SVEUČILIŠTE U RIJECI

POMORSKI FAKULTET U RIJECI

Marin Oplanić

MODEL KONFIGURACIJE VATROZIDA ZA ECDIS SUSTAV S INMARSAT POVEZIVANJEM NA INTERNET

DIPLOMSKI RAD

Rijeka, 2014.

SVEUČILIŠTE U RIJECI

POMORSKI FAKULTET U RIJECI

MODEL KONFIGURACIJE VATROZIDA ZA ECDIS SUSTAV S INMARSAT POVEZIVANJEM NA INTERNET

Firewall Configuration Model for ECDIS with INMARSAT Internet Connection

DIPLOMSKI RAD

Kolegij: Sigurnost informacijskih sustava

Mentor: prof.dr.sc. Boris Sviličić

Student: Marin Oplanić

Matični broj: 0112039827

Studij: Elektroničke i informatičke tehnologije u pomorstvu

Rijeka, 2014.

Student: Marin Oplanić

Studijski program: Elektroničke i informatičke tehnologije u pomorstvu

JMBAG: 0112039827

IZJAVA

kojom izjavljujem da sam diplomski rad s naslovom „Model konfiguracije vatrozida za ECDIS sustav s INMARSAT povezivanjem na Internet“ izradio samostalno pod mentorstvom dr. sc. Borisa Sviličića.

U radu sam koristio literaturu koja je navedena na kraju diplomskog rada. Tuđe spoznaje, stavove, zaključke, teorije i zakonitosti koje sam izravno ili parafrazirajući naveo u diplomskom radu na uobičajen, standardan način citirao sam i povezao s korištenim bibliografskim jedinicama.

Suglasan sam s objavom diplomskog rada na službenim stranicama.

Marin Oplanić

ZAHVALA

Tijekom izrade diplomskog rada nailazio sam na niz problema, pa bih stoga posebno zahvalio mentoru prof. dr. sc. Borisu Sviličiću na razumijevanju, podršci i korisnim savjetima.

SADRŽAJ:

1. UVOD

Sigurnost informacijskih sustava danas je nezaobilazan pojam koji se veže uz informatičko doba u kojem živimo. Moderni informacijski sustavi neizbježno postaju kompleksniji, sa ciljem postizanja bolje konkurentnosti. Obzirom na tu činjenicu, konfiguriranje sigurnosnih mjera sa ciljem očuvanja povjerljivosti, cjelovitosti i raspoloživosti podataka osnovna je stavka za razmatranje prilikom uspostavljanja svake informatičke infrastrukture. Sigurnost bilo kojega informatičkog sustava morala bi biti primjerena sigurnosnim rizicima.

Ovaj rad prezentira problematiku koja obuhvaća zaštitu brodskog informacijskog sustava ECDIS, uporabom vatrozida. „Vatrozid je softver ili hardver kojim se provjeravaju podaci pristigli putem Interneta ili mreže, a zatim, ovisno o postavkama, odbacuju ili propuštaju do računala.“ [1]

ECDIS (Electronic Chart Display and Information System) je kompjuterski navigacijski sistem koji se koristi kao zamjena za klasične navigacijske karte. Objedinjujući i obrađujući brojne informacije u realnom vremenu, sustav je sposoban konstantno određivati točnu poziciju broda. Postoji stoga, potreba za osvježavanjem navigacijskih karata i trenutne pozicije. Neophodno je spajanje na poslužitelj, a jedino kvalitetno rješenje predstavlja povezivanje na Internet putem satelita.

Danas postoje brojni davatelji usluga satelitskog Interneta u domeni pomorstva. Jedan od najpopularnijih je INMARSAT, koji je obrađen u ovom radu. Predstavila ga je IMO organizacija 1979. godine, kako bi omogućila brodovima stalnu vezu sa kopnom. Rad pretpostavlja spajanje sustava ECDIS na Internet putem INMARSAT satelitske veze. Pozivanjem na konkretne službene tekstove, jasno se dokazuje ili opovrgava mogućnost korištenja INMARSAT usluge prilikom spajanja na Internet za sustave ECDIS.

U radu su predstavljene opasnosti koje prijete informacijskom sustavu broda, osobito sustavu ECDIS, sigurnosni rizici, te metode minimiziranja istih. Drugo poglavlje se bavi analiziranjem sustava ECDIS koji je predstavljen kao novija alternativa klasičnim navigacijskim kartama. Prikazana su svojstva ECDIS-a, te je navedeno zašto ga je potrebno štiti i od čega. Temeljna pretpostavka cijelog rada je pristup

sustava ECDIS Internetu, pa su predstavljeni razlozi zbog kojih je nužno spajanje na Internet radi automatskog ažuriranja karata.

Nakon definiranja sustava ECDIS, odnosno načina spajanja na Internet, i vrste veze koju zahtjeva, potrebno je pronaći odgovarajuće davatelje usluge Interneta. U slučaju kada je brod u plovidbi, nije moguće spajanje na Internet uobičajenim putem. Stoga se postavlja pitanje kako se spojiti na Internet, za vrijeme plovidbe. Satelitsko povezivanje je najučinkovitiji način, te je u današnje vrijeme vrlo rašireno. Pojavile su se na tržištu mnoge kompanije koje pružaju usluge satelitskog Interneta, a INMARSAT je jedna od vodećih i vjerojatno najraširenijih. Treće poglavlje prikazuje dva INMARSAT servisa koja su pogodna za sustave ECDIS. Predstavljeni su svaki posebno, te su navedene njihove osnovne karakteristike.

Prva tri poglavlja daju uvod u sustav ECDIS i servise koji se upotrebljavaju za povezivanje na Internet. Poznavanje rada ECDIS-a prilikom ažuriranja, te poznavanje servisa i njihovih osnovnih karakteristika nužan je preduvjet za detaljniji uvid u tematiku zaštite ECIDS-a. Stoga, tek nakon definiranja osnovnih svojstava INMARSAT servisa može se dublje analizirati način prijenosa podataka putem satelita. Četvrto poglavlje daje uvid u protokole i portove koje koristi INMARSAT internetska veza. Upotrebljava se IP referentni model, kojega se uspoređuje sa osnovnim OSI referentnim modelom. Opisuju se osnovni slojevi IP modela, te protokoli koji se koriste unutar istog. Objašnjena je pouzdanost TCP protokola i nepouzdanost IP protokola, te su navedeni nazivi podataka po slojevima i protokolima. Definiran je način uspostave veze na tehničkoj razini za TCP protokol (tzv. trostruko rukovanje) koji je osnova za prijenos podataka.

Nakon definiranja protokola i portova, te analize istih moguće je prihvatiti da svaka vrsta veze ima određene „propuste“. Treba naglasiti da sve poruke integrirane unutar protokola („Echo“ kod ICMP primjerice) imaju ulogu olakšati ili doprinijeti bržem, kvalitetnijem i sigurnijem prijenosu podataka, a opet danas postoje mnogi načini kako ih zlorabiti. Iz tog je razloga nepravedno nazivati „propustima“ poruke koje mogu u značajnoj mjeri unaprijediti prijenos podataka. Primjer protokola koji se može iskoristiti na zlonamjeran način je ICMP. Poruke koje ICMP šalje od velike su koristi za otkrivanje grešaka prilikom slanja podataka, međutim mnoge od njih mogu

biti zlorabljene za otkrivanje informacija zlonamjernom napadaču. Glavne tehnike koje iskorištavaju dobru prirodu TCP/IP protokola predstavljene su u petom poglavlju.

U šestom poglavlju definiran je i predstavljen zaštitni uređaj. Opisane su vrste vatrozida, i njihove osnovne značajke. Također, bitno je naglasiti da su u radu prezentirane postavke Windows vatrozida budući je besplatan, a većina proizvođača ECDIS uređaja se odlučuje za Windows operativni sustav. Ono na što se mora također obratiti pozornost je razlika između hardverskih i softverskih vatrozida. U radu je korišten Windowsov vatrozid, dok se u praksi uz softverske koriste i hardverski poput Stratos Trench-a i sličnih.

U završnom, sedmom poglavlju prikazana je konfiguracija postavki Windows vatrozida za ECDIS sustav, koja je izrađena za pretpostavljenu situaciju spajanja (slika 23). Jasno je da je svaka unutarnja konfiguracija mreže različita za svaki brod. Stoga je nemoguće odraditi jednu konfiguraciju postavki za svaku vrstu unutarnje mreže. Upravo iz tog razloga situacija spajanja sustava ECDIS na Internet određena je proizvoljno. Postavke vatrozida prate sve protokole navedene u prethodnim poglavljima, te su konfigurirane na takav način da sprječavaju napade opisane u petom poglavlju. Kako bi se maksimalno iskoristile mogućnosti Windows vatrozida, potrebno je poznavati sve njegove mogućnosti, pa se u završnom poglavlju i tome posvećuje pažnja. Za svaki protokol posebno su postavljene restrikcije. Definirane su postavke za dolazni i za odlazni promet, te je dan detaljan uvid, u sve postavke konfiguracije vatrozida.

2. ECDIS – Electronic Chart Display and Information System

Izrada konfiguracije vatrozida u radu temelji se na spajanju sustava ECDIS na Internet putem satelita. Stoga, potrebno je prezentirati što je sustav ECDIS u svojoj osnovi, te objasniti zašto mu je potreban izlaz na Internet.

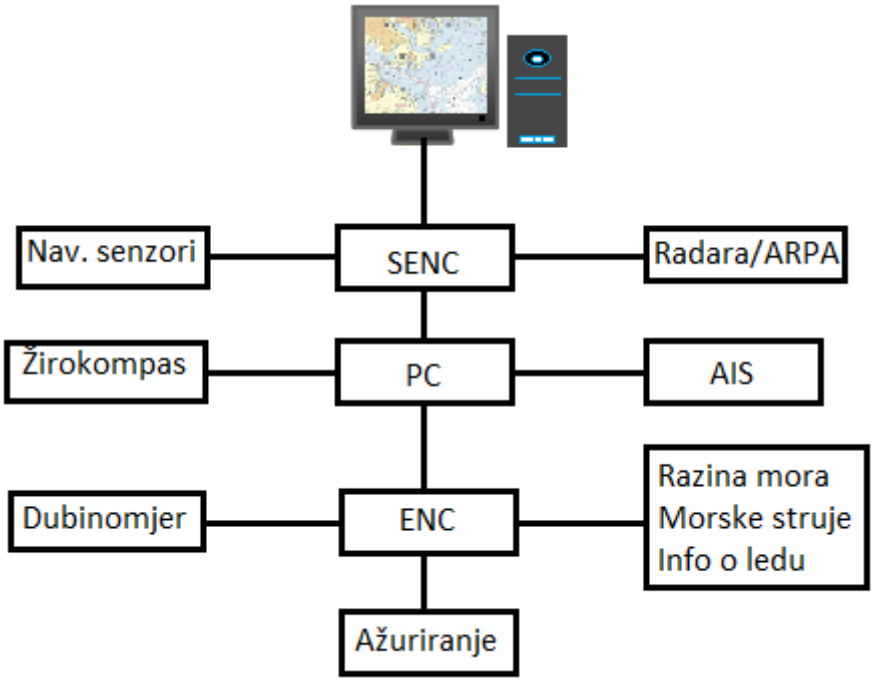
Elektroničke karte su relativno nova tehnologija koja pruža značajne prednosti u sigurnosti navigacije. Važno je napomenuti da u sustav elektroničkih karata ne ulazi samo elektronički prikaz istih na ekranu, već je to sustav koji u realnom vremenu objedinjuje i procesuira mnoge različite informacije. ECDIS u svakom vremenskom trenutku kontinuirano određuje poziciju broda u odnosu na kopno ili neku drugu točku na karti.

