tajni ključ propuste kroz hash algoritam. Koji za rezultat ima hash vrijednost. Nakon toga se usporedi dobivena hash vrijednost s hash vrijednošću koja je bila poslana uz poruku. Ako vrijednosti odgovaraju integritet poruke (paketa) je potvrđena. Ako je poruka na putu mijenjana onda hash veličine ne odgovaraju.

[93] Engl. Secure Hash Algorithm
[94] Engl. Message-Digest



Slika 4.7. Hash funkcija (izvor: vlastiti rad)

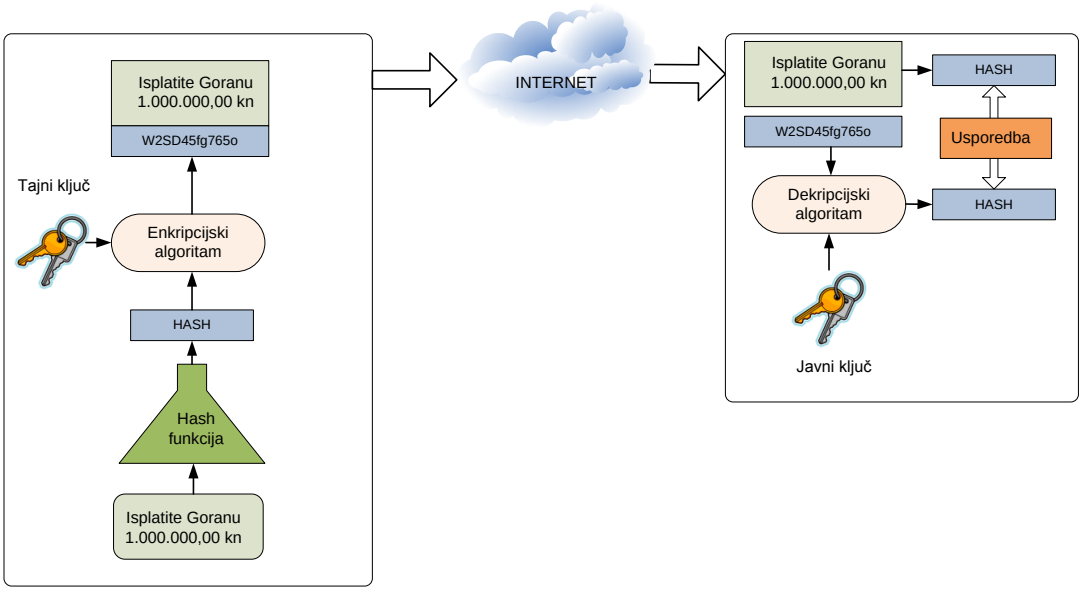
Dva općepoznata algoritma koja se koriste za integritet podataka ili autentifikaciju su:

- HMAC-MD5 – koristi 128-bitni dijeljeni tajni ključ. Poruka i 128-bitni ključ se propuste kroz ovaj algoritam i kao rezultat imamo 128-bitna hash vrijednost,
- HMAC-SHA-1 – koristi 160-bitni tajni ključ. Poruka i 160-bitni ključ se propuste kroz ovaj algoritam i kao rezultat imamo 160-bitna hash vrijednost.

HMAC-SHA-1 se smatra jačim algoritmom od HMAC-MD5 i preporuča se kod primjena gdje je sigurnost vrlo važna.

4.1.3. AUTENTIFIKACIJA IZVORA

Načini autentifikacije su se vremenom mijenjali. Nekada je žig bio garancija neke naredbe ili odluke. Kasnije se uz žig koristio i popis. U današnje vrijeme dokument se digitalno potpisuje, korištenjem privatnog ključa. Potpisnik se autorizira ako se poruka može pročitati korištenjem javnog ključa. Na slici 4.8. prikazan je princip rada autentifikacije korištenjem sustava s javnim ključem.



Slika 4.8. Autentifikacija (izvor: vlastiti rad)

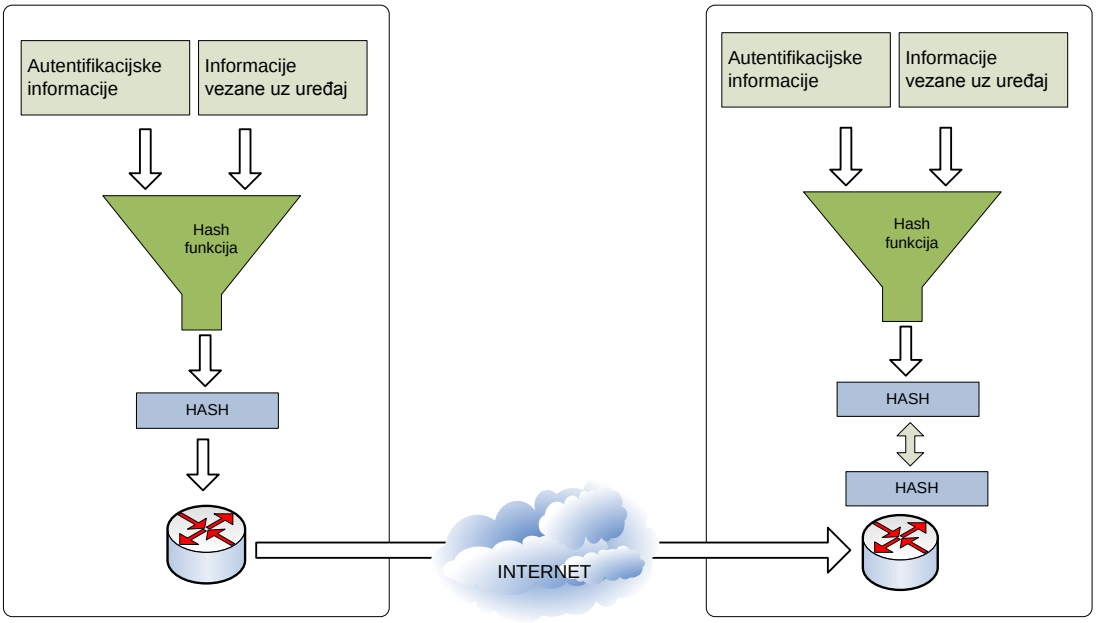
Na uređaju pošiljatelja iz poruke se kreira hash i on se kriptira s tajnim ključem. Kriptirani hash se dodaje poruci i prosljeđuje primatelju. Primatelj iz poruke kreira hash vrijednost a s javnim ključem pošiljatelja poruke dekriptira hash vrijednost. Ako su vrijednosti tako dobivenih hash-a jednake potvrđen je identitet pošiljatelja poruke.

Načini na koje možemo provesti autentifikaciju (za implementacije koje će ovdje biti razmatrane) su:

- Predefinirani ključ,
- Certifikat (potvrda o identitetu osobe),
- Kerberos.

4.1.3.1. Predefinirani ključ

Predefinirani ključ (engl. Preshared key) je metoda u kojoj oba para koriste isti predefinirani ključ. Na svakom kraju se predefinirani ključ kombinira s drugim informacijama da bi se oformio autentifikacijski ključ. Na slici 4.9. prikazan je proces.

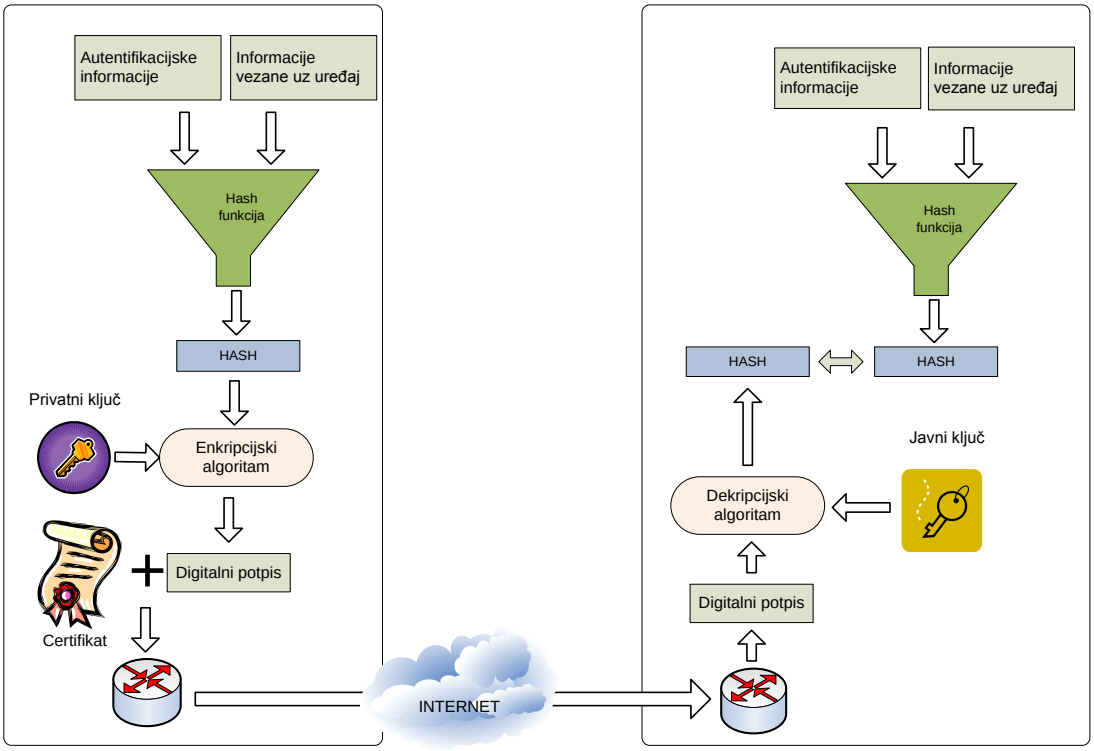


Slika 4.9. Preshared key (izvor: vlastiti rad)

Predefinirani ključ i identifikacijske informacije (specifične informacije uređaja) prođu kroz hash algoritam i kreiraju formu koju šaljemo drugoj strani. Ako druga strana može neovisno kreirati isti hash onda je druga strana identificirana. Autentifikacijski proces mora biti proveden i u drugom smjeru. Ovaj način je jednostavan za konfiguriranje no traži intervenciju kod svih sudionika u komunikaciji.

4.1.3.2. Certifikat

Ove metoda ima sličnosti s metodom u kojoj se koristi predefinirani ključ. Proces je prikazan na slici 4.10.



Slika 4.10. RSA algoritam (izvor: vlastiti rad)

Počinje se s autentifikacijskim ključem i identifikacijskim informacijama (specifične informacije uređaja) koji prođu kroz hash algoritam. Dobivena forma (hash) se kriptira s lokalnim privatnim ključem. Rezultat je digitalni potpis kome se dodaje digitalni certifikat te se to proslijedi drugoj strani (javni ključ za dekriptiranje potpisa uključen je u digitalni certifikat koji se izmijeni između parova). Na strani primalaca odvija se dva procesa. Prvi, verificira digitalni potpis na način da ga dekriptira koristeći se javnim ključem uključenoga u certifikat. Rezultat je hash vrijednost. Lokalno se kreira hash iz spremljenih podataka i ako je dobivena vrijednost ista s primljenom par je autoriziran. Isti proces slijedi u obratnom smjeru.

4.1.3.3. Kerberos

Mnogi oblici računalne autentifikacije zasnivaju se na ideji da pojedini entitet (osoba, proces...) može dokazati vlastiti identitet na način da dokaže da zna neki ključ (npr. zaporku) koji ne može znati nitko drugi osim tog entiteta. Očit problem koji treba riješiti prilikom autentifikacije zasnovane na tajnom ključu (zaporki) jest taj da treba osigurati metode kojima se mora očuvati tajnost ključa. Naime, nipošto nije pametno

da korisnik koji traži pristup nekim resursima direktno odaje svoju zaporku – netko bi mogao prisluškivati komunikacijski kanal (koji je najčešće neosiguran) ili bi korisnik mogao tražiti pristup na krivome mjestu (najčešće uz prijevaru). Da bi zaporka ostala tajna prilikom autentifikacije, mora postojati način da korisnik dokaže da zna zaporku bez da ju pritom otkrije. Protokol Kerberos zasnovan je na toj ideji, kod njega se radi o autentifikaciji putem ključa, no riječ je o tajnoj autentifikaciji kod koje se sadržaj ključa zapravo nikad ne otkriva. Kako bi bilo moguće ostvariti navedenu tajnu autentifikaciju, obje strane (npr. klijent i poslužitelj) koje sudjeluju u transakciji moraju posjedovati jedan sjednički ključ, koji također mora biti tajni, odnosno poznat samo njima. Riječ je o simetričnom kriptografskom ključu (dakle, koristi se i za enkripciju i za dekripciju). Princip autentifikacije tada je sljedeći: jedna strana (klijent) dokazuje svoje znanje ključa (a time i svoj identitet) enkriptiranjem nekakve poruke, dok druga strana (poslužitelj) isto potvrđuje dekriptiranjem te iste poruke. Autentifikacija je obavljena, a da zaporka (u ovom slučaju sjednički ključ) nije ugrožena direktnim (javnim) obznanjivanjem.

4.2. IPSEC PROTOKOLI

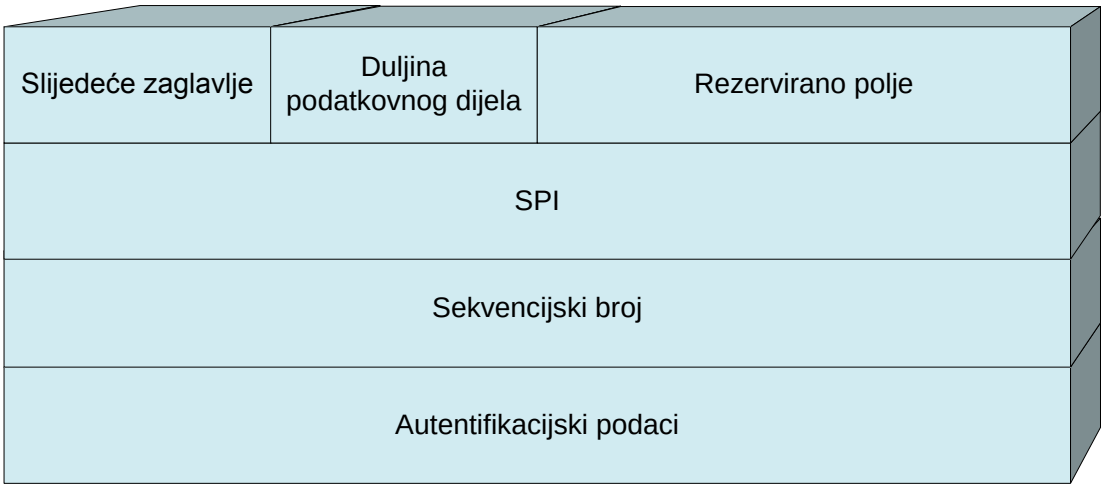
IPsec je standard definiran od strane IETF[95]-a, s ciljem da se osigura siguran transport informacija preko javnih IP mreža. Protokoli definirani u RFC[96] 4303 ESP i RFC 4302 AH dio su IPsec arhitekture. Oba protokola, AH i ESP, modificiraju standardni oblik IP datagrama [24], [25].

4.2.1. AH

AH protokol (IP protokol 51) osigurava besprijekornost (integrity - nemogućnost promijene podataka od strane neovlaštene osobe), i autentičnost (authentication - verifikacija identiteta pošiljaoca) IP datagrama, ali ne može osigurati i tajnost (confidentiality - isključivo ovlaštena osoba može pristupiti podacima). Protokolom je definirano vlastito (AH) zaglavlje, koje se umeće između IP zaglavlja i IP podataka

[95] Engl. Internet Engineering Task Force
[96] Engl. Request for Comments

koji slijede [26]. Specifičnost AH jest u tome što on, za razliku od ostalih protokola TCP/IP stoga, ne enkapsulira podatke protokola kojima pruža uslugu. Slika 4.11. prikazuje AH zaglavlje, zajedno s pripadajućim poljima. Sva prikazana polja su obvezna, odnosno uvijek su prisutna u AH zaglavlju. U nastavku su opisane njihove funkcije.



Slika 4.11. AH zaglavlje (izvor: vlastiti rad)

Sljedeće zaglavlje (engl. *next headef)* - Sljedeće zaglavlje je 8-bitno polje koje identificira tip podataka koji slijedi nakon AH zaglavlja. Polje može poprimiti vrijednost iz definiranog skupa brojeva koji označavaju IP protokole (npr. 6 - TCP, 17 - UDP, 51 - ESP). U dokumentu RFC 3232, dan je trenutno važeći skup brojeva, odnosno protokola.

Duljina (engl. *payload lengtti)* - Duljina je polje koje specificira duljinu AH zaglavlja. Duljina se računa kao duljina u 32-bitnim riječima umanjena za vrijednost 2.

Rezervirano (engl. *reserverd)* - Ovo polje duljine 16 bita je rezervirano za buduće potrebe. Ono mora biti postavljeno na vrijednost "0".

Popis sigurnosnih parametara (engl. **S**ecurity **P**arameters **I**ndex) - Ovo polje duljine 32 bita sadrži proizvoljnu vrijednost koja uz IP adresu i sigurnosni protokol (u ovom slučaju AH) definira jedinstveni skup sigurnosnih parametara (engl. security association - SA) koji se koristi u sigurnoj komunikaciji između dvaju entiteta. SA

skup sigurnosnih parametara definira se prilikom uspostave IPsec spoja. Vrijednosti od 1 do 255 rezervirane su od lANA[97]-e za buduću uporabu.

Sekvencijski broj (engl. seguence numbef) - Ovo polje duljine 32 bita služi za osiguranje od napada ponavljanjem paketa, a povećava se prilikom svakog slanja paketa koji ima identični SA skup sigurnosnih parametara. Pošiljatelj mora nužno generirati ovo polje, dok ga primatelj može ili ne mora interpretirati. Prilikom inicijacije komunikacije ovo polje se postavlja na vrijednost "1".

Autentikacijski podaci (engl. authentication data) - Polje koje sadrži autentifikacijske podatke je varijabilne duljine. U njemu je sadržana ICV[98] vrijednost na temelju koje se provjerava integritet i autentičnost poruke. Duljina polja za autentifikacijske podatke mora biti cjelobrojni višekratnih 32-bitne riječi. Ukoliko polje samo po sebi ne ispunjava taj uvjet dodaje se (proizvoljna) ispuna kojom se nadopunjava odgovarajući broj bitova. Za razliku od "obične" funkcije sažimanja, ICV nastane kao rezultat HMAC[99]-a. Radi se o skraćenim verzijama HMAC-MD5-96 ili HMAC-SHA-1-96 algoritama. Kao i s bilo kojim MAC-om možemo ga koristiti za verifikaciju integriteta podatka i autentifikaciju pošiljaoca. Kao takav, pruža zaštitu integriteta i autentičnosti podataka prema čemu je sličan digitalnom potpisu. Za razliku od digitalnog potpisa, ne osigurava zaštitu od poricanja. Izračunavanje ICV vrijednosti na temelju sadržaja i ključa je mnogo sigurnije nego koristiti "čistu" jednosmjernu sumu tj. izračunati sažetak samo na temelju podataka koji se štite, ali ne i ključa. Kada se primi poruku zaštićenu nekim od tih algoritama primalac obavlja provjeru ICV vrijednosti. Izračunava HMAC ICV vrijednost nad unaprijed dogovorenim poljima IP paketa dogovorenim autentifikacijskim algoritmom te provjerava da li su dobivena i izračunata vrijednost jednake. AH štiti gotovo sve dijelove IP paketa, isključeni su samo oni koji se pri svakom skoku kroz mrežu (u

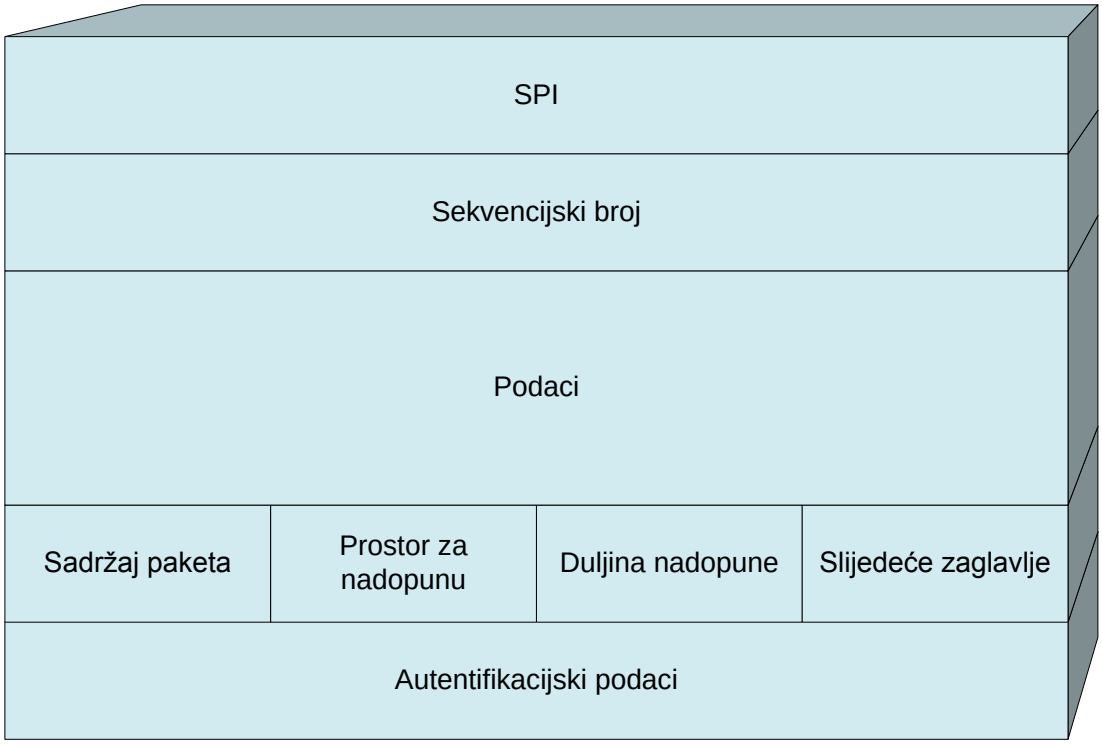
[97] Engl. Internet Assigned Numbers Authority
[98] Engl. Integrity Check Value
[99] Engl. keyed-Hash Message Authentication Code

ruterima) mijenjaju - TTL[100] i suma zaglavlja (engl. *header cheksum*) te TOS[101] , *flgs* i *frag offset*. Važno je uočiti da AH štiti i polja s izvorišnom i odredišnom adresom što za posljedicu ima "probleme" kod AH+NAT funkcionalnosti

Algoritam koji se upotrebljava za računanje ICV-a, definira se prilikom uspostave komunikacije i dio je SA skupa sigurnosnih parametara.

4.2.2. ESP

ESP protokol (IP protokol 50) osigurava autentičnost, integritet i tajnost paketa, primarno osigurava tajnost IP datagrama [27]. Protokol također definira vlastito zaglavlje koje se umeće iza IP zaglavlja, te enkapsulira sve podatke protokola višeg sloja, dodajući pri tom završni slog u kojem mogu biti sadržani autentifikacijski podaci. Slika 4.12. prikazuje ESP zaglavlje zajedno s pripadajućim poljima. U nastavku su opisane funkcije tih polja.



Slika 4.12. ESP zaglavlje (izvor: vlastiti rad)

Popis sigurnosnih parametara SPI[102] - Popis sigurnosnih parametara je 32-bitno polje u kojem se, isto kao i kod AH, definira jedinstveni SA skup sigurnosnih

[100] Time To Live
[101] Type Of Service

parametara (određen prilikom uspostave komunikacije) koji se koristi u komunikaciji između dvaju entiteta. Kao i kod AH, vrijednosti od 1 do 255 su rezervirane za buduću uporabu.

Sekvencijski broj - Ovo polje duljine 32 bita, isto kao i kod AH, služi za osiguranje od napada ponavljanjem paketa, a povećava se prilikom svakog slanja paketa koji ima identični SA skup sigurnosnih parametara. Pošiljatelj mora nužno generirati ovo polje, dok ga primatelj može ili ne mora interpretirati. Prilikom inicijacije komunikacije ovo polje se postavlja na vrijednost "0", za razliku od AH gdje je inicijalna vrijednost tog polja "1".

Podaci (engl. *Payload data)* - Ovo polje proizvoljne duljine sadrži podatkovni dio IP paketa i ispunu. Vrsta podataka koja se nalazi u podatkovnom dijelu definirana je poljem "sljedeće zaglavlje". Osim samih podataka, u tom polju mogu biti i eksplicitno sadržani podaci koji su nužni za kriptografsku sinkronizaciju (npr. inicijalizacijski vektor - IV), ukoliko to kriptografski algoritam koji se koristi zahtijeva (npr. DES u CBC načinu rada). Ovisno o načinima rada kriptografskih protokola koji koriste inicijalizacijskih vektor, on može biti sadržan na samom početku šifriranog bloka podataka ili zasebno od šifriranih podataka, što ovisi o konkretnim implementacijama algoritama. Ispuna se koristi iz dva razloga:

- Neki kriptografski algoritmi za šifriranje koriste blokove fiksne duljine, te je podatkovni dio paketa potrebno dopuniti do odgovarajuće duljine,
- Zbog implementacijskih razloga nužno je da duljina podataka ispune, te dva sljedeća polja ("duljina ispune" i "sljedeće zaglavlje") zajedno daju cjelobrojni višekratnik 32-bitne riječi, odnosno da je ta duljina poravnata na 4-okteta.

Duljina nadopune (engl. *Payload length)* - Ovo 8-bitno polje definira duljinu prethodno korištene ispune u oktetima. Dozvoljene vrijednosti su od 0 do 255, s time da vrijednost 0 označava da ispuna ne postoji.

[102] Engl. security parameter index

Sljedeće zaglavlje - Sljedeće zaglavlje, ponovno kao i kod AH, je 8-bitno polje koje identificira tip podataka koji slijedi nakon ESP zaglavlja. Polje može poprimiti vrijednost iz definiranog skupa brojeva koji označavaju IP protokole.

Autentifikacijski podaci - Ovo polje proizvoljne duljine nije obvezno, a koristi se samo u slučaju kad je u SA skupu sigurnosnih parametara specificirana usluga autentifikacije. U tom slučaju ovo polje sadrži ICV koji se računa za cijeli ESP datagram (ESP zaglavlje, podatkovni dio i ispuna), ne uključujući pri tom samo polje namijenjeno autentifikacijskim podacima, a njegova duljina ovisi o autentifikacijskom algoritmu koji se koristi.

4.3. NAČIN RADA

IPsec je može raditi na dva načina i to:

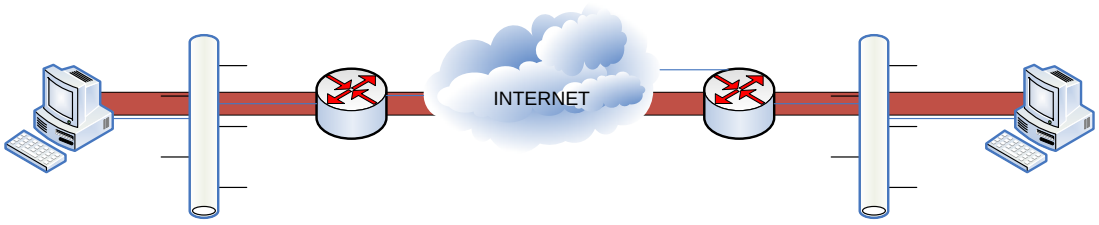
- Transportni način rada,
- Tuneliranje paketa.

U prvom slučaju paketi se šalju između dva krajnja računala na mreži, pri čemu računalo koje prima paket izvršava sigurnosne provjere prije nego ga proslijedi višim slojevima. U drugom slučaju nekoliko računala (ili cijela lokalna mreža) se nalazi iza jednog čvora te je kao takva nevidljiva ostatku mreže (a samim time i zaštićena od napada). U oba slučaja moguće je izgraditi Virtualne Privatne Mreže – VPN (eng. Virtual Private Network), što je i osnovna ideja zaštite IPsec protokolima.

4.3.1. TRANSPORTNI NAČIN RADA

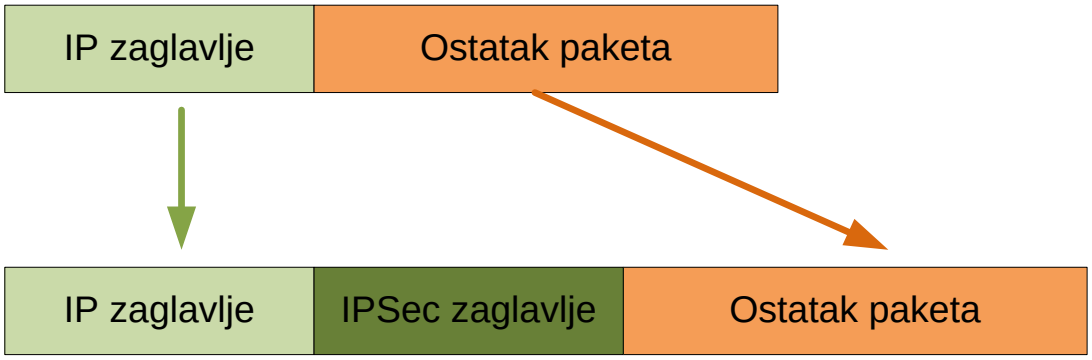
Transportni način rada namijenjen je prvenstveno za uspostavu sigurne komunikacije između entiteta, odnosno tzv. host-to-host komunikacije u privatnim LAN[103] ili WAN[104] računalnim mrežama, slika 4.13. Za transportni način rada nužno je da obje krajnje točke (izvor i odredište) podržavaju IPsec

[103] Engl. Local Area Network
[104] Engl. Wide Area Network



Slika 4.13. Transportni način rada (izvor: vlastiti rad)

Izgled paketa u transportnom načinu rada prikazan je na slici 4.14.

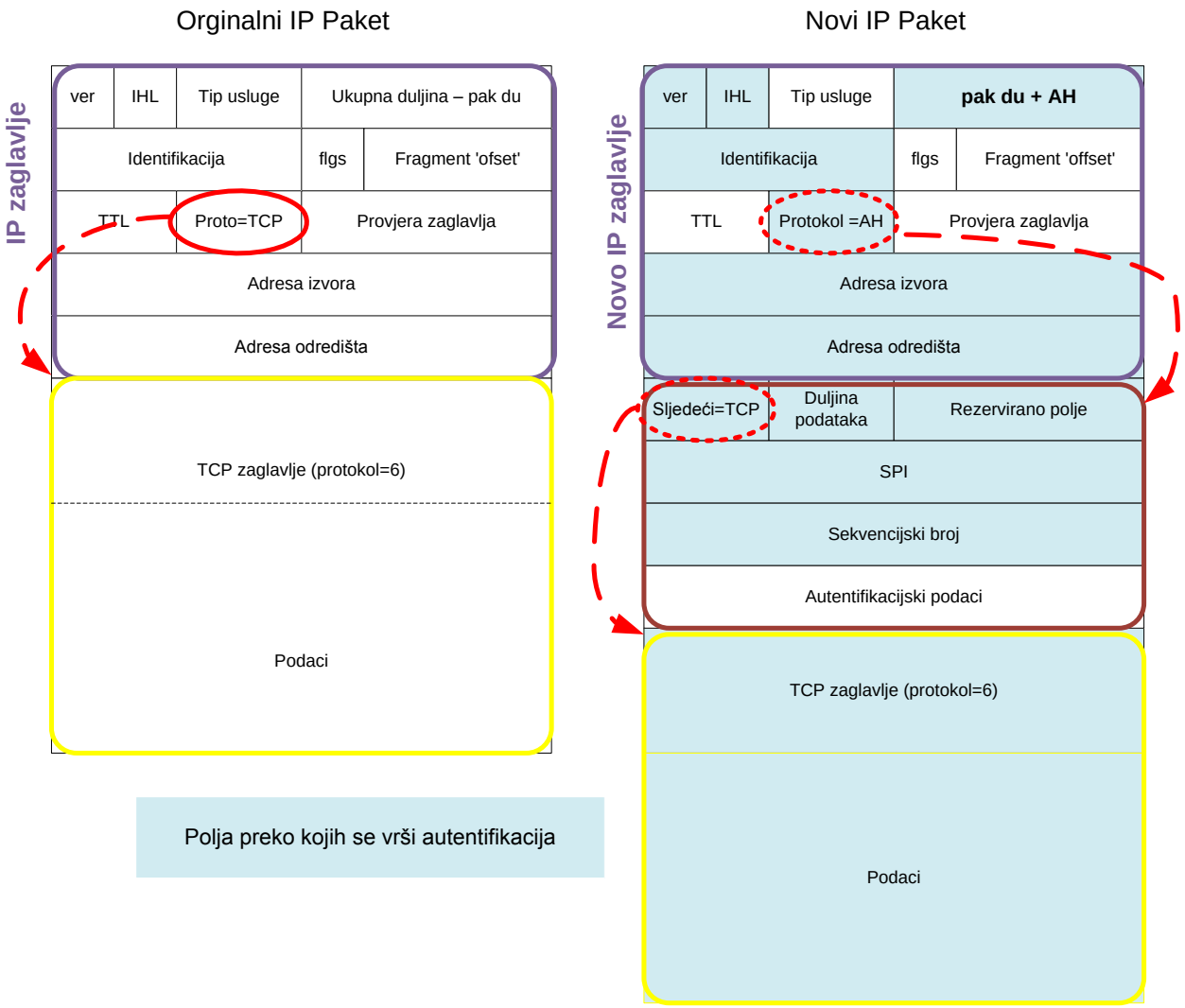


Slika 4.14. Paket u transportnom načinu rada (izvor: vlastiti rad)

U transportnom načinu rada štiti se samo podatkovni dio IP paketa, dok IP zaglavlja ostaju u originalnom obliku. Zbog toga u zaštićenom paketu postoji samo jedna izvorišna i odredišna adresa IP adresa. Između dviju strana se ne formira sigurni tunel i ovo je jedna od osnovnih razlika između transportnog i tunel načina rada.

4.3.1.1. AH

Ako AH protokol koristimo u transportnom načinu rada originalni je IP paket tek neznatno promijenjen - između originalnog IP zaglavlja i *payload-a* IP paketa (transportnog segmenta) umetnuto je AH zaglavlje, slika 4.15. Jasno, u novom IP zaglavlju polje sljedeći protokol (Protokol=AH) više ne pokazuje na protokol transportnog sloja nego na AH protokol, dok polje 'slijedeći protokol' u AH zaglavlju sada pokazuje na prijenosni protokol (TCP).



Slika 4.15. AH u transportnom modu (izvor: vlastiti rad)

Polje verzija (engl. version) kaže koju verziju protokola koristi datagram. S obzirom da je duljina zaglavlja promjenljiva, u IHL[105] polju je naznačena duljina zaglavlja (pet ili šest riječi). U polju tip usluge (engl. type of service) host govori podmreži koju vrstu usluge želi (moguće su različite kombinacije pouzdanosti i brzine). Polje ukupna duljina (engl. total length) daje ukupnu duljinu datagrama (zaglavlje i podaci). Maksimalna duljina je 65535 bytova. Polje identifikacija (engl. identification) omogućava odredišnom hostu određivanje kojem datagramu pripada pristigli fragment. Slijedi polje 'flgs', prvo neiskorišteni bit, zatim DF bit i MF bit. DF (Don't Fragment) bit naređuje router-ima da ne fragmentiraju datagram, jer ga odredište ne

[105] Engl. Internet Header Length

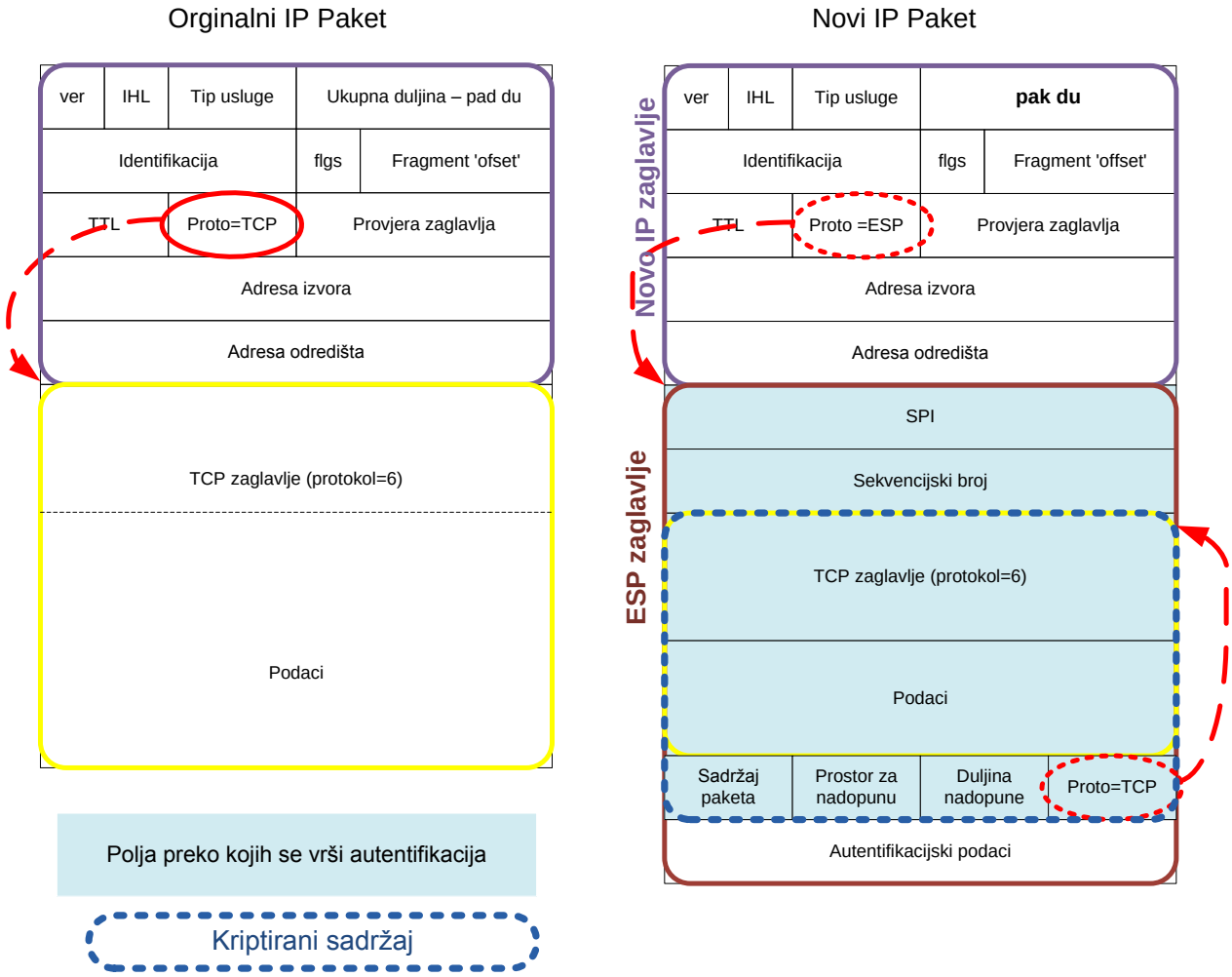
može složiti. MF (More Fragments) bit imaju postavljeni svi fragmenti osim zadnjeg kao znak da dolazi još fragmenata istog datagrama. Polje "ofset" fragmenta kaže gdje se u datagramu nalazi taj fragment. Polje vrijeme života paketa (engl. time to live) predstavlja brojač za ograničavanje životnog vijeka paketa. Smanjuje se pri svakom skoku i kad dosegne nulu paket se odbacuje. Ovo polje sprječava paket da kruži mrežom, što se može dogoditi ako se poremete tabele u routerima. Polje protokol govori mrežnom sloju koji će se protokol prijenosnog sloja koristiti. Polje za provjeru zaglavlja (engl. header checksum) provjerava samo zaglavlje. IP dostavlja datagram tako da čita adresu odredišta (peta riječ). Adresa odredišta je standardna 32-bitna IP adresa. Ako je adresa odredišta adresa u lokalnoj mreži paket se dostavlja direktno. Ako adresa nije u lokalnoj mreži, paket se predaje router-u za prijenos. Polje opcija (engl. options) služi za uključivanje informacija koje će biti potrebne u sljedećim verzijama protokola (trenutno je definirano pet opcija). Zatim slijedi polje s podacima.

Slika 4.15 prikazuje IP paketa s umetnim AH zaglavljem (AH *transport* IP paket) i označenim zaštićenim poljima IP datagrama . Na slici je vidljivo da je autentificiran i zaštićen po pitanju integriteta gotovo cijeli IP paket uključujući izvorišnu i odredišnu adresu. Jasno je da zbog toga AH autentifikacija ne može funkcionirati ukoliko se na putu IP paketa od izvorišta do odredišta događa prepisivanje adresa (NAT: *Network Address Translation*) - ako neki mrežni uređaj prepiše ili izvorišnu ili odredišnu adresu, zaštitna suma više neće biti jednaka. Ovo je svojstvo nekompatibilnosti AH i NAT-a neovisno o načinu rada, isto se događa i u tunnel načinu rada.

4.3.1.2. ESP

Kod ESP protokol koristimo u transportnom načina rada također se između originalnog IP zaglavlja i IP podataka dodaje ESP zaglavlje, a IP podaci se kriptiraju. Opcionalno se na kraj IP paketa dodaju autentifikacijski podaci. Sa slike 4.16. se vidi da je IP paketa s ESP kriptiranim podacima autentificiran i zaštićen po pitanju

integriteta i to samo kriptirani sadržaj. Izvorišna i odredišna adresa se ne nalaze pod zaštitnom sumom.



Slika 4.16. ESP u transportnom modu (izvor: vlastiti rad)

Za transportni moda rada možemo reći da je zbog šifriranja aplikacijskog zaglavlja ograničena mogućnost pregledavanja paketa. Prednost ovog načina rada je da se svakom paketu dodaje svega nekoliko okteta. U ovom načinu rada uređaji (usmjerivači) na javnoj mreži mogu vidjeti adrese izvora i odredišta poruka, što potencijalnom napadaču donekle omogućava određene mogućnosti analize prometa. Prva dva polja ESP zaglavlja (SPI, Sekvencijski broj) zaštićena su obzirom na zahtjev autentičnosti, dok označena polja (- - -) ispod zaštićeno su obzirom na zahtjev tajnosti. Dio koji je kriptiran (dakle, zaštićen po pitanju tajnosti) obuhvaća

samo sadržaj kao i polje koje u sebi nosi tip protokola poruke višeg sloja koja je inkapsulirana u tom IP paketu. Na ovaj način, osim što su podaci kriptirani, napadač čak ni ne zna što je inkapsulirano unutar.

Zaštita s obzirom na zahtjev autentifikacije je opcionalno i sadržano je u polju 'Autentifikacijski podaci' koje se prema izboru dodaje na kraj zaglavlja. Za razliku od AH protokola, u ovom slučaju, autentificiraju se samo ESP zaglavlje i kriptirani sadržaj, a ne cijeli IP paket. Zaštita protokola više razine se primjenjuje na podatkovni dio paketa. Usmjeravanje paketa (engl. routing) kroz mrežu vrši se na osnovu IP zaglavlja originalnog paketa.

4.3.2. TUNELIRANJE

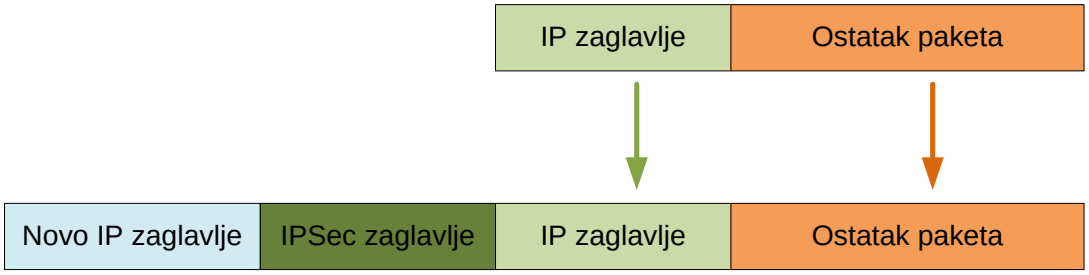
U ovom načinu rada IPsec služi za uspostavu sigurne komunikacije između gateway[106] uređaja na udaljenim mrežama (engl. gateway-to-gateway) slika 4.17, osiguravajući tako virtualnu privatnu komunikaciju. Kod tuneliranja krajnji entiteti u komunikaciji ne moraju podržavati IPsec: čitava komunikacija za njih je potpuno transparentna jer sve operacije nužne za sigurnu komunikaciju korištenjem IPsec-a obavljaju gateway uređaji. Gateway uređaji na udaljenim mrežama predstavljaju ulaznu, odnosno izlaznu točku sigurnog komunikacijskog kanala. Oni preko nesigurnog medija formiraju sigurni tunel, zbog čega se ovaj način rada i zove tuneliranje

Slika 4.17. Tunel način rada (izvor: vlastiti rad)

Korištenje tunelskog načina rada također je moguće i u host-to-host\\.\ host-to-gateway komunikaciji, no tada ponovno krajnji entiteti ili entitet moraju podržavati IPsec. IPsec tuneliranje koristi dogovorene mehanizme za inkapsulaciju i šifriranje

[106] Gateway je uređaj koji se nalazi u čvoru računarske mreže i služi za komuniciranje sa nekom drugom mrežom

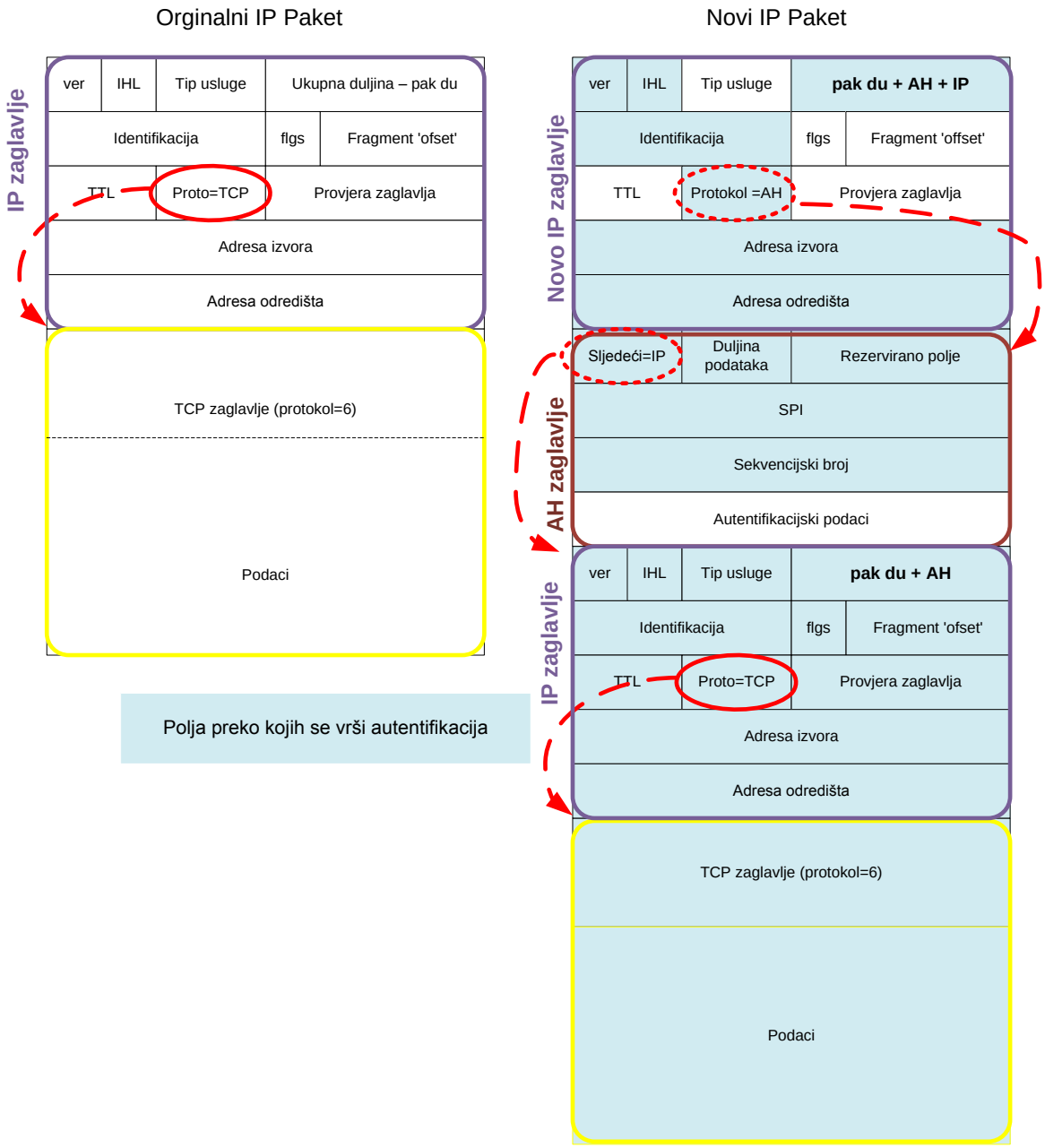
čitavih IP paketa što osigurava potpuno siguran prijenos preko javnih ili privatnih mreža. Šifrirani podaci se spajaju s odgovarajućim nešifriranim IP zaglavljima, formirajući tako IP pakete koji se na kraju tunela dešifriraju i oblikuju u IP pakete namijenjene krajnjem odredištu, slika 4.18.



Slika 4.18. Paket u tunel modu rada (izvor: vlastiti rad)

4.3.2.1. AH

Ukoliko se želi osigurati samo autentifikacija, integritet i neporecivost poruka, a tajnost nije nužna, moguće je koristiti AH protokol. U tom slučaju originalni IP datagram, koji sadrži adresu krajnjeg odredišta, se inkapsulira u novi IP datagram kojem se dodaje odgovarajuće AH zaglavlje, slika 4.19. U ovom slučaju polje protokol novog IP zaglavlja koje sadrži adresu krajnje točke IPsec tunela ima vrijednost 51 (AH), dok polje sljedeće zaglavlje unutar AH zaglavlja ima vrijednost 4 (inkapsulirani IP) [31].

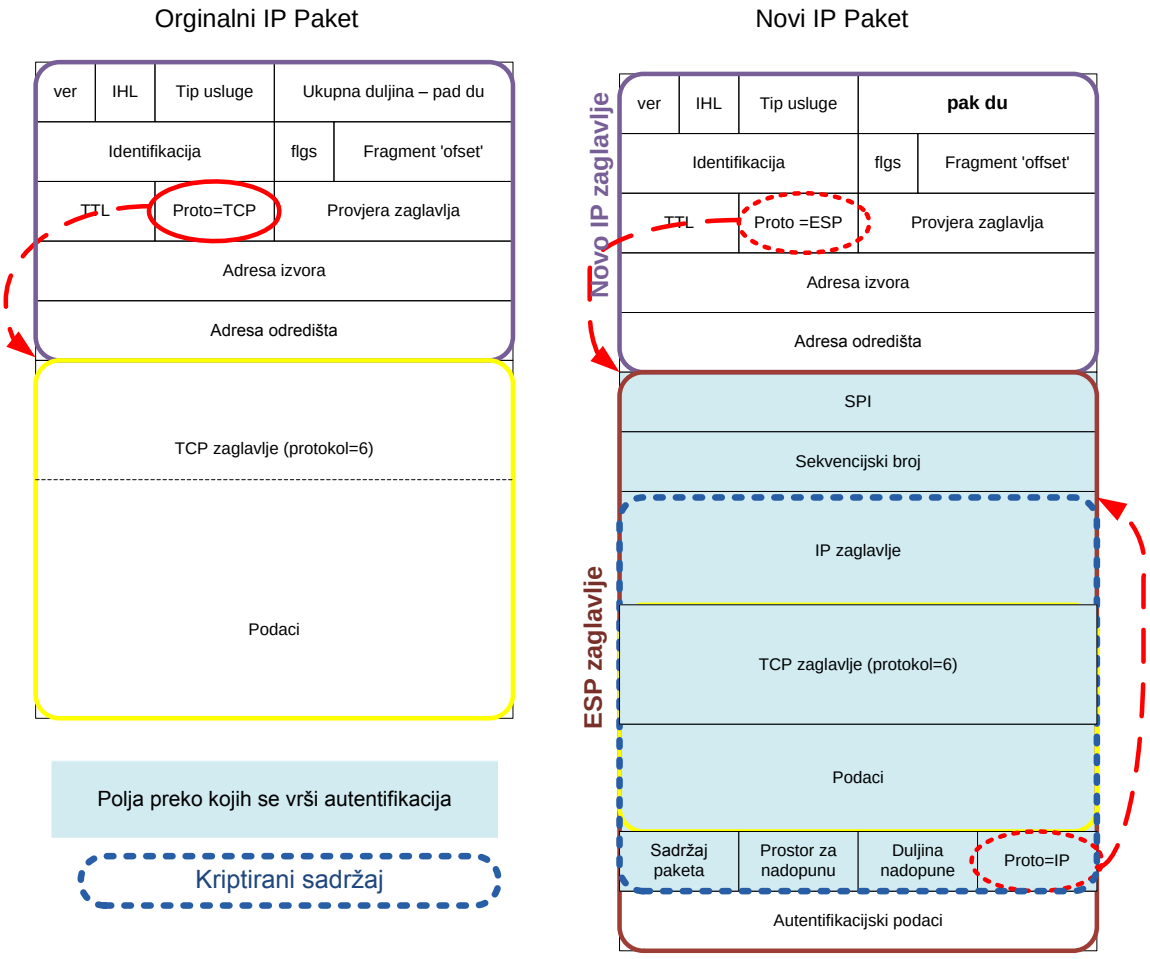


Slika 4.19. AH u tenel modu rada (izvor: vlastiti rad)

4.3.2.2. ESP

Ukoliko se osim autentifikacije, integriteta i neporecivosti želi osigurati i tajnost komunikacije, nužna je upotreba ESP protokola. Korištenjem ESP u tunelskom načinu rada, za razliku od transportnog načina, vrši se šifriranje čitavog originalnog IP datagrama, a također je osigurana autentikacija, integritet i neporecivost čitavog datagrama, pošto je sam datagram inkapsuliran u novi IP paket, slika 4.20. U ovom slučaju polje protokol novog IP zaglavlja koje, isto kao i kod AH, sadrži adresu krajnje

točke IPsec tunela ima vrijednost 50 (ESP), dok polje 'sljedeće zaglavlje' unutar ESP zaglavlja ima vrijednost 4 (inkapsulirani IP).



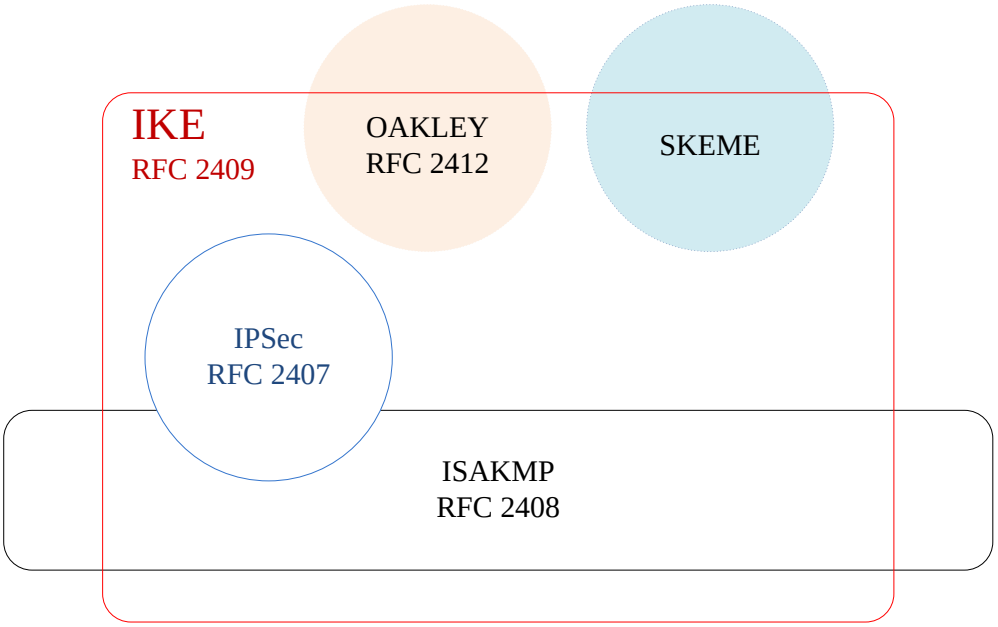
Slika 4.20. ESP u tunel modu rada (izvor: vlastiti rad)

Za tunelski način možemo reći da štiti se cijeli paket. Cijeli paket se uzima kao IP podaci drugog IP paketa (koji potencijalno ima različite IP adrese izvorišta i odredišta u odnosu na originalan paket). ESP u 'tunel' modu kriptira i opcionalno autentificira cijeli unutarnji IP paket. AH u 'tunel' modu autentificira cijeli unutarnji IP paket i odabrana polja IP zaglavlja vanjskog paketa .

4.4. MEHANIZAM IZMJENE KLJUČEVA

ISAKMP [28] protokol definira okvir za identifikaciju, izmjenu ključeva, proceduru dogovaranja, uspostavu, promjenu i brisanje SA. Ne definira koji mehanizam izmjene ključeva koristiti već samo okvir. IPsec zahtjeva podršku za ručno i automatsko upravljanje sa SA i izmjenom ključeva. IKE definira automatsko upravljanje

ključevima za IPsec. IKE je hibridni protokol jer u sebi sadrži dijelove Oakley [30] protokola za izmjenu ključeva i SKEME protokola za tehnike ključeva. Na slici 4.21. prikazan je odnos između ISAKMP, IKE, Oakly i SKEME protokola.



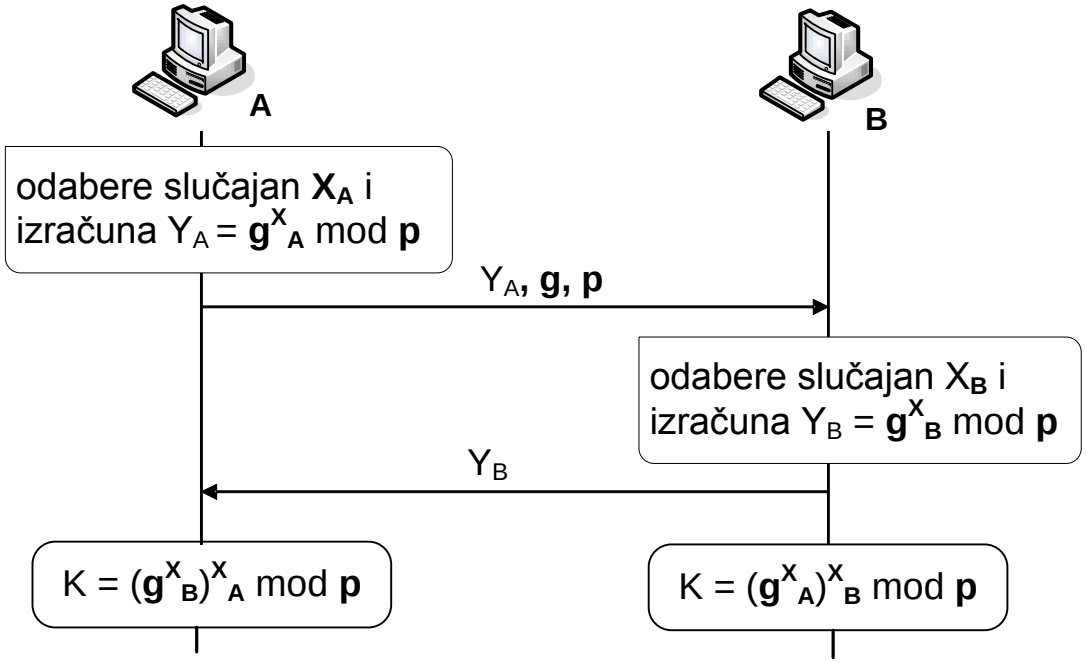
Slika 4.21. ISAKMP protokol

Oakley protokol koristi Diffe-Hellman[107] način za izmjenu ključeva tj. algoritam za kreiranje jedinstvenog, dijeljenog sigurnog ključa koji će biti iskorišten za generiranje ostalih ključeva za kriptiranje.

4.4.1. DIFFIE-HELLMAN ALGORITAM

Na slici 4.22. prikazan je tok podataka između dva korisnika A i B koji žele uspostaviti sigurnu komunikaciju i za to im treba tajni ključ kojime će kriptirati sadržaj poruka. Postupak generiranja zajedničkog tajnog ključa algoritmom Diffie-Hellman najlakše je ilustrirati primjerom. Pretpostavimo da A i B žele generirati sjednički ključ komunicirajući nesigurnim kanalom. Prvo, A i B se moraju složiti oko dva broja, **p** i **g**. **p** je veliki prosti broj, a za **g** se uzima ostatak dijeljenja nekog još većeg prostog broja s *n*. Ova dva broja ne moraju biti tajna - A i B mogu ih dogovoriti preko nesigurnog kanala. štoviše, ti brojevi mogu biti poznati i čitavoj grupi suradnika.

[107] Autori algoritma W. Diffie i M.E. Hellman



Slika 4.22. Diffie-Hellman protokol (izvor: vlastiti rad)

Protokol za generiranje ključa odvija se po sljedećim koracima:

Dijeljeni javni elementi

p prosti broj

g $g < p$: g je primitivni korijen broja p

Korisnik A generira ključeve

Odaberi privatan ključ X_A $X_A < p$

Izračunaj javni ključ Y_A $Y_A = g^{XA} \bmod p$

Korisnik B generira ključeve

Odaberi privatan ključ X_B $X_B < p$

Izračunaj javni ključ Y_B $Y_B = g^{XB} \bmod p$

Korisnik A generira tajni (simetrični) ključ

$K_{AB} = (Y_B)^{XA} \bmod p$

Korisnik B generira tajni (simetrični) ključ

$K_{BA} = (Y_A)^{XB} \bmod p$

Iz ovoga proizlazi da su se A i B dogovorili oko zajedničkog tajnog ključa

$$K = K_{AB} = K_{BA} = \mathbf{g}^{\mathbf{XA}\ \mathbf{XB}} \bmod \mathbf{p}$$

Na primjer, takav dijeljeni siguran ključ može biti korišten od algoritama DES. Diffie-Hellman algoritam koristi jednu od grupa kojom se definira dužina ključa koji se definira tijekom procesa. Duži broj znači jači ključ i koriste se Grupe 1, 2 i 14.

Oakley protokola definira nekoliko načina procesa izmjenu ključeva. Ovi načini odgovaraju dvjema fazama definiranim ISAKMP protokolom. U Fazi 1, Oakley prtokol definira dva principijelna modela, 'main' i 'aggressive'. IPsec u Windowsima koristi samo 'main' mode. Za Fazu 2 Oakley protokol definira 'single mod i 'quick' mod.

4.4.2. IKE

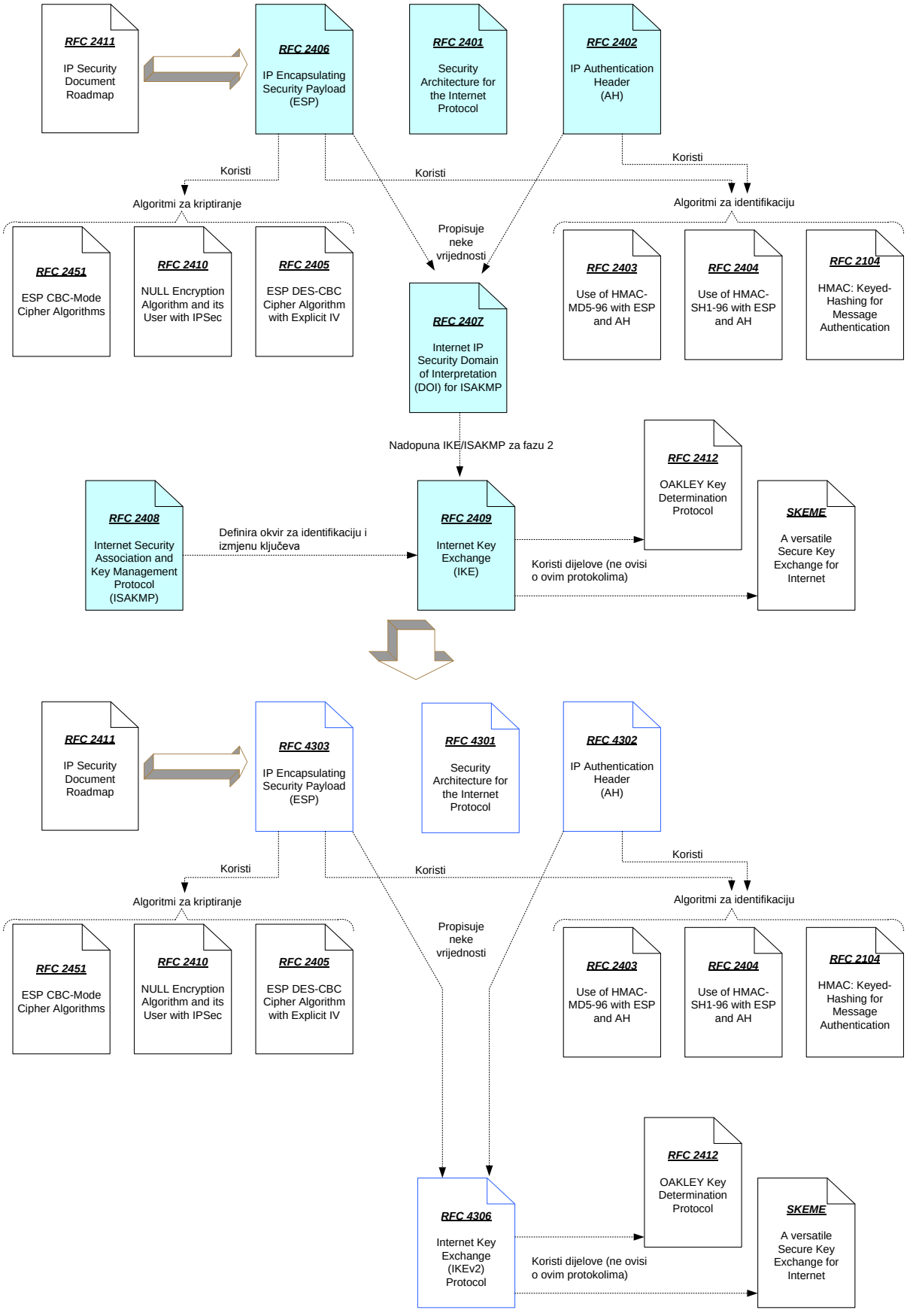
IKE protokol rješava najizraženiji problem pokretanja sigurne komunikacije - autentifikaciju krajnjih točaka i izmjenu simetričnih ključeva. IKE protokol stvara SA-e i dodaje ih u SAD[108] [29]. IKE protokol obično zahtijeva 'daemon'[109] i nije implementiran unutar operacijskog sustava. IKE protokol koristi port 500 i protokol UDP za svoju komunikaciju. Protokol funkcionira u dvije faze. Prva faza vrši uspostavu ISAKMP[110] SA. U drugoj fazi, ISAKMP SA se koristi za dogovor i postavljanje IPsec SA-a. Autentifikacija krajnjih točaka u prvoj se fazi se može dovijati s predefiniranim ključem (PSK – Pre-Shared Key) (samo kad se sustav implemetira i testira), s RSA ključeva i X.509 certifikata. Prva faza može se izvesti na dva načina, glavni (engl. main mode) i agresivni (engl. aggressive mode). Oba načina autentificiraju krajnje točke i uspostavljaju ISAKMP SA, ali agresivnim načinom se za to izmjeni dvostruko manje poruka između krajnjih točaka. Naravno da to povlači i nedostatke, jer agresivni način ne podržava zaštitu identiteta, pa je ovaj način ranjiv na 'man-in-the-middle' napad za slučaj kad se koristi PSK

[108] Engl. Security Policy Database
[109] Daemon (ili servis) je program čija je svrha raditi nešto u pozadini, bio korisnik prijavljen na računar ili ne. Glavna svrha servisa nije interakcija s korisnikom.
[110] Engl. Internet Security Association Key Management Security Association

autentifikacije. S druge strane, ovo i je jedini cilj agresivnog načina rada jer glavni način ne dozvoljava korištenje različitih preraspodjeljenih ključeva za nepoznate krajnje točke. Kako je rečeno, agresivni način rada ne podržava zaštitu identiteta, pa prenosi podatke o identitetu klijenta u nekriptiranom obliku. Stoga krajnje točke znaju s kime komuniciraju prije nego se izvrši autentifikacija i mogu odabrati odgovarajući predefinirani ključ za svakog pojedinog klijenta. U drugoj fazi IKE protokola vrši se izmjena zahtjeva za SA-ima i dogovor o SA-ima na temelju ISAKMP SA. ISAKMP SA pruža autentifikaciju da bi se zaštitio od 'man-in-the-middle' napada. Druga faza koristi takozvani brzi način rada (engl. quick mode). Obično dvije krajnje točke uspostavljaju samo jedan ISAKMP SA, koji se zatim koristi za dogovor oko nekoliko (najmanje dva) jednosmjerna SA-a.