IMO (International Maritime Organization) propisuje standarde za sustav ECDIS. Prema tome, postoje određena pravila koja detaljno određuju način na koji mora sustav raditi, kako bi bio kvalitetna alternativa običnim nautičkim kartama. Kongsberg-ov sustav ECDIS se može vidjeti na slici 1.

Slika 1. Prikaz K – „bridge“ ECDIS (Kongsberg) sistema [1.1]

Standarde vezane za ECDIS propisuje SOLAS konvencija poglavljem V (V/19, V/27), gdje su jasno navedeni minimalni zahtjevi za brodove opremljene sustavom elektroničkih karata. Ovi zahtjevi jasno definiraju prihvatljivost ECDIS-a samo u slučaju mogućnosti osvježavanja karata u realnom vremenu. ECDIS mora imati

najmanje jednu vezu sa sistemima za određivanje pozicije, i jednu sa žiro-kompasom. Sa stanovišta raspoloživosti, zahtjeva se zaštita sustava elektroničkih karata UPS-om (uninterruptible power supply) koji je sposoban 45 sekundi održavati u radu ECDIS, dok se ne uključi glavni pomoćni izvor napajanja broda.



Slika 2. Prikaz sustava ECDIS i njegovih veza [2.1]

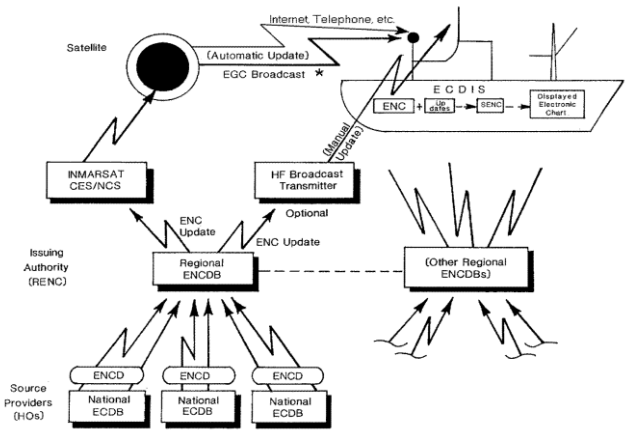
Slika 2 predstavlja sustav ECDIS kroz razinu blokova. Središte sustava ECDIS je računalo (PC) koje usklađuje, obrađuje i zaprima informacije od svih veza. Pretpostavljena je redundancija većine navigacijskih senzora, (npr. GPS-a), stoga kvar jednoga od njih neće onesposobiti cijeli sustav. Međutim, pojavom kvara na računalu, cijeli sustav elektroničkih karata gubi svoju funkciju.

Upravo iz razloga što se cijeli sustav temelji na ispravnosti računala, očuvanju integriteta i vjernosti podataka na njemu, postoji zahtjev za povećanjem sigurnosti računala. Najveća opasnost za ECDIS dolazi iz bloka „ažuriranje“ (slika 2). Unutar tog bloka, sadržana je cijela logistika vezana za osvježavanje karata.

Prema [2] postoje dva glavna načina osvježavanja karata :

- Ručno ažuriranje – operater ubacuje informacije ručno u sustav ECDIS. Struktura tih informacija mora biti kompatibilna sa zahtjevima danima propisima IHO organizacije.
- Automatsko ažuriranje – sastoji se od procesa osvježavanja baze podataka bez potrebe za intervencijom. Naravno, i u ovom slučaju informacije moraju biti usklađenog formata danog propisima IHO organizacije. Automatsko ažuriranje može biti:
    - Potpuno automatsko ažuriranje - metoda osvježavanja kod koje nije nužna intervencija operatera. Postiže se najčešće povezivanjem putem Interneta na server sa kartama.
    - Polu – automatsko ažuriranje – metoda osvježavanja koja zahtjeva intervenciju operatera do određene mjere. Uloga je operatera da uspostavi vezu između medija korištenog za ažuriranje i baze sustava ECDIS.

Prikaz ažuriranja ECDIS baze podataka na razini blokova dan je slikom 3.



Slika 3. Blokovski prikaz ažuriranja ECDIS baze podataka [3.1]

Legenda:

ECDB – „Electronic chart data base“

EGC – „Enhanced group call“

ENC – „Electronic navigational chart“

ENCD – „Electronic Navigational Chart Data“

ENCDB – „Electronic Navigational Chart Data Base“

HO – „Hydrographic Office“

INMARSAT –„ International Mobile Satellite Organization“

RENC – „Regional ENC Coordinating Centre“

SENC – „System Electronic Navigational Chart“

IHO publikacija S - 52 [3] u prilogu 1, poglavlju 3, detaljno daje naputke za ECDIS proizvođače u vezi ažuriranja. ECDIS mora imati sposobnost povezivanja sa INMARSAT C EGC SafetyNET prijemnicima za direktni prijenos podataka. Ovaj način povezivanja odnosi se na automatsko ažuriranje.

S druge strane, kod polu-automatskog ažuriranja ECDIS mora imati sposobnost ažuriranja u standardnom formatu propisanom od IHO organizacije, te preko telefonske mreže. Budući da je za ovaj rad bitno automatsko ažuriranje preko Interneta, interesantno je primijetiti kako IHO organizacija podupire korištenje INMARSAT C usluge za osvježavanje elektroničkih karata. Danas postoji C-MAP „CM-93/3“ standardni format za prijenos elektroničkih karata koji je u skladu sa IHO zahtjevima (S-57/3).

2.1. Zaključak poglavlja

ECDIS je sustav elektroničkih karata kojim se povećava sigurnost plovidbe. Zahtjeva povezivanje na Internet zbog mogućnosti primanja aktualnih novosti vezanih za sigurnost plovidbe, te zbog automatskog osvježavanja karata. Budući da su u ovom poglavlju definirani razlozi spajanja na Internet, slijedeće što treba razmotriti je način spajanja na Internet putem satelita. Treće poglavlje opisuje osnovne značajke INMARSAT servisa, te njihove pogodnosti za ECDIS sustave.

3. INMARSAT

Za izradu konfiguracije postavki vatrozida nužno je poznavati kakvu vezu na Internet koristi ECDIS, odnosno kakvu vezu na Internet omogućava INMARSAT kao davatelj usluge satelitskog Interneta. Ovo poglavlje definira dva INMARSAT servisa koja su pogodna za primjenu kod sustava ECDIS.

INMARSAT je vodeći davatelj usluga za satelitske komunikacije na svijetu. Danas već postoji veliki broj raznih servisa koji omogućuju satelitsku telefoniju, Internet, prijenos podataka itd.. Postoji pet INMARSAT ogranaka:

- INMARSAT Maritime
- INMARSAT Government US
- INMARSAT Global Government
- INMARSAT Enterprise
- INMARSAT Aviation

Svakako za ovaj rad je najinteresantniji INMARSAT Maritime koji se fokusira na pružanje usluga satelitskih veza u pomorstvu. Iz područja pomorske satelitske komunikacije, INMARSAT nudi dva servisa koja mogu poslužiti za ažuriranje elektroničkih karata ECDIS-a.

- INMARSAT C EGC safetyNET
- INMARSAT FleetBroadband

3.1. INMARSAT C EGC safetyNET

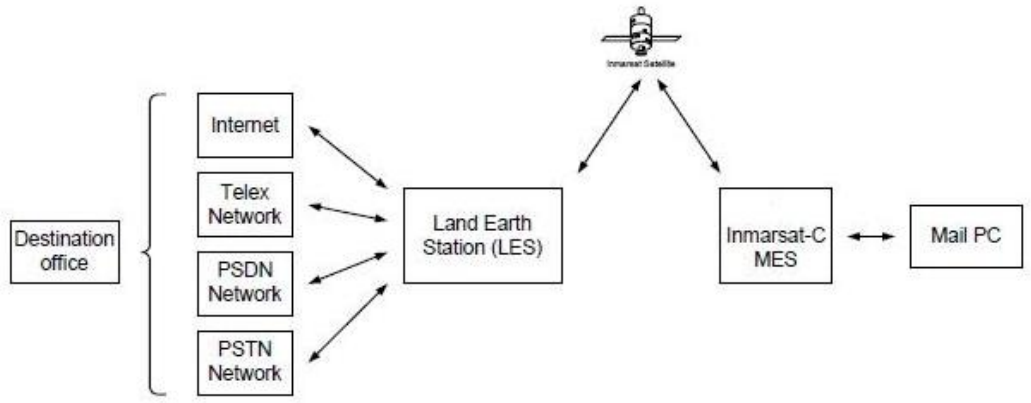
INMARSAT C je dvosmjerni komunikacijski sistem koji omogućuje manipulaciju podacima i porukama do 32 kb dužine. Svi noviji INMARSAT C terminali imaju integriran GNSS prijemnik (Globalni Navigacijski Satelitski Servis) za automatsko ažuriranje pozicije, što je korisno kod poziva u pomoć (engl. distress call). Također, INMARSAT C omogućuje EGC SafetyNET poruke.

EGC (Enhanced Group Call) označava globalni automatski servis koji omogućuje prosljeđivanje komercijalnih i MSI (Marine Safety Information) poruka grupama

brodova koji se nalaze u određenom geografskom području. Brzina prijenosa podataka je 600 bit/s.

Kombiniranjem INMARSAT C i SafetyNET usluga dobije se cjelokupni servis pogodan za ažuriranje karata, budući da promjene u navigacijskim kartama spadaju pod sigurnosne informacije u pomorstvu, MSI.

Prema [4] u distributere sigurnosne informacije (MSI) spadaju između ostaloga nacionalni uredi za upozorenja o promjenama u elektroničkim kartama. Upravo to dokazuje da je INMARSAT EGC SafetyNET servis pogodan za ažuriranje karata. Stoga, ključno je poznavati protokole kojima se podaci šalju preko satelitskog Interneta, kako bi se mogle konfigurirati sigurnosne postavke vatrozida za zaštitu sustava ECDIS. Slika 4 prikazuje način prijenosa podataka putem INMARSAT C servisa.



Slika 4. Blokovski prikaz prijenosa podataka putem INMARSAT C sistema [4.1]

LES – „Land Earth Station“ (Kopnena stanica)

MES – „Mobile Earth Station“ (Brod)

Iz slike se može zaključiti kako je za rad INMARSAT C servisa ključna posredna kopnena stanica koja prosljeđuje podatke preko satelita do brodske stanice. Stoga, protokoli kojima se podaci šalju određuju se u kopnenoj stanici.

INMARSAT C omogućuje slijedeće funkcionalnosti :

- Teleks

- Internet e-mail
- Fax
- „Distress call“

Ažuriranje karata sustava ECDIS sustava INMARSAT C servisom moguće je preko e-pošte. Protokoli korišteni za ažuriranje putem e-pošte su:

- IMAP - (Internet Message Access Protocol) standardan protokol za pristup e-pošti sa lokalnog servera. To je klijent/server protokol pri kojemu je e-mail primljen i sačuvan sa strane Internet servera. Tek nakon što se pošalje zahtjev za čitanjem , e-mail će biti preuzet sa servera.
- POP 3 – (Post Office Protocol 3) protokol omogućuje standardizirani način pristupanja poštanskom sandučiću i preuzimanje e-pošte na računalo. Korištenjem POP 3 protokola sve poruke e-pošte preuzimaju se sa poslužitelja na lokalno računalo. Prednost uporabe ovog protokola je mogućnost da se nakon preuzimanja, e-pošta može čitati bez povezivanja na poslužitelj.
- SMTP – (Simple Mail Transfer Protocol) koristi se za dostavljanje e-pošte poslužitelju primatelja. Ovaj se protokol koristi jedino za slanje e-pošte, dok se ne može koristiti za primanje.
- HTTP – ovaj protokol ne spada direktno u e-mail komunikacijske protokole, međutim, može se koristiti za pristupanje elektroničkom poštanskom sandučiću.