4.5. IPSEC ARHITEKTURA

Skup RFC-ova koji su definirali arhitekturu i komponente IPsec-a te grupa RFC-ova koja sad definira IPsec prikazana je na slici 4.23. Promjene su nastale na dijelu komponenti koje su zadužene za autentifikaciju para i osiguravanje tajnoga ključa kao i ESP protokola.



Slika 4.23. RFC koji definiraju IPsec (izvor: vlastiti rad)

Ako se želi opisati mehanizam rada IPsec-a treba opisati nekoliko logičkih elemenata i to:

- Sigurnosne poveznice – SA,
- SA i mehanizam izmjene ključeva,
- IPsec protokoli,
- Algoritmi i metode.

4.5.1. SIGURNOSNE POVEZNICE

Kada dvije strane žele ostvariti sigurnu vezu, njihova IPsec implementacija mora znati dvije stvari:

- Što zaštiti?
- Kako to zaštiti?

Što želimo zaštiti definiramo kroz skup parametara koje nazivamo sigurnosna politika – SP. U ovom skupu parametara se nalazi izvorna i odredišna IP adresom para koji žele uspostaviti komunikaciju, tipom protokola višeg sloja (promet koji želimo zaštiti), smjerom komunikacije, tipom sigurnosnog protokola (AH ili ESP), načinom rada i dr. Jednom smjeru komunikacije pripada jedan takav zapis u SPD bazi. SP-ovi uvijek dolaze u parovima - za dvosmjernu komunikaciju potrebna su dva SP unosa u SPD bazu.

Kako definirati način da se promet zaštiti? Način kako se određena komunikacija štiti zapisano je u sigurnosnim poveznicama koje nastaju kao rezultat IKE protokola. SA je kombinacija međusobno prihvatljivih sigurnosnih postavki, mehanizama i ključeva za zaštitu komunikacije između IPsec para za danu SP. Svaka SA osigurava sigurnosni servis za jedan smjer protoka podataka. IPsec u komunikaciji koristi informacije iz dvije baze podataka: SPD i SAD[111]. U SPD se nalaze slijedeće informacije:

- Način na koji se IP paket može obraditi:
    - Odbaciti,

[111] Engl. Security Association Database

- Prihvatiti/proslijediti bez IPsec obrade,
- Prihvatiti/proslijediti s IPsec obradom, gdje se definira:
  - Da li će paket biti enkipritiran,
  - Da li će integritet paketa biti zaštićen,
  - Da li će paket biti enkriptira sa zaštićenim integritetom.

- Definiranje IP prometa kroz:
  - IP adresa odredišta,
  - IP adresa izvora,
  - Protokola,
  - Port izvora ili odredišta (TCP ili UDP).

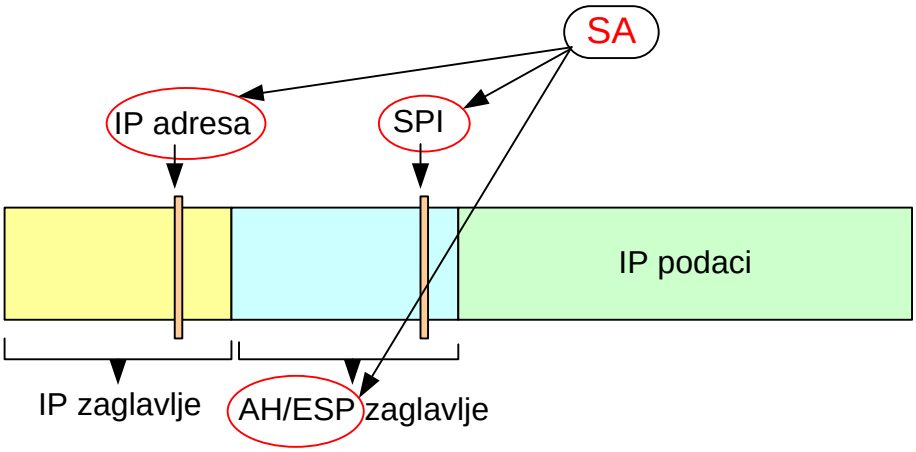
U SAD bazi se nalaze slijedeće informacije:

- Podatak o SPI,
- Kriptografskom ključu,
- Kriptografskom algoritmu,
- Sekvencijskom broju.

IKE protokol popunjava SAD bazu, dok se SPD baza popunjava ručno definiranim IPsec opcijama (prije prikazanu kroz grafičku konzoli).

4.5.2. IPSEC PROTOKOLI

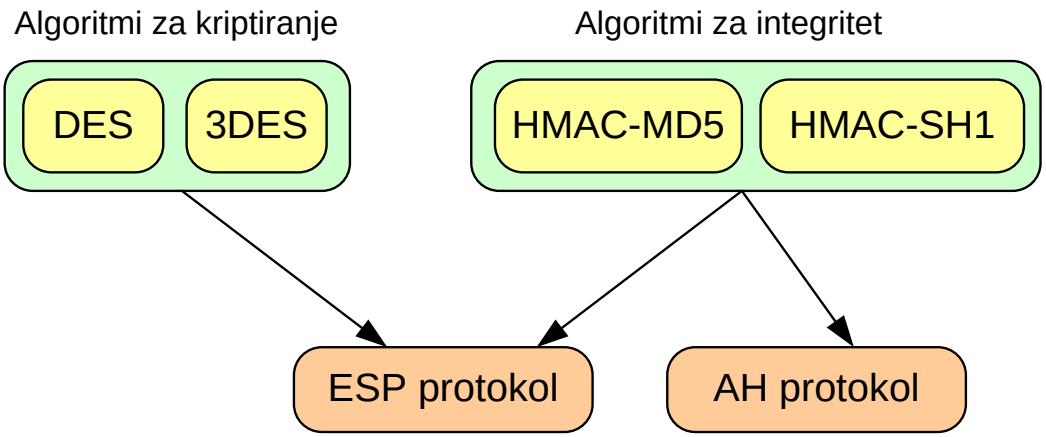
Za osiguranje IP mrežnog protokola IPsec definira dva protokola AH i ESP. Ovi protokoli osiguravaju sigurnosni servis za SA. Svaki SA se identificira s parametrom SPI, IP odredišnom adresom, identifikatorom sigurnosnog protokola (AH ili ESP). SPI je jedinstven i služi za identifikaciju SA kad je s parom uspostavljeno više sigurnosnih tokova podataka ili veza.. Na primjer, IPsec komunikacija između dva računala zahtjeva dva SA na svakom računalu. Jedan SA se odnosi na dolazni promet a drugi na odlazni promet, slika 4.24. Kako se radi o istoj IP adresi i istom sigurnosnom protokolu jedino je parametar SPI taj preko kojega razlikujemo o kojem se SA radi i koje ključevi za kriptiranje koristimo u kojem smjeru.



Slika 4.24. IPsec protokoli i SA (izvor: vlastiti rad)

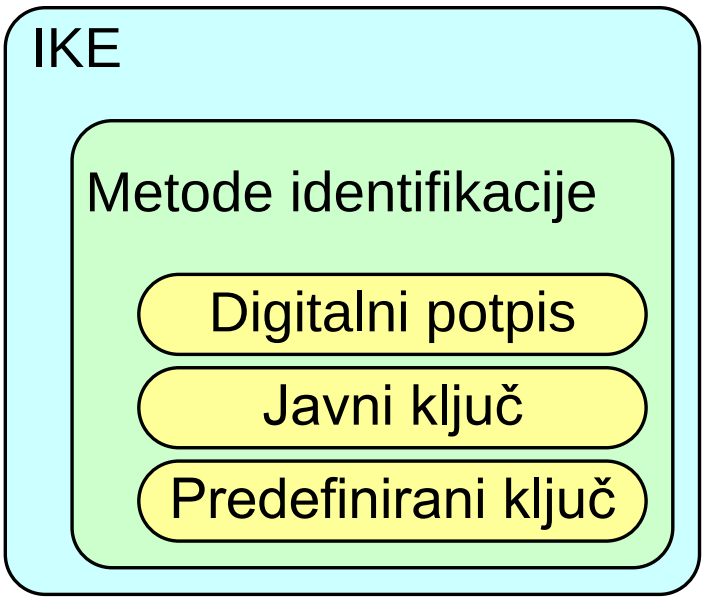
4.5.3. ALGORITMI I METODE

U IPsec protokolu koriste se algoritmi za integritet, kriptiranje i izmjenu ključeva. Algoritmi za integritet (hash algoritmi) koju se ovdje koriste su HMAC-MD5 (Hash Message Authentication Code - MD5) i HMAC-SHA-1. Oba algoritma koristimo u AH i ESP protokolu. Algoritmi za kriptiranje su DES i 3DES i koriste se u ESP sigurnosnom protokolu. Na slici 4.25. je prikazan odnos između algoritama i sigurnosnih protokola AH i ESP.



Slika 4.25. Odnos algoritama i sigurnosnih protokola (izvor: vlastiti rad)

Metode identifikacije IPsec protokola, koje su definirane kroz IKE protokol, grupirane su u tri kategorije, digitalni potpis, javni ključ i predefinirani ključ. Na slici 4.26. je prikazan odnos između IKE protokola i metode identifikacije.

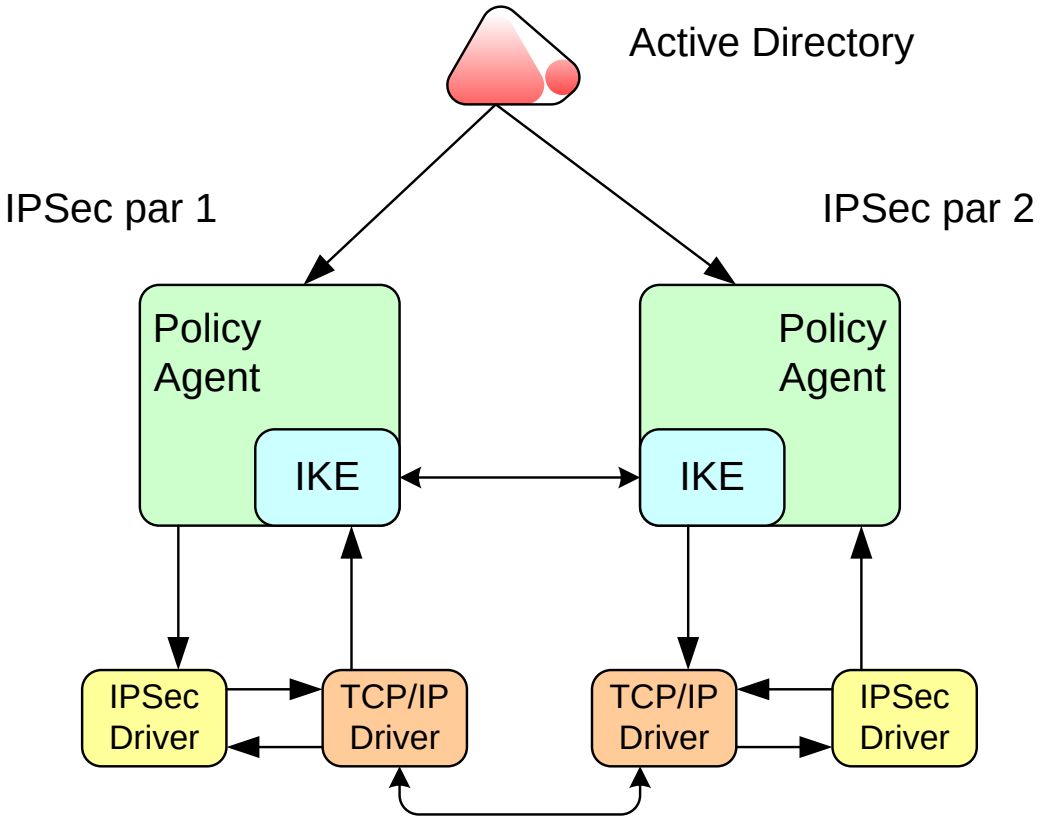


Slika 4.26. IKE protokol i metode identifikacije (izvor: vlastiti rad)

Arhitektura IPsec-a u Windows 2003 Serveru sastoji se od slijedećih komponenti:

- Active Directory,
- Policy Agent,
- IKE protokola,
- IPsec driver,
- TCP/IP driver.

Na slici 4.27. prikazan je međusobni odnos komponenti.



Slika 4.27. Arhitektura IPseca (izvor: vlastiti rad)

U tabeli 4.1 opisane su komponente.

Komponenta	Opis
Active Directory	U Active Directory se nalazi IPsec sigurnosne postavke za sva računala koja su članovi domene. IPsec postavke se isporučuju Policy Agentima i od njih se dobivaju iste
Policy Agent	Policy Agent dobiva IPsec postavke iz AD domene i konfigurira lokalne postavke. Distribuira identifikacijske i sigurnosne postavke IKA komponenti i IP filtru od IPsec driver-a.
IKE	IKE dobivene identifikacijske i sigurnosne postavke od Policy Agenta i čeka zahtjev za dogovaranje IPsec SA. Na zahtjev IPsec drive IKE dogovara obje vrste SA (main i quck mode) prema prije definiranim postavkama dobivenim od Policy Agent-a. Nakon dogovora oko SA, IKE šalje SA postavke IPsec drive.

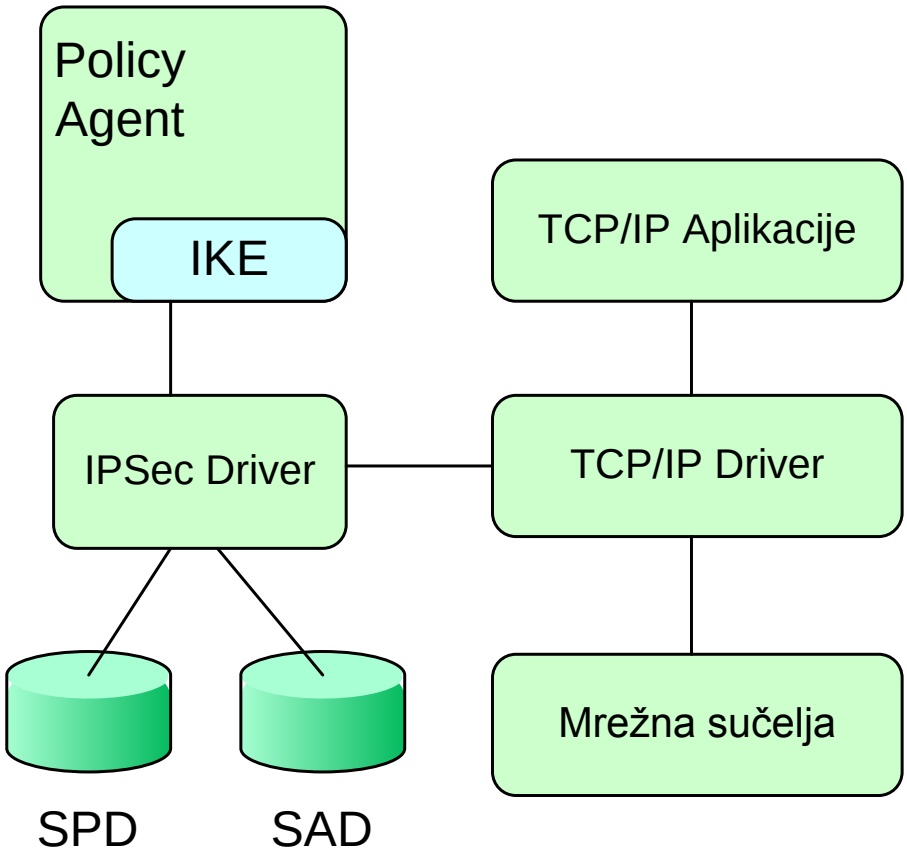
IPsec Driver	IPsec drive nadgleda i osigurava odlazni IP promet te nadgleda, dekriptira i provjerava ulazni IP promet. Nakon što IPsec drive primi postavke filtra od Policy Agenta on na osnovu njih odlučuje koje pakete će propustiti, koje blokirati a koje osigurati. Za osiguranje prometa koriste se aktivne SA postavke ili se da zahtjev za novim SA. IPsec driver je vezan s TCP/IP driver-om da se omogući obrada IP paketa koji prolaze kroz TCP/IP driver
TCP/IP Driver	TCP/IP driver je implementirani TCP/IP protokol.

Tabela 4.1. Opis komponenti IPsec arhitekture (izvor: vlastiti rad)

Detaljnije će biti opisan IPsec Driver. To je komponenta jezgre OS koja ima zadaću nadzora i osiguranja IP paketa. Osim prije spomenutih Policy Agenta i IKE, IPsec driver koristi i ove komponente:

- Security Association Database (SAD),
- Security Policy Database (SPD),
- TCP/IP driver,
- TCP/IP applications,
- Network interface.

IPsec Driver kontrolira IP pakete pomoću IP filtra čija se definicija nalazi u SPD. Ako paket ili promet mora biti osiguran koristi se odgovarajući SA koji definira na koji način se promet štiti ili se IKE moduli proslijedi zahtjev za SA. Nakon što IPsec driver odredi pravi SA slijedi provjera kriptiranja ili dekriptiranja, kreiranje ili interpretacija hash AH i ESP zaglavlja od IPsec zaštićenog paketa. Slika 4.28. prikazuje IPsec Drive arhitekturu i kako međusobno djeluju.



Slika 4.28. IPsec Drive arhitekturu (izvor: vlastiti rad)

U tabeli 4.2. dat je kratak opis komponenti IPsec driver.

Komponenta	Opis
SAD	IKE modul popunjava ovu bazu u kojoj se nalaze informacije o aktivnim SA, tj. parametri koji su dogovoreni
SPD	U ovoj bazi se nalaze definirane filtar liste i pripadne postavke kojima se definira statusi dolaznog i odlaznog prometa. Dolazni promet se provjerava da li je osiguran prema dogovorenim postavkama. Odlazni promet se dozvoljava, blokira ili osigurava. Informacija o vrsta osiguranja nalazi se u SA smještenim u SAD bazi.

TCP/IP driver	Implementacija TCP/IP protokola
TCP/IP aplikacije	Aplikacije koje koriste TCP/IP za pristup mrežnom servisu kroz neki od mrežni API koa što su Windows Sockets, NetBios, RPC
Mrežna sučelja	Logički i fizički definirana mrežna sučelja. Detalji o Network Driver Interface Specification (NDIS) sučelju, mrežnom driveru adaptera, fizičkom mediju preko kojega se IP paketi šalju i primaju se također nalaze u ovom modulu.

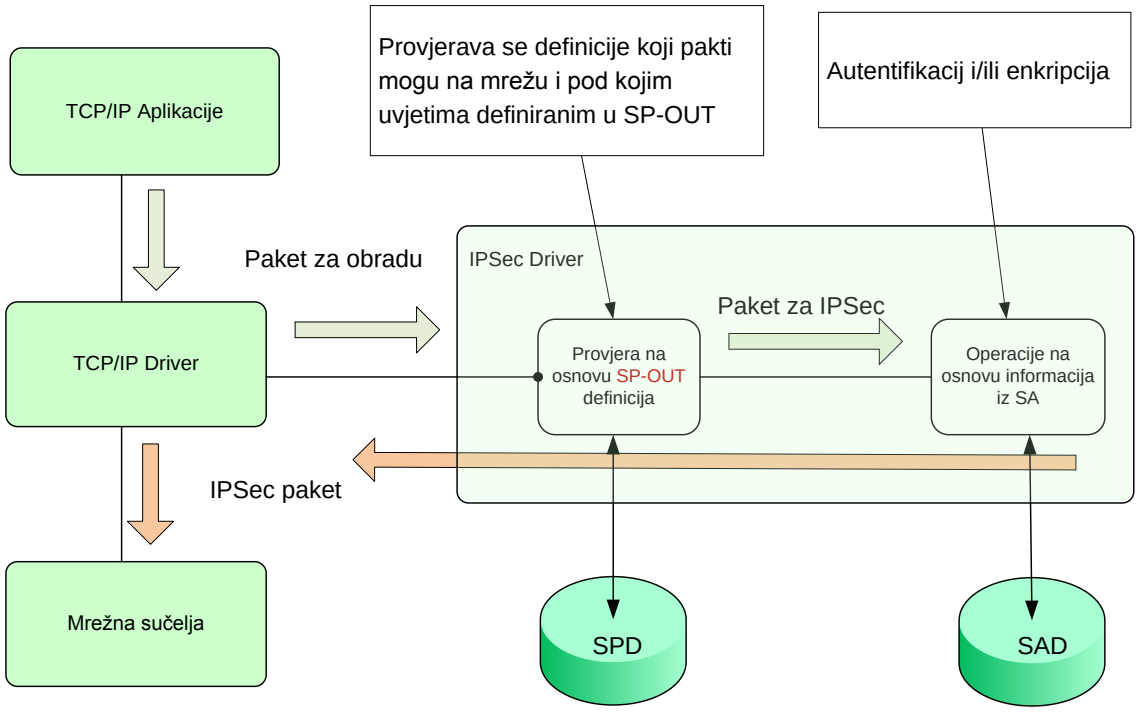
Tabela 4.2. Komponente IPsec Driver-a (izvor: vlastiti rad)

Prije detaljnijeg opisa kako teče komunikacija između para na mreži treba pojasniti kako se obrađuju dolazni i odlazni paketi. Obrada odlaznog paketa, slika 4.29., provodi se ovim redom:

1. Ponovno sastaviti paket,
2. Iz IP zaglavlja se izvlače informacije:
    a. IP adresa izvora,
    b. IP adresa odredišta.
    c. Port izvora.,
    d. Port odredišta (iz ovoga se vidi da je moguće izvući informacije za UDP i TCP protokole).
3. Ustanovi se SP u SPD za dobivene informacije iz IP zaglavlja,
4. U SAD se potraži par SA koji je vezan za identificiran SP,
5. Ako ne postoji SA par za taj SP, inicira se IKE protokol, koji nakon autentificiranja i dogovaranja sigurnosnih parametara kreira SA par,
6. Ako je SA u SAD pronađen onda se prije upotrebe provjerava vrijeme koje definira koliko se dugo dotični SA može koristiti prije nego se mora obnoviti. Ako je vrijeme isteklo pronađeni SA se briše iz SAD baze i inicira se IKE

protokol. Ako je SA valjani onda se paket modificira prema informacijama koje su sadržane u SA kako slijedi:

a. Primjeni se algoritam za kriptiranje na cijeli paket ili samo na dio paketa bez IP zaglavlja što ovisi da li je način rada tunel ili transport,
b. Dodaju se zaglavlja (enkapslulira) ESP/AH s prilagođavanje polja za slijedeći protokol, i sekvencijski broj za zaštitu od 'replay attacks' napada,
c. Ako je u procesu dogovaranja dogovoren i prijelaz preko NAT uređaja dodaje se i UDP zaglavlje,
d. Dodaje se novo (ili vanjsko) IP zaglavlje za tunel mod. Ako se za isti paket koristi ESP i AH onda se oba zaglavlja dodaju prije IP zaglavlja,
e. Tako kreirani paket se šalje van.

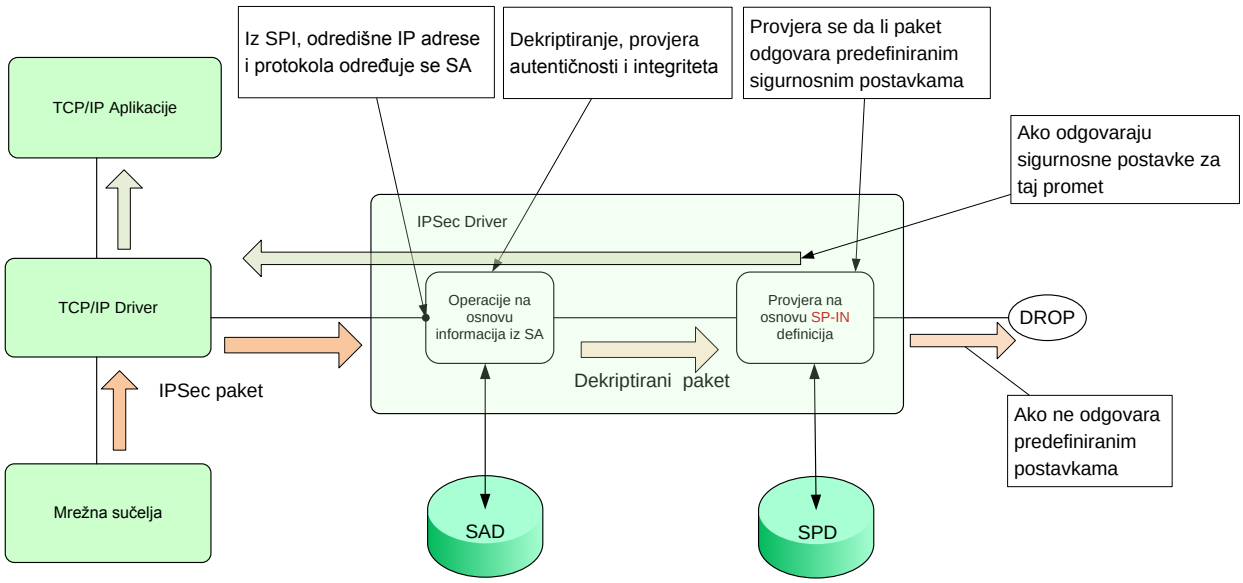


Slika 4.29. Obrada odlaznog paketa (izvor: vlastiti rad)

Obrada dolaznog paketa, slika 4.30., provodi se ovim redom:

1. Ponovno se sastavi paket,

2. Iz IP zaglavlja se izvuku informacije o protokolu i odredišnoj IP adresi. Ako se u zaglavlju nalazi informacija koja upućuje da je slijedeći protokol ESP ili AH i odredišna adresa pripada segmentu u kome se nalazi uređaju koji obrađuje paket tada se iz ESP ili AH zaglavlja izvlači informacija iz SPI polja. Ako postoji zaglavlje koje je dodano zbog NAT uređaja ono se preskače da bi se došlo do ESP ili AH zaglavlja,
3. Nađe se SA u SAD na osnovu informacije iz SPI, odredišne IP adrese i protokola,
4. Ovisno o modu (tunel ili transport), koristi se definirani sigurnosni algoritam na dijelu paketa. Nakon toga se miče ESP ili AH zaglavlje uz kontrolu informacija o 'replay attacks',
5. Ažurira se SA koristeći se informacijom o sekvencijskom broju.
6. Provjera se polje slijedećeg protokola. Ako je pronađen ESP ili AH protokol tada je potrebno ponoviti sve korake od koraka 2,
7. Ovaj se proces ponavlja sve dok paket ne bude čist (npr. da protokol nije AH ili ESP ili IP adresa odredišta nije u segmentu u kome se nalazi uređaj koji obrađuje paket),

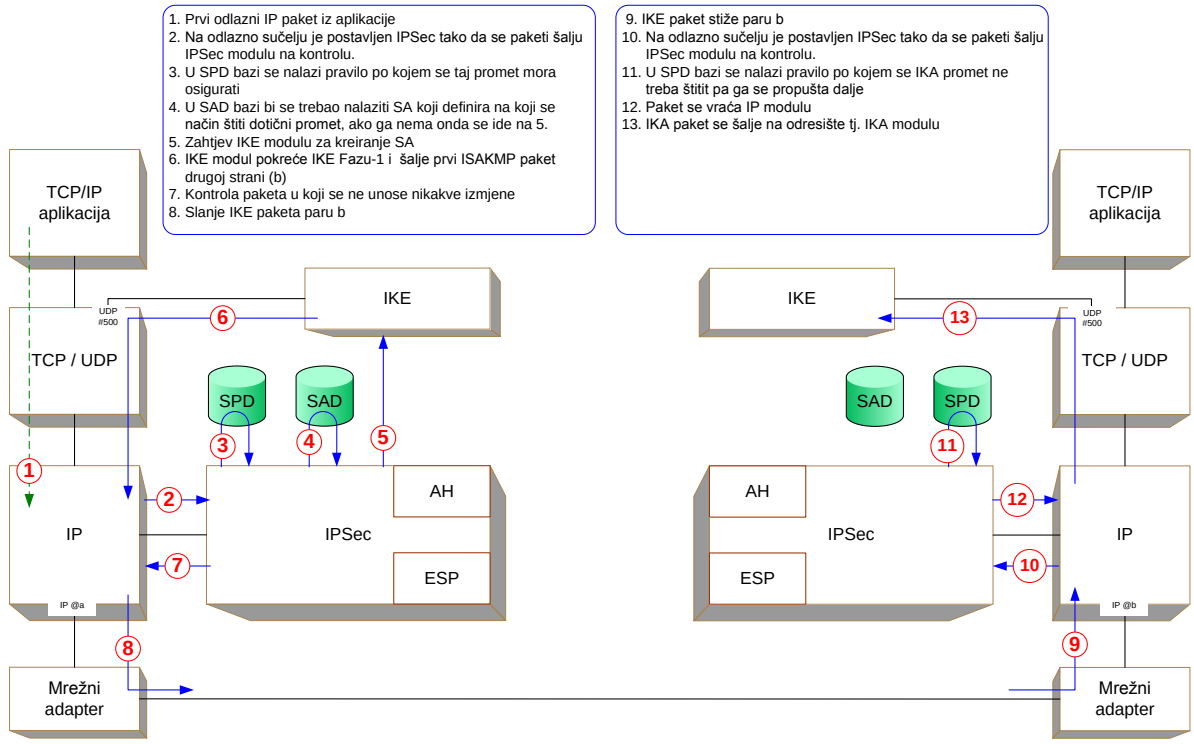


Slika 4.30. Obrada dolaznog paketa (izvor: vlastiti rad)

8. Izvlače se informacije koje se koriste u SPD bazi da se dobiju informacije o tome što treba uraditi s paketom, poslati ga dalje ili proslijediti višem sloju.

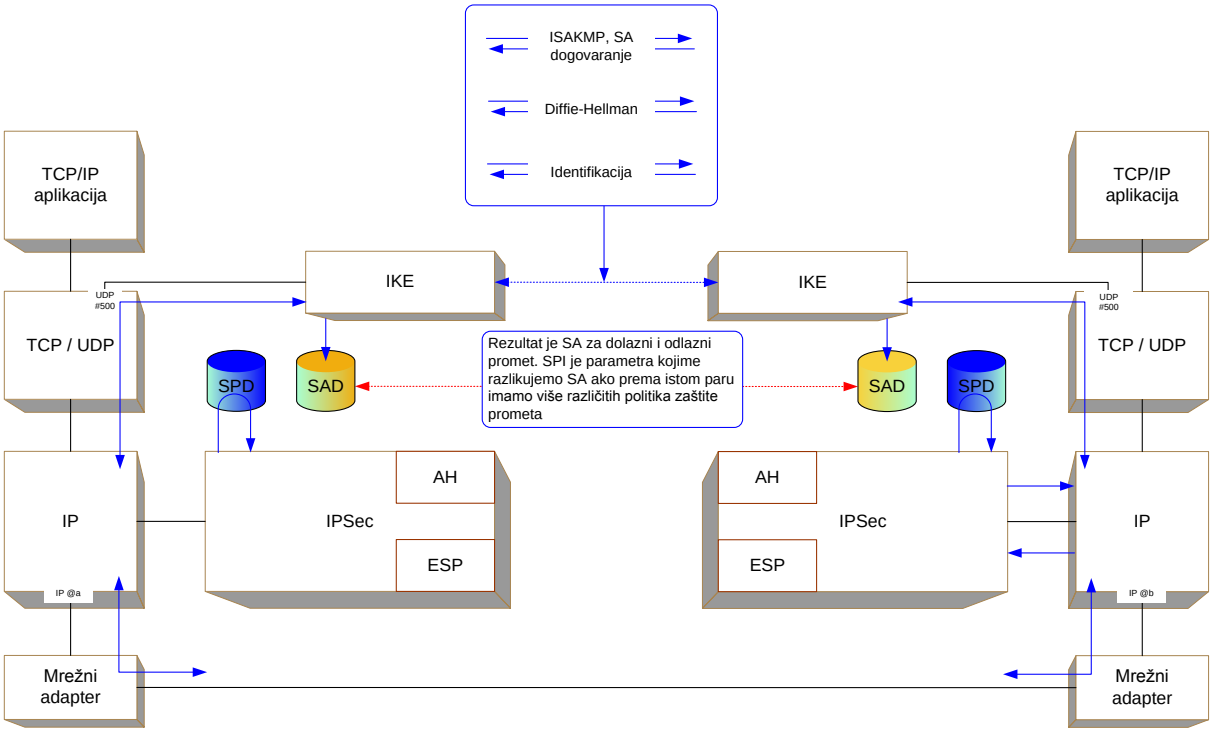
4.6. USPOSTAVA IPSEC KOMUNIKACIJE

Kako se uspostavlja i na koji način teče IPsec komunikacija prikazano je na slici 4.31. Ako se AD koristi za definiranje IPsec postavki i distribuciju na računala tada se kroz GPO definiraju sigurnosne postavke za promet. Ako ne, postavke se definiraju na računalu kroz konzolu. Kroz sigurnosne postavke definiramo što će se štititi i popunjavamo SPD bazu. Na slici 4.31. prikazana je situacija kad prvi paket krene s višeg nivo. Aktiviranje IPseca na računalu postavljen je IPsec modul kroz koji prolaze paketi prije nego se predaju na mrežu. Paket koji prolazi kroz IPsec modul uspoređuje se sa zapisima u SPD bazi gdje je definirano koji promet se štititi. Ako je pristigli paket dio prometa koji želimo štititi provjerava se SAD baza da se nađe zapisa koji definira način na koji će se promet štititi. Ako tog zapisa nema, daje se nalog IKE modulu da s drugom stranom dogovori parametre po kojima će se promet štititi. ISAKMP paket se šalje paru s prijedlogom parametara za komunikaciju. Na drugoj strani paket prolazi isti put tj. paket se kontrolira i uspoređuje sa zapisima u SPD bazi. Kako nema potrebe da se IKE promet štiti propušta se dalje i dolazi do IKE modula.



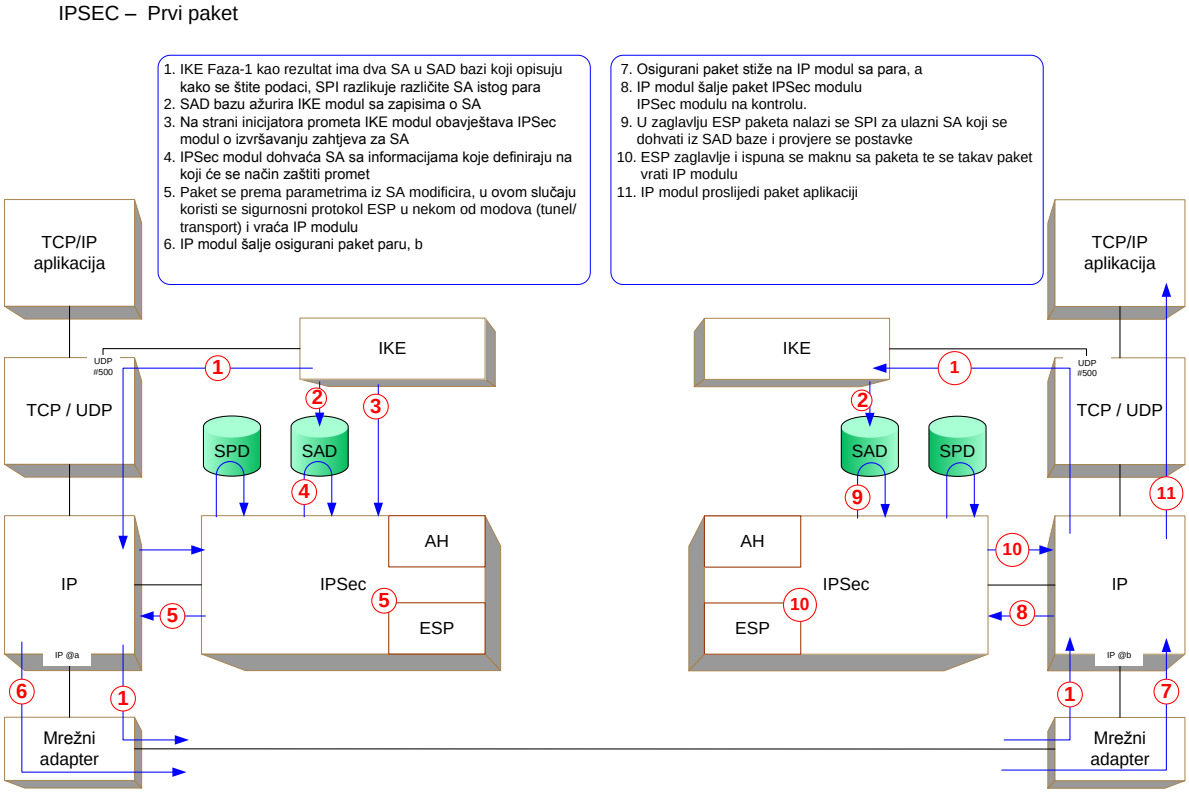
Slika 4.31. IKE Faza 1 (izvor: vlastiti rad)

Na slici 4.32. prikazani su paketi koji se izmjenjuju između para za vrijeme dogovaranja parametara komunikacije. Rezultat je kao što se iz slike vidi popunjavanje SAD baze gdje sad postoji zapis koji definira na koji način će biti štićen određeni promet.



Slika 4.32. IKE Faza 1 (izvor: vlastiti rad)

Na slici 4.33. prikazan je nastavak komunikacije za prvi paket koji još čeka u IPsec modulu. IKE je ispunio nalog i popunio SAD bazu te tako definirao na koji način će biti paket zaštićen. Paket se prema definiranim parametrima mijenja i kao takav se predaje mrežnom adapteru za slanje. Kad tako modificirani paket stigne na drugu stranu proslijedi se IPsec modulu koji iz zaglavlja saznaje vrijednost SPI parametra. Ovaj parametar je nastao u IKE fazi dogovaranja i kao zapis se nalazi u SAD bazi. Dohvaća se iz baze i provjeravaju se postavke. Nakon što se maknu dodatna zaglavlja i eventualne ispune paket se vrati IP modulu koji ga proslijedi aplikaciji.



Slika 4.33. IPsec komunikacija (izvor: vlastiti rad)

4.7. IPSEC REDUNDANCIJA

Jedno od pitanja koje se često postavlja jesu dodatni resursi koje IPsec zahtijeva. Osim zahtijeva za procesorskim resursima, IPsec također povećava ukupan mrežni promet što je očito ako se IPsec datagrami promatraju u odnosu na standardne IP datagrame. Povećanje mrežnog prometa, odnosno redundancija (engl. *overhead)* koju IPsec unosi, a što može rezultirati degradacijom mrežnih performansi, proizlazi iz dva funkcionalna razloga:

- Zbog dodatnih zaglavlja koja se mogu pojaviti u različitim načinima IPsec rada,
- Zbog kriptografskih algoritama koji se koriste, odnosno ispune (engl. *padding)* koja je nužna za njihovo ispravno funkcioniranje.

4.7.1. REDUNDANCIJA ZAGLAVLJA

Redundancija zaglavlja ovisi o načinu rada IPsec-a, kao i o IPsec protokolima koji se koriste. Korištenje AH protokola (ukoliko se koriste propisane *hash* funkcije MD5 ili SHA-1) unosi redundanciju od 24 okteta od čega 12 okteta otpada na zaglavlje bez

polja *autentifikacijski podaci,* dok preostalih 12 okteta (96 bita) otpada na to polje koje sadrži ICV vrijednost generiranu od strane *hash* funkcija. Ovdje valja napomenuti da iako MD5 daje izlazni rezultat duljine 128 bita a SHA-1 160 bita, te se vrijednosti za potrebe IPsec-a svode na 96-bitni duljinu.

Ukoliko se koristi ESP protokol, redundancija ovisi o tome da li se ESP koristi samo za osiguravanje tajnosti, ili služi također za osiguranje integriteta, neporecivosti i autentifikacije poruke. Također, redundancija ovisi i o kriptografskom protokolu koji se koristi. ESP zaglavlje samo po sebi dodaje 8 okteta.

4.7.2. REDUNDANCIJA ISPUNE

Redundancija ispune ovisi o IPsec protokolima koji se koriste, odnosno direktno o kriptografskim algoritmima i *hash* funkcijama koje su odabrane u SA skupu sigurnosnih parametara. Ta ispuna je nužna iz razloga što kriptografski algoritmi i *hash* funkcije kao ulaz koriste blokove fiksne duljine, čija duljina ovisi o specifičnom algoritmu koji će se koristiti. Kod kriptografskih algoritama (DES, 3DES, AES) to konkretno znači da će svaki datagram imati ispunu takvu da IP datagram bude poravnat na 64 bitni odnosno 128 bitni blok. Kod *hash* funkcija (MD5 i SHA-1), zbog implementacijske specifičnosti, datagram će biti poravnat na 448 bitni blok. Razlog tome je što oba algoritma ulaznim podacima implicitno dodaju 64-bitni blok podataka, što skraćuje duljinu ulaznog bloka koji može biti procesuiran u *hash* funkciji.

4.8. IMPLEMENTACIJSKI PROBLEMI

IPsec protokol, sam po sebi donosi neke probleme koje je ponekad, u specifičnim mrežnim okruženjima teško ili nemoguće riješiti. To se prvenstveno odnosi na korištenje NAT-a, te IP fragmentaciju koja se može pojaviti prilikom IPsec komunikacije.

4.8.1. NAT

Obzirom na poznata ograničenja adresiranja kod IPv4 protokola, velik broj lokalnih mreža koristi privatno adresiranje, a pristup Internetu, odnosno udaljenim lokacijama,

implementira se korištenjem NAT-a (engl. *Network Address Translatiori)* koji može biti statički ili dinamički, odnosno NAPT-a (engl. *Netvork Address Port Translatiori).*

Ukoliko se između entiteta koji žele uspostaviti IPsec komunikaciju provodi NAT, korištenje AH u transportnom ili u tunelskom načinu rada to neće biti moguće pošto će provođenje NAT-a rezultirati narušavanjem integriteta IP datagrama i uzrokovati njegovo odbacivanje na strani primatelja. Ukoliko se za IPsec koristi samo ESP, stvar je donekle drugačija. U transportnom načinu rada provođenje NAT-a također će rezultirati nemogućnošću ostvarivanja IPsec komunikacije. U tunelskom modu ESP može funkcionirati. IPsec za rješenje ovog problema koristi *NAT-Traversal*, tj. zaobilaženje utjecaja NAT-a. Zaobilaženje se izvodi na način da se ESP pakete enkapsulira unutar UDP paketa. Računalo koje vrši NAT bez problema će razlikovati stvorene UDP pakete prema portrovima. Pretpostavljene port je 4500 za UDP protokol.

Pri korištenju NAT-a pažnju valja obratiti i na IKE/ISAKMP, jer autentifikacija temeljena na tajnom ključu koristi i kolačiće koji se generiraju ovisno o IP adresi entiteta, što također rezultira gubitkom integriteta, te nemogućnošću uspostave komunikacije. Ovaj se nedostatak može riješiti korištenjem drugih IKE autentikacijskih metoda (korištenje digitalnih potpisa ili kriptografije temeljene na javnim ključevima).

4.8.2. FRAGMENTACIJA

Pri korištenju IPsec komunikacije, prvenstveno u tunelskom načinu rada, a isto tako i IKE/ISAKMP komunikacije, može doći do IP fragmentacije. U tom slučaju mogu se pojaviti dodatni problemi. Naime, neki vatrozidi ili usmjerivači mogu biti konfigurirani da odbacuju IP fragmentirane datagrame, jer na taj način osiguravaju mrežu od nekih oblika DoS napada (npr. *Teardrop*[112]*).* Očiti problem kod toga jest da će u tom slučaju i legitimni IPsec ili IKE paketi isto biti odbačeni, što će onemogućiti uspostavu sigurnog kanala među udaljenim entitetima

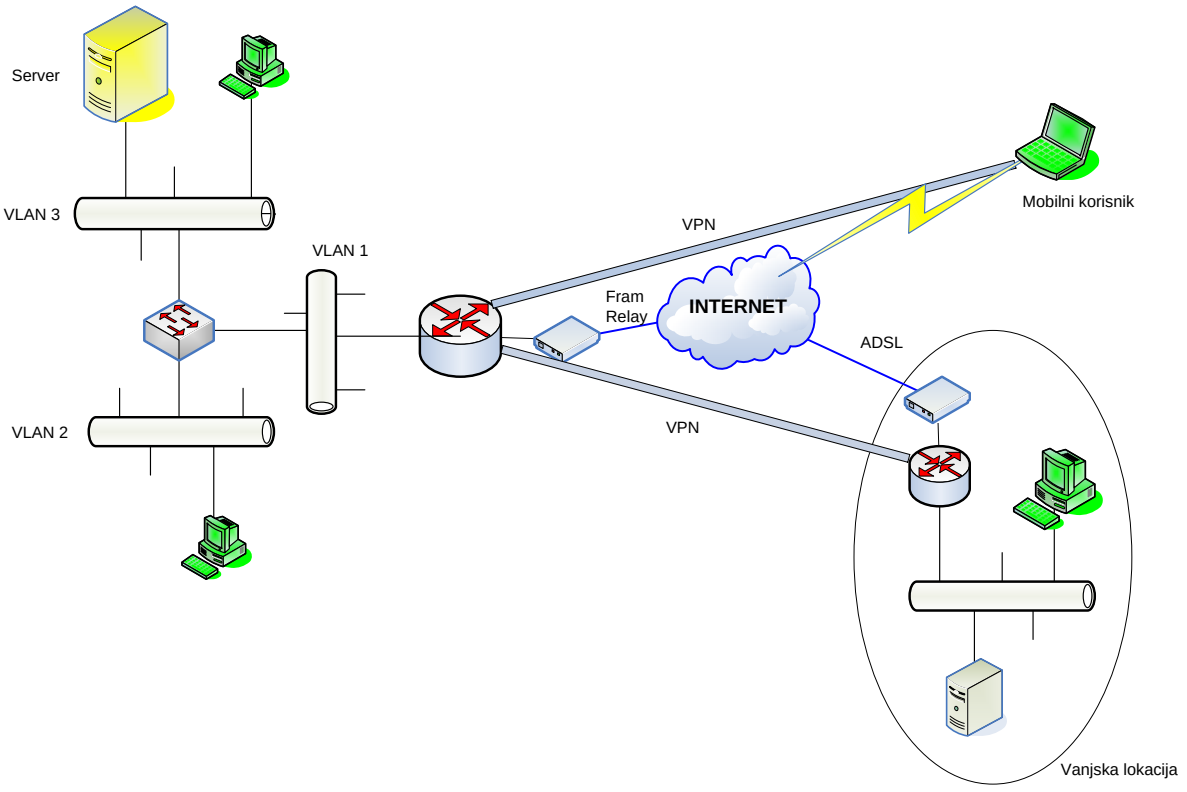
[112] Ovaj tip DoS napada iskorištava način na koji IP protokol paket koji je preveliki za router dijeli na fragmente

5. MODEL ZA ISPITIVANJE UČINKOVITOSTI IPSEC-A

Nakon što je korisnik informacijskog sustava promatran u kontekstu unutrašnji počinitelj i mogućih prijetnji koje može na razna načine provesti na sustavu pokazana je metoda koju Microsoft predlaže za povećava sigurnost informacijskog sustava. Protokol na kome se zasniva ovo metoda je IPsec. Teoretske osnove IPsec-a su date s ciljem da se razumije kako protokol funkcionira te da budu jasne sigurnosne opcije koje treba definirati tijekom implementacije. Da se ocjeni koliko ovaj alat stvarno doprinosi u smanjivanju prijetnji promatrat će se ponašanje određenih servisa, programa i prometa na model. Na modelu koji odražava realnu situaciju nekog informacijskog sustava analizirat će se provedba prijetnji s kakvom učinkovitošću se one smanjuju.

5.1. MODEL

Izgled modela prikazan je na slici 5.1. Na slici je prikazan sustav na kome s elementima koji se nalaze u standardnim informacijskim sustavima [4].



Slika 5.1. Model za procjenu učinkovitosti IPsec-a

Na serveru se nalazi Oracle baza i njemu pristupaju svi korisnici s lokalne mreže. U lokalnoj mreži postoji centralni switch koji ima mogućnost kreiranja VLAN-ova tako da korisnici pristupaju i iz različitih mrežnih segmenata. Vanjski korisnici podacima pristupaju preko VPN[113] koji se ostvaruje na dva načina. Prvi je da dio korisnika koji se nalaze na lokalnoj mreži koji preko VPN servera uspostavlja vezu s VPN serverom centralne lokacije i na taj način omogućava svim korisnicima s tog segmenta pristup podacima. Drugi način se odnosi na mobilne korisnike koji ostvaruju VPN vezu s centralnim VPN serverom i pristupaju željenim podacima. Softver korišten u modelu prikazan je u tabeli 5.1.

Server		
	Operacijski sustav	Windows 2003 Server
	Baza podataka	Oracle 10g
Klijent		
	Operacijski sustav	Windows XP Professional
		Windows Vista Business
Switch	Cisco	Cisco WS-C3550-48isco
VPN server	Centralna lokacija	Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(3f)
	Vanjska lokacija	Cisco IOS Software, C1700 Software (C1700-K9O3SY7-M), Version 12.3(8)T6
VPN klijent		VPN Client version 5.0.01.0600

Tabela 5.1. Softverska konfiguracija modela

5.2. PRIJETNJE ZA ANALIZU

Prijetnje koje će se analizirati na ovom modelu biti će samo one za koje postoji realna pretpostavka da se mogu smanjiti ili ukloniti ovom tehničkom metodom, a to su slijedeće:

[113] Engl. Virtual Private Network

Prijetnje i načini provedbe		Mogućnosti IPsec-a
Neovlašteno otkrivanje lozinki drugih osoba		
	Dešifriranje lozinki s računalnih sustava	-
	Uvid u nešifrirane lozinke	-
	Pogađanje lozinki	-
	Uvid u sadržaj prometa po mreži (sniffing)	+

Tabela 5.2. Neovlašteno otkrivanje lozinki drugih osoba (izvor: vlastiti rad)

Tabela 5.2. prikazuje prijetnju od otkrivanja lozinki drugih osoba. Načina izvođenja ove prijetnje ima više, na modelu će biti analizirana situacija kad se do korisničkih podataka pokušava doći uvidom u sadržaj prometa na mreži.

Prijetnje i načini provedbe		Mogućnosti IPsec-a
Neovlašteno korištenje sigurnosnih alata		
	Korištenje alata u svrhu prikupljanja informacija o sustavu	+

Tabela 5.3. Neovlašteno korištenje sigurnosnih alata (izvor: vlastiti rad)

Tabela 5.3. prikazuje prijetnje od neovlaštenog korištenja sigurnosnih alata za prikupljanje informacija o sustavu.

Prijetnje i načini provedbe		Mogućnosti IPsec-a
Prisluškivanje komunikacijskog tijeka		
	Instalacija hardverskog 'keylogger' alata	-
	Instalacija softverskog 'keylogger'	+-
	Korištenje 'sniffing' alata	+-

Tabela 5.4. Prisluškivanje komunikacijskog tijeka (izvor: vlastiti rad)

Tabela 5.4. prikazuje prijetnju prisluškivanja komunikacijskog kanala. Način provedbe gdje bi IPsec pomogao je prvenstveno za slučaj kad se radi o alatima za analizu paketa po mreži. Kad se radi o 'keylogger' izvedenog hardverski IPsec nam ne bi mogao pomoći. Kad se koristi softversko rješenje 'keylogger' ovisno o načinu

sakupljanja informacija IPsec bi mogao pomoći. Ako se podaci snimaju u datoteku i ručno sakupljaju tu nam tehničko rješenje ne bi mnogo pomoglo. Ako je definirano pravilo po kome sav odlazni promet mora biti kriptiran mogli bi smanjiti opasnost od ove prijetnje uz uvjet da nije vezan uz program za automatsko slanje elektroničke pošte.

Prijetnje i načini provedbe	Mogućnosti IPsec-a
Pojava ili unošenje malicioznih programa	
Namjerno unošenje računalnog virusa	+
Namjerno unošenje Trojanaca ili Backdoor programa	+
Izvođenje 'hackerskih' napada	+

Tabela 5.5. Pojava ili unošenje malicioznih programa (izvor: vlastiti rad)

Tabela 5.5. prikazuje prijetnju kojom korisnik namjerno unosi zlonamjerni program i pokušava ostvariti željeni cilj. Prema načinu na koji se prijetnja može izvesti korištenje kriptiranog prometa može osigurati zaštitu rizičnih resursa na način da je pristup moguć samo za definirane grupe korisnika ta definirani promet. Sav ostali promet neće biti prihvaćen. Problem može biti ako se zlonamjerni program pokrene s takvih resursa a nije definirana politika u kojoj sav promet mora biti kriptiran. Kao dodatak ove prijetnje je za slučaj kad će se IPsec promatrati kao maliciozni program. Pretpostavka je da unutrašnji počinitelj želi pristup resursu s različitih lokacija i da kontrola sadržaja paketa neće ukazati na kompromitaciju sustava.

Prijetnje i načini provedbe	Mogućnosti IPsec-a
Neovlašteni logički pristup	
Pristup pomoću lozinke otkrivene na nedozvoljeni način	+-
Pristup dijeljenim pristupnim pravima	+-
Pristup pomoću važećih ali nekonzistentnih prava	+-
Pristup 'default' korisničkim pravima	+-

	Pristup 'backdoor' korisničkim pravima	+-
	Pristup temeljem iskorištavanja sistemskih ranjivosti	+-
	Zloupotreba administratorskih prava	-

Tabela 5.6. Neovlašteni logički pristup (izvor: vlastiti rad)

Tabela 5.6. prikazuje prijetnju od neovlaštenog logičkog pristupa. Prema načinu izvođenja ove prijetnje postoji mogućnost da se prijetnja smanji uz korištenje IPsec-a uz uvjet da se uz autentifikaciju veže i računalo. U tom slučaju će pristup resursima biti moguć uz poznavanje pristupnih podataka samo s definiranih računala.

Prijetnje i načini provedbe		Mogućnosti IPsec-a
Neovlašten uvid u povjerljive podatke		
	Uvid u sistemske podatke	+-
	Uvid u povjerljive podatke koji su u strukturiranom obliku	+-
	Uvid u povjerljive podatke koji su u nestrukturiranom obliku	+-
	Nestandardna pretraga podataka	+-

Tabela 5.7. Neovlašten uvid u povjerljive podatke (izvor: vlastiti rad)

Tabela 5.7. prikazuje prijetnju od uvida u povjerljive podatke. Kad se radi o nestrukturiranim podacima moguće je koristiti IPsec. Uvjet da se opasnost od prijetnje smanji zahtjeva definiranje kriptiranog prometa za pristup takvom resursu uz kvalitetnu autetifikaciju.

Prijetnje i načini provedbe		Mogućnosti IPsec-a
Sabotaža		
	Unošenje destruktivnog programa	+-
	Narušavanje integriteta hardverskog okruženja	-
	Narušavanje integriteta softverskog okruženja	-

Tabela 5.8. Sabotaža (izvor: vlastiti rad)

Tabela 5.8. prikazuje prijetnju koja može biti posljedica sabotaže. Kao i u slučaju vandalizma kontrola pristupa je metoda koja će zaštiti vrijedne resurse poduzeća.

Ako korisnik posjeduje ovlasti onda će bez obzira da li se promet kriptira moći pokrenuti svaki destruktivni program lokalno ili s udaljene lokacije.

Prijetnje i načini provedbe		Mogućnosti IPsec-a
Prikrivanje podataka o nedozvoljenim aktivnostima		
	Neovlašteni pristup i/ili izmjena evidencijskih zapisa	+-
	Sigurno brisanje podataka s diskovnog prostora	-
	Prikrivanje identiteta u komunikaciji	-

Tabela 5.9. Prikrivanje podataka o nedozvoljenim aktivnostima (izvor: vlastiti rad)

U tabeli 5.9. prikazana je prijetnja vezana uz prikrivanje tragova o nedozvoljenoj aktivnosti. Kriptirani promet će biti od koristi ako se sustav za nadzor nalazi na računalu kojemu se može pristupiti samo određenim kriptiranim prometom. Ako se korisnik nalazi na tom računalu onda neće biti problem da obriše tragove svojih aktivnosti.

Ostale prijetnje neće biti razmatrane iz razloga što tehnička metoda tj. alat kojime se povećava sigurnost ne može biti zamjena za tehničku zaštitu kontrole pristupa, nedostatak propisanih politika i procedura i internu reviziju i sl.

5.3. REVIZIJSKI PRISTUP KONTROLI IPSEC-A

ISACA[114]-in „Vodič za reviziju informacijskih sustava— (eng. *IS Audit Guidelines*) daje upute o primjeni IS[115] Auditing Standarda na VPN na jedan sistematičan i jednostavan način temeljen na SDLC[116] metodologiji, odnosno na životnom ciklusu razvoja sustava. Ovaj koncept revizijskog pristupa oslanja se na CONCT[117], kontrolni ciljevi za mrežno orijentiranu tehnologiju, ISACF (istraživački dio ISACA-e), 1999, kao referentni okvir za kontrolne ciljeve koji su u vezi s VPN-om. Važno je napomenuti da je CONCT naslonjen, odnosno usklađen i s COBIT[118]-om.

[114] Engl. Information Systems Audit and Control Association
[115] Informacijski sustavi
[116] Engl. System Development Life Cycle
[117] Engl. Control Objectives for Net Centric Technology
[118] Engl. Control Objectives for Information and related Technology

Osnovni koncept VPN tehnologije je implementacija sigurnog medija između privatnih mreža, a preko javne mreže. Sigurnost VPN-a temelji se na šifriranju. Cilj je ograničiti pristup podacima koji se prenose samo odgovarajućim korisnicima, odnosno računalima [9].

Proces enkapsulacije jednog tipa paketa u drugi tip paketa, formiranjem sigurnog tunela preko nesigurnog javnog medija (Interneta), zove se tuneliranje. Na taj način se osigurava siguran prijenos čitavih paketa preko javnih ili privatnih mreža.

Osnovni ciljevi revizijskog postupka ili revizije VPN-a su utvrditi jesu li zadovoljena osnovna tri principa sigurnosti:

- Povjerljivost informacija,
- Cjelovitost podataka,
- Raspoloživost ili dostupnost sustava.

u odnosu na ukupne troškove implementiranog modela VPN-a (eng. *cost-effective model*). Takav pristup reviziji temelji se na procjeni rizika koji su povezani s korištenjem VPN-a. Stoga se moraju uzeti u obzir slijedeći tipova rizika:

- Sigurnosni rizik (eng. *security risk*),
- Utjecaj treće strane (eng. *third party risk*),
- Poslovni rizik (eng. *business risk*),
- Implementacijski rizik (eng. *implementation risk*),
- Operativni rizik (eng. *operating risk*).

U ovoj metodi provođenja revizije VPN-a, baziranoj na procjeni rizika, revizor se treba usredotočiti na postojeće potencijalne ranjivosti u odnosu na te rizike i to u svakoj od faza provođenja revizije VPN-a.

No, prije toga revizor IS-a, treba prikupiti sve relevantne informacije vezane uz poslovanje firme u kojoj se radi revizija VPN-a i sve poslovne zahtjeve za uspostavom VPN-a, kako bi jasno definirao opseg i revizijske ciljeve revizije VPN-a.

5.3.1. PROCES PROVOĐENJE REVIZIJE VPN-A

Proces provođenja revizije VPN-a može se podijeliti na pet faza:

1. Pred implementacijska faza,
2. Implementacijska faza,
3. Post implementacijska faza,
4. Pisanje izvješća,
5. Praćenje provedenih korektivnih aktivnosti.

Općenito gledajući, ova revizija VPN-a se oslanja na metodologiju ocjenjivanja životnog ciklusa razvoja sustava (SDLC) tijekom kojih se provodi procjena rizika te adekvatna revizijska testiranja unutar osnovnih faza sustava: dizajna, razvoja i implementacije. Kao i kod svake revizije, procjena rizika i revizijski testovi trebaju biti potpuno dokumentirani, kako bi potkrijepili revizorsko mišljenje, kao i sve slabosti kontrola.

5.3.1.1. Pred implementacijska faza

Ovaj dio revizijskog procesa provodi se tijekom perioda od dokumentiranja zahtjeva za VPN-om do dovršenja njegovog razvoja. Glavni kontrolni ciljevi tijekom ove faze uključuju slijedeće:

- Utvrditi dali dokument koji definira zahtjeve za VPN-om, sadrži cost-benefit analizu (odnosno, analizu koristi predložene tehnologije u odnosu na troškove implementacije iste) uključujući model i konfiguraciju hardvera i softvera, sigurnosne zahtjeve, primjenu redundancije, uključujući zahtjeve za kontinuitetom sustava, zakonske zahtjeve i posljedice te uključivanje bilo koje treće strane,
- Utvrditi dali dokument dizajna uključuje detaljne planove načina i metoda koje bi zadovoljile sigurnosne i zakonske zahtjeve za postizanje svrhe i ciljeva poslovnih zahtjeva koji se očekuju od VPN sustava i IT sustava, zahtjeve za integracijom ostalih softvera, automatizirani način monitoriranja i izvještavanja menadžmenta o mogućim problemima, definiranje potrebe funkcioniranja i održavanja sustava te za kreiranje revizijskih tragova (eng. audit trails) pomoću

kojih se mogu vršiti naknadne analize. Treba utvrditi da li su svi mjerodavni zahtjevi sadržani u dokumentu dizajna,

- Utvrditi da dokument koji definira razvoj i testiranje VPN-a uključuje detalje koji se odnose na programiranje (kodiranje) sučelja, eventualno uvođenje vanjskog softvera u testno okruženje, implementaciju sigurnosnih pravila i audit trails. Nadalje, treba utvrditi jesu li svi elementi dizajna cross-referencing metodom verificirani kao dio dokumenta razvoja. Testna dokumentacija treba potvrditi ispunjavanje svih zahtjeva i elemenata dizajna. Na kraju, IS auditor treba verificirati da su potrebe za osposobljavanjem ljudi dio razvoja te da su mu dodijeljeni odgovarajući resursi, uključujući funkcije i zahtjeve održavanja. Kao i u svim SDLC revizijama, tako i u ovoj, IS auditor treba verificirati da je dokumentirano odobrenje odgovarajuće razine vlasnika poslovnog procesa i IT višeg menadžmenta, čime se potvrđuje uspješno izvršenje svake faze prije prelaska na sljedeću fazu. Sastavni dio revizorskog mišljenja treba biti utvrđivanje da li menadžment projekta ima kontrolu nad praćenjem napretka, troškovima i kvalitetom projekta.

5.3.1.2. Implementacijska faza

Ovaj dio revizijskog procesa provodi se tijekom perioda testiranja rješenja u testnom okruženju i implementacije tog rješenja u produkcijsko okruženje. Glavni kontrolni ciljevi tijekom ove faze uključuju procjenu napredovanja projekta u odnosu na plan projekta, predviđene troškove i adekvatnost odabrane tehnologije, uključujući slijedeće:

- Adekvatnost i djelotvornost sigurnosnih shema (eng. security shames) i tehnologije kriptiranja,
- Utvrđivanje udovoljavanja zahtjevima za određeni nivo usluge, kao što su potreba za redundancijom i backup uređaji,

- Zadovoljavanje svih zakonskih zahtjeva.

Nadalje, ostali standardni ciljevi kontrole obično uključuju verifikaciju adekvatnosti izvršenog testiranja, odobrenje i migraciju VPN-a u produkcijsko okruženje. Također, nedostaci zapaženi u ranijim fazama (npr. punch list – popis nezavršenih poslova), trebaju biti provjereni, kako bi se utvrdilo jesu li se dogodile ikakve korektivne akcije kojima se ublažio eventualni rizik.

5.3.1.3. Post implementacijska faza

Ovaj dio revizijskog procesa provodi se nakon perioda implementacije VPN-a u produkciju, i to ovisno o vremenskom periodu koji je prošao nakon implementacije, revizor će ocijeniti da li je prošlo dovoljno vremena od implementacije rješenja, kako bi period u produkciji bio reprezentativan. Glavni kontrolni ciljevi tijekom ove faze uključuju procjenu, da su dobiti i funkcije VPN-a u skladu s onima koji su originalno definirani. Posebno IS revizor u ovoj fazi treba utvrditi slijedeće:

- Jesu li planiranim koristima postignuti efikasnost i djelotvornost,
- Da li je korištenje VPN-a u skladu sa sigurnosnim politikama i procedurama (npr. jeli upotrebom IPsec-a osigurana povjerljivost podataka), uključujući klasifikaciju podataka,
- Jesu li na snazi svi ugovorni sporazumi, uključivši i one koji se odnose na extranet, s aspekta sigurnosti i povjerljivosti,
- Provjerava li se i nadzire li se usklađenost s ugovorima o razini usluga (eng. Service Level Agreements), i da li se, ako se pojave problemi, isti podižu na nivoa akcije menadžmenta? (npr. jeli uspostavljen proces problem menadžmenta),
- Jesu li uspostavljene dodatne sigurnosne mjere, kao što su provjera virusa i otkrivanje upada (eng. Intrusion Detection),
- Jesu li uspostavljene kontrole neprekidnosti poslovanja (eng. Continuity Controls) i da li se periodički testiraju.

Kao i kod implementacijske faze provođenja revizije, i u ovoj fazi je potrebno utvrditi jesu li nedostaci zapaženi u ranijim fazama (npr. punch lista) praćeni, kako bi se utvrdilo jeli bilo ikakvih korektivnih mjera u cilju ublažavanja rizika.

5.3.1.4. Pisanje izvješća

U ovom djelu revizijskog procesa, trebaju se formalizirati opseg, ciljevi, metodologija provođenja revizije i nalazi, koji trebaju biti potkrijepljeni dokazima pronađenim tijekom provođenja revizijskog procesa. Također, menadžment treba biti obaviješten o slabostima kontrola, čim se njihova slabost ili nedostatak uoče.

5.3.1.5. Praćenje provedenih korektivnih aktivnosti

U ovom dijelu revizijskog procesa, revizor treba pratiti provođenje svih planove i akcije koje je utvrdio i donio menadžment u cilju ublažavanja i otklanjanja rizika.