Uobičajeni portovi:

- POP 3 – 110 (995 za „secured POP3“)
- IMAP – 143 (993 za „secured POP3“)
- SMTP – 25 ili 2525 (465 za „secured POP3“)

3.2. INMARSAT FleetBroadband

FleetBroadband je globalni servis koji omogućuje satelitski Internet, telefoniju, slanje SMS poruka i razne druge mogućnosti ovisno o odabiru Broadband paketa. INMARSAT u svojoj ponudi daje tri različita rješenja:

- FleetBroadband 150
- FleetBroadband 250
- FleetBroadband 500

Paketi se uglavnom razlikuju po broju telefonskih linija, brzini „IP streaminga“, te u ostalim detaljima. Za sustave ECDIS pogodni su FleetBroadband 250 i 500. U daljnjoj analizi uzimati će se FleetBroadband 250.

FB 250 temelji se na radu tri satelita smještenih u orbiti (I-4), koji omogućuju izuzetno dobru pokrivenost. Približavanjem prema polovima pokrivenost slabi, a karakterizira ga uporaba L pojasa.

Budući da FB 250 omogućuje stalno dostupnu internetsku vezu, brzine 284 kbps, pogodan je servis za primjenu na aplikacije kao što su e-mail, meteorološko izvještavanje i elektroničke karte u realnom vremenu [5].

Značajke FB 250:

- Standardni IP promet - brzina 284 kbps za „real-time“ aplikacije
- Satelitska telefonija – do 9 telefonskih linija sa jednim FB terminalom
- „Streaming IP“ – 128 kbps dostupno za video konferencijske pozive i slično
- SMS – slanje i primanje poruka sa drugih FB terminala
- Poboljšani glasovni servisi – standardni glasovni servisi plus identifikacija broja
- Fax – standardne mogućnosti
- GSM – omogućuje slanje SMS-a koristeći osobnu SIM karticu

Neke od primjena FB 250 servisa:

- Telephone, ISDN, SMS, VoIP
- Širokopojasni (broadband) Internet

- E-mail and file transfer
- Video konferencijski pozivi
- GSM
- Enkripcija
- Fax preko IP protokola
- Usmjeravanje plovila
- Zaprimanje vremenske prognoze
- GPS lociranje
- ECDIS
- Zaprimanje pravila za pojedine luke

FleetBroadband omogućuje konstantnu internetsku vezu sa kopnom, e-mail poštu, te prijenos podataka. Budući da je tako, ovaj servis pogodan je za ECDIS spajanje na poslužitelj. Ažuriranje karata putem e-maila pogodno je za karte koje nisu velike, i dolaze u obliku privitka. Protokoli korišteni za e-mail poštu navedeni su i opisani u prethodnom pod-poglavlju, pa se nadalje neće opisivati.

3.3. Zaključak poglavlja

Postoje dva INMARSAT servisa koja su pogodna za ECDIS primjenu. Prvi je INMARSAT C EGC SafetyNET koji omogućuje sustavu ECDIS primanje komercijalnih i MSI (Marine Safety Information) poruka. Drugi je FB 250, koji uz primanje sigurnosnih informacija omogućuje i transfer podataka putem satelitske veze. Nakon definiranja INMARSAT servisa, potrebno je ući malo dublje u strukturu satelitske Internet veze. Nužno je upoznati protokole na kojima se temelji izrada konfiguracije postavki vatrozida. Uvid u protokole koji se koriste prilikom satelitske internetske veze daje četvrto poglavlje.

4. Protokoli i portovi

Ovo poglavlje daje uvid u osnovne mrežne slojeve i protokole koji se koriste prilikom INMARSAT povezivanja na Internet. Mrežni slojevi i protokoli su ključni pojmovi razmatranja prilikom konfiguracije bilo koje satelitske veze.

Razmjena podataka između izvora (poslužitelja) i destinacije (broda) zahtjeva povezivanje preko satelita. Kako bi se veza ostvarila, moraju prethodno biti definirana standardizirana pravila koja se poštuju prilikom uspostave mrežne veze. Za bolje razumijevanje povezivanja poslužitelja i destinacije korisno je definirati određene zadatke i podijeliti ih u grupe. Funkcije sistema se tako dijele na slojeve za koje vrijede specificirana pravila koja se zovu protokoli. Protokolima se kontrolira razmjena podataka između slojeva.

Referentni model omogućuje dodjelu zadataka određenim grupama funkcija koje odgovaraju svakom pojedinom sloju, te koordinira vezama među slojevima. Slika 5 prikazuje OSI slojeve, od kojih se gornja tri sloja odnose na korisnika i višeg su nivoa, dok su ostali slojevi nižeg nivoa.

Slika 5. Slojevi OSI mreže – referentni model

Sloj je dizajniran za pružanje servisa slojevima iznad. Svaki sloj ima sučelje sa primitivnim operacijama (tipovi podataka koji se sastoje od brojeva, način pristupa podacima, način procesiranja podataka) koje se koriste za pristup servisima. Entitetima se smatraju aktivni elementi unutar svakog sloja (terminali, premosnici,

ruteri…). Postoje ravnopravni entiteti (uređaji) koji imaju sposobnost komuniciranja istim protokolima.

Protokol je skup pravila koja se koriste u komunikaciju između dvije strane. Osnovne funkcije protokola su sastavljanje, rastavljanje, kriptiranje, kontrola protoka, usmjeravanje itd..

Referentni model:

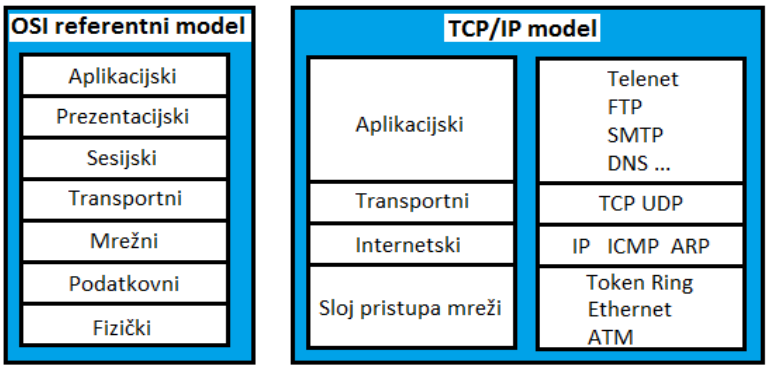
- Od korisničkog sloja (aplikacijskog) kreću sve informacije u razmjeni i vraćaju se na tom nivou. Taj sloj je ishodište i odredište informacija koje se šalju. Opskrbljuje servisima aplikacije (procese). Primjeri protokola na ovom sloju su: HTTP, FTP, Telenet, SMTP itd..
- Prezentacijski sloj koordinira transformacijom podataka, formatima podataka i sintaksama. Ukratko, omogućuje prijelaz informacija između različitih formata.
- Sloj sesije (sjednički sloj) omogućuje sinkronizaciju dijaloga između dvije strane, te razmjenu podataka među njima. Također, osigurava vezu među procesima.
- Prijenosni sloj osigurava pouzdanu dostavu podataka za procese, koji koriste prenesene podatke na višim slojevima. Brine o prijenosu paketa između dva računala. Osnovni protokoli na transportnom sloju su TCP i UDP. Prvi protokol pogodan je za slanje paketa kod kojih je bitna točnost prijenosa svih paketa, odnosno integritet podataka, dok je brzina prijenosa u drugom planu. Tako, primjerice ako se koji paket zagubi tijekom prijenosa, TCP/IP će tražiti ponovno slanje. UDP protokol se više bazira na brzini prijenosa, i nema kontrolu dostave paketa, pa nije pogodan za ažuriranje sustava ECDIS.
- Mrežni sloj osigurava usmjeravanje paketa iz izvora do destinacije, preciznije od jednog kraja mreže na drugi. Njegov zadatak je uspostava, održavanje i raskid mrežnih veza. Osnovni je zadatak ovog nivoa određivanje puta kojim će se paket prenositi (engl. routing).
- Podatkovni sloj upravlja fizičkim, na način da regulira dodjelu fizičkih resursa između komunikacijskih terminala. Točnije, bavi se pitanjem kako

kontrolirati pristup dijeljenom mediju. Bitan je za detekciju grešaka na fizičkom sloju. Ovdje su bitne MAC (Medium Access Control) adrese koje posjeduju svi mrežni uređaji. Komunikacija na ovom sloju osigurana je samo unutar lokalne mreže. Usmjernici rade na principu MAC adresa, na način da zapamte adrese svih uređaja unutar lokalne mreže. Unutar paketa nalaze se odredišne MAC adrese, te šalju odgovarajućem uređaju njegove pakete.

- Fizički sloj odnosi se na električke veze i medije za fizičku razmjenu podataka . Kod satelitskih mreža ovaj se nivo odnosi na modulacijske tehnike i tehnike kodiranja kanala koje osiguravaju prijenos podataka u specificiranim formatima i alociranim frekventnim pojasevima.

4.1. IP referentni model

Standardni TCP/IP glavni je model preko kojega INMARSAT omogućuje satelitsko povezivanje na Internet. Prema tome, za bolje razumijevanje opasnosti koje prijete informacijskom sustavu broda prilikom uspostave satelitske veze sa ECDIS-om, potrebno je detaljnije poznavati protokole koji se koriste.



Slika 6. Arhitektura IP referentnog modela

Slika 6 prikazuje TCP/IP referentni model, odnosno pripadajuće slojeve, te protokole koje model podržava. Glavni dijelovi IP referentnog modela su IP protokoli i TCP protokoli. Unutar modela nalazi se četiri od sedam pripadajućih slojeva osnovnog referentnog OSI modela:

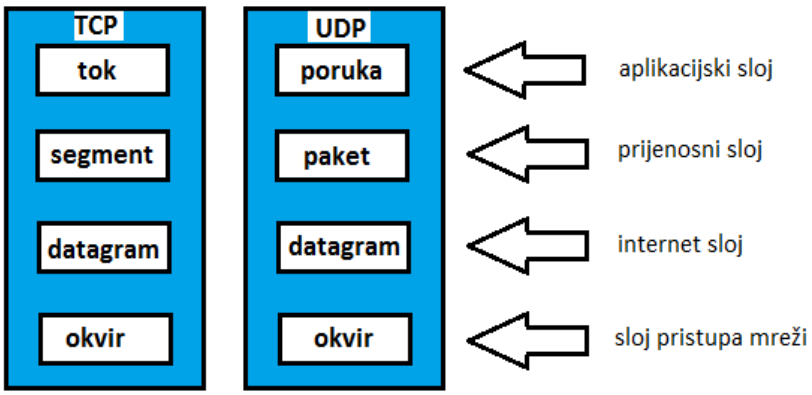
- Aplikacijski sloj
- Transportni sloj

- Mrežni sloj (odnosno Internet sloj kod IP referentnog modela)
- Sloj pristupa mreži (obuhvaća podatkovni i fizički sloj)

Neki od protokola na različitim slojevima, koje podržava IP model su slijedeći:

- Internet protocol (IP)
- Transmission Control Protocol(TCP)
- User Datagram Protocol (UDP)
- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP),
- File Transfer Protocol (FTP),
- Protocol to Interface Terminal and Applications (Telnet)
- Real-time Transfer Protocol (RTP)
- Real-time Transfer Control Protocol (RTCP)

Za bolje razumijevanje IP modela potrebno je poznavati termine koji se koriste za opisivanje ove arhitekture, kao i strukturu samog modela. Nazivi za podatke mijenjaju se sa promjenom protokola i slojeva, pa to može biti malo zbunjujuće. Tako, kod UDP protokola na aplikacijskoj razini, se koristi naziv za podatke „message“, dok se kod TCP-a zove „stream“. Također, na prijenosnom nivou UDP zove podatke „packet“, a TCP „segment“. Kod Internet sloja datagram oponaša podatke, a na sloju pristupa mreži su predstavljeni okvirom.