5.4. MODIFIKACIJA REVIZIJSKOG POSTUPKA IPSEC-A

Poglavlje o reviziji VPN daje dobar primjer kako bi se trebalo pristupati realizaciji projekta koji ima za cilj povećanje sigurnosti informacijskog sustava. Realna situacija u proizvodnim organizacijama je da se u projekte vezane uz informatičku i telekomunikacijsku infrastrukturu ide prvenstveno zbog smanjivanja troškova. Sigurnosnu komponentu, ako ima priliku, onaj tko vrši implementaciju stavi u drugi plan dok su korisniku bitne performanse i funkcionalnost i često nije ni svjestan posljedica zanemarivanja sigurnosti. Da se izbjegnu problemi koji će prije ili kasnije isplivati na površinu dobro je znati kako se provode revizorski postupak. Razlog je u dobrom pristupu praćenja postupka implementacije, poslova koje treba obaviti i zahtjeva koje treba zadovoljiti da rješenje na kraju bude kvalitetno, dokumentirano i da zadovoljava sve zahtjeve koji se pred njega postave na početku projekta. Ova znanja bi korisniku dala mehanizam kojim bi se od implementatora tražila dodatna objašnjenja, dokumentacija i zadovoljenje sigurnosnih

zahtjeva. Ovaj stav je rezultat projekta implementacije VPN IPsec-a u kome je neznanja korisnika implementator iskoristio i implementirao rješenje koje zadovoljava zahtjeve za funkcionalnošću ali je zanemarena sigurnosna komponenta.

Kako je to prvenstveno revizorska metoda njezinom modifikacijom i prilagođavanjem korisniku koji sam implementira rješenje ili definira zahtjeve dobila bi se metoda koja garantira korisniku da će u projektu pokriti sve zahtjeve koje će eventualna revizija tražiti da budu zadovoljeni. Osim toga korisnik ima metodu koja mu garantira sistematsko pristup u procesu implementacije. Korištenje alata za detekciju VPN IPsec implementacija na sustavu koje koriste revizoru daje korisniku kvalitetan alat za kontrolu pojedinih faza implementacije.

Prikazana metodologija revizije IPsec-a ovdje neće biti korištena jer izlazi iz okvira ovoga rada zbog toga što cilj nije napraviti reviziju implementacije IPsec-a već detektirati prisustvo VPN servera i analizirati realizacije prijetnji na model prije i nakon implementacije IPsec-a. Za otkrivanje VPN servera [40] koristit će se alat 'ike-scan'[119] kad IPsec bude promatran kao zlonamjerni program koga je unutrašnji počinitelj implementirao u sustavu. Na modelu će se kroz praktičan primjer pokazati kako IPsec utječe na smanjenje pojedinih prijetnji i tu neće biti korištena neka poznata metodologija.

[119] Dostupan na http://www.nta-monitor.com/tools/ike-scan/ (10.12.2007)

6. ANALIZA IPSEC-A NA MODELU

Analiza IPseca na modelu će se provesti u dva koraka. U prvom koraku IPsec će biti promatran kao 'zlonamjeran program'. U ovom poglavlju će biti prikazano kako se IPsec ponaša na modelu i na koji način ga je moguće otkriti. Ovoga treba biti svjestan kad se odlučuje o verziji IPsec-a koja se implementira na sustav. U drugom koraku (slijedeće poglavlje) IPsec će biti promatran kao alat za smanjivanje prijetnji od unutrašnji počinitelj, na modelu će biti analizirana njegova učinkovitost.

6.1. IPSEC KAO ZLONAMJERNI PROGRAM

Zbog krivog vjerovanja da korištenjem IPseca [32][33], za uspostavu sigurnih kanala i razmjenu podataka, imamo siguran sustav potencijalnim napadačima se olakšava djelovanje. Ovakvi sustavi se ne testiraju redovito iako se za njih objavljuju pronađeni sigurnosni propusti i ranjivosti. Treba biti svjestan činjenice da je VPN interesantan napadaču zbog slijedećeg [34]:

- VPN-om se prenose povjerljive informacije kroz nesigurnu okolinu. Korisnici generalno vjeruju da su informacije u VPN sigurne jer je s tom namjenom i izgrađen VPN. Zbog tog vjerovanja se kroz takve kanale prenose povjerljive informacije bez da se koristi dodatno kriptiranje. Često se koriste protokoli koji informacije za identifikaciju prenose u čistom tekstu,
- Spajanje s udaljenih lokacija četo osigurava puni pristup resursima interne mreže. Zbog konfiguriranja VPN servera na način da omogući puni pristup internoj mreži osiguravamo napadaču da kompromitiranjem VPN servera ima nesmetan pristup do svih resursa,
- VPN promet je često nevidljiv za IDS - sustava za otkrivanja napada. Zbog smještaja IDS ispred VPN servera, IDS ne može vidjeti promet

unutar VPN tunela zato što je kriptiran. Kompromitiranje VPN servera zaobilazi se IDS sustav bez bojazni da aktivnosti budu otkrivene,

- Povećavanje sigurnosti ostalih područja. Kako se mnogi javno dostupni servisi sele u DMZ, implementiraju se sustavi za automatsko implementiranje zakrpa i sl., VPN postaje sve zanimljivija meta.

6.1.1. OPĆI SIGURNOSNI PROPUSTI VPN

Mnogi VPN serveri odaju svoj identitet bilo kroz 'UDP Backoff fingerprinting[120]' ili 'Vendor ID fingerprinting[121]'. Neki proizvođači smatraju da ovo nije neki problem što je istina, no dobivene informacije mogu koristiti napadaču za planiranje napada. Neki sistem daju samo opće informacije, imena proizvođača, dok neki daju informaciji i o verzijama implementiranog softvera.

6.1.1.1. Nesiguran smještaj identifikacijskih podataka

Nesiguran smještaj identifikacijskih podataka od VPN klijenta je također sigurnosni problem. Da bi se VPN konekcija jednostavnije i lakše ostvarila neki VPN klijenti nude mogućnost spremanja identifikacijskih podataka (korisničko ime i lozinka) ili im je to predefinirana postavka. Iako je povećana funkcionalnost smanjili smo sigurnost jer se te informacije spremanju na mjesta koja nisu dobro zaštićena. Mjesta gdje se obično ovi podaci smještaju su:

- Spremanje identifikacijskih podataka u datoteku ili registar[122]. Svatko tko dođe na to računalo može doći do tih podataka. Ako klijent koristi IKE Agresiv Mod za uspostavu konekcije s VPN serverom onda poznavanje korisničkog imena omogućava offline krekiranje lozinke,
- Spremanje kriptirane lozinke. Kriptiranje nije prava riječ koja opisuje oblik lozinke kako se pohranjuje u registru jer se u pretvorbi ne koristi

[120] Vrsta identifikacije na osnovu UDP
[121] Vrsta identifikacije na osnovu informacije o proizvođaču
[122] Registar (Engl. Registry) je velika kompleksna struktura od temeljnog značaja za ispravan rad operativnog sustava

ključ. Koristi se neki algoritam koji lozinku prikazuje u nečitljivom obliku i ako se dozna o kojem se algoritmu radi onda je jednostavno doći do lozinke,

- Spremanje identifikacijskih podataka u čistom tekstu u memoriju. Ako se identifikacijski podaci nalaze u registru u neprepoznatljivom obliku neki VPN klijeti ih pretvaraju u čitljive i spremaju u memoriju. U ovom slučaju napadaču je dovoljno pokrenuti VPN klijenta i spremiti sadržaj memorije s nekim od alata za tu namjenu, recimo '*pwdump*[123]'. Ili je dovoljno izazvati pad računala da bi se došlo do sadržaja memorije,
- Slaba zaštita registra ili datoteke s podacima. Iako je loša izbor smještaj identifikacijskih podataka u registru ili datoteku još je lošije imati njihovu slabu zaštitu. Dozvoliti bilo kojem korisniku da dođe do ovih podataka veliki je sigurnosni propust.

6.1.2. PENETRACIJSKO TESTIRANJE IPSEC

Cilj penetracijskog testiranja je otkriti ranjivosti u VPN implementaciji koje se kasnije mogu iskoristiti za napad. Da bi to saznali potrebno je na dijelu mreže koju testiramo pronaći sve VPN server, detektirati o kojoj se implementaciji radi (IPsec, SSL, PPTP,…) i po mogućnosti o kojoj verziji.

6.1.3. OTKRIVANJE VPN SERVERA

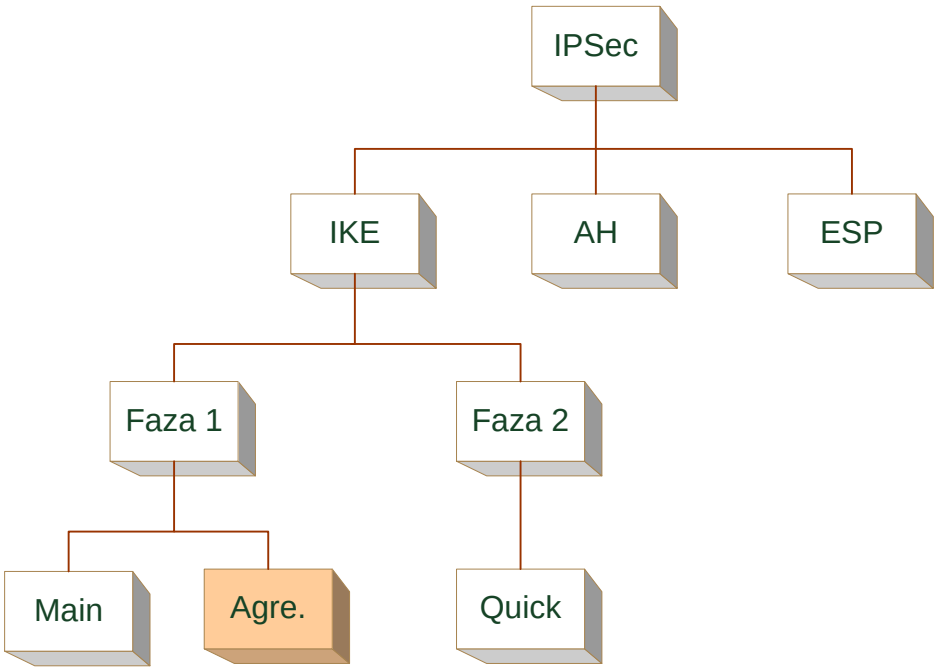
Kako je već prije spomenuto alata za otkrivanje VPN servera, dobivanje informacije o VPN serveru i testiranje je 'ike-scan'. Konstruiran je da pošalje inicijalni paket (IKE Faza 1) na definirani host i prikaže bilo kakav odgovora koji dobije. Ovaj alat omogućava [35]:

- Slanje paketa na proizvoljan broj odredišta uz mogućnost reguliranja odlaznog prometa (bandwith) što je korisno kad se radi o skeniranju velikog broja hostova),

[123] Program koji uzima SAM (Secutiry Account Manager - sadrži podatke o korisnicima računala, sažetke lozinki, ovlasti, te još neke podatke), dekodira ga, te ga takvog sprema u svojem formatu

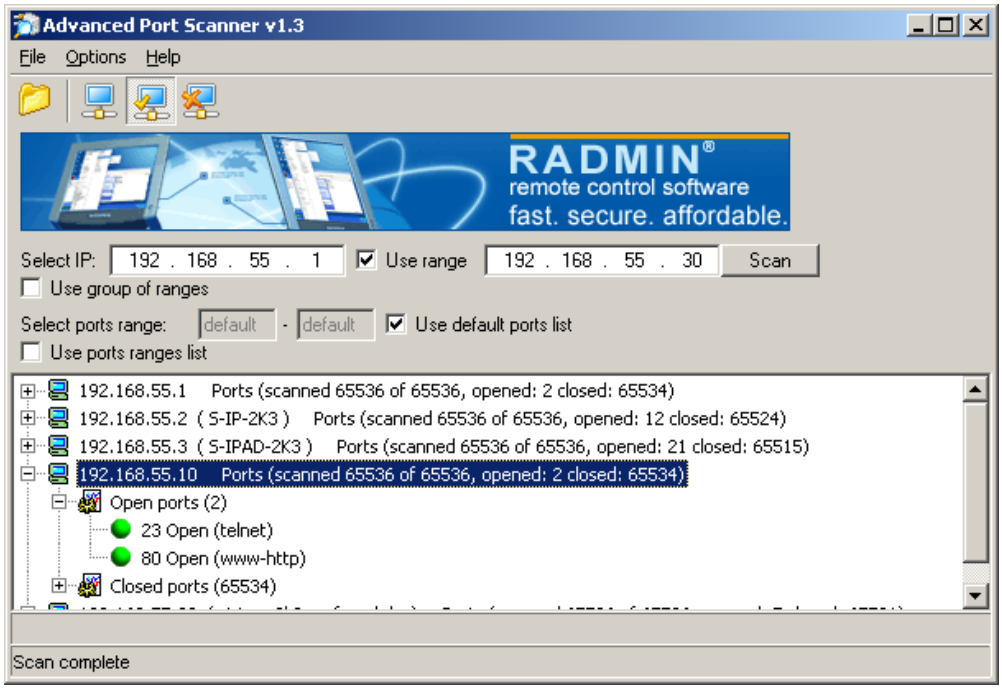
- Konstruiranje odlaznih IKE paketa na jednostavan način s mogućnošću kreiranja paketa koji nisu po RFC zahtjevima,
- Prikaz bilo kakvog odgovora,
- Mogućnost krekiranja predefiniranog ključa kad se IKE Faza 1 odvija u agresivnom modu. Koristi se hash vrijednost koja se ne prenosi kriptirana.

Da bi pripremili vezu za korištenje AH i ESP sigurnosnih protokola, potrebno je dogovoriti neke sigurnosne parametre. Ovo se odvija kroz 'protokol' IKE gdje se provodi identifikacija i dogovaranje ključeva u dvije faze, kako je to prikazano na slici 6.1. U prvoj fazi se izvrši identifikacija para i izmjene se ključevi dok se u drugoj uspostavi sigurnosni kanal kojime će se izmjenjivati podaci. Prva faza se odvija na dva načina dok se druga odvija na jedan. Sigurnosni problemi prvenstveno mogu nastati u 'Agresiv' modu kad se za identifikaciju koristi predefinirani ključ gdje se zbog brzine uspostavljanja veze zanemaruje sigurnost.



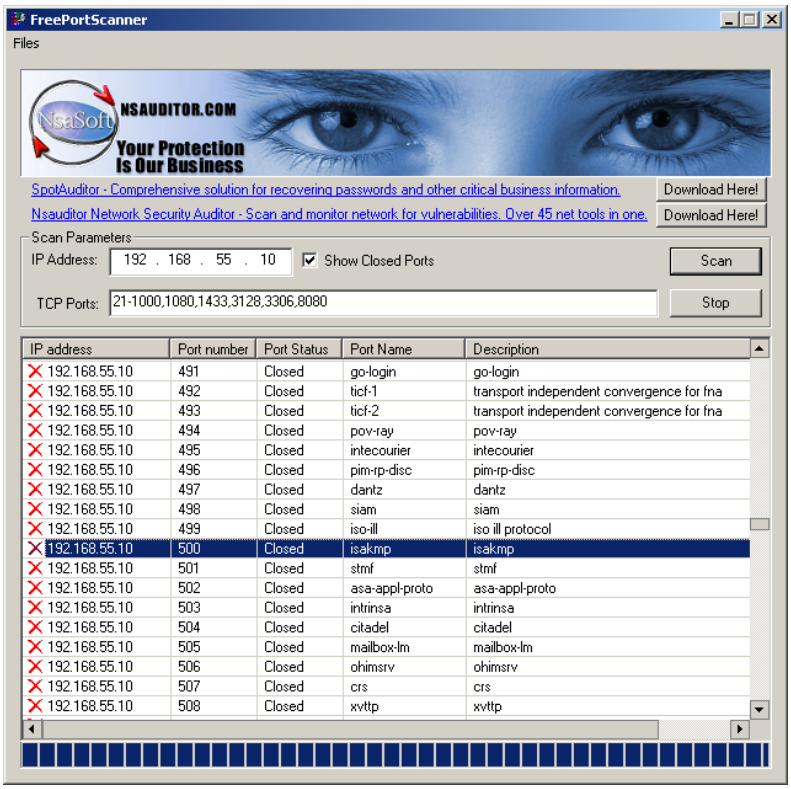
Slika 6.1. Agresiv mod (izvor: vlastiti rad)

U ovom se modu hash vrijednost predefiniranog ključa prenosi nekriptiran. Kako se zajedno s ovom informacijom prenosi i informacija o algoritmu koji se koristi u kreiranju hash vrijednosti ostaje nam samo da korištenjem neke od metoda (library, brute-force) dođemo do vrijednosti predefiniranog ključa i mogućnosti da sami ostvarimo vezu s VPN serverom. Ovaj mod rada je opcionalan i neke implementacije ga ne podržavaju. Prvenstveno se upotrebljava kod uspostavljanja veza mobilnih korisnika i VPN servera. IPsec VPN server nije moguće naći standardnim skenerima za otvorene portove. Korištenjem standardnih, besplatno dostupnih alata za skeniranje portova, kao što je Advanced Port Scanner [124], slika 6.2. i FreePortScanner [125] slika 6.3.



Slika 6.2. Skeniranje portova (izvor: vlastiti rad)

[124] Skinuto sa http://www.famatech.com/products/utilities/portscanner.php (21.11.2007)
[125] Skinuto sa http://www.softpedia.com/get/Network-Tools/Network-IP-Scanner/FreePortScanner.shtml (21.11.2007)



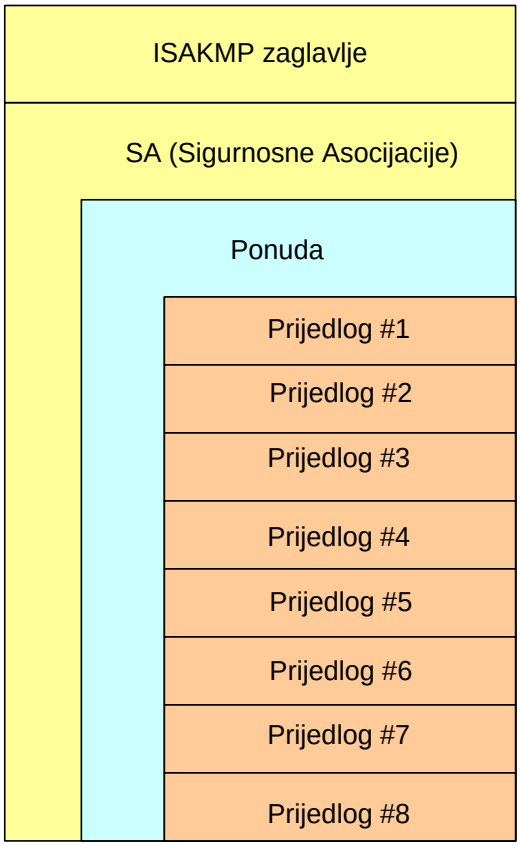
Slika 6.3. Skeniranje portova (izvor: vlastiti rad)

Razlog leži u činjenici da nema servisa koji sluša i čeka na nekom TCP portu. UDP skeniranje neće dobiti odgovor (ICMP 'unreachable[126], poruku) s porta 500 gdje se standardno ostvaruje konekcija, nit će IP skeniranje uhvatiti pakte koja će imati u zaglavlju informaciju o protokolima 50 ili 51 (AH ili ESP). Efikasan način da se detektira IPsec VPN server je slanje korektno formatiranog IKE paketa i prikaz bilo kakvog IKE odgovora. Ova metoda je u stanju otkriti željene informacije uz uvjet da IKE odgovor nije uvjetovan određenom IP adresom.

6.1.4. UPOTREBA IKE-SCAN ALATA S PREDEFINIRANIM POSTAVKAMA

Da bi se otkrio VPN sistem 'ike-scan' [36][37] šalje korektno formatirane IKE pakete svakom hostu kojeg želimo provjeriti. Paket je konfiguriran za Main mod, kako je prikazano na slici 6.4.

[126] Nedostupan



Slika 6.4. Main mode (izvor: [28])

Iza ISAKMP zaglavlja slijedi SA teret u kome se nalazi jedna ponuda s nekoliko prijedloga ili kombinacija. Struktura paketa definirana je RFC 2408. Ovih 8 prijedloga u sebi sadrži kombinaciju slijedećih atributa, tabela 6.1.:

Atribut	Vrijednost
Algoritam za kriptiranje	DES ili 3DES
Hash algoritam	MD5 ili SHA1
Metoda identifikacije	Pre-Shared Key (PSK)
Diffie-Hellman grupa	1 ili 2
SA Lifetime	28800

Tabela 6.1. Kombinacije u ponudi (izvor: [28])

Kako to izgleda po pojedinom prijedlogu prikazano je u tabeli 6.2.

Broj prijedloga	Algoritam za kriptiranje	Hash algoritam	Metoda identifikacije	Diffie-Hellman grupa	Lifetime (secund)
1	3DES	SHA1	PSK	2 (1024 bit)	28800
2	3DES	MD5	PSK	2 (1024 bit)	28800

3	DES	SHA1	PSK	2 (1024 bit)	28800
4	DES	MD5	PSK	2 (1024 bit)	28800
5	3DES	SHA1	PSK	1 (768 bit)	28800
6	3DES	MD5	PSK	1 (768 bit)	28800
7	DES	SHA1	PSK	1 (768 bit)	28800
8	DES	MD5	PSK	1 (768 bit)	28800

Tabela 6.2. Prijedlozi za Main mode (izvor: [28])

Ako takav upit pošaljemo na segment mreže možemo dobiti slijedeće odgovore, prikazano na slici 6.5.

Slika 6.5. Ike-scan s paketom za Main mode (izvor: [28])

Sama naredba ima opciju –M što znači da će svaki odgovor biti prikazan u posebnoj liniji. Prvi host je odgovorio s 'Notify' porukom koja znači da sistem sa nama ne žili dogovoriti oko sigurnosnih postavki. Razlozi tome mogu biti da nismo pogodili pravu kombinaciju prijedloga ili se server odgovara samo s predefiniranim IP adresama. Kako je ovo korak kad se želi samo otkriti koji hostovi imaju implementiran IPsec VPN onda je ova informacija dovoljna. Drugi host je odgovorio s prihvaćanjem jednog od prijedloga. Postoji i treća situacija kad nam host uopće nije odgovorio zato što neke implementacije odgovaraju samo na dobro definirane prijedloge.

6.1.5. PROMJENA PRIJEDLOGA

Zbog toga što postoje implementacije koje će odgovoriti samo na dobro definiran prijedlog potrebno je promijeniti atribute ponuda. Treba naći prihvatljiv prijedlog u pravilnom redoslijedu da dobijemo odgovor.

Iako postoji više atributa u praksi ih je dovoljno promatrati četiri, algoritam za kriptiranje, hash algoritam, metodu identifikacije i Diffe-Hellman grupe. SA

Lifetime može ostati kako je predefiniran, 28800 sec., jer je obično prihvatljiva vrijednost. Kako je svaka od ove četiri atributa definirana 16-bitnim brojem koji može definirati 65536 različiti vrijednosti pa sad to kombinirati između njih dobivamo jako veliki broj mogućih kombinacija (oko 18 milijuna trilijuna). U praksi svaki atribut koristi samo nekoliko mogućih vrijednosti a i one se ne koriste istom učestalošću. U tabeli 6.3. prikazane su neke vrijednosti promatranih atributa i njihova učestalost upotrebe.

	Vrijednost	Algoritam	Učestalost
Algoritmi za kriptiranje	1	DES	Često
	2	IDEA	Vrlo rijetko
	3	Blowfish	Rijetko
	4	RC5	Vrlo rijetko
	5	3DES	Često
	6	CAST	Rijetko
	7	AES	Često (128,192,256 - dužina ključa)
	8	Camellia	Vrlo rijetko
Hash algoritmi	1	MD5	Često
	2	SH1	Često
	3	Tiger	Rijetko
	4	SHA2-256	Rijetko
	5	SHA2-384	Rijetko
	6	SHA2-512	Rijetko
Metoda identifikacije	1	Pre-Share Key	Često
	2	DSS Potpis	Rijetko
	3	RSA Potpis	Često
	4	RSA kriptiranje	Rijetko
	5	Revidirano RSA kriptiranje	Rijetko
	6	ElGamel Kriptiranje	Rijetko
	7	Revidirano ElGamel kriptiranje	Rijetko
	8	ECDSA potpis	Rijetko
	64221	Hybrid Mod	Često u Chackpoint-u

	65001	XAUTH	Često kod udaljenog pristupa
Diffe-Hellman grupe	1	MODP 768	Često
	2	MODP 1024	Često
	3	EC2N 155	Rijetko
	4	EC2N 185	Rijetko
	5	MODP 1536	Često
	6	EC2N 163	Rijetko
	7	EC2N 163	Rijetko
	8	EC2N 183	Rijetko
	9	EC2N 183	Rijetko
	10	EC2N 409	Rijetko
	11	EC2N 409	Rijetko
	12	EC2N 571	Rijetko
	13	EC2N 571	Rijetko
	14	MODP 2048	Rijetko
	15	MODP 3072	Rijetko
	16	MODP 4096	Rijetko
	17	MODP 6144	Rijetko
	18	MODP 8192	Rijetko

Tabela 6.3. Učestalost korištenja atributa (izvor: [28])

Ako se izaberu samo atributi koji se često koriste onda za algoritme za kriptiranje imamo pet vrijednosti (AES se posebno računa za svaku dužinu ključa), dvije vrijednosti za hash algoritme, četiri metode identifikacije i tri Diffie-Hellman grupe. Kombinacijom ovih atributa dobivamo 120 mogućih kombinacija prijedloga koje treba ponuditi. Ovaj broj je puno manji i u realnim uvjetima je izvedivo ispitati hostove. Opcija '**- *-trans***' omogućava mijenjanje pojedinih atributa u prijedlogu. Primjenom ove opcije i korištenjem svih 120 kombinacija ne rješavamo potrebu pronalaska mogućih IPsec VPN sistema. Razlog leži u činjenici što predlaganje nije moguće izvesti u jednom koraku jer gotovo sve implementacije ograničavaju broj prijedloga koji će biti prihvaćeni na razmatranje. Broj nije isti i razlikuje se među

implementacijama, tako da Checkpoint[127] prihvaća maksimalno 12 ponuda u jednom prijedlogu. Zbog toga treba planirati višestruko skeniranje s razumnim brojem prijedloga u ponudi.

Metoda koja donosi iznenađujuće dobre rezultate je samo promjena načina identifikacije. Koristi se opcija '***- -auth***' i to na način da se definiraju slijedeće četo korištene metode:

- - -auth=3: RSA potpis,
- - -auth=64221: Hybrid Mod, Checkpoint,
- - -auth=65001: XAUTH, često korištena metoda za udaljen pristup.

6.1.5.1. Druge korisne opcije kod otkrivanja VPN sistema

Ako se radi o velikim količinama hostova koje treba pregledati korisno je upotrijebiti slijedeće opcije:

- ***- -retry*** – maksimalni broj pokušaja uspostave komunikacije s hostom. Predefinirana je vrijednost tri za slučaj da se paket izgubi na putu. Smanjivanjem na jedan ubrzavamo postupak skeniranja,
- ***- -bandwidth*** – definira korištenu količinu prometa. Povećavanjem možemo ubrzati skeniranje ako imamo na raspolaganju brze veze ili smanjivanjem ako želimo da nam skeniranje ne privlači pozornost na mreži. Predefiniran vrijednost je 56kbit/sec,
- ***- -random*** – redoslijed hostova koji se skeniraju. Skeniranje korištenje ovom opcijom neće izgledati kao skeniranje.

6.2. INFORMACIJE O IPSEC VPN SISTEMU

Kad se otkriju VPN serveri, slijedeći korak je prikupljanje što više informacija o njemu. Korištenjem ovog alata dolazimo do informacija o kojem se prodavaču ili implementatoru radi te o modelu. Nekad se dobiju informacije o verziji softvera. Ove informacije se mogu iskoristiti za napad jer pretragom ranjivosti sustava na Internetu možemo doći do primjerenih alata u obliku

[127] Ime poduzeće Check Point Software Technologies Ltd., specijaliziran za vatrozide

VPN klijenata kojima možemo pokušati pogoditi korisnička imena i lozinke za prijavu na server. Nekad je dovoljno koristiti jednu tehniku da se dobije informacija o implementiranom sustav, no često je potrebno koristit kombinaciju nekoliko metoda da se dođe do željene informacije.

6.2.1. USPOSTAVA IKE KONEKCIJE

Uspostava IKE konekcije znači da smo pogodilo o kojoj se kombinaciji atributa radi i od druge strane se dobije potvrda da će ponuđena kombinacija algoritama i metoda biti korištena za uspostavljanje veze. Ako se dobije 'Notify' poruka znači da nije pogođena kombinacija ili ako se ne dobije ništa može biti da sustav na krivu kombinaciju atributa ne odgovara. Postupak je isti kao i kod detektiranja IPsec VPN sustava.

6.2.1.1. Informacije dobivene UDP Backoff

IKE koristi UDP način prijenosa podataka što ga čini nesigurnim. Da bi osigurao siguran prijenos implementira se strategija ponovnog slanja paketa. Nekoliko varijabli utječe na tu strategiju:

- Koliko dugo čekati prije ponovnog slanja paketa?
- Da li vremenski razmak između ponovnog slanja paketa ostaje fiksan ili se po nekoj funkciji povećava?
- Koliko ponovnih paketa poslati?

Kako se ni u jednom RFC ne definira precizno strategija ponovnog slanja (Backoff strategy) svaki proizvođač je implementirao svoju. Ove strategije su proučene i došlo se do zaključka:

1. Većina, ali ne svi, implementatori IPsec VPN imaju različite strategije ponovnog slanja,
2. Moguće je na osnovu uzorka ponašanja s određenom sigurnošću definirati o kojem se sistemu radi.

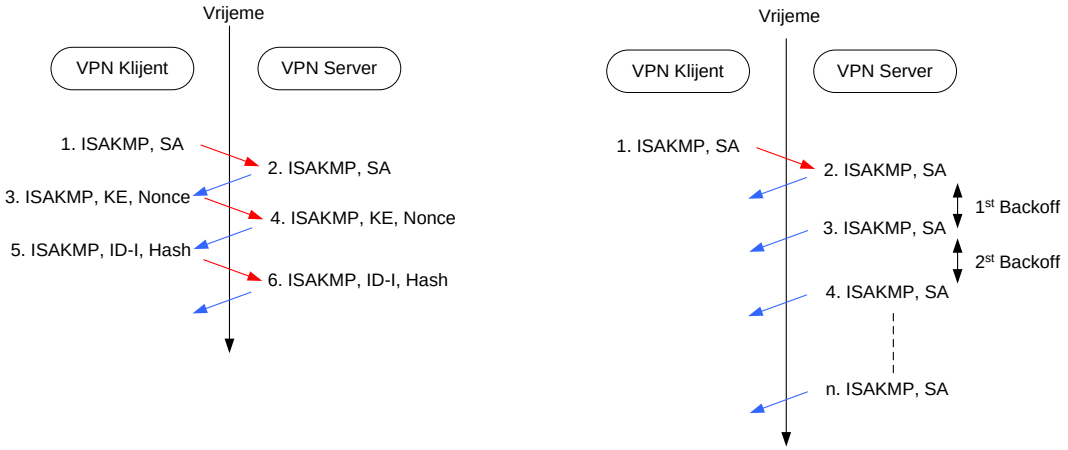
Ponekad se strategija mijenja od verzije do verzije istog proizvođača opreme čime se ostvaruje mogućnost da razlikujemo i verzije implementacija međusobno.

Iako otkrivanje o kojem se IPsec VPN sistemu radi nije prijetnja sama po sebi, dobivene informacije mogu voditi do prijetnji. Za svaki sustav moguće je saznati otkrivene sigurnosne propuste ili korištenjem odgovarajućeg klijenta može se pokušati pogoditi korisničko ime i lozinku za spajanje na sustav. Neke IKE implementacije ne bilježe aktivnosti vezane uz neuspješno spajanje ili ono koje nije završeno, tako da se može izvršiti skeniranje a da odgovorna osoba nije s time upoznata. Problem leži u tome što RFC ostavljaju implementatorima na izbor da li će ovakve aktivnosti bilježiti ili ne. Zbog uštede procesorskog vremena i memorije ovakve aktivnosti ostanu nezabilježene. Bilo kojom tehnologijom izveden VPN za napadače predstavlja izazov jer korisnici naprave slijedeće:

- Konekcija na VPN server osigurava puni pristup internim resursima mreže,
- Korisnici pretpostavljaju da je VPN server nevidljiv i neprobojan.

Kako korištenje ovog programa pokazuje da je IPsec VPN server vidljiv i da ga se može identificirati te kako se otkrivaju ranjivosti pojedinih implementacija pitanje je vremena napada na ove sustave.

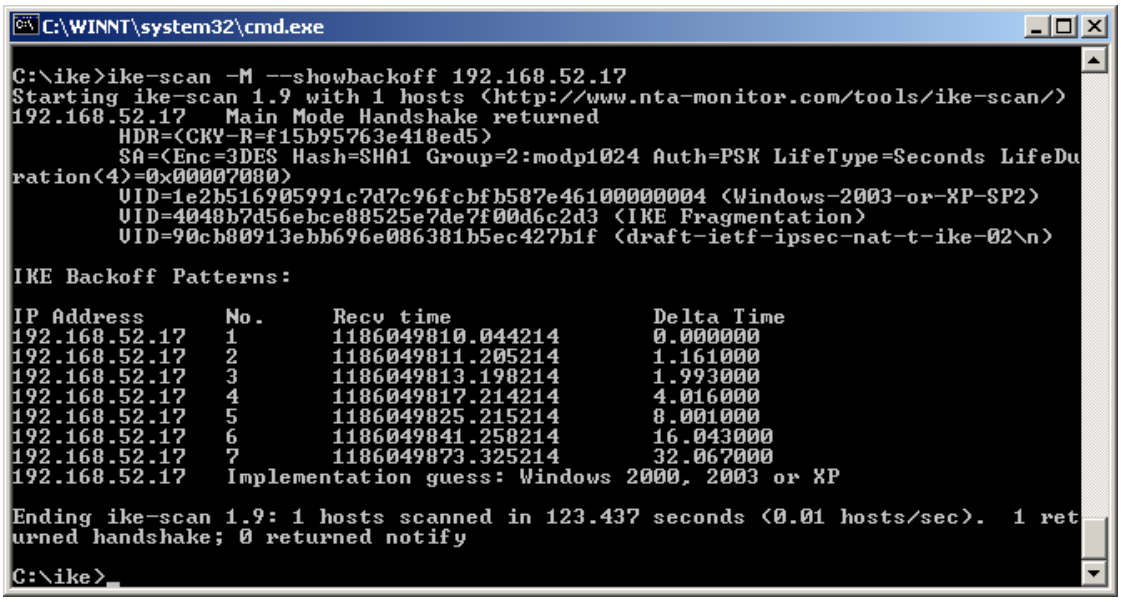
Da bi došli do ovih informacija, pošaljemo IKE paket s prihvatljivom ponudom VPN serveru i ne odgovaramo na njegove pakete. VPN server kad ne dobije odgovor pretpostavi da je paket izgubljen i po implementiranoj strategiji šalje određeni broj paketa u određenim vremenskim razmacima. Bilježenjem ovog vremena i broja paketa određujem se o kojem je sistem riječ. Na slici 6.6. prikazana je normalna izmjena paketa u Main mod-u i na koji način se inicira komunikacija te sakupljaju informacije ponovno slanih paketa da bi se dobila informacija o IPsec VPN sistemu.



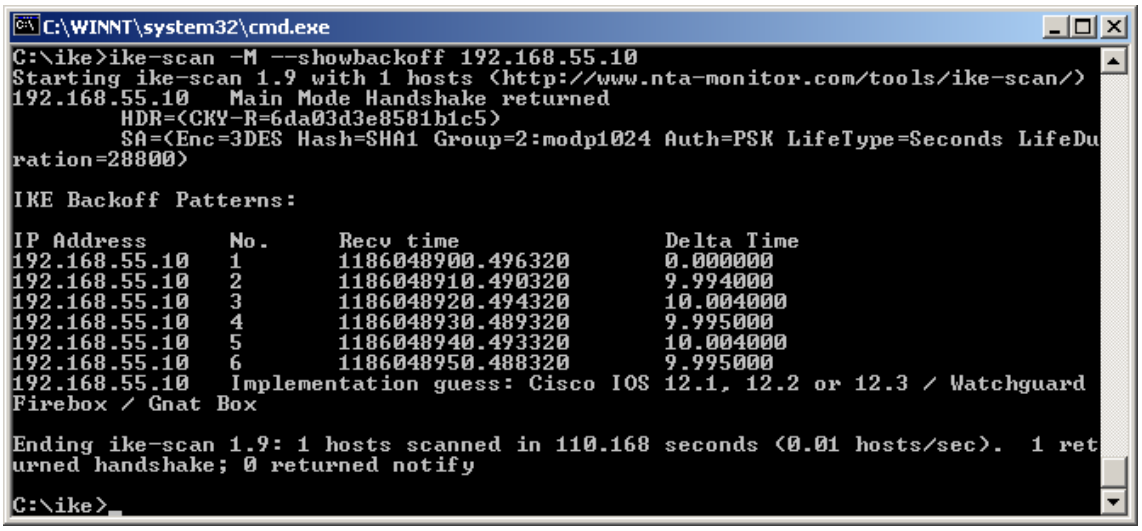
Slika 6.6. Uspostavljanje komunikacije (izvor: vlastiti rad)

Da bi izvršili ovo 'Backoff' skeniranje koristimo se opcijom '***- -showbackoff***' koja snima vrijeme svih pristiglih ponovno poslanih paketa. Jedna minuta je maksimalno vrijeme koje se čeka na odgovor nakon svakog poslanog paketa. Ako unutar toga vremena ne stigne više ništa onda se sa zadnjim primljenim paketom zaključuje skeniranje i prikazuju se rezultati. Na slici 6.7., i 6.8. prikazan je slučaj kad je korištena predefinirana ponuda s prijedlozima i kako je sustav na ponudu odgovorio. Kolone koje se pojavljuju na izlazu imaju slijedeća značenja:

- IP Address – IP adresa skeniranog VPN servera,
- No. – Broj primljenih paketa,
- Recv time – Vrijeme kad su paketi pristigli prikazani u sekundama i milisekundama u odnosu na ponoć 1.1.1970 (korišten prikaz kao u UNIX sustavima),
- Delta time – razlika u vremenu između pojedinih paketa.



Slika 6.7. Upotreba ike-scan na testnoj okolini (izvor: vlastiti rad)



Slika 6.8. Upotreba ike-scan na testnoj okolini (izvor: vlastiti rad)

Dva skenirana sustava, slika 6.7. i 6.8., imaju različito implementiranu strategiju ponovnog slanja paketa za koje se misli da su izgubljeni i prema njima se može zaključiti o kojoj se implementaciji radi. U tabeli 6.4. prikazani su još neki sustavi.

Checkpoint Firewall-1	0, 2, 2, 2, 2, 2, 2, 4, 4, 4, 4, 4
Cisco VPN Concentrator	0, 8, 8, 8
Nortel[128] Contivity[129]	0, 16, 16, 16

Tabela 6.4. Ponovno slanje paketa (izvor: [37])

[128] Ime poduzeća Nortel Networks
[129] Tip routera

U datoteci 'ike-backoff-patterns' su uključene i druge implementacije, datoteka dolazi zajedno s programom 'ike-scan'.

6.2.1.2. Vendor[130] ID informacije

U IKE protokolu kao opcija je definiran skup podataka 'Vendor ID payload' (u daljnjem tekstu VID). Uključeni su u IKE Faza-1 paket i služi za prepoznavanje implementacija i dodatne informacije. Proizvođači koje su iskoristili ovu opciju i implementirali informacije 'ike-scan' ih prikazuje. Obično se radi o hash vrijednosti koja je nastala na način da je neki tekst propušten kroz MD5 hash algoritam. Dobivene VID informacije od VPN servera mogu poslužiti za njegovu identifikaciju kroz pretraživanje baze s poznatim proizvođačima. Problem je u tome što neki proizvođači ne isporučuju automatski VID informacije u IKA paketima. On će VID podatke poslati samo ako primi specifične VID informacije u IKA paketu ili ih isporučuje automatski u Agresiv Mod-u. Dodavanje ovih informacija u odlazni paket omogućen je s opcijom '***- -vendor***'. Ako skeniranjem ne dobijemo VID informaciju nije loše pokušati snimiti promet između klijenta i servera (tcpdump ili ethereal)[131] i vidjeti da li postoji neki oblik VID podatka koji se između njih izmjenjuje.

Primjer koji slijedi vezan je uz Microsoft. Na slici 6.9. je prikazan rezultat skeniranja i VID informacija. Prvi dio (označen crvenom linijom) je hash vrijednost teksta 'MS NT5 ISAKMPOAKLEY' propuštenog kroz MD5 hash algoritam i prikazan kao 32-bitna vrijednost. Sve Microsoft IPsec implementacije šalju isti VID uz dodatak (označen plavo linijom) koji ovisi o verziji operacijskog sustava.

[130] Prodavač
[131] Alati za nadgledanje mrežnog prometa i dobivanje informacija o paketima u mreži

Slika 6.9. Otkrivanje proizvođača (izvor: [37])

Vrijednosti koje se mogu nalaziti na kraju prikazane su u tabeli 6.5.

Vrijednost	Operacijski sustav
00000002	Windows 2000 Server
00000003	Windows XP SP1
00000004	Windows 2003 Server i Windows XP SP2
00000005	Windows Vista

Tabela 6.5. VID informacije (izvor: [37])

Slijedeći primjer, slika 6.10, je o prije spomenutoj situaciji kad VPN server ne šalje VID informacije dok ne dobije u prvom paketu VID informacije specifične za svog proizvođača. Ubacivanje VID informacija u IKE paket moguće je korištenjem opcije '***- -vendor***'. Radi se o Checkpoint Firewall-1 koji da bi poslao svoje VID informacije u inicijalnom paketu treba dobiti '*f4ed19e0c114eb516faaac0ee37daf2807b4381f*'. Prvih 19 bitova šalju svi Checkpoint produkti.

Slika 6.10. Korištenje VID informacije u ike-scan. (izvor: [37])

Iz primjera se vidi da osim informacije o produkta šalje informaciju i o verziji softvera koji je se na njemu nalazi. Idući primjer, slika 6.11. vezan je za Nortel koji da bi poslao svoje VID informacije mora primiti u inicijalnom paketu makar jedan bit.

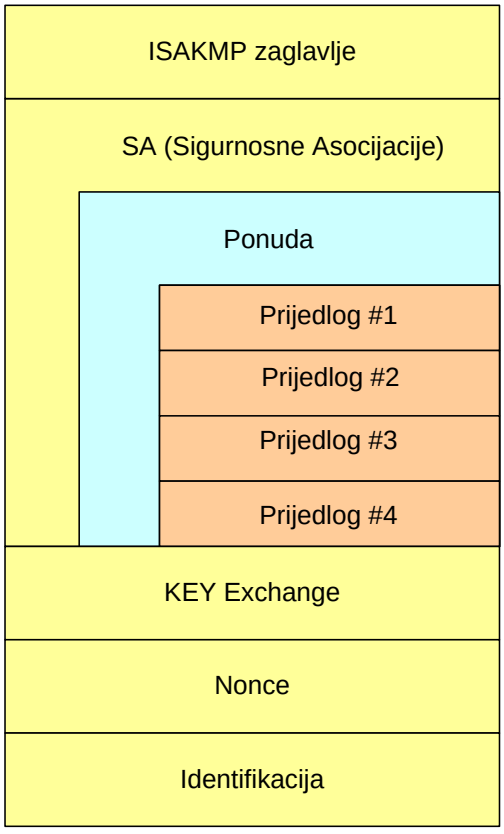
```
ike-scan --trans=5,2,1,2 --vendor=00 --multiline 10.0.0.3
arting ike-scan 1.7 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
.0.0.3     Main Mode Handshake returned
      SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080)
      VID=424e455300000009 (Nortel Contivity)
```

Slika 6.11. VID informacije od Nortela u ike-scan (izvor: [37])

Na primjeru se vidi da dobiveni odgovor sadrži VID informaciju. Prvi dio se odnosi na riječ BNES (Bay Networks Enterprise Switch) ime produkta kupljenog od strane Nortela i drugi dio koji vjerojatno označava verziju softvera.

6.2.1.3. IKE Agresiv Mod

Dio servera koji imaju ulogu osigurati konekciju mobilnih korisnika podržava Agresiv Mod. Ovu činjenicu možemo iskoristiti ako se želi doći do dodatnih informacija o skeniranom IPsec VPN sistemu. Za razliku od Main Moda, o kojem je do sada bilo riječ, u Agres Mod struktura IKE paketa je složenija, kako je i prikazano na slici 6.12.



Slika 6.12. Agresiv mod (izvor: vlastiti rad)

Paket sadrži tri dodatna dijela, tabela 6.6.:

Key Exchange	Diffie-Hellman vrijednosti
Nonce	Slučajno izabran broj za dokazivanja da je aktivan i zaštite od 'replay' napada
Identifikacija	Identifikacija para

Tabela 6.6. Dodatak u Agresiv modu (izvor: [37])

Kako se inicijalnom paketu nalaze i Diffe-Hellman vrijednosti jedino je moguće ponuditi jednu grupu tako da ponuda sadrži samo četiri prijedloga. Ovi prijedlozi sadrže atribute prikazane u tabeli 6.7.

Atribut	Vrijednost
Algoritam za kriptiranje	DES ili 3DES
Hash algoritam	MD5 ili SHA1
Metoda identifikacije	Pre-Shared Key (PSK)
Diffie-Hellman grupa	2
SA Lifetime	28800

Tabela 6.7. Prijedlozi u Agresiv modu (izvor: vlastiti rad)

Kako to izgleda po pojedinom prijedlogu prikazano je u tabeli 6.8.

Broj prijedloga	Algoritam za kriptiranje	Hash algoritam	Metoda identifikacije	Diffie-Hellman grupa	Lifetime (secund)
1	3DES	SHA1	PSK	2 (1024 bit)	28800
2	3DES	MD5	PSK	2 (1024 bit)	28800
3	DES	SHA1	PSK	2 (1024 bit)	28800
4	DES	MD5	PSK	2 (1024 bit)	28800

Tabela 6.8. Prijedlozi za Agresiv mod (izvor: vlastiti rad)

Mnogi serveri neće odgovoriti na inicijalni paket u Agresiv Mod-u dok ne postoji valjani ID identifikacijski podatak, korisničko ime ili mail adrese. Na žalost uvođenjem korisničkog imena u identifikaciju omogućavamo ranjivost sustava jer osiguravamo mehanizam za detekciju dobrog korisničkog imena od krivog. Na slijedećem primjeru prikazan je odgovor Cisco VPN

Conecentrator, slika 6.13. Novije verzije ne zahtijevaju da se u inicijalnom paketu kao ID nalazi korisničko ime.

Slika 6.13. Odgovor Cisco VPN Conecentrator (izvor: [37])

Odgovor sadrži nekoliko zanimljivih informacija, prikazanih u tabeli 6.9.

ID	Server za identifikaciju koristi svoju IP adresu. Ako se nalazi iza NAT onda se otkriva prava adresa.
Hash	Radi se o MD5 HMAC. Možemo ga iskoristiti da offline krekiranje lozinke
VIDs	Svih 5 proizvođačkih informacija

Tabela 6.9. Dio odgovora na ike-scan (izvor: vlastiti rad)

Slijedeći primjer navodi se iz dva razloga. Prvi je da za odgovor nije potrebno u prvi paket staviti ID jer koristi svoje ime, prikazano u zagradi. Drugi razlog je zbog toga što iako se radi o istom proizvođaču razlikuju im se redoslijedi argumenata u prijedlogu, kako je to prikazano na slici 6.14.

Slika 6.14. Odgovor na ike-scan upit (izvor: [37])

6.2.2. RAZLIKE U PONAŠANJU

Do sad smo identificirali razlike u ponašanju različitih implementacija u 'backoff' strategiji, Vendor ID i redoslijedu atributa u ponudi IKE paketa. Postoje još neke razlike na koje treba voditi računa kad se želi sakupiti što više informacija o nekom IPsec VPN sistemu. Razlike nastaju zbog toga što neke stvari nisu točno definirane ili zbog toga što RDC-ovi mogu biti interpretirani na više različitih načina. Na linku http://www.nta-monitor.com/wiki/index.php/IKE_Implementation_Analysis nalazi se primjeri pojedinih proizvođača kako odgovaraju na različite IKE pakete. Dobro mjesto za početak istraživanja ako se želi identificirati sistem kojemu se backoff uzorak ili Vendor ID ne nalazi u bazi.

6.2.2.1. Ključ za kriptiranje s fiksnom dužinom

Kad se koristi AES algoritam za kriptiranje, koristi se ključ s promjenjivom dužinom. Kad se koriste algoritmi DES ili 3DES, dužina ključa je fiksna i po zahtjevu RFC 2409, atribut koji definira dužinu ključa (key length) ne smije se koristiti. No različite implementacije različito se ponašaju kad je u pitanju korištenje ovog atributa s algoritmom kojemu je dužina ključa fiksna. U tabeli 6.10. dati su primjeri kako se neke implementacije ponašaju.

Checkpoint Firewall-1	Prihvaća prijedlog i vraća istu dužinu ključa i odgovoru

```
ike-scan --trans=5/27,2,1,2 -M 10.0.0.1
tarting ike-scan 1.7 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
0.0.0.1      Main Mode Handshake returned
       SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 KeyLength=27 LifeType=Seconds LifeDuration(4)=0x0
```

Cisco VPN Concentrator	Ne odgovara

```
$ ike-scan --trans=5/27,1,1,2 -M 10.0.0.2
Starting ike-scan 1.7 with 1 hosts (http://www.nta-monitor.com/ike-sca
```

Nortel Contivity	Odgovara da nema ponude koja bi bila prihvatljiva

```
ike-scan --trans=5/27,2,1,2 -M 10.0.0.3
tarting ike-scan 1.7 with 1 hosts (http://www.nta-monitor.com/ike-sc
).0.0.3     Notify message 14 (NO-PROPOSAL-CHOSEN)
```

Windows 2003	Prihvaća prijedlog ali ne vrača atribut u odgovoru

```
 ike-scan --trans=5/27,2,3,2 -M 10.0.0.4
tarting ike-scan 1.7 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
0.0.0.4 Main Mode Handshake returned
        SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=RSA_Sig LifeType=Seconds LifeDuration(4)=0x0
        VID=1e2b516905991c7d7c96fcbfb587e46100000004 (Windows-2003-or-XP-SP2)
        VID=4048b7d56ebce88525e7de7f00d6c2d3 (IKE Fragmentation)
        VID=90cb80913ebb696e086381b5ec427b1f (draft-ietf-ipsec-nat-t-ike-02\n)
```

Tabela 6.10. Upit ike-scan s argumentom s fiksnom dužinom ključa (izvor: vlastiti rad)

6.2.2.2. Promjenjiva dužina atributa za male vrijednosti

U ponudi atributi mogu biti opisani fiksnom dužinom riječi (16-bita) ili dužinom koja može biti koliko treba. Primjer za ovo je atribut koji opisuje koliko dugo će jedna SA biti valjana. Ika-scan šalje ovaj atribut u sekundama dok neki sistemi odgovor šalju u promjenjivoj varijabli. U tabeli 6.11. prikazana je razlika među sistemima.

	28800 sec	0x00007080
Checkpoint Firewall-1		X
Cisco VPN Concentrator	X	
Cisco PIX[132]	X	
Nortel Contivity		X
Windows 2003		X

Tabela 6.11. Izgled atributa za pojedine sisteme (izvor: vlastiti rad)

6.2.2.3. Maksimalan broj prijedloga u ponudi

Maksimalan broj ponuda u prijedlogu ograničen je veličinom IP datagrama koja iznosi 64 kbayta, što odgovara broju od oko 1800 prijedloga. Mnoge implementacije ograničava ovaj broj i mnogo je manji nego što je teoretski moguć. Kroz RFC 2409 mogućnost ograničavanja broja prijedloga se dozvoljava. Način na koji bi saznali koliki je za neki sustav se satoji u tome da prvo nađemo prihvatljivu kombinaciju atributa a zatim mijenjamo broj prijedloga u ponudi dok ne dobijemo broj nakon kojega dobijemo (ili prestanemo dobivati) pozitivan odgovor.

[132] Vatrozid

6.2.2.4. ISAKMP 'Responder Coocki'[133] format

U odgovoru od servera bi se trebao nalaziti i 64 bitni broj koji je jedinstveni a naziva se 'Responder Coocki'. kod nekih implementacija ovaj broj je specifičan i prepoznatljiv. Primjer je Checkpoint Firewall-1 koji uvijek šalje 0 u 'Notify' poruci, slika 6.15.

```
 ike-scan -M 172.16.2.2
tarting ike-scan 1.8.4 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
72.16.2.2      Notify message 14 (NO-PROPOSAL-CHOSEN)
       HDR=(CKY-R=0000000000000000, msgid=d44ad35f)
```

Slika 6.15. 'Responder Coocki' za Checkpoint Firewall-1 (izvor: [37])

Cisco PIX će uvijek u odgovoru vratiti isti vrijednost slika 6.16.

```
; ike-scan -M 10.0.38.226
tarting ike-scan 1.8.4 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
!17.205.38.226  Main Mode Handshake returned
       HDR=(CKY-R=ff553a4d65572e8a)
       SA=(Enc=3DES Hash=SHA1 Group=1:modp768 Auth=PSK LifeType=Seconds LifeDuration=28800)
```

Slika 6.16. 'Responder Coocki' za Cisco PIX (izvor: [37])

6.2.2.5. Promjena redoslijeda atributa

Redoslijed atributa u ponudi može biti proizvoljna. Ike-scan ih uvijek šalje u slijedećem rasporedu:

1. Algoritam za kriptiranje,
2. Hash algoritam,
3. Metoda identifikacije,
4. Diffie-Hellman grupa,
5. Key Length (ako je specificirana)[134],
6. LifeType (sekunde ili KB),
7. LifeDuration[135].

Međutim moguće je promijeniti raspored atributa po volji korištenjem opcije '- -trans=(attr1=val1, attr2=val2, …)'. Svaki atribut može biti opisan s 16-

[133] Cookies nazivamo kratke informacije koje serveri ostavljaju kod klijenata
[134] Kad enkripcijski algoritam ima promjenjivu dužinu ključa
[135] Vrijeme u kojem je SA valjan

binom vrijednošću (engl. basic attribute) koja može poprimiti vrijednosti od 0 do 65535 ili promjenjivom varijablom (engl. varijable attribute) koja će biti dana u heksadecimalnom obliku 0x.. U RFC 2409 definirane su vrijednosti atributa kao je to prikazano u slijedećoj tabeli 6.12.

Vrijednost atributa	Ime atributa	Basic ili Variable
1	Encryption Algorithm	Basic
2	Hash Algorithm	Basic
3	Authentication Method	Basic
4	Group Description	Basic
5	Group Type	Basic
6	Group Prime/Irreducible Polynomial	Variable
7	Group Generator One	Variable
8	Group Generator Two	Variable
9	Group Curve A	Variable
10	Group Curve B	Variable
11	Life Type	Basic
12	Life Duration	Variable
13	PRF	Basic
14	Key Length	Basic
15	Field Size	Basic
16	Group Order	Variable

Tabela 6.12. Vrijednosti atributa kako je to definirano u RFC 2409 (izvor: [37])

Neke implementacije bez obzira na redoslijed atributa prihvaća vezu ako ponuda zadovoljava a odgovor se šalje u svom ili dobivenom redoslijedu.

6.2.2.6. Odgovor na izobličene ili nekompletne IKA pakete

Kad su u pitanju nepotpuni ili izobličeni IKE paketi implementacije se tu različito ponašaju. Iz ponašanja se mogu dobiti informacije o kojem se sistemu radi tako da i ovako kreirane pakete koristimo u procesu sakupljanja informacija. Mora se biti pažljiv jer izobličeni paket koji pošaljemo na VPN server može uzrokovati njegovo rušenje čime smo uzrokovali DoS napad. U

fazi testiranja sistemi bi trebali biti izloženi ovakvim vrstama IKE paketa da se procjeni rizik i prihvati takvo rješenje ili ako su visoki sigurnosni zahtjevi da se odabere drugo rješenja. Neki vatrozidi i IDS mogu prepoznati ovako definirane pakete i blokirati ih jer predstavljaju napad na pojedini sistem.

Općenito, skenirani IPsec VPN sistem će na izobličene ili nepotpune pakete odgovoriti na slijedeći način:

- Ignorirati paket i neće odgovoriti ni na bilo koji način,
- Odgovoriti normalno uz to da ignorira ili ne provjerava oštećeni dio,
- Odgovoriti s 'Notify' porukom.

Neki primjeri izobličenih ili nepotpunih IKE paketa su:

- No Acceptable Transforms - An SA payload where none of the transforms have acceptable attributes,
- Bad IKE version - The version number in the ISAKMP header is not valid. Either the major version, the minor version or both may be invalid,
- Invalid DOI - The *Domain of Interpretation* in the SA header is not valid,
- Invalid Situation - The Situation in the SA header is not valid,
- Invalid Initiator Cookie - The initiator cookie is zero,
- Invalid Flags - The flags field in the ISAKMP header is not valid,
- Invalid Protocol - The protocol ID in the proposal payload is invalid,
- Invalid SPI - The size of the SPI in the proposal payload is not valid,
- Non-Zero Reserved Fields - The reserved (must be zero or MBZ) fields in the IKE packet are non-zero.

U tabeli 6.13. prikazan su opcije 'ike-sacn' alata kojima se kreiraju pojedini paketi i što se kaže u RFC zahtjevima o tome kako se s njima treba odnositi.

Tip	ike-scan options	RFC Ref
No Acceptable Transforms	--trans=2,3,5,3	RFC 2408 Sec 5.4: *If the Security Association Proposal is not accepted ... An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity*
Bad IKE version	--headerver=0x30 --headerver=0x11 --headerver=0x31	RFC 2408 Sec 5.2: *Check the Major and Minor Version fields to confirm they are correct. If the Version field validation fails ... An Informational Exchange with a Notification payload containing the INVALID-MAJOR-VERSION or INVALID-MINOR-VERSION message type MAY be sent to the transmitting entity*
Invalid DOI	--doi=2	RFC 2408 Sec 5.4: *Determine if the Domain of Interpretation (DOI) is supported ... If the DOI determination fails ... An Informational Exchange with a Notification payload containing the DOI-NOT-SUPPORTED message type MAY be sent to the transmitting entity*
Invalid Situation	--situation=2	RFC 2408 Sec 5.4: *Determine if the given situation can be protected. If the Situation determination fails ... An Informational Exchange with a*

		Notification payload containing the SITUATION-NOT-SUPPORTED message type MAY be sent to the transmitting entity
Invalid Initiator Cookie	--cookie=0000000000000000	RFC 2408 Sec 5.2: *Verify the Initiator and Responder "cookies". If the cookie validation fails ... An Informational Exchange with a Notification payload containing the INVALID-COOKIE message type MAY be sent to the transmitting entity'*
Invalid Flags	--hdrflags=255	RFC 2408 Sec 5.2: *Check the Flags field to ensure it contains correct values. If the Flags field validation fails ... An Informational Exchange with a Notification payload containing the INVALID-FLAGS message type MAY be sent to the transmitting entity*
Invalid Protocol	--protocol=2	RFC 2408 Sec 5.5: *Determine if the Protocol is supported. If the Protocol-ID field is invalid ... An Informational Exchange with a Notification payload containing the INVALID-PROTOCOL-ID message type MAY be sent to the transmitting entity*
Invalid SPI	--spisize=32	RFC 2408 Sec 5.5: *Determine if the SPI is valid. If the SPI is*

		invalid ... An Informational Exchange with a Notification payload containing the INVALID-SPI message type MAY be sent to the transmitting entity
Non-Zero Reserved Fields	--mbz=255	RFC 2408 Sec 5.3: *Verify the RESERVED field contains the value zero. If the value in the RESERVED field is not zero ... An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message type MAY be sent to the transmitting entity*

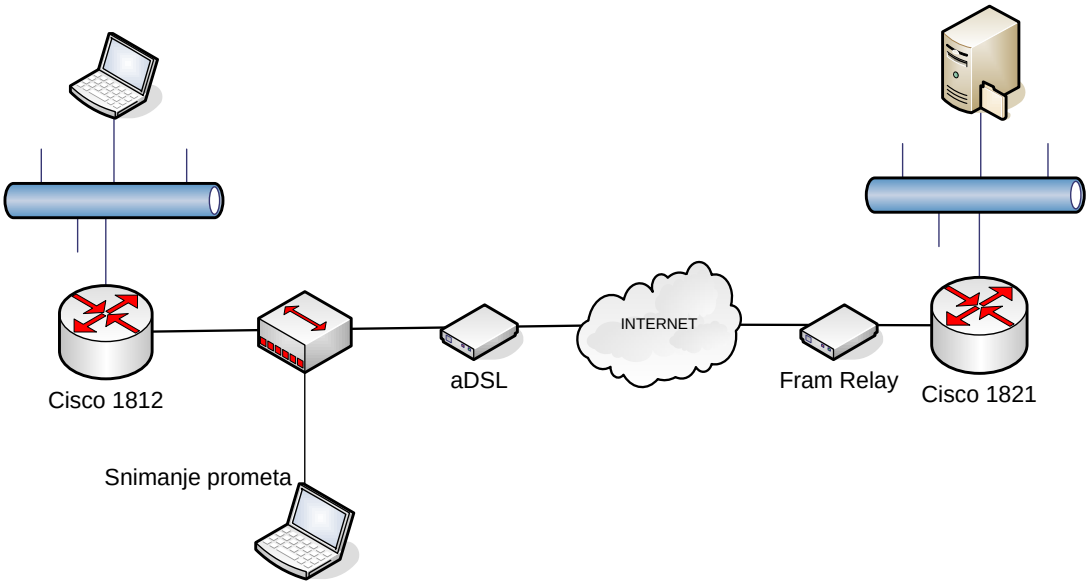
Tabela 6.13. Opcije 'ike-scan' (izvor: [37])

6.2.2.7. Podrška za vrijednost atributa

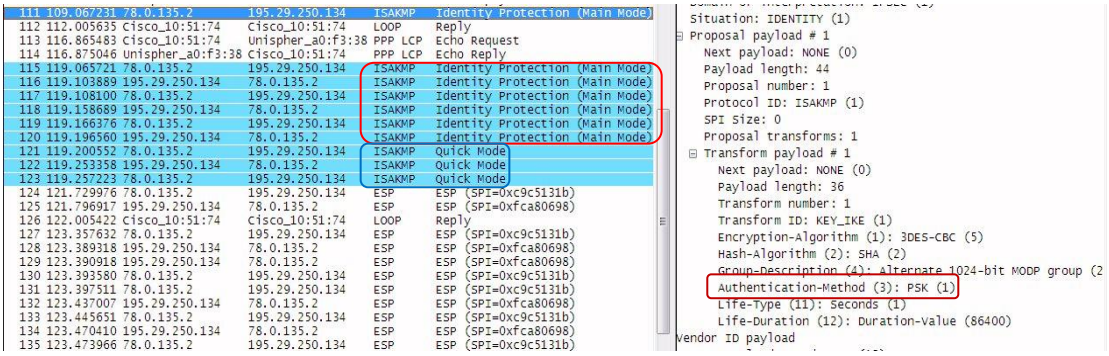
Različite implementacije često prihvaćaju različite vrijednosti pojedinih atributa. Primjer je da neki sustav može prihvatiti algoritme za kriptiranje DES i 3DES dok drugi prihvaća samo 3DES. Poteškoća je u tome što nepodržavanje određenog algoritma može biti rezultat implementacije ili korisničke intervencije u konfiguriranju servera. Podrška samo nekih verzija, recimo algoritama, može dati informaciju o starosti uređaja i vremenu njegove implementacije.

6.2.3. TESTIRANJE VPN-A NA MODELU

Na slici 6.17. prikazana je konfiguracija iz modela na kojoj je vršeno testiranje. s prikazanim uređajima je ostvarena je sigurna veza između dvije udaljene lokacije. Promet je promatran na strani onoga tko je inicirao komunikaciju.

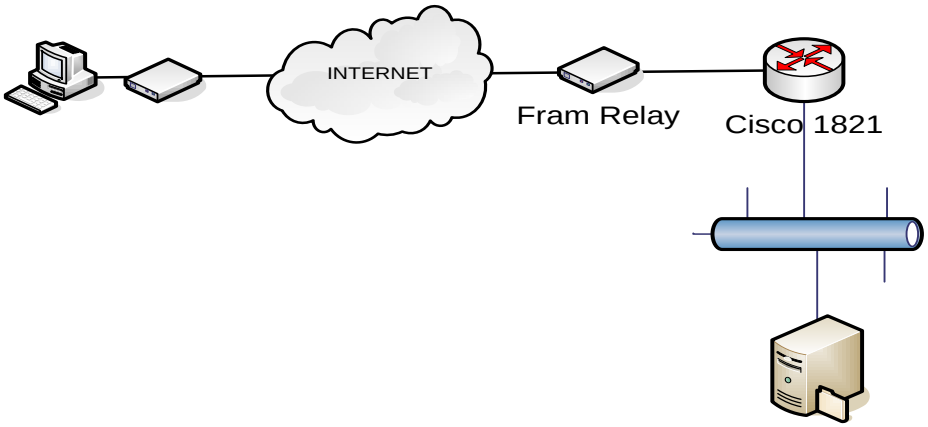


Slika 6.17. Primjer testiranja (izvor: vlastiti rad)



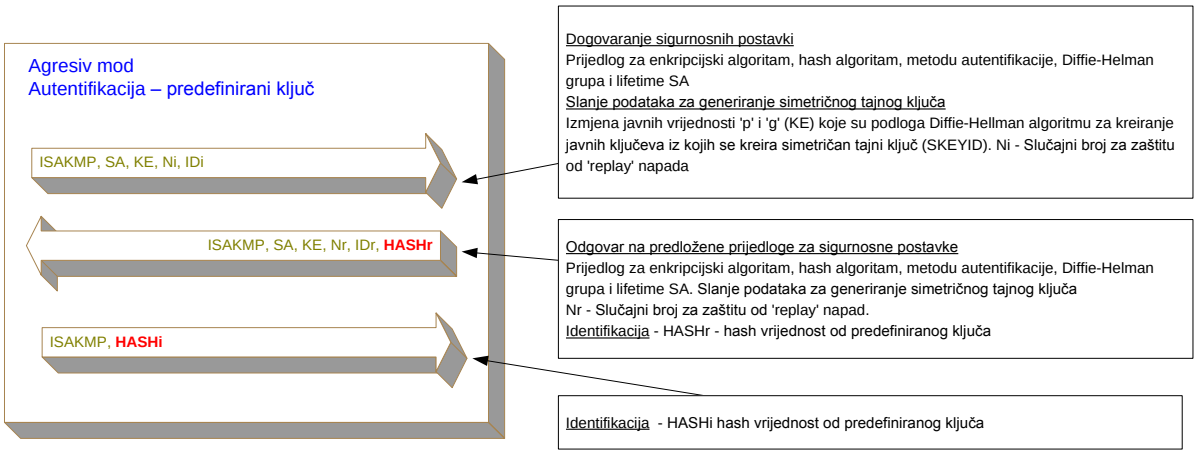
Slika 6.18. Rezultat snimanja prometa (izvor: vlastiti rad)

Na slici 6.18. se vidi kako se uspostavlja komunikacija tj. faza 1 i 2. Zanimljiva je informacija na koji način se vrši autentifikacija. U ovom slučaju se koristi predefinirani ključ. No kako se koristi 'Main mode' autentifikacijske informacije se počinju prenositi po mreži nakon što se dogovori simetrični tajni ključ tako da je promet između para kriptiran. Na slici 6.19. prikazan je slučaj kad se mobilni korisnik spaja na istu centralnu lokaciju.