Slika 7. Naziv podataka po slojevima i protokolima IP modela

4.1.1. Sloj za pristup mreži

Osnovna jedinica za prijenos podataka je datagram. Obzirom na to, kod sloja za pristup mreži, vrši se raspakiravanje IP datagrama u okvire koji su pogodni za korištenje unutar istog. Ovaj sloj osigurava primitak podataka sa mrežnog medija i slanje podataka putem mrežnog medija. Sloj pristupa mreži objedinjuje podatkovni i fizički sloj osnovnog OSI modela. TCP/IP protokol unutar IP modela kompatibilan je sa različitim tipovima mreža. Zbog svoga dizajna, podržava LAN mrežu, Ethernet i Token Ring. Također, podržava ATM (asynchronous transfer mode) asinkroni transfer modul. Upravlja greškama na fizičkom mediju za prijenos, te specificira kako će se podaci slati preko fizičkog medija (električki, optički…)

4.1.2. Internet sloj

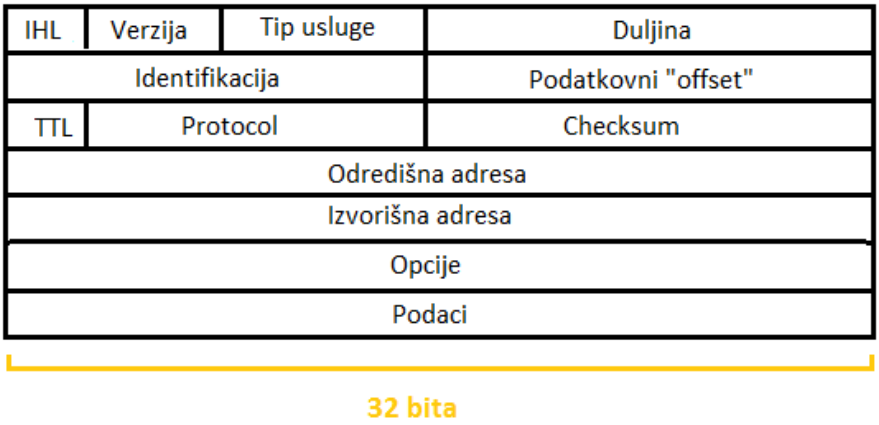
Internet sloj kod IP modela je analogija mrežnom sloju kod osnovnog OSI modela. Internet protokol kod IP modela omogućuje upravljanje adresama, te pakiranje paketa. Bitne karakteristike ovog protokola su usmjeravanje paketa i fragmentacija. ARP (Adress Resolution Protocol) osigurava pretvaranje adresa internetskog sloja u adrese pogodne za sloj pristupa mreži. ICMP (Internet Control Message Protocol) koristi se za detektiranje i javljanje o pogreškama prilikom neuspješnog slanja IP paketa. ICMP poruke uokviruju se u datagram. IGMP (Internet Group Management Protocol) koristi se za upravljanje grupama. Internet sloj je odgovoran za uspostavu veze između dva uređaja. Svaki uređaj ima svoju adresu koja se sastoji od 32-bitnog broja. Na ovom se sloju analizira zaglavlje paketa i šalju podaci dalje na viši nivo.

IP protokol je nepouzdani protokol, budući da njegova namjena nije osigurati sigurnu dostavu paketa. Nakon nekog vremena, ako potvrda o primitku paketa nije stigla, tada IP ponovo šalje pakete. Ovim se protokolom ne može štititi od dupliciranja, krivog redoslijeda paketa ili sličnog. Što se tiče sigurnosti dostave paketa, IP se oslanja na ostale protokole drugih slojeva (TCP). Već je rečeno da je osnovna jedinica na ovom sloju datagram. Datagram je skup podataka koji se šalje kroz mrežu. Sastoji se od zaglavlja i podataka. Veličina od prvih pet ili šest 32-bitnih

riječi je kapacitet koji se čuva za podatke zaglavlja. Slika 8 prikazuje izgled IP datagrama.

Unutar zaglavlja nalaze se slijedeći podaci:

- Adresa izvora – izvorišna adresa IP datagrama
- Odredišna adresa – IP adresa destinacije na koju mora datagram stići
- Identifikacija – koristi se za identifikaciju segmenata IP datagrama prilikom fragmentacije
- Protokol – definira se protokol prijenosnog sloja kojim se želi slati podatke
- Checksum – matematički izračun koji se koristi za provjeru integriteta podataka u IP zaglavlju
- TTL (Time To Live) – određuje konačan broj mrežnih segmenata kojima je dopušteno datagramu putovati. Uloga je spriječiti beskonačno putovanje datagrama IP mrežom. Određuje se u sekundama, a vrijednost ovog polja smanjuje se prilikom svake obrade datagrama u nekom mrežnom uređaju. Mora biti najmanje jednak broju mrežnih uređaja kroz koje datagram prolazi.
- IHL (Internet Header Length) – specificira dužinu zaglavlja u 32-bitnoj riječi.
- Verzija – definira se koja vrsta IP-a se koristi (IPv4 ili Ipv6)
- Fragment „offset“ – nakon fragmentacije, definira kako se po redoslijedu slažu fragmenti da se dobije pravilna poruka (prvi fragment ima „offset“ 0)
    - MF (more fragments) – bit na ovom području imaju svi fragmenti osim zadnjeg, i on označava da dolazi još fragmenata od istog datagrama.
    - DF (dont fragment) – nema više fragmenata istog datagrama
- Ukupna duljina – 65535 bytova



Slika 8. Izgled zaglavlja IP Datagrama sa šest 32-bitnih riječi

Računala koja su na mreži, šalju podatke ili ih primaju, moraju imati uključen ARP (Address Resolution Protocol) protokol. Svako računalo ima svoju IP adresu, pa tako imaju i uređaji u mreži (npr. usmjerivači). Računala se spajaju u mrežu preko mrežne kartice, koja ima svoju MAC adresu koja se sastoji od 48 bita. Mrežne kartice nakon što prime datagram šalju ga na osnovu 48 bitne adrese. To znači da za slanje datagrama nije dovoljno poznavati IP adresu računala kojem se šalje nego i MAC fizičku adresu mrežne kartice računala. Upravo ARP protokol daje informaciju o MAC adresi. Npr. računalo „A“ koje šalje datagram poznaje IP adresu računala „B“ u mreži. ARP šalje upit svim računalima u lokalnoj mreži (broadcast upit), a računalo koje prepoznaje svoju IP adresu šalje ARP odgovor (daje svoju MAC adresu).

Internet Control Message Protocol:

ICMP protokol koristi se za komunikaciju odredišnog računala sa izvorišnim, sa svrhom upozoravanja na greške koje su se pojavile prilikom slanja datagrama. Sastavni je dio svake IP komunikacije, budući da je integriran unutar IP-a. ICMP protokolom šalju se poruke kada datagram nije/ne može stići do odredišta. Također, u slučaju kada je kapacitet primjerice usmjernika prenizak tada se ICMP porukom upozorava na taj problem. Moguće je da se ICMP porukom upozori na postojanje kraće rute za prijenos podataka. Budući da je IP protokol nepouzdan, ICMP ga nadopunjuje porukama o greškama. ICMP koristi zaglavlje IP datagrama, te unutar

njega upisuje vrijednosti. Prvi oktet polja „podaci“ se koristi za ICMP poruke. Vrijednost ovog polja određuje format ostalih podataka.

Destination Unreachable Message – Kada mrežni uređaj primjerice usmjernik (engl. gateway) mrežu sa odredišnom IP adresom vidi kao nedostižnu, tada on šalje ICMP poruku na izvorišnu IP adresu kako je odredište nedostižno. Također, ako je odredišni port na koji se šalje datagram zatvoren, DUM porukom se obavještava izvor o stanju porta. U slučaju kada je potrebno fragmentirati poruku, a već je stigla do usmjernika, mora ju odbaciti i poslati izvoru DUM poruku. Polje datagrama „code“ može imati 6 različitih vrijednosti. Vrijednosti 0,1,4,5 šalje usmjernik, a 2 i 3 šalje izvor. Svaki broj označava jedno od mogućih stanja zbog kojih je odredište nedostižno.

Polje „Type“ =3.

Polje „Code“:
0 = nedostižna mreža
1 = nedostižno računalo u mreži
2 = nedostižan protokol
3 = nedostižan port
4 = potrebna fragmentacija DF set
5 = neuspješna izvorišna ruta

Time Exceeded Message – ako je TTL polje jednako nuli, znači da usmjernik mora otpustiti paket jer je vrijeme slanja paketa isteklo i šalje TEM poruku izvoru. Također, ako je došlo do slanja fragmenata poruke sa izvora na odredište, a odredišni „gateway“ ne može sastaviti poruku (engl. reassembly) na vrijeme (ovisno o TTL-u), tada se šalje TEM upozorenje i otpušta paket. Kod 1 šalje usmjernik, a kod 2 računalo.

Polje „Type“:
11
Polje „Code“:

0 = isteklo vrijeme slanja (TTL=0)
1 = vrijeme za sastavljanje fragmenata isteklo

Parameter Problem Message - Ako se pojave greške u zaglavlju, zbog kojih se ne može izvršiti obrada datagrama, tada se otpušta paket i šalje PPM poruka. Primjer pogreške je nepravilna vrijednost polja „optional“ u datagramu. Pokazivač je dio datgrama koji se šalje prilikom ovakve pogreške i prikazuje u kojem oktetu se pogreška dogodila.
Polje „Type“:
12
Polje „Code“:
0 = pokazivač pokazuje na grešku

Source Quench Message – ovu poruku šalje usmjernik na vanjskoj mreži koji je posredna točka prilikom slanja paketa do odredišta. Javlja se zbog premalog prostora za pohranu paketa, pa se otpušta i šalje SQM poruka do izvora. Također, ovu poruku može poslati i odredišni usmjernik ako je promet došao prebrzo pa ga ne stigne procesuirati. Potrebno je smanjiti brzinu kojom se šalje promet.

Polje „Type“:
4
Polje „Code“:
0

Redirect Message – Promet se šalje sa izvorišnog računala K na odredište F, a na K je spojen usmjernik U1. Promet se šalje od U1 do U2 što predstavlja novi „gateway“. Ako su U2 i izvorišno računalo na istoj mreži, tada se šalje RM poruka sa prijedlogom nove rute.

Polje „Type“:
5
Polje „Code“:

0 = Preusmjeravanje datagrama prema mreži
1 = Preusmjeravanje datagrama prema „hostu“
2 = Preusmjeravanje datagrama za „Type of Service and Network“
3 = Preusmjeravanje datagrama za Type of Service and Host.

Echo or Echo Reply Message – adresa izvora u „Echo“ poruci je odredište „Echo“ poruke. Podaci koji se šalju u „Echo“ poruci moraju biti vraćeni izvoru jednaki. U datagramu se pojavljuju polja „identifier“ i „sequence number“ čije vrijednosti se mogu koristiti prilikom slanja poruke. To znači da se vrijednosti tih polja moraju vratiti u „Echo“ odgovoru.
Polje „Type“:
8 – „Echo“ poruke
0 - „Echo“ odgovore
Polje „Code“ :
0

Timestamp or Timestamp Reply Message – Postoji originalna vremenska marka (engl. timestemp) koja ima zabilježeno vrijeme kada je poruka poslana. Također, postoji povratna vremenska marka koja obilježava vrijeme kada je prijemnik dobio poruku. Adresa izvora „timestamp“ upita je odredište „timestamp“ odgovora.

Polje „Type“:
13 for timestamp message;
14 for timestamp reply message.
Polje „Code“ :
0
Information Request or Information Reply Message – ove se poruke koriste kako bi „host“ saznao na kojoj se mreži nalazi. To znači da se „information request“ poruka šalje sa odredišnom adresom 0. Na taj način šalje upit svojoj mreži, i dobiva odgovor „Information Replay“. Odgovor sadrži iste podatke kao i upit. Može se stoga zaključiti da je odredišna adresa ujedno i izvorišna.

Polje „Type“:

15 for information request message;

16 for information reply message.

Polje „Code“ :

0

4.1.3. Prijenosni sloj

Prijenosni sloj podržava TCP i UDP protokole, i zadužen je za opskrbu aplikacijskog sloja datagramima. TCP je za razliku od IP-a spojni i pouzdani protokol. Zaslužan je za uspostavu komunikacijske veze, slanje potvrde o primitku paketa, i obnavljanja paketa ukoliko je došlo do gubitka podataka. UDP je s druge strane, ne spojni i nepouzdani komunikacijski servis. Koristi se za slanje malih paketa, kada se ne želi upotrijebiti TCP, jer je brzina prijenosa značajnija od preciznosti.

Slika 9. Izgled zaglavlja TCP segmenta

Slika 9 prikazuje zaglavlje TCP segmenta. Pouzdanost TCP protokola dobije se uporabom sekvencijalnih brojeva. Budući da se na prijenosnom sloju radi sa segmentima, svakom se od njih dodjeljuje sekvencijalni broj. Potvrda se šalje pošiljatelju ako je segment uspješno stigao. Ako potvrda ne stigne u definiranom vremenu, tada se segment ponovno šalje. Unutar jednog IP datagrama moraju stati TCP zaglavlje i pojedini segment. Ako je veličina segmenta koji se šalje prevelika za brzinu mreže (maximal transfer unit - MTU) tada na „routeru“ dolazi do fragmentacije odnosno podjele na manje segmente, gdje svaki manji segment dobije svoje IP zaglavlje.

Unutar zaglavlja TCP segmenta nalaze se:

- Izvorišni port (16 bit) – broj porta izvora
- Prijemni port (16 bit) – broj porta prijemnika
- Sekvencijalni broj (32 bit) – sekvencijalni broj kojim se potvrđuje uspješno primanje segmenta
- Broj potvrde (32 bit) – sadrži broj bitova koji označavaju vrijednost sekvencijalnog broja slijedećeg segmenta kojega prijemnik očekuje
- Podatkovni „offset“ (4 bit) – označava od kuda podaci započinju, pomaže pri slaganju korisne informacije nakon de-fragmentacije
- Rezerva (6 bit) – koristi se kod novijih verzija TCP/IP protokola, inače nula.
- Kontrolni bitovi (6 bit):
    - URG – hitna poruka
    - SYN – sinkronizacija
    - ACK – potvrda primitka segmenta
    - FIN – prekid veze
    - PSH – pražnjenje spremnika
    - RST – resetiranje veze
- Prozor (16 bit) – broj okteta podataka
- Checksum (16 bits) - matematički izračun koji se koristi za provjeru integriteta podataka u IP zaglavlju
- Hitni pokazivač (16 bit) – pokazivač na segment sa hitnim sadržajem. Radi se „offset“ odnosno pomak na sekvencijalni broj segmenta sa hitnim sadržajem. Koristi se samo kod segmenata kojima je URG bit setiran
- „Padding“ – punjenje TCP zaglavlja nulama, kako bi se osigurao početak podataka na 32 bitnoj granici
- Veličina prozora – pokazuje koliko 32-bitnih riječi ima zaglavlje

Za razliku od IP protokola, što je već napomenuto TCP mora uspostaviti vezu prije slanja podataka. Uspostavljanje veze izvodi se trostrukim rukovanjem, odnosno razmjenom upravljačkih informacija. Izvorna strana šalje segment prijemnoj strani koji sadrži poziv za sinkronizacijom (vezom) gdje je bit SYN setiran (1). Također pošalje svoj sekvencijalni broj od kojega izvorna strana počinje označavati segmente

koje šalje. Nakon toga prijemna strana, šalje bit potvrde veze ACK setiran (1), bit SYN setiran (1) i svoj sekvencijalni broj od kojega počinje računati nadolazeće segmente. Nakon toga kako bi se završilo trostruko rukovanje, prva strana šalje također SYN i ACK za uspostavu veze. Slika 10 prikazuje trostruko rukovanje.

Slika 10. Uspostavljanje TCP veze trostrukim rukovanjem

4.1.4. Aplikacijski sloj

Aplikacijski sloj omogućuje programima da pristupe servisima drugih slojeva. On definira protokole koje programi koriste za razmjenu podataka. Danas postoji već mnogo aplikacijskih protokola, i mnoštvo ih se konstantno razvija. Neki od najpoznatijih aplikacijskih protokola su :

- HTTP (Hypertext Transfer Protocol) – služi za prijenos podataka sa web stranica
- FTP (File Transfer Protocol) – koristi se za transfer podataka
- SMTP (Simple Mail Transfer Protocol) – koristi se za dostavljanje e-pošte poslužitelju primatelja. Ovaj se protokol koristi jedino za slanje e-mail pošte, dok se ne može koristiti za primanje.
- Telnet – koristi se za logiranje na udaljene poslužitelje
- DNS (Domain Name Server) – služi za pretvaranje imena računala u IP adresu

- RIP (Routing Inforamtion Protocol) – je protokol kojega koriste usmjerivači

Telenet, FTP i SMTP koriste TCP protokol, dok DNS i RIP koriste UDP protokol.

4.2. Zaključak poglavlja

Za izradu konfiguracije postavki vatrozida nužno je poznavati protokole koje koristi satelitska internetska veza. Osnovni protokoli na kojima se temelje postavke vatrozida u ovom radu su ICMP, TCP i UDP. Za razmatranje protokola, koristi se osnovni OSI referentni model. ICMP protokol radi na mrežnom sloju glavnog OSI referentnog modela (Internet sloj kod IP referentnog modela), dok su TCP i UDP protokoli prijenosnog sloja. Nužno je poznavati na kojim slojevima se protokoli javljaju, kako bi se mogli detektirati sigurnosni rizici koje uključuju. O sigurnosnim rizicima koji se javljaju, te o tehnikama napada na ICMP, TCP i UDP protokol govori peto poglavlje.

5. Sigurnosni rizici, prijetnje i napadi na TCP/IP

Naglasak rada do sada bio je na analizi osnovnih svojstava sustava ECDIS i na upoznavanju sa servisima davatelja usluga (INMARSAT) za satelitski Internet. Definirana su dva INMARSAT servisa koja se koriste za satelitsku vezu sa ECDIS sustavima. Navedene su osnovne značajke tih servisa, te vrsta veze. Uspostavilo se da je osnovni tip satelitske veze preko IP referentnog modela, odnosno glavni protokoli koji se koriste pri satelitskoj vezi sa ECDIS-om su TCP/IP protokoli. U prethodnom poglavlju dane su osnovne informacije o tim protokolima, njihove značajke i principi rada. U ovom poglavlju naglasak će se dati na sigurnosne rizike koji su vezani za TCP/IP protokole. Također, biti će prezentirane tehnike napada na informacijske sustave pri kojima će se koristiti slabosti IP veze.

5.2.Tehnike napada

IP referentni model ima više mana koje se mogu promatrati sa stajališta sigurnosti. One se javljaju zbog principa rada, te dizajna samog IP modela. Danas se koriste različite tehnike napada na TCP/IP protokole, ali ove se često upotrebljavaju:

- Lažno predstavljanje IP adresom
- DOS napad
- Skeniranje portova
- Otimanje IP veze
- Predikcija sekvencijalnih brojeva
- RIP napadi
- DOS napad na ICMP

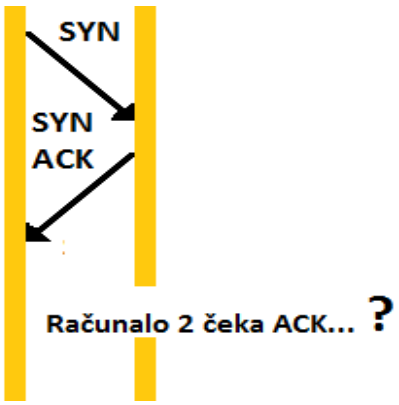
5.2.1. Lažno predstavljanje IP adresom

Paketi koji se šalju kroz mrežu sadrže izvorišnu IP adresu i odredišnu adresu unutar IP zaglavlja. To su ključne informacije za usmjernik koji na temelju istih usmjerava

paket kroz mrežu. Svatko tko ima pristup IP sloju, može lažirati izvorišnu IP adresu paketa i na taj način predstaviti kao da paket dolazi od strane ovlaštenog izvora. Takvo se lažiranje izvodi sa ciljem kamufliranja prave IP adrese sa koje stiže TCP/IP paket. Izvorišna IP adresa potrebna je primatelju paketa da na nju da odgovor na poslani paket. Budući da je izvorišna adresa lažirana, primatelj šalje odgovor na lažnu adresu. Ako napadač želi saznati odgovor mora prisluškivati promet koji ide prema lažiranoj IP adresi. Ovakvo ponašanje napadača može uzrokovati probleme u raspoloživosti.

5.2.2. DOS napad

Napad kod kojega se uzastopno šalje veliki broj paketa zove se DOS napad (Denial Of Service). Odgovori koje primatelj šalje biti će proslijeđeni na lažiranu IP adresu, a ne na adresu napadača. Pretpostavimo TCP vezu između dva računala, koja se sastoji od trostrukog rukovanja. Ako računalo 1 želi uspostaviti TCP vezu sa računalom 2, šalje paket sa setiranom SYN zastavicom. Računalo 2 odgovara paketom sa ACK setiranom zastavicom (odgovor). Treće „rukovanje“ sastoji se od slanja ACK zastavice računala br. 1. Nakon trostrukog rukovanja uspostavljena je TCP veza između računala 1 i 2. Dakle, trostruko rukovanje mora biti izvršeno do kraja kako bi veza bila uspostavljena. Veze koje su započele sa uspostavom rukovanja, ali nisu završile sva tri rukovanja zovu se „polu-otvorene veze“.



Slika 11. Posljedica polu-otvorene TCP veza

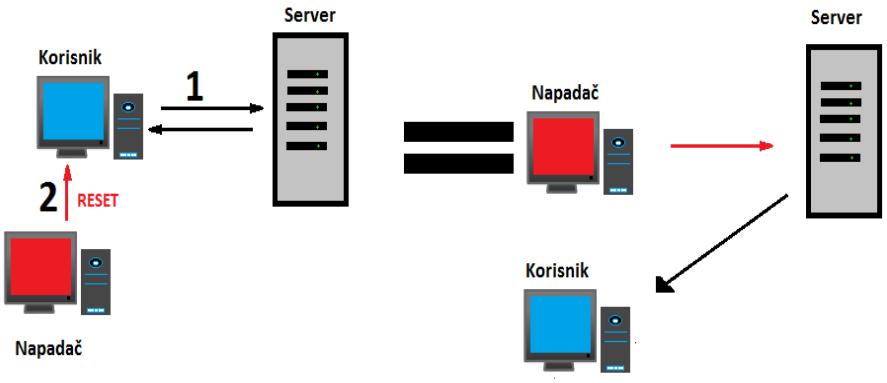
Princip DOS napada obuhvaća veliki broj polu-otvorenih veza. Napadač šalje SYN paket žrtvi, ali sa lažne IP adrese. Žrtva vraća SYN ACK paket na lažnu adresu. Treće rukovanje neće se izvršiti, i nastati će polu-otvorena veza budući da je adresa izvora lažirana. Na taj način ponovnim slanjem novih zahtjeva za TCP vezama, popuniti će se maksimalni broj veza, od kojih nijedna neće biti funkcionalna. Zbog toga se više ne može poslati zahtjev ni za jednom TCP vezom, jer je kapacitet popunjen pa se na taj način uskraćuje raspoloživost računala kojem su zahtjevi slani. Slika 11 prikazuje polu-otvorenu vezu.