Slika 6.19. Testiranje (izvor: vlastiti rad)

Zbog načina rada u 'Agresivnom modu' u IKE Fazi 1 po nesigurnoj mreži prenosi se podatak koji može biti iskorišten za dobivanje informacije kojom si osiguravamo spajanje na VPN server. Na slici 6.20. je prikazan način komunikacije koji se odvija između dva korisnika koji žele uspostaviti sigurnu vezu.



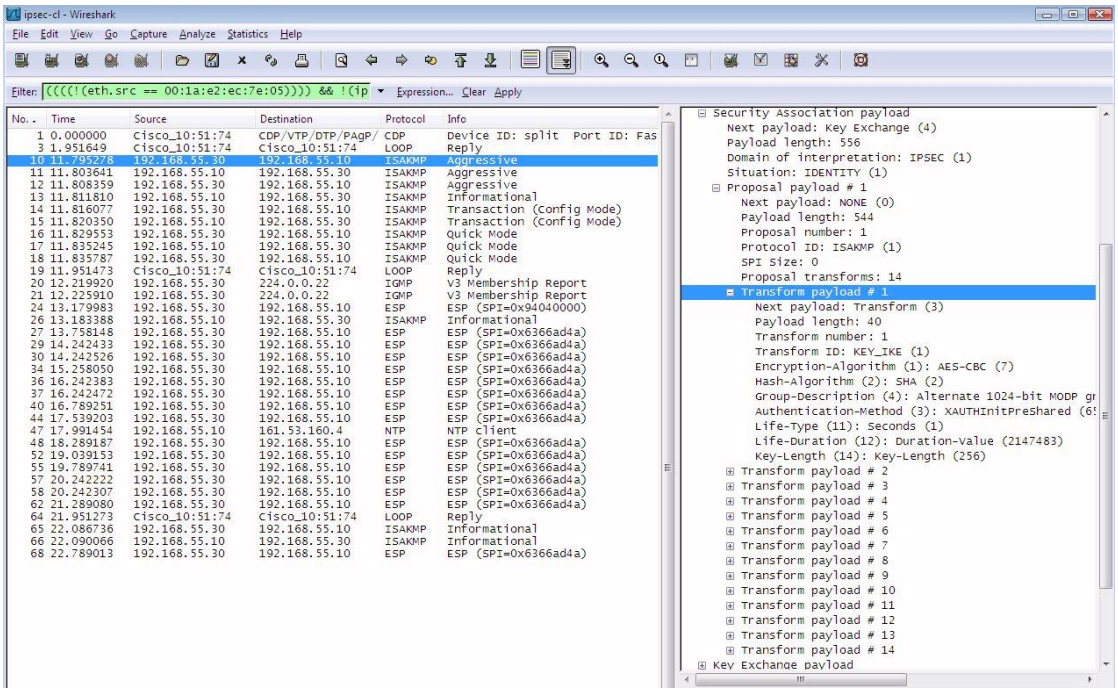
ISAKMP – paket
KE – javno dostupne vrijednosti (p-modul i g-baza) za kreiranje javnih ključeva iz kojih se izračuna zajednički ključ SKEYID
SKEYID - simetričan tajni ključ koji uz druge vrijednosti služi za kreiranje tri dodatna ključa
- SKEYID_e – ISAKMP SA koristi ovaj ključ za osiguranje tajnosti svojih poruka
- SKEYID_a - ISAKMP SA koristi ovaj ključ za autentifikaciju svojih poruka
- SKEYID_d - ISAKMP SA koristi ovo kao materijal za kreiranje novih NE ISAKMP SA
Nx - slučani broj koji služi za zaštitu od replay napada
ID – identifikator, može biti IP adresa
HASH – hash funkcija se primjeni na predefinirani ključ (vrsta identifikacije)

Slika 6.20. Agresiv mod (izvor: vlastiti rad)

Kako se iz priloženoga vidi u dugoj poruci se nalazi hash vrijednost od predefiniranog ključa. U istoj poruci se nalazi i informacija koji se algoritam koristi za dobivanje hash vrijednosti.

6.2.4. SAKUPLJANJE PODATAKA

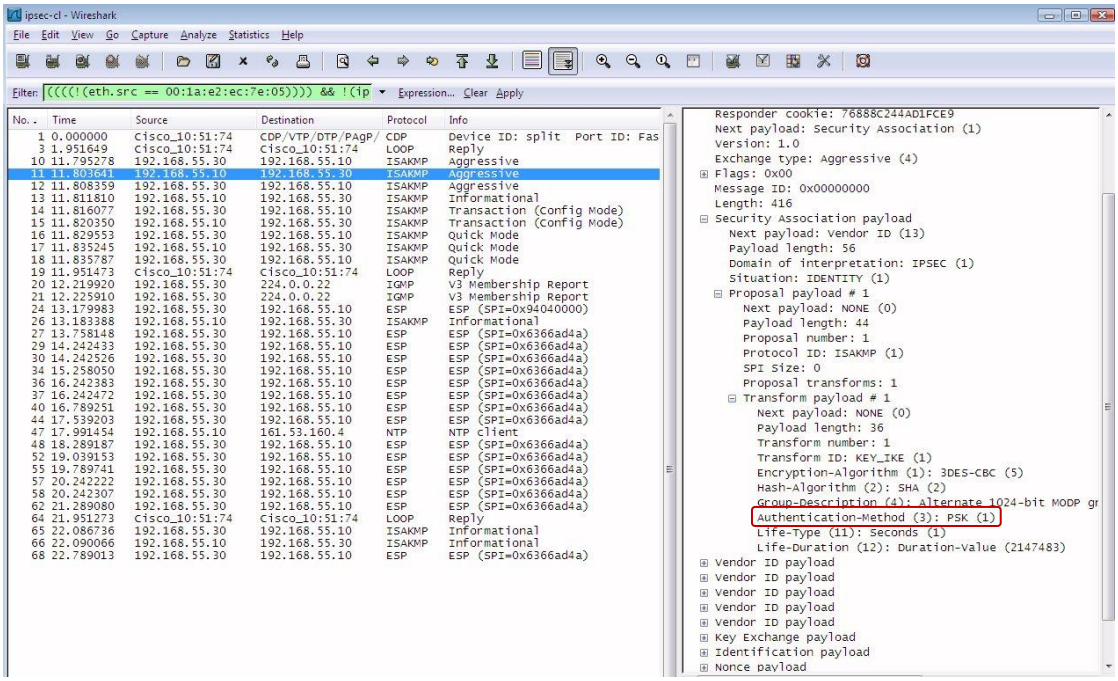
Da bi došli do hash vrijednosti potreban je alat kojime se može inicirati konekciju na VPN server u agresiv modu, da bi se pokupio promet s mreže koji se odvija između njih. Ako napadač pokuša uspostaviti IPsec tunel možemo pokupiti pakete s mreže između njih. Postoje alati (kao što je PGPNet) koji omogućavaju konfiguriranje VPN klijenta da radi u agresiv modu. VPN server, kao što je Cisco, omogućavaju konekciju korisnicima koji na takav način žele uspostaviti vezu. U prvom pokušaju i nije potrebno uspostaviti vezu, već je potrebno pokupiti hash vrijednost koja se dobije u odgovoru na inicijalni paket. Ovaj scenarij je vjerojatan zato što su VPN serveri konfigurirani na način da prihvaćaju zahtjeve s bilo kojih IP adresa zbog mobilnih korisnika koji vezu na Internet ostvaruju na različitim mjestima.



Slika 6.21. Paketi kod uspostave veze (izvor: vlastiti rad)

Na slici 6.21. Prikazani su paketi koji se izmjenjuju s naglaskom na prvi paket u kome se šalju prijedlozi za parametre komunikacije.

Na slici 6.22. Prikazan je sadržaj jednog od prijedloga u kome se vidi da je metoda autentifikacije.



Slika 6.22. Paketi kod uspostave veze (izvor: vlastiti rad)

Kompleksnost IPseca [38] i različitost implementacije omogućava da se ovaj siguran protokol promatra kao još jedan od sigurnosnih problema na mreži. Sigurnost je jedan od osnovnih zahtjeva za VPN. Nju ugrožava veliki broj napada, koji se mogu svrstati u veći broj grupa kao što su: napadi autentifikacije, kriptografski napadi, napadi integriteta, falsificiranje servera, falsificiranje paketa, napadi uskraćivanja usluga i pasivno nadgledanje. IPsec protokol pruža znatno veći broj sigurnosnih servisa kao što je PKI infrastruktura javnog ključa, verifikacija ključeva od strane Certifikacijsko tijela (CA) i IKE mehanizam upravljanja ključevima osigurava siguran kontrolni kanal u fazi pregovaranja sigurnosnih atributa između dva računara, koji se ovim mehanizmima međusobno autentificiraju na zaštićen način. I AH i ESP format IPsec protokola autentificira svaki paket, a s HMAC-MD5 ili HMAC-

SHA-1 hash funkcijama osiguravaju i integritet podataka svakog paketa. ESP tuneliranje i kriptiranje podataka paketa i originalnog IP zaglavlja s 3DES algoritmom je potpuno otporno na kriptografske napade, s obzirom da algoritam 3DES s ključem od 168 bita i HMAC-SHA-1 hash funkcija još uvijek nisu kompromitirani. IPsec protokol ima sve mehanizme zaštite od standardnih napada na Internetu, ugrađen je u protokole IPv4 i IPv6 i otvoren je za ugradnju novih zaštitnih mehanizama za slučajeve kompromitiranja postojećih. Najteža odbrana na Internetu je od napada uskraćivanja usluga, jer ti napadi potiču uglavnom od slabosti TCP/IP protokola na koji se IPsec protokol oslanja. I IPsec protokol ima svoje slabosti. Uspostavljeni tunel ne mora uvijek da je potpuno siguran, jer se tunel uspostavlja automatski pregovaranjem sigurnosnih atributa računara krajnjih točaka tunela, i ako ne postoje s obije strane mehanizmi najvećeg stupnja zaštite, koriste se oni raspoloživi s nižim stupnjevima zaštite (ključ s manjim brojem bita, slabija hash funkcija). Jedina slabost IKE protokola je ta da nema indikaciju predanoj strani da je sesija prekinuta, što ostavlja mogućnost napada na server ako je korišten slabiji ključ. Uspostavljena sesija i duži period obnavljanja ključa povećava mogućnost uspješnost napada. Otpornost ugrađenih sigurnosnih mehanizama na Internet napade su prikazani u tabeli 6.14. [39]

Vrsta napada	IPsec	
	Sigurnosni mehanizam	Nivo sigurnosti
Napad Autentifikacije	PKI / CA	dobar
Kriptografski napad	3DES	jak
	DES	dobar
Napadi integriteta podataka	HMAC-SHA-1	jak
	HMAC-MD5	dobar
Falsificiranje identiteta servera	PKI/Diffie-Hellman	dobar

Lažno predstavljanje paketa	AH / ESP	dobar
Napadi uskraćivanja usluge	PKI / IKE	osrednji
Pasivno promatranje	ESP enkripcija	dobar

Tabela 6.14. Otpornost na napade (izvor: vlastiti rad)

VPN mreže su ekonomična zamjena za prave privatne mreže s iznajmljenim linijama. Iako VPN mreže s IPsec protokolom imaju visok nivo sigurnosti, one imaju i neke slabosti koje mogu da ugroze njihovu privatnost.

7. ANALIZA PRIJETNJI NA MODELU

Analizirat će se slijedeće prijetnje i načini na koji se oni mogu provesti, tabela 7.1.

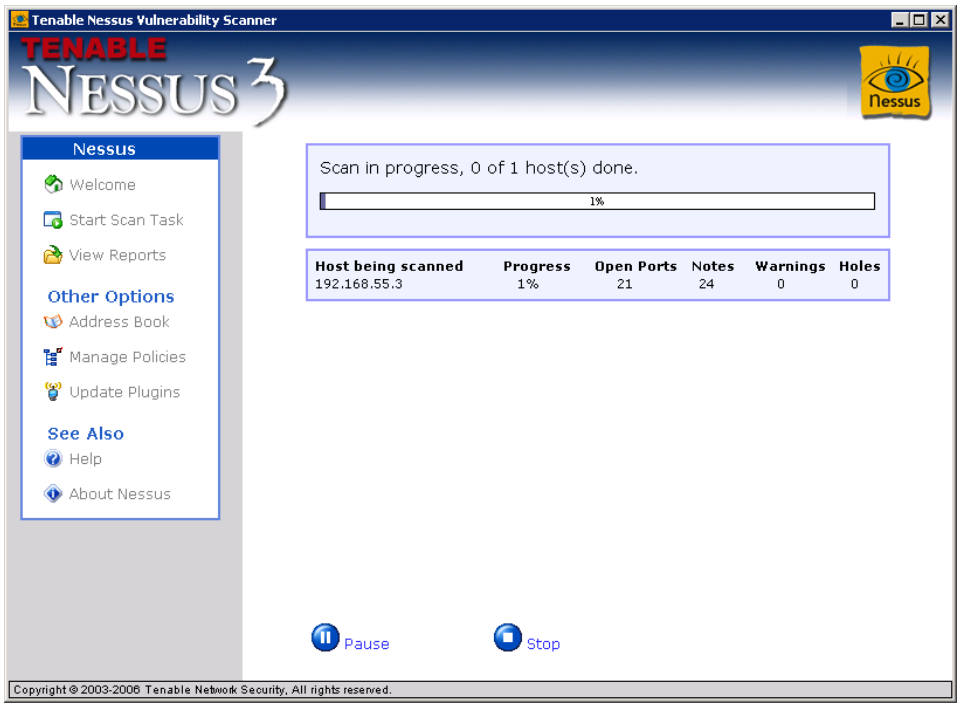
Prijetnje i načini provedbe	Mogućnosti IPsec-a
Neovlašteno otkrivanje lozinki drugih osoba	
Uvid u sadržaj prometa po mreži (sniffing)	+
Neovlašteno korištenje sigurnosnih alata	
Korištenje alata u svrhu prikupljanja informacija o sustavu	+
Prisluškivanje komunikacijskog tijeka	
Instalacija softverskog 'keylogger'	+-
Korištenje 'sniffing' alata	+-
Pojava ili unošenje malicioznih programa	
Namjerno unošenje računalnog virusa	+
Namjerno unošenje Trojanaca ili Backdoor programa	+
Izvođenje 'hackerskih' napada	+
Neovlašteni logički pristup	
Pristup pomoću lozinke otkrivene na nedozvoljeni način	+-
Pristup dijeljenim pristupnim pravima	+-
Pristup pomoću važećih ali nekonzistentnih prava	+-
Pristup 'default' korisničkim pravima	+-
Pristup 'backdoor' korisničkim pravima	+-
Pristup temeljem iskorištavanja sistemskih ranjivosti	+-
Neovlašten uvid u povjerljive podatke	
Uvid u sistemske podatke	+-
Uvid u povjerljive podatke koji su u strukturiranom obliku	+-

	Uvid u povjerljive podatke koji su u nestrukturiranom obliku	+-
	Nestandardna pretraga podataka	+-
Sabotaža		
	Unošenje destruktivnog programa	+-
Prikrivanje podataka o nedozvoljenim aktivnostima		
	Neovlašteni pristup i/ili izmjena evidencijskih zapisa	+-
	Prikrivanje identiteta u komunikaciji	+

Tabela 7.1. Prikrivanje podataka o nedozvoljenim aktivnostima (izvor: vlastiti rad)

7.1. SAKUPLJANJE PODATAKA O RESURSU

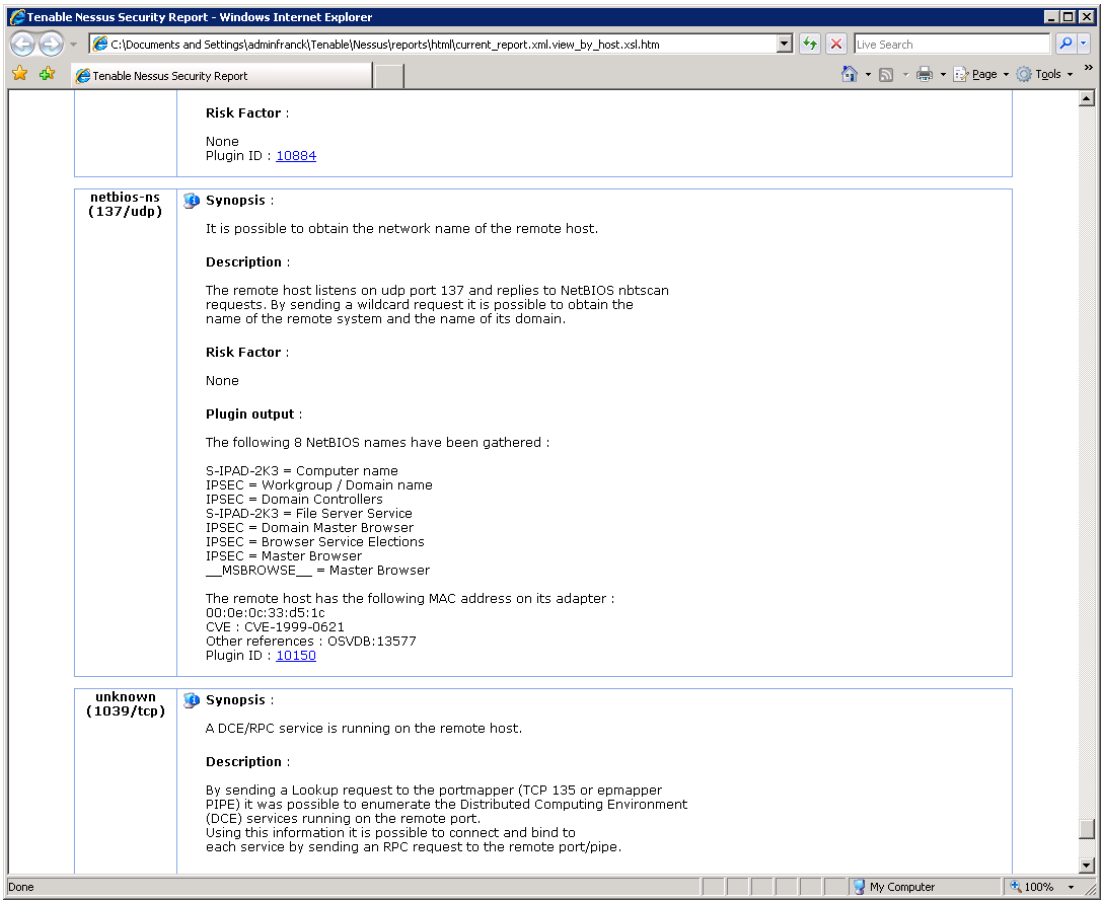
Sakupljanje informacija o resursu može biti prvi korak u planiranju napada tj. iskorištavanja nekih sigurnosnih ili programskih propusta. Program koji je korišten za skeniranje je Nessus[136], slika 7.1. Na modelu je skeniran jedan server.



Slika 7.1. Skeniranje servera (izvor: vlastiti rad)

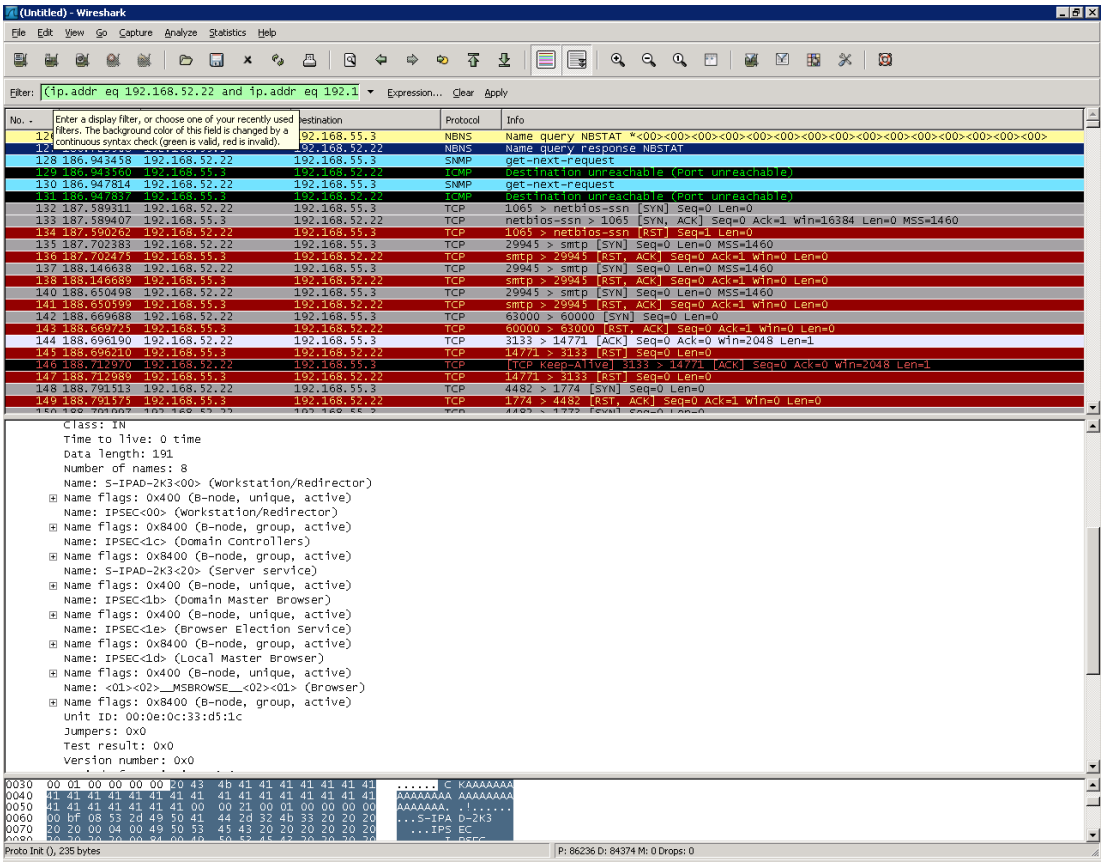
[136] Dostupno na http://www.nessus.org/nessus/ (4.12.2007)

Nessus je skenirao server i dio rezultat koji mogu biti bitni za uspješnost napada su prikazani na slici 7.2.



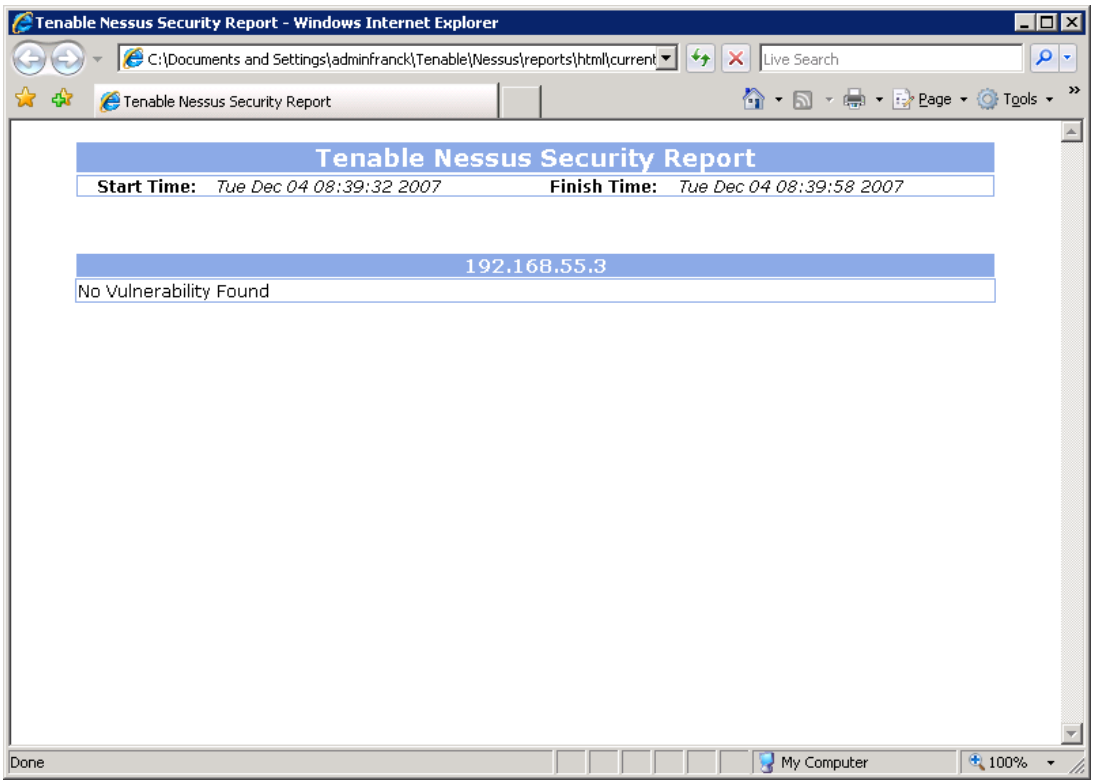
Slika 7.2. Rezultat skeniranja (izvor: vlastiti rad)

Kad se promatra promet na mreži onda upit s računala koje je skeniralo server i odgovor za gore prikazani je na slici 7.3.



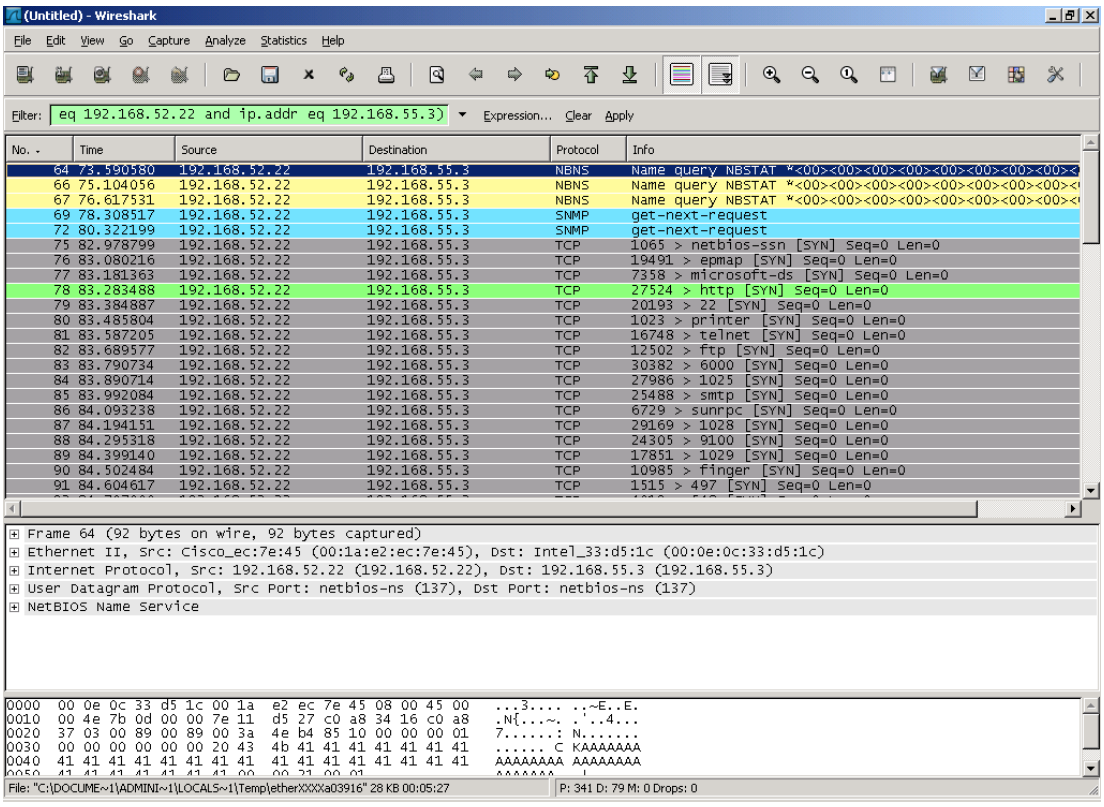
Slika 7.3. Promet na mreži i paket s odgovorom o NetBIOS imenu (izvor: vlastiti rad)

Ako se server izolira na način da sav promet koji dolazi mora biti kriptiran, onda server postaje 'nevidljiv' na mreži. Rezultat skeniranja je sad drugačiji, slika 7.4.



Slika 7.4. Rezultat skeniranja (izvor: vlastiti rad)

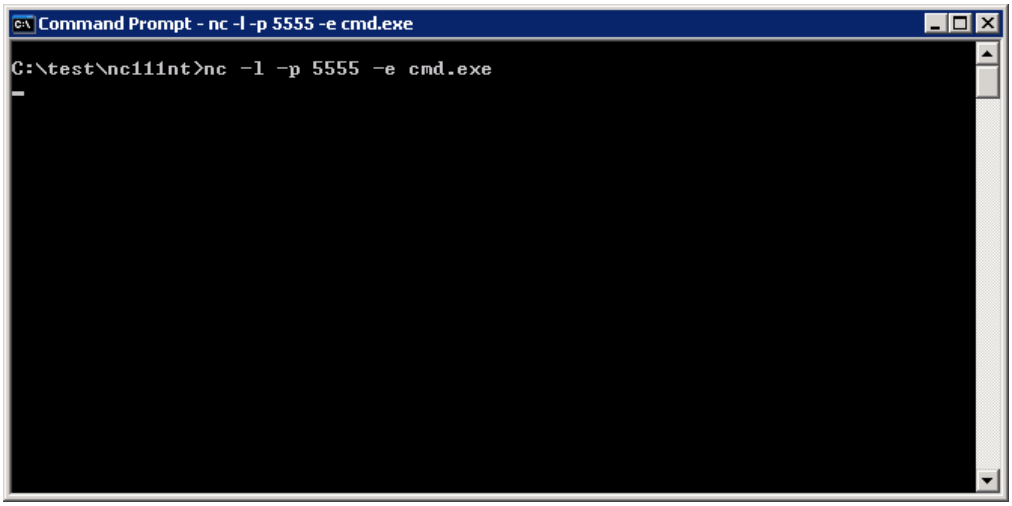
Promet koji je snima na mreži, slika 7.5. pokazuje da server odbija odgovoriti jer nisu zadovoljeni uvjeti koji kažu da promet koji dolazi mora biti kriptiran.



Slika 7.5. Promet na mreži za vrijeme skeniranja (izvor: vlastiti rad)

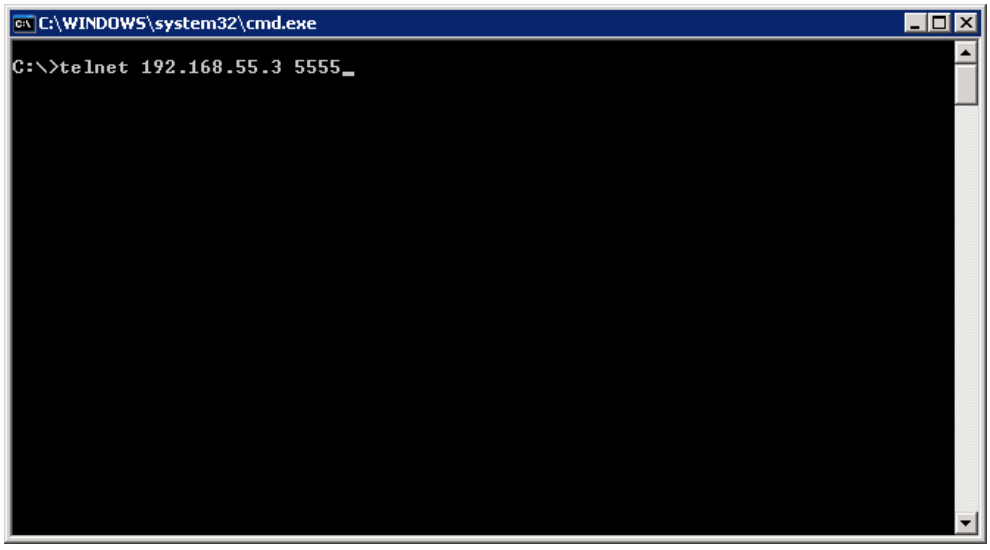
7.2. HAKERSKI NAPADI

Za odabir alata kojim bi se simulirao hakerkerski napada uvjeti su bili da se lako nađe i da je dobro opisan. U ovakvoj situaciji će se biti unutrašnji počinitelj kad se odluči za neku aktivnost. Za ovaj slučaj odabran je alat koji zadovoljava prije navedene uvijete. Radi se o 'netcat'[137] alatu [5]. Da se otvore 'stražnja vrata' i omoguće unutrašnji počinitelju nesmetan ulaz na serveru izvrši se slijedeća naredba, slika 7.6.