5.2.3. Skeniranje portova

Drugi motiv napada lažiranjem IP adrese je skeniranje informacija o portovima, stanju vatrozida, operativnom sustavu i sličnom. Kada napadač pošalje SYN zahtjev, očekuje odgovor od primatelja zahtjeva, i „prisluškuje“ (engl. sniffing) odgovor sa ciljem sakupljanja informacija. Prikupljaju se informacije o otvorenim aktivnim portovima. Prema karakterističnim brojevima portova napadač može donijeti razne zaključke s obzirom na stanje sistema koji napada. Kod prisluškivanja odgovora lažirana IP adresa mora biti na istoj pod-mreži (engl. subnetwork).

5.2.4. Otimanje IP veze

Presretanjem TCP konekcija, i poznavanjem algoritma generiranja sekvencijalnih brojeva, napadač može poslati poruku za poništavanje veze jednom od računala u mreži. Nakon toga lažno preuzima IP adresu tog računala i predstavlja se kao to računalo koje je u mreži provjereno i sigurno. Na taj se način mogu iskoristiti prednosti povjerljivog (engl. thrusted) računala u mreži. Takav se napad zove otimanje IP veze, vrlo je opasan, te je prikazan slikom 12.



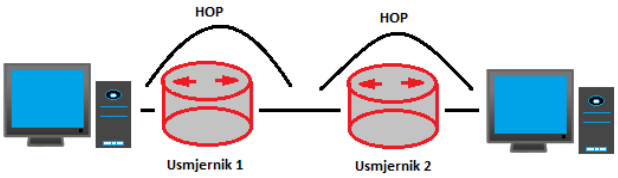
Slika 12. Otimanje TCP veze

5.2.5. Predikcija sekvencijalnih brojeva

Napadač može koristiti TCP vezu za skeniranje algoritma kojim se generiraju sekvencijalni brojevi paketa koji su nužni za poznavanje redoslijeda slanja. Stoga, skeniranjem odgovora koje primatelj šalje na SYN upit, napadač dobiva uvid u algoritam sekvencijalnih brojeva, i na taj način može ga iskoristiti za presretanje postojećih TCP veza.

5.2.6. RIP napadi

RIP (routing information protocol) je protokol za usmjeravanje, kojega obuhvaća IP referentni model. Služi za usmjeravanje paketa na najbrži mogući način do odredišta. Mreža se sastoji od većeg broja različitih putova kojima paket može doći od izvora do odredišta. Ti putovi se mogu podijeliti na segmente koji se zovu „hop-ovi“ (slika 13). RIP protokol ustvari prebrojava koliko ima tih segmenata kroz sve različite putove kojima paket može proći i odabire onaj najkraći sa najmanjim brojem segmenata.

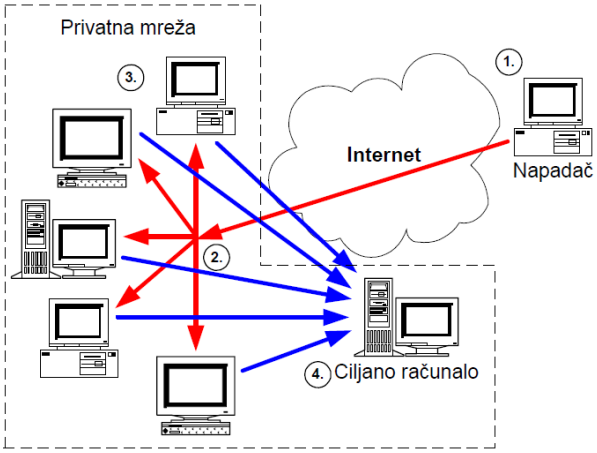


Slika 13. Segmenti mreže „hop-ovi“

Nedostatak RIP protokola je mogućnost neautorizirane promjene puta usmjeravanja. Naime, napadač može neautorizirano izmijeniti rutu, i prikazati čvorište na kojem se nalazi on sam kao najbliže. Stoga je napadač u mogućnosti lakše izvesti napad primjeren svome cilju.

5.2.7. DOS napad na ICMP

ICMP (Internet Control Message Protocol) koristi se za detektiranje i javljanje o pogreškama prilikom neuspješnog slanja IP paketa. Najznačajniji ICMP upit je „ping“ kojim se provjerava dostupnost primatelja zahtjeva. Primatelj upita šalje svoj status, a budući da „pinganje“ ne zahtjeva nikakvu autorizaciju, napadač može presresti ICMP upite. Osim neprekidnim zahtjevima za TCP vezama, DOS napad može se izvršiti i „ping“ upitima, dakle ICMP protokolom.



Slika 14. DOS napad ICMP protokolom [14.1]

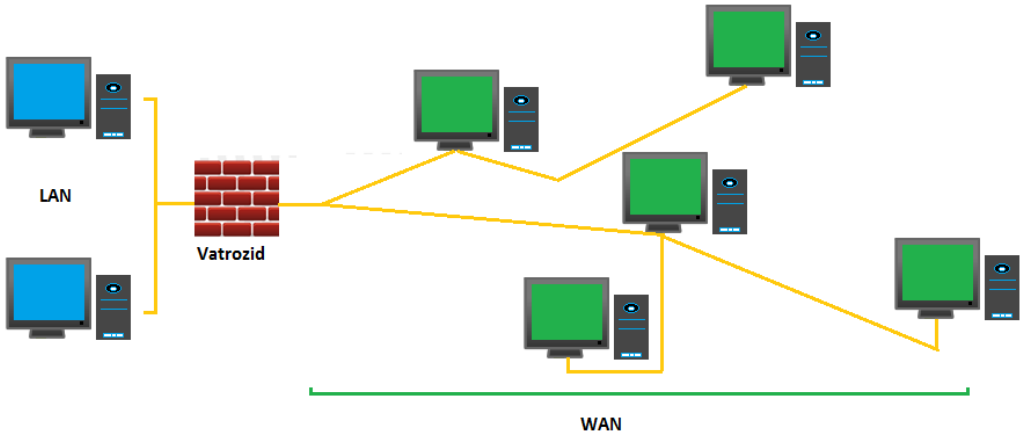
Slika 14 prikazuje DOS napad upitima gdje napadač šalje „broadcast ping“ upit svim računalima koristeći lažnu adresu. Dakle, uzima IP adresu ciljanog računala kojeg želi zasuti „ping“ odgovorima koje šalju sva računala kojima je došao upit. Na taj način uzrokuje manjak raspoloživosti ciljanog računala.

5.3. Zaključak poglavlja

TCP/IP protokoli podložni su lažiranju IP adrese pa se mogu iskoristiti za krađu informacija ili DOS napade. ICMP je osobito podložan DOS napadima na raspoloživost. Na TCP protokol mogu se izvesti napadi otimanja veze i slijepo prekidanje veze pri kojem se također utječe na raspoloživost, budući da ostaje veliki broj polu otvorenih veza. Dobre metode zaštite od ovih napada su uporaba pristupnih kontrolnih listi, te filtriranje paketa. Ova svojstva posjeduje svaki bolji vatrozid. Postoji više podjela vatrozida s obzirom na zaštitna svojstva koja pružaju. Za efikasno postavljanje postavki vatrozida potrebno je detaljno poznavati sve mogućnosti koje pruža. U šestom poglavlju se razmatraju osnovna svojstva vatrozida kao zaštitnog uređaja.

6. Zaštita vatrozidom

Vatrozid je sigurnosni uređaj između dvije mreže, koji djeluje kao posrednik, blokirajući ili dozvoljavajući uspostavu veze. On osigurava prolaz dolaznog i odlaznog prometa, pa s obzirom na ograničenja i sigurnosne postavke odbija ili propušta određeni promet. Njegova je uloga propuštanje prometa koji dolazi samo od autoriziranih izvora (slika 15).



Slika 15. Prikaz LAN mreže štićene vatrozidom

Postoje hardverski i aplikacijski (programski) vatrozidi. Prilikom konfiguracije postavki vatrozida, potrebno je odabrati adekvatna ograničenja koja su sukladna sigurnosnim rizicima. Također, vatrozidi imaju implementirane log datoteke u koje se zapisuju svi pokušaji uspostavljanja prometa između mreža odijeljenih istim. Log datoteke vrlo su učinkovite za otkrivanje anomalija u dolaznom prometu. Može se dogoditi da vatrozid radi poteškoće prilikom DOS napada, budući da pregledava i dolazni i odlazni promet. Ako ga se napadne velikim brojem upita, može zagušiti propusnost mreže.

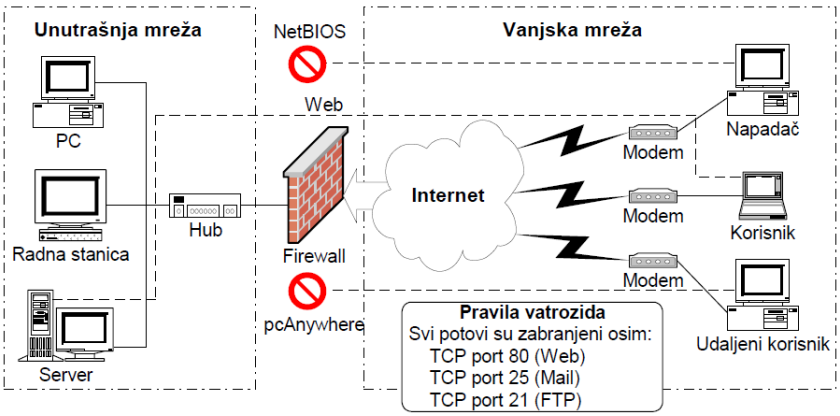
Vatrozide se može podijeliti u kategorije na nekoliko načina. S obzirom na sloj OSI modela na kojem funkcioniraju dijele se na:

- Vatrozide sa filtriranjem paketa
- Proxy vatrozide
- Vatrozide sa translatiranjem mrežnih adresa (NAT)

Kvalitetniji vatrozidi sadrže sve funkcije implementirane unutar istog uređaja.

6.1. Vatrozidi sa filtriranjem paketa

Vatrozidi koji rade na mrežnom sloju se obično ponašaju kao obični usmjernici, i koriste dva pristupa filtriranju prometa. Statičkim filtriranjem paketa, propušta se ili brani pristupanje određenom prometu. Kriteriji za propuštanje ili odbijanje paketa su kod ovog principa statični, dakle ne mijenjaju se. Drugi način filtriranja prometa je dinamički, gdje se pravila mogu promijeniti ovisno o potrebi. Drugim riječima, dopušta se prolaz samo onim paketima koji su odgovor na poslani upit iz unutarnje mreže. To znači da vatrozid pamti odlazni paket iz unutarnje mreže koju štiti i prihvaća pakete koji su odgovor na ovaj upit, a blokira ostale dolazne pakete. Moderni vatrozidi sa paketnim filtriranjem mogu raditi na trećem i četvrtom nivou OSI referentnog modela, odnosno na mrežnom i prijenosnom sloju .



Slika 16. Prikaz paketnog filtriranja [16.1]

Slika 16 prikazuje paketno filtriranje vatrozidom, gdje je prema definiranim pravilima dozvoljen prolaz samo TCP paketima na portovima 80 (Web), 25 (Mail) i 21 (FTP). Ostali su portovi zabranjeni, pa je aplikacijama poput pcAnywhere-a onemogućen pristup štićenoj mreži.

Vatrozidi sa paketnim filtriranjem služe za preispitivanje dolaznih paketa s obzirom na korištene protokole, izvorišnu adresu, veličinu paketa, odredišni port i druge parametre. Ako parametri dolaznih paketa zadovoljavaju referentne vrijednosti, tada se paketi propuštaju u štićenu mrežu. Vatrozidi sa paketnim filtriranjem obično nisu

skupi, i relativno jednostavno im je konfigurirati postavke. Težina namještanja postavki ovisi o složenosti mreže na koju se želi ostvariti pristup. Ako postavke vatrozida nisu podešene pravilno, može se dogoditi da se blokira i koristan promet.

Postoje određeni nedostaci koji su prisutni kod paketnog filtriranja. Primjerice, paketima se ne pregledava sadržaj, niti se uspoređuje sa ostalim paketima, pa je moguće izvesti „ping“ napad na raspoloživost sustava korištenjem ICMP protokola. Nadalje, kod paketnog filtriranja nema provjere autentičnosti izvora, pa stoga, vatrozid neće biti u stanju primijetiti ako dolazi puno paketa sa iste izvorišne adrese. U takvom slučaju se često radi o napadu na raspoloživost sustava, dakle DOS napadu.

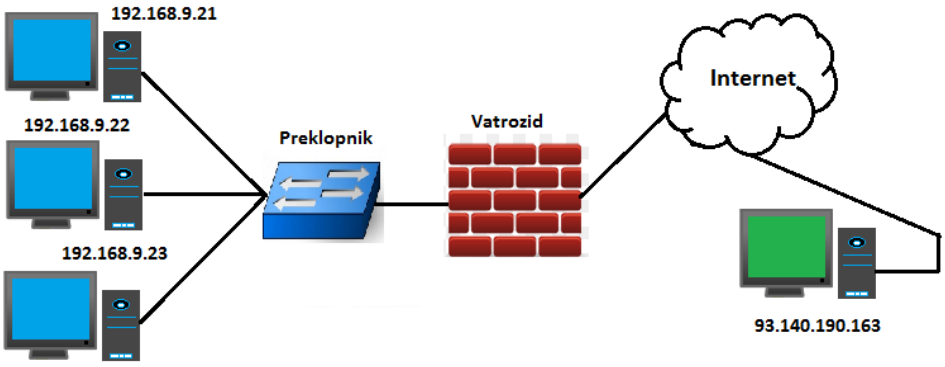
Vatrozidi sa paketnim filtriranjem koriste pristupne liste, kojima se definiraju parametri. Primjer pristupne kontrolne liste [6]:

```
!
hostname R1
!
interface Ethernet0/0
  ip address 16.1.1.2 255.255.0.0
  ip access-group 126 in
!
interface Ethernet0/1
  ip address 16.2.1.1 255.255.255.0
  ip access-group 128 in
!
router ospf 44
network 16.1.0.0 0.0.255.255 area 0
network 16.2.1.0 0.0.0.255 area 1
!
! Access list 80 applies to SNMP hosts allowed to access this router
no access-list 80
access-list 80 permit host 16.2.1.2
access-list 80 permit host 16.2.1.3
!
!snmp-server community snmp-host1 ro 80

! Access list 126 applies to traffic flowing from external networks
to
                                                ! the internal network
or to the router itself
no access-list 126
! This entry below prevents any IP packets containing the source
address
                                                ! of any internal
hosts or networks, inbound to the private network.
access-list 126 deny ip 16.2.1.0 0.0.0.255 any log
```

```
! This set of entries below prevents any IP packets containing the
invalid
                                                    ! source address such
as the local loopback
access-list 126 deny ip 127.0.0.0 0.255.255.255 any log
access-list 126 deny ip 0.0.0.0 0.255.255.255 any log
access-list 126 deny ip 10.0.0.0 0.255.255.255 any log
access-list 126 deny ip 172.16.0.0 0.15.255.255 any log
access-list 126 deny ip 192.168.0.0 0.0.255.255 any log
access-list 126 deny ip 224.0.0.0 15.255.255.255 any log
! The following prevents DoS-Smurf attacks
access-list 126 deny ip any host 16.2.1.255 log
access-list 126 deny ip any host 16.2.1.0 log
! The following line prevents DoS-TCP SYN Attacks
access-list 126 permit tcp any 16.2.1.0 0.0.0.255 established
! The following filters ICMP
access-list 126 deny icmp any any Echo log
access-list 126 deny icmp any any redirect log
access-list 126 deny icmp any any mask-request log
access-list 126 permit icmp any 16.2.1.0 0.0.0.255
access-list 126 permit ospf 16.1.0.0 0.0.255.255 host 16.1.1.2
access-list 126 deny tcp any any range 6000 6063 log
access-list 126 deny tcp any any eq 6667 log
access-list 126 deny tcp any any range 12345 12346 log
access-list 126 deny tcp any any eq 31337 log
access-list 126 permit tcp any eq 20 16.2.1.0 0.0.0.255 gt 1023
access-list 126 deny udp any any eq 2049 log
access-list 126 deny udp any any eq 31337 log
access-list 126 deny udp any any range 33400 34400 log
access-list 126 permit udp any eq 53 16.2.1.0 0.0.0.255 gt 1023
access-list 126 deny tcp any range 0 65535 any range 0 65535 log
access-list 126 deny udp any range 0 65535 any range 0 65535 log
access-list 126 deny ip any any log
!
! Access list 128 applies to traffic flowing from the internal
network to
                                                    ! external networks or
to the router itself
no access-list 128


access-list 128 permit icmp 16.2.1.0 0.0.0.255 any Echo
access-list 128 permit icmp 16.2.1.0 0.0.0.255 any parameter-problem
access-list 128 permit icmp 16.2.1.0 0.0.0.255 any packet-too-big
access-list 128 permit icmp 16.2.1.0 0.0.0.255 any source-quench
access-list 128 deny tcp any any range 1 19 log
access-list 128 deny tcp any any eq 43 log
access-list 128 deny tcp any any eq 93 log
access-list 128 deny tcp any any range 135 139 log
access-list 128 deny tcp any any eq 445 log
access-list 128 deny tcp any any range 512 518 log
access-list 128 deny tcp any any eq 540 log
access-list 128 permit tcp 16.2.1.0 0.0.0.255 gt 1023 any lt 1024
access-list 128 permit udp 16.2.1.0 0.0.0.255 gt 1023 any eq 53
access-list 128 permit udp 16.2.1.0 0.0.0.255 any range 33400 34400
log
access-list 128 deny tcp any range 0 65535 any range 0 65535 log
access-list 128 deny udp any range 0 65535 any range 0 65535 log
```

```
access-list 128 deny ip any any log
!
snmp-server community snmp-host1 ro 80
!
```

Vatrozidi sa dinamičkim filtriranjem paketa (engl. Stateful firewalls), koriste uspješniji način paketnog filtriranja. Zovemo ih vatrozidima sa praćenjem veze, budući da imaju mogućnost praćenja stanja veze u svakom trenutku, bilo da se radi o aktivnoj vezi, ili vezi koja je u postupku gašenja. Bolje štite mrežu od običnog statičkog paketnog filtriranja, jer omogućuju promet prema van, a dolazni promet blokiraju. Međutim, ne blokira se sav dolazni promet,već se propuštaju samo oni dolazni paketi koji su odgovor na pokretanje veze sa štićenom mrežom. Dinamičko filtriranje prikazano je primjerom:



Slika 17. Prikaz rada vatrozida sa dinamičkim filtriranjem

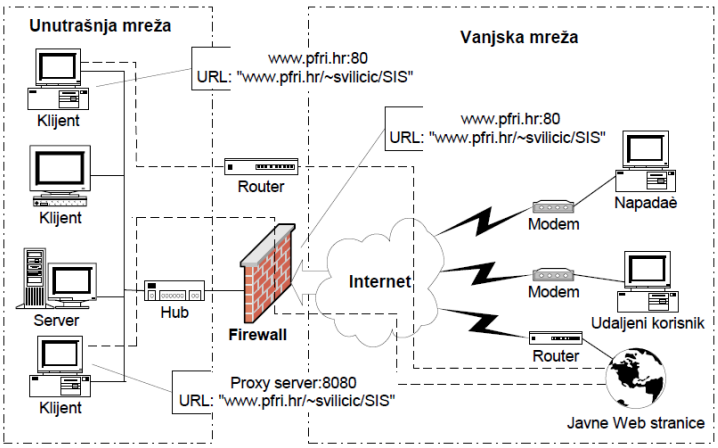
Slika 17 prikazuje privatnu mrežu računala koju štiti vatrozid sa dinamičkim paketnim filtriranjem. Postoji dakle, mreža računala sa IP rangom od 192.168.9.21 – 192.168.9.23 koja se smatra unutarnjom. Pretpostavka je da je zabranjen dolazni promet i da se koristi TCP veza prilikom uspostave sesije. Prema tome, vanjsko računalo 93.140.190.163 ne može ostvariti SYN zahtjev prema računalu 192.168.9.21 u unutarnjoj mreži. Međutim, odlazni promet nije zabranjen, pa unutarnje računalo može poslati SYN zahtjev za uspostavom TCP veze računalu 93.140.190.163. Budući da se radi o TCP vezi, i trostrukom rukovanju, vanjsko računalo šalje nazad SYN/ACK odgovor. Kod vatrozida sa statičkim filtriranjem paketa ovaj bi odgovor bio odbijen, budući da nema mogućnost spoznaje da je štićena mreža inicirala vezu. S druge strane, vatrozid sa dinamičkim paketnim

filtriranjem ima sposobnost spoznaje da je paket kojega šalje vanjsko računalo SYN/ACK odgovor, pa ga propušta. Naravno, na kraju se mora završiti trostruko rukovanje ACK odgovorom štićenog računala.

Upravo zbog mogućnosti čitanja TCP zaglavlja i razlikovanja zastavica (SYN, ACK, FIN…), vatrozid sa praćenjem veze prepoznaje da li se radi o legitimnom paketu koji dolazi zbog iniciranog zahtjeva za vezom sa unutarnje mreže ili dolazi na potencijalno opasan način „sam od sebe“ budući da ga nitko nije tražio. Vatrozid sa dinamičkim filtriranjem radi na trećem, četvrtom ali i petom sloju OSI referentnog modela. Ta se činjenica može potkrijepiti detaljem da je sesijski sloj zadužen za ostvarivanje ili prekid veze.

6.2. Proxy vatrozidi

Ovo su vatrozidi aplikacijskog sloja. Koristi proxy server kao posrednik između različitih upita. U ovom slučaju posrednik ne djeluje tako da odbacuje ili prihvaća određeni promet s obzirom na izvorišnu i odredišnu adresu, već pohranjuje upite koji se često ponavljaju. To se zove „cashing“. Dakle proxy nije vatrozid, već je servis implementiran unutar njega. Slika 18 prikazuje postavke proxy vatrozida.



Slika 18. Prikaz proxy postavki vatrozida [18.1]

Proxy server se koristi kao maskirni servis za sakrivanje konfiguracije unutarnje štićene mreže. Preciznije rečeno, pomoću proxy servisa sakrivaju se IP adrese računala unutarnje mreže. To se postiže na način da svi upiti iz unutarnje mreže

izlaze na Internet preko proxy servisa, što znači da vanjska računala na Internetu dobivaju promet uvijek iz jedne IP adrese, a to je adresa proxy servera odnosno vatrozida na kojem je implementiran. Isto vrijedi i za dolazni promet, gdje svaki upit dolazi najprije do proxy servera, koji ga prosljeđuje računalu u mreži. Dakle, proxy je posrednik između unutarnje štićene mreže i vanjske mreže. Mehanizam skrivanja konfiguracije unutarnje mreže smanjuje rizik od napada lažnim predstavljanjem (engl. IP spoofing), jer napadač ne može provesti napad na ciljano računalo u mreži ako mu ne zna IP adresu.