Slika 7.6. Otvaranje stražnjih vrata na serveru (izvor: vlastiti rad)

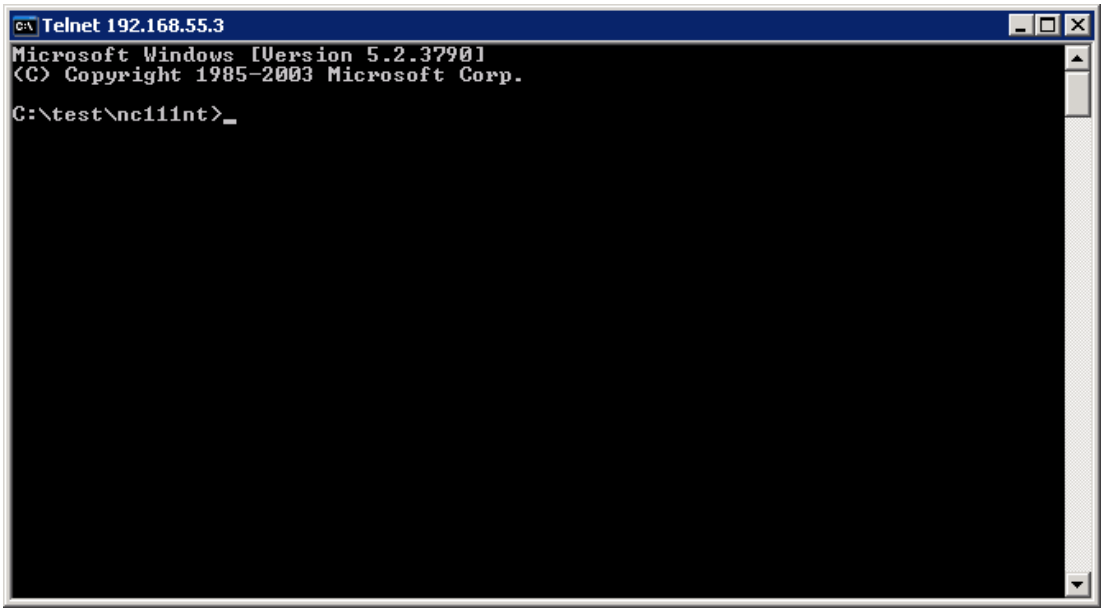
Na svom računalu unutrašnji počinitelj upiše slijedeću naredbu, slika 7.7.



Slika 7.7. Pristup otvorenom portu na serveru (izvor: vlastiti rad)

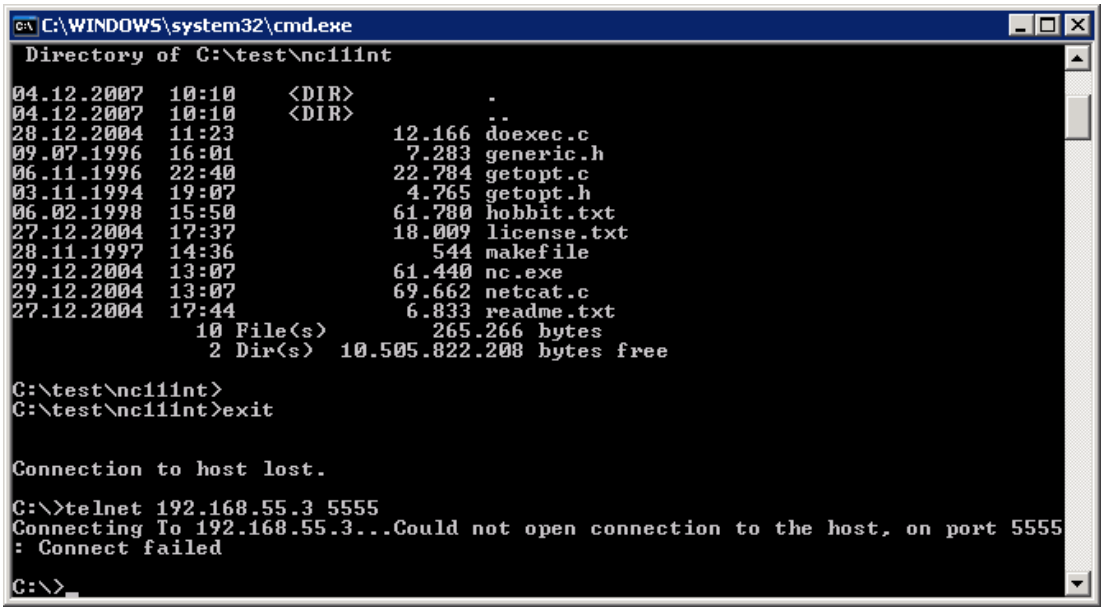
[137] Dostupno na http://www.vulnwatch.org/netcat/ (4.12.2007)

Nakon što se naredba izvrši, slika 7.8., unutrašnji počinitelj ima pristup sistemskom disku s pravima koja mu osiguravaju nesmetano pregledavanje sistemskih datoteka, te kopiranje ili brisanje željenog sadržaja.



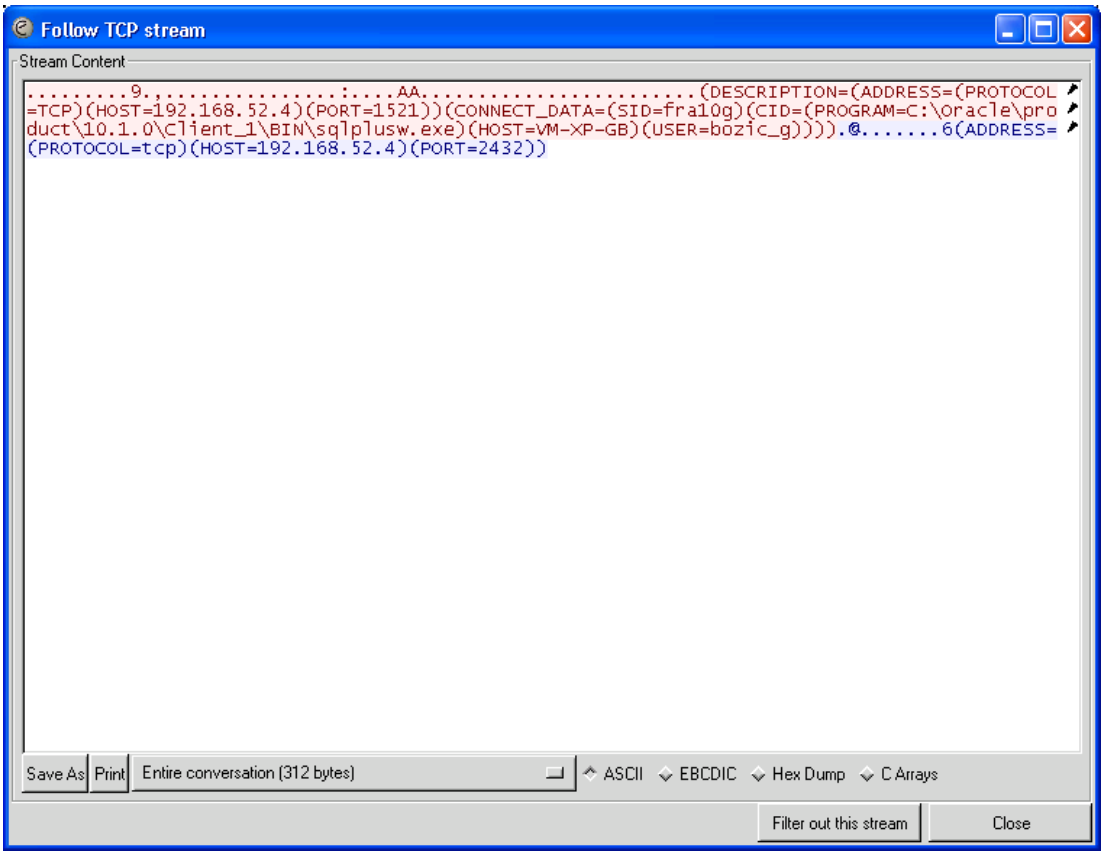
Slika 7.8. Pristup lokaciji s koje je pokrenut program na serveru (izvor: vlastiti rad)

Kad se na serveru implementira IPsec te se kroz politiku definira gdje sav dolazni promet mora biti kriptiran, unutrašnji počinitelj će pri pokušaju da uđe na stražnja vrata dobiti odgovor kako je to prikazano na slici 7.9.

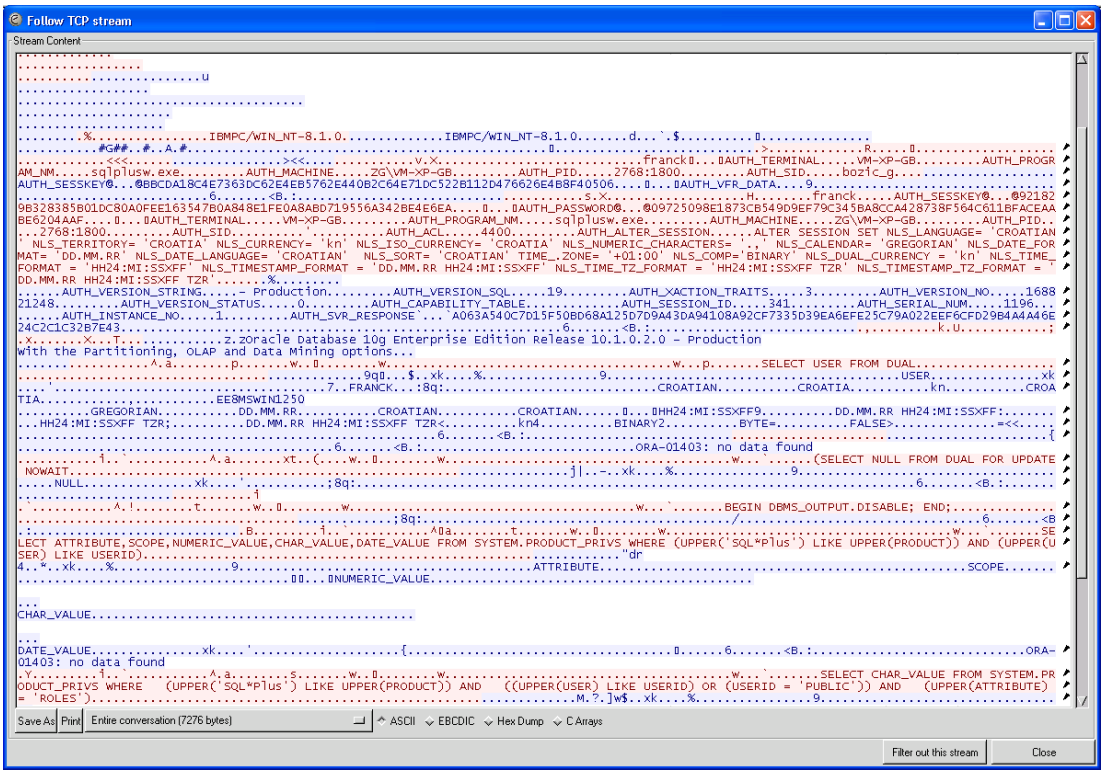


Slika 7.9. Pristup stražnjim vratima kad je IPsec aktivan (izvor: vlastiti rad)

Kad se radi o spajanju korisnika sa SQL*Plus klijentom na bazu podataka promet na mreži izgleda kao na slici 7.10. i 7.11. Iz slike je vidljivo da je moguće doći do 'zanimljivih' podataka o 'connect string' i korisničkom imenu s kojim se ostvaruje konekcija, a koji su važni za neovlašteno dobivanje informacija o drugim korisnicima. Ovo je način da se uz tuđe korisničke informacije povećaju i ovlasti na sustavu.

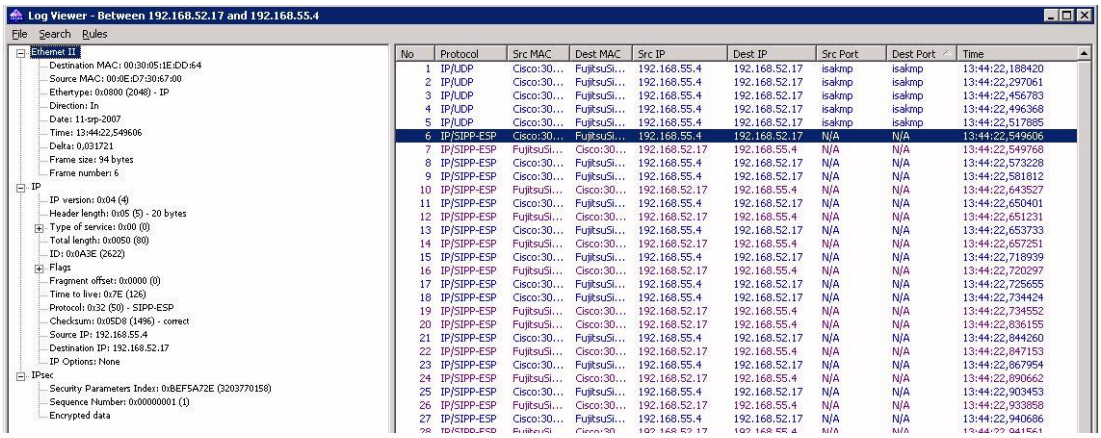


Slika 7.10. Analiza paketa u kome se vide podaci za spajanje na bazu (izvor: vlastiti rad)



Slika 7.11. Analiza paketa u kome se između ostalog nalazi i korisničko ime za spajanje na bazu (izvor: vlastiti rad)

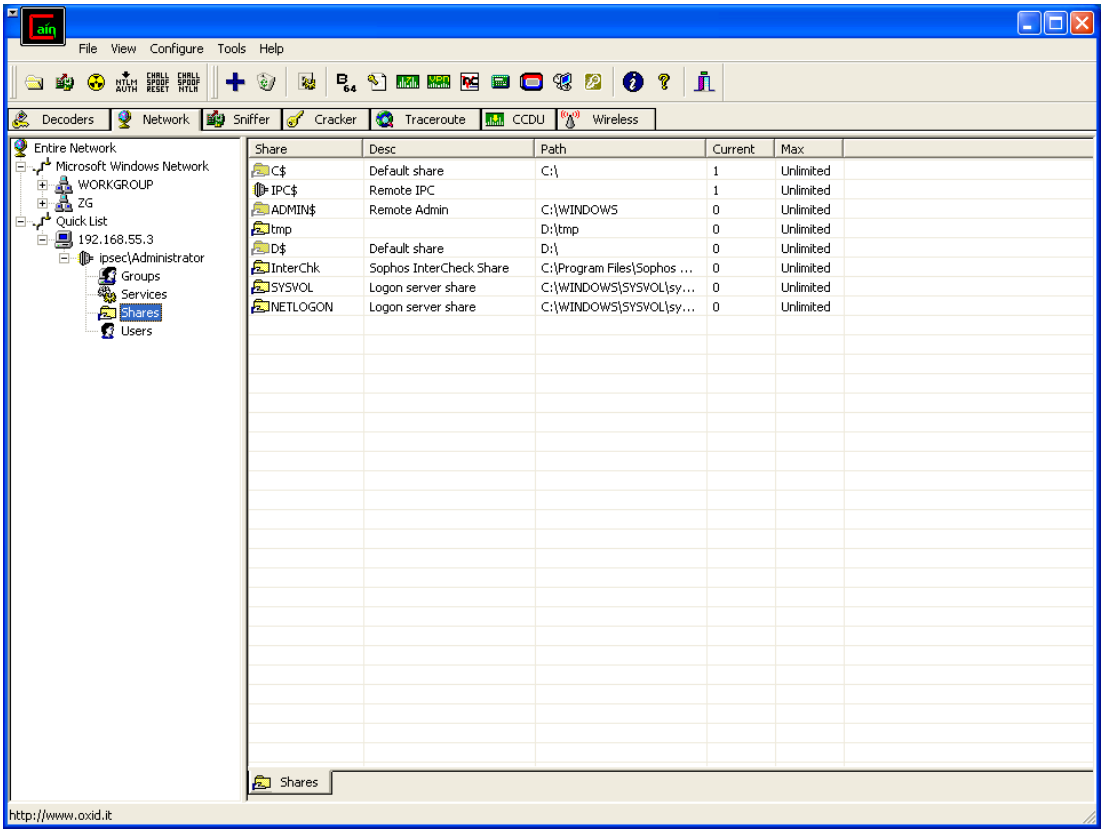
Nakon što se promet kriptiran paket kojima se vrši spajanje izgledaju kao na slici 7.12. Na ovaj način je onemogućeno dobivanje bilo kakvih informacija koje se koriste pri spajanju na bazu podataka.



Slika 7.12. Kriptiran promet za vrijeme spajanja na bazu (izvor: vlastiti rad)

Ako smo na neki način došli do pristupnih prava i ako nam je fizički pristup do resursa onemogućen možemo se poslužiti nekim od programa koji će nam osigurati neograničeni pristup resursu i provedbu željenih akcija. Alat treba

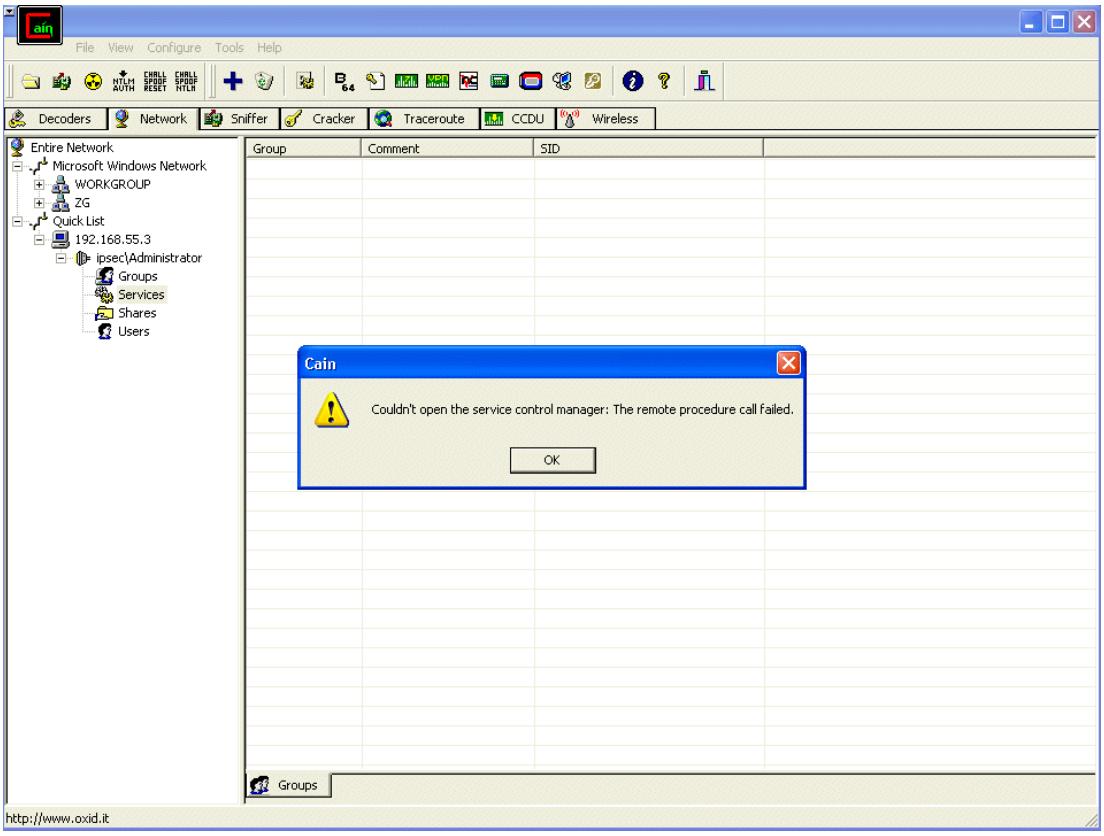
zadovoljiti uvijete da je lako dobavljiv i da je dobro opisan. Za ovaj slučaj odabran je programa 'Cain & Abel'[138]. Na slici 7.13. prikazana je situacija kad se programom pristupa resursu za koga imamo pristupna prava.



Slika 7.13. Pristup serveru s programom 'Cain&Abel' (izvor: vlastiti rad)

Nakon što se primijeni IPsec nije više moguće pristupit resursima. Pristupna prava i dalje vrijede ali server odbija svaki nekriptirani promet ili promet koji nije s predefiniranih IP adresa, slika 7.14.

[138] Dostupno na http://www.softpedia.com/progDownload/Cain-and-Abel-Download-38678.html (4.12.2007)



Slika 7.14. Onemogućen pristup resursa s drugog računala ili ako računalo nema kriptirani promet (izvor: vlastiti rad)

Kroz ove primjere pokazano je da korištenjem IPseca na lokalnoj mreži možemo smanjiti ili ukloniti određene prijetnje kojima unutrašnji počinitelj prijeti informacijskom sustavu na kome se nalazi. Alati koji su korišteni su lako dobavljivi i dobro dokumentirani što je preduvjet da ih unutrašnji počinitelj koristi. Visoko motivirani unutrašnji počinitelj ili informatički obrazovan će koristiti druge metode i tehnike da ostvare svoje ciljeve. No ako mu se ovom tehničkom metodom onemogući provedba dio prijetnji onda mu se izbor smanjuje i pred unutrašnji počinitelj se postavljaju visoke zahtjeve koje mora zadovoljiti da bi ostvario svoje ciljeve.

8. ZAKLJUČAK

Da bi se povećala sigurnost informacijskog sustava nije uvijek nužno da se kupuju razni produkti ili implementiraju sustavi. Dovoljno je poznavati sustav i iskoristiti funkcionalnosti koje su implementirane. Također ne treba uvijek razmišljati o napadaču koji sjedi u nekoj mračnoj sobi u pokušava doći do naših resursa sa kojima možda neće znati što dalje činiti. Dovoljno je pogledati djelatnike u susjednoj sobi koji svjesno ili nesvjesno kompromitiraju sigurnost informacijskog sustava na kome rade i koji dobro znaju što će sa informacijama ili resursima do kojih dođu.

U radu su analizirani unutrašnji zlonamjerni korisnici i načini na koji oni mogu provesti prijetnje. Unutrašnji počinitelji imaju veliki potencijal u kompromitiranju sigurnosti informacijskog sustava, a sustavno se zanemaruje u većem broju sredina. Svjesnost postojanja unutrašnji počinitelj preduvjet je za uspostavljanje kvalitetnije zaštite informacijskog sustava. Na osnovu načina na koje se prijetnje provode identificirane su moguće metode zaštite. Dio prijetnji moguće je smanjiti ili ukloniti tehničkom metodom. Iskorišten je IPsec kao već postojeća implementirana funkcionalnost. IPsec je standard i skup protokola. Model na kome je provedena analiza učinkovitosti odražava realne uvijete kakvi vladaju na informacijskom sustavu. Na modelu su provedeni napadi kad nije bio aktivan IPsec da bi se potvrdio zaključak o mogućnostima unutrašnji počinitelj. Alati kojima su provedeni napadi morali su zadovoljiti uvijte da su lako dobavljivi sa interneta i da su dobro dokumentirani. Na ovaj način unutrašnji počinitelju se povećavaju šanse da se napad izvede. Zbog jednostavnosti analize perimetar je postavljen na jedan resurs i napadi su ponovljeni u takvim uvjetima. Na osnovu rezultata provedene analize može se potvrditi hipoteza koja kaže da koristeći IPsec na lokalnoj mreži mogu biti smanjene prijetnje

unutrašnjih zlonamjernih korisnika i na taj način povećati sigurnosti informacijskog sustava.

Ostale spoznaje do kojih se tokom analize su:

- IPsec omogućava fino definiranje perimetra, a da pri tome nisu potrebna financijska ulaganja ili fizičke intervencije.
- IPsec smanjuje ili uklanja samo dio prijetnji te ga čini primjenjivim za podizanje sigurnosti informacijskog sustava.
- Pokazala se potreba za metodologijom implementacije i testiranja IPsec-a na lokalnoj mreži.
- IPsec treba promatrati i u kontekstu unutrašnji počiniteljskog alata.
- Unutrašnji počinitelju su zlonamjerni korisnici kojima se ne pridaje dovoljno pažnje u usporedbi sa štetom koju mogu napraviti.

Sigurnost IPsec-a u mnogome ovisi o znanju, jer implementirana rješenja danas omogućavaju krajnjim korisnicima korištenje manje sigurnih metoda autentifikacije i mogućnost odabira manje sigurnosnih protokola. Promjene u standardima i preporukama pokazuju da se pronađeni sigurnosni propusti ugrađuju a shodno tome se prilagođavaju i proizvođači. Zbog različitih kompromisa koji su proizvođači prisiljeni raditi, imamo i različita 'ponašanja' IPseca. Ovom činjenicom se koriste i napadači da bi otkrili o kojem se IPsec VPN sustavu radi i prema tome prilagodili plan napada. s druge strane je otežan način detekcije takvih sustava na lokalnoj mreži ako se njime služe unutrašnji počinitelji.

LITERATURA

Popis literature

[1] UNUTRAŠNJI POČINITELJ THREAT: PROTECTING THE ENTERPRISE FROM SABOTAGE, SPYING, AND THEFT, Eric Cole and Sandra Ring, Syngress,

[2] Bača, M. (2004) Uvod u računalnu sigurnost, Narodne novine, Zagreb

[3] Smith, B., Komar, B. (2005) Microsoft Windows Security Resource Kit, Second Edition, Microsoft

[4] Lewis, M. (2004) Trobleshooting Virtual Private Networks, Cisco Press

[5] Keith, J. J., (2002) Anti-hacker Tool Kit, McGraw-Hill/ Osborne

[6] White, G., Conklin, A., Cothren, C., Davis, R., Williams, D., (2003) Security+ CertificationA ll-in-One Exam Guide, McGraw-Hill/ Osborne

[7] Doyle, J., DeHaven Carroll, J., (2001) Routing TCP/IP, Volume I, Cisco Press

[8] Doyle, J., DeHaven Carroll, J., (2001) Routing TCP/IP, Volume II, Cisco Press

[9] Isaca, (2001) Virtual Private Networking: New Issues for Network Security, Isaca

Popis Internet izvora

[10] http://www.cert.org/archive/pdf/ecrimesummary07.pdf

(Preuzeto: 01.09.2007)

[11] http://www.cert.org/archive/pdf/bankfin040820.pdf

(Preuzeto: 01.09.2007)

[12] "Domain Isolation with Microsoft Windows Explained" na http://go.microsoft.com/fwlink/?LinkId=44642

[13] "Server Isolation with Microsoft Windows Explained" na http://go.microsoft.com/fwlink/?LinkId=44641.

[14] "Domain Isolation Planning Guide for IT Managers" http://go.microsoft.com/fwlink/?LinkId=44645

[15] "A Guide to Domain Isolation for Security Architects" at http://go.microsoft.com/fwlink/?LinkId=44643

[16] http://www.unixwiz.net/techtips/iguide-IPsec.html (Preuzeto: 30.10.2007)

[17] http://technet2.microsoft.com/windowsserver/en/library/2a2f7792-5a4a-438b-8711-23694ae56e3a1033.mspx?mfr=true (Preuzeto: 30.10.2007)

[18] Message Authentication Code - Wikipedia, the free encyclopedia, dostupno na http://en.wikipedia.org/wiki/Message_Authentication_Code (Preuzeto: 30.10.2007)

[19] SA Security - 2.1.7 What are Message Authentication Codes?, dostupno na http://www.rsasecurity.com/rsalabs/node.asp?id=2177 (Preuzeto: 30.10.2007)

[20] HMAC - Wikipedia, the free encyclopedia, dostupno na http://en.wikipedia.org/wiki/HMAC (Preuzeto: 30.10.2007)

[21] IETF Web stranica vezana uz protokol je sljedeća: http://www.ietf.org (Preuzeto: 30.10.2007)

[22] The MD5 Message-Digest Algorithm, http://www.ietf.org/rfc/rfc1321.txt, (Preuzeto: 30.10.2007)

[23] US Secure Hash Algorithm 1 (SHA1), http://www.ietf.org/rfc/rfc3174.txt, (Preuzeto: 30.10.2007)

[24] IP Encapsulation within IP, http://www.ietf.org/rfc/rfc2003.txt, (Preuzeto: 30.10.2007)

[25] Security Architecture for the Internet Protocol, http://www.ietf.org/rfc/rfc2401.txt, (Preuzeto: 30.10.2007)

[26] IP Authentication Header, RFC 2402, http://www.ietf.org/rfc/rfc2402.txt, (Preuzeto: 30.10.2007)

[27] IP Encapsulating Security Payload (ESP), RFC2406, http://www.ietf.org/rfc/rfc2406.txt, (Preuzeto: 30.10.2007)

[28] The Internet Security Association and Key Management Protocol, RFC 2408, http://www.ietf.org/rfc/rfc2408.txt, (Preuzeto: 30.10.2007)

[29] The Internet Key Exchange, http://www.ietf.org/rfc/rfc2409.txt, RFC 2409, http://www.ietf.org/rfc/rfc2409.txt, (Preuzeto: 30.10.2007)

[30] The OAKLEY Key Determination Protocol, RFC 2412, http://www.ietf.org/rfc/rfc2412.txt, (Preuzeto: 30.10.2007).

[31] "An Illustrated Guide to IPsec." Steve Friedl, (Preuzeto: 21.11.2007).

[32] "Cryptography in Theory and Practice: The Case of Encryption in IPsec." Kenneth G. Paterson and Arnold K.L. Yau, ePrint Archive, (Preuzeto: 21.11.2007)

[33] "A DoS Attack Against the Integrity-Less ESP (IPsec)." Ventzislav Nikov, ePrint Archive, (Preuzeto: 21.11.2007)

[34] Common VPN Security Flaws, Publication Date: 25th January 2005, Author: Roy Hills, http://www.nta-monitor.com/posts/2005/01/vpn-flaws.html, (Preuzeto: 21.11.2007)

[35] http://www.nta-monitor.com/wiki/index.php/Ike-scan_Documentation, (Preuzeto: 21.11.2007)

[36] Penetration Testing IPsec VPNs, http://www.securityfocus.com/infocus/1821, (Preuzeto: 21.11.2007)

[37] Ike-scan User Guide, http://www.nta-monitor.com/wiki/index.php/Ike-scan_User_Guide, (Preuzeto: 21.11.2007)

[38] A Cryptographic Evaluation of IPsec, *N. Ferguson and B. Schneier*, http://www.schneier.com/paper-IPsec.html, (Preuzeto: 21.11.2007)

[39] Bezbednost IP Virtuelnih Privatnih Mreža, http://www.telfor.org.yu/telfor2003/radovi/2-7.pdf, (Preuzeto: 21.11.2007)

[40] Penetration Testing IPsec VPNs http://www.securityfocus.com/infocus/1821 (Preuzeto: 03.12.2007)

Popis normi

[41] BS ISO/IEC 17799:2005 BS 7799-1:2005, Informacijska tehnologija – Sigurnosne tehnike – Kodeks postupaka za upravljanje informacijskom sigurnošću

Bazična dokumentacijska kartica na hrvatskom jeziku

MRIZ (FOI – Sveučilište Zagreb) UDK: 004.056(043)

Specijalistički rad

Primjena IPsec-a u sprječavanju unutarnjih

zlonamjernih počinitelja

G. Božić

Fakultet organizacije i informatike

Varaždin, Hrvatska

Virtual Private Network (VPN) je tehnologija koja omogućava sigurno povezivanje računala u virtualne privatne mreže preko javne mrežne infrastrukture, a IPsec se vrlo često koristi kao 'protokol'. U posljednje se vrijeme IPsec sve više implementira i u mrežne operacijske sustave. Proizvođači mu primjenu vide u povećanju sigurnosti na mreži. Kolika je stvarna korist ove tehnike analizirano je na testnom sustavu na kojem je korišten operacijski sustav od Microsoft-a. Učinkovitost je analizirana kroz smanjivanje prijetnji unutrašnjih zlonamjernih korisnika ili unutrašnji počinitelj. Tijekom analize prijetnji i načina izvođenja došlo je do spoznaje da IPsec može biti iskorišten i od strane unutrašnji počinitelj, da se zaštiti od kontrole sadržaja. Različite implementacije IPsec-a se različito ponašaju za vrijeme penetracijskog testiranja tako da će se neki IPsec VPN sustave lakše detektirati, a druge teže. Standardi i preporuke neke 'opcije' nisu strogo definirali tako da su ih proizvođači implementirali prema svojim mišljenjima. Rezultati analize učinkovitosti IPsec-a na lokalnoj mreži pokazuju da se određene prijetnje smanjuju ili potpuno uklanjaju.

Voditelj rada: prof.dr.sc. Miroslav Bača

Povjerenstvo za ocjenu i obranu: prof.dr.sc. Miroslav Bača,
prof.dr.sc. Zdravko Krakar,
prof.dr.sc. Željko Hutinski.

Obrana: 17. Lipanj 2008 **Promocija**:

Rad je pohranjen u Biblioteci Fakulteta organizacije i informatike u Varaždinu.

(168 stranica, 88 slike, 29 tablica, original na hrvatskom)

G. Božić

MRIZ-5

UDK: 004.056(043)

1. Primjena IPsec-a u sprječavanju unutarnjih zlonamjernih počinitelja

I Božić, G

II. Fakultet organizacije i informatike, Varaždin, Hrvatska

IPsec

Prijetnje

Unutrašnji počinitelj

Penetracijsko testiranje

Revizija

Sigurnost

Basic documentation card in English language

MRIZ (FOI – University of Zagreb) UDK: 004.056(043)

Using IPsec for decrease threat from Insiders

G. Božić

Faculty of Organization and Information Science

Varaždin, Croatia

Virtual Private Network is technology for safe connection computer in virtual private networks over public infrastructure, where IPSec is usually used like 'protocol'. Today many vendors implement IPSec in operation system for increase security on local area connection. How many had useful this technique we analyzing on system where are implement Microsoft operation system. Efficacy IPsec was analyzing through decrease threat from insiders. Analysis method of Insiders threat we conclude that IPSec malicious users can use IPSec for your needs, for example protect content own traffic on LAN. Different implementation IPsec has different behavior during penetration testing. For this reason we some IPsec implementation easily detect and some very hardly. Some options were not define strong and vendors they options implement on different way. Result analyze, on test model, indicate that IPsec decrease threat from insiders.

Supervisior: Dr.sc. Miroslav Bača

Examiniers: Dr.sc. Miroslav Bača, Dr.sc. Zdravko Krakar,
Dr.sc. Željko Hutinski

Oral examination: 06/17/2008

The Paper is stored at the Library of the Faculty of Organization and

Information Science in Varaždin.

(168 pages, 88 figures, 29 tables, original in Croatian)

G. Božić

MRIZ-5

UDK: 004.056(043)

1. Using IPsec for decrease threat from insiders

I Božić, G

II. Faculty of Organization and Information Science, Varaždin, Croatia

IPsec

Treats

Insider

Penetration test

Audit

Security