Proxy omogućuje kontrolni log mehanizam u kojemu se zapisuje sav izlazni promet, pa je moguće kontrolirati kojim web stranicama se pristupalo sa unutarnje mreže. Za svaku vrstu aplikacije mora postojati odgovarajući proxy servis. Primjerice, za e-mail server, potrebno je imati e-mail proxy servis, za web server web proxy itd.. Budući da danas ima puno različitih aplikacija i primjena, nema dovoljan broj odgovarajućih proxy servisa. Upravo je to jedan od glavnih nedostataka. Kako bi podržavao veliki broj servisa mora imati pokrenute specifične servise za različite protokole (SMTP, HTTP, FTP…).
Današnji proxy vatrozidi koriste se za filtriranje web sadržaja. Administratori mreže mogu zabraniti posjetu određenim web stranicama i na taj način smanjuju rizik od zagađenja unutarnje mreže. Proxy vatrozidi pružaju bolju zaštitu od vatrozida sa paketnim filtriranjem, budući da mogu dublje istražiti dolazni promet, pa se prema tome mogu postaviti stroži kriteriji za filtriranje paketa. Zbog detaljnijeg istraživanja dolaznih paketa, vrijeme potrebno za odlučivanje je veće nego kod običnog filtriranja paketa, pa u mrežu može uvesti vremensko kašnjenje.

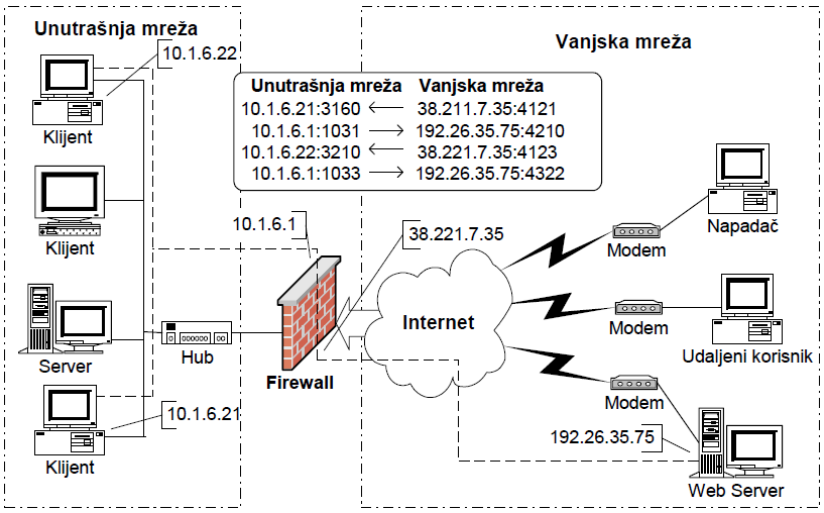
6.3. Translatiranje mrežnih adresa (NAT)

Postoji nekoliko vrsta translatiranja:

- Statički NAT
- Dinamički NAT izlaznog prometa
- Prosljeđivanje portova (engl. port forwarding)

6.3.1. Statičko translatiranje

Na Internetu postoje privatne i javne adrese. Prema tome, uređaji koji moraju biti javno dostupni (npr. e-mail server) koriste javne adrese. S druge strane, privatne adrese su namijenjene za uporabu unutar lokalne mreže i nisu za vanjsko usmjeravanje. NAT se koristi za translatiranje između privatnih i javnih adresa. Translatiranje mrežnih adresa omogućuje uređaju konfiguriranom sa privatnom adresom da se vani prikazuje kroz javnu adresu i na taj način mu dozvoljava komunikaciju sa drugim uređajem preko Interneta. Vatrozid obično omogućuje translatiranje privatne na javnu adresu, javne na privatnu, javne na javnu ili privatne na privatnu adresu. Korištenjem statičkog translatiranja ne rješava se problem manjka IP adresa, budući da je potreban jednak broj privatnih i javnih adresa za translataciju. Glavni cilj translatiranja adresa je skrivanje konfiguracije uređaja unutar mreže vanjskim uređajima na Internetu. Slika 19 prikazuje maskiranje mrežnih adresa vatrozidom.



Slika 19. Maskiranje mrežnih adresa [19.1]

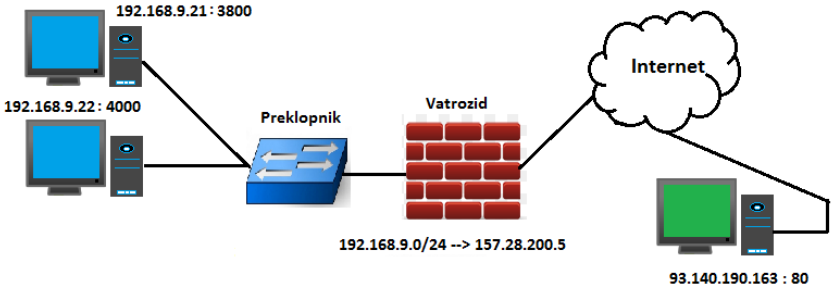
6.3.2. Dinamičko translatiranje

Translatiranje mrežnih adresa podržava gotovo svaki bolji vatrozid. Osim skrivanja konfiguracije unutarnje mreže NAT ima i drugih prednosti po kojima se razlikuje od proxy servisa. Dinamičko translatiranje ima sličnu ulogu kao i proxy u smislu prikaza prometa prema van, kao da se šalje sa jedne IP adrese. Vatrozidi za dinamičkim mrežnim translatiranjem u memoriji posjeduju tablicu sa postojećim

vezama prema vani. Unutar nje zabilježene su adrese unutarnjih računala i vanjskih kojima ista pristupaju.

Na slici 20 dan je primjer tablice sa vezama i prikazana je konfiguracija unutarnje mreže sa pripadajućim IP adresama i portovima. Pretpostavka je da u unutarnjoj mreži postoje dva računala, koja se žele spojiti preko Interneta na računalo 93.140.190.163. Vatrozid je izveden sa dinamičkim translatiranjem mrežnih adresa.

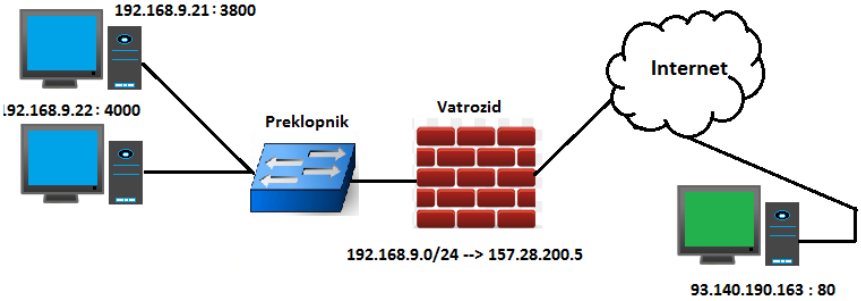
Izvorišna IP adresa	Izvorišni port	Odredišna IP adresa	Odredišni port
192.168.9.21	3800	93.140.190.163	80
192.168.9.22	4000	93.140.190.163	80



Slika 20. Prikaz dinamičkog translatiranja mrežnih adresa

Računalo 192.168.9.21 koristi TCP port 3800 za spajanje na vanjski poslužitelj, a računalo 192.168.9.22 koristi TCP port 4000. Iz slike je vidljivo da vatrozid prikazuje sve unutarnje upite prema vani kao da dolaze iz jedne IP adrese 157.28.200.5. Na taj način izvodi se maskiranje unutarnje mrežne konfiguracije. Oba su računala iz štićene mreže spojena na vanjski poslužitelj svako preko svojega porta i svoje IP adrese.

Izvorišna IP adresa	Izvorišni port	NAT port	Odredišna IP adresa	Odredišni port
192.168.9.21	3800	3800	93.140.190.163	80
192.168.9.22	4000	4000	93.140.190.163	80
192.168.9.21	4000	5000	93.140.190.163	80



Slika 21. Prikaz translatiranja portova

Iz slike 21 može se vidjeti da je računalo 192.168.9.21 pokušalo ostvariti još jednu konekciju na vanjski poslužitelj, međutim TCP port kojim se prvo računalo htjelo poslužiti je zauzet. Stoga, NAT vatrozid radi translatiranje portova i dodjeljuje prvom računalu novi port (obično iznad 1023).

6.3.3. Prosljeđivanje portova

Mrežno translatiranje adresa dozvoljava samo upite koji odlaze iz unutarnje mreže prema vani, pa je nemoguće da vanjsko računalo šalje promet prema štićenoj mreži. Preciznije rečeno, vanjsko računalo može poslati upit ali će biti odbačen. Iz takvoga načina rada, može se zaključiti da postoji potreba za pristupom nekom serveru u unutarnjoj mreži. Zato se koristi prosljeđivanje portova. To znači da se vatrozid može konfigurirati tako da se sav dolazni promet prosljeđuje na određeni port točno specifičnom uređaju. Ako se računalo iz vanjske mreže želi spojiti na web server u unutarnjoj, tada se vatrozid konfigurira na način da se svi TCP paketi prosljeđuju na port 80 (web server).

6.4. Hardverski i softverski vatrozidi

Postoje programski i hardverski vatrozidi. Hardverski vatrozidi osiguravaju prvu liniju obrane od uobičajenih napada na mrežu izvana. Obično imaju visoku učinkovitost, pružajući odličnu zaštitu svim računalima u unutarnjoj mreži. Prednost je hardverskog vatrozida upravo u tome, što jedan može zaštititi cijelu mrežu iza njega, dok softverski štite samo računalo na kojem se nalaze. Nedostatak hardverskih vatrozida je što označavaju izlazni promet (iz štićene mreže prema van) sigurnim, što podrazumijeva određeni rizik. Hardverski vatrozidi ne mogu zaštiti od zaraženih e-poruka, budući da ne pregledavaju privitke u porukama. Primjerice, ako je privitak neki zlonamjerni program, računalo unutar štićene mreže može se zaraziti, a budući da je sav izlazni promet smatran legalnim zlonamjerni se program može širiti dalje izvan mreže. Rješenje za takav problem bi bio u blokiranju porta kojega koristi takav zlonamjerni program, međutim prepoznati koji port se koristi za slanje zlonamjernog sadržaja van mreže je gotovo nemoguće zbog velikog broja portova koji prelazi 65 500. Čak i u slučaju poznavanja porta, kako bi se onemogućilo slanje zlonamjernog

programa na druge e-mail adrese van mreže, bilo bi potrebno pogasiti port 25 kojega koristi SMTP protokol za slanje e-pošte. Dakle, kao posljedica zaraze zlonamjernim programom, javljaju se mnogi značajni problemi.

Programski vatrozidi obično se upotrebljavaju za osiguravanje računala od web prometa, dakle uporabom HTTP protokola. Najčešće se instaliraju na osobna računala i web servere. Nije rijetko da se unutar programskog vatrozida mogu naći implementirani antivirusni programi. Sami po sebi, nisu dovoljni za kompletnu zaštitu računala na kojima se nalaze, već se koriste zajedno sa hardverskim zaštitnim uređajima i sa sistemima za zaštitu od upada (IPS). Programski vatrozidi mogu jednostavnije riješiti problem sa e-poštom, budući da imaju mogućnost prepoznavanja programa koji pokušava ostvariti vezu na Internet, i njegove naravi (dobronamjeran ili zlonamjeran). Ako program ne može sam ocijeniti narav programa koji traži vezu na Internet, softverski vatrozid obično pita korisnika što da čini, tako da promet neće izaći van dok to on ne odobri. Glavni nedostatak ove vrste vatrozida je nemogućnost štićenja cijele mreže kao kod hardverskog. Softverski se moraju instalirati na svako računalo u mreži posebno, a to zahtjeva veliki broj licenci i povećava troškove. Dakle, za razliku od hardverskih, softverski vatrozidi nisu u mogućnosti štititi cijelu unutarnju mrežu.

Za model vatrozida kojim se štiti sustav ECDIS, korišten je Windowsov softverski vatrozid, budući da je prema [7] i [8] glavni operativni sustav kojega ugrađuju ECDIS proizvođači upravo Windows. Bilo bi korisnije uz softverski, što se i prakticira, koristiti hardverski vatrozid za obranu cijele unutarnje mreže broda. Međutim, iz jasnih razloga model je prezentiran samo na Windows vatrozidu, pretpostavljajući zaštitu samo ECIDS sustava.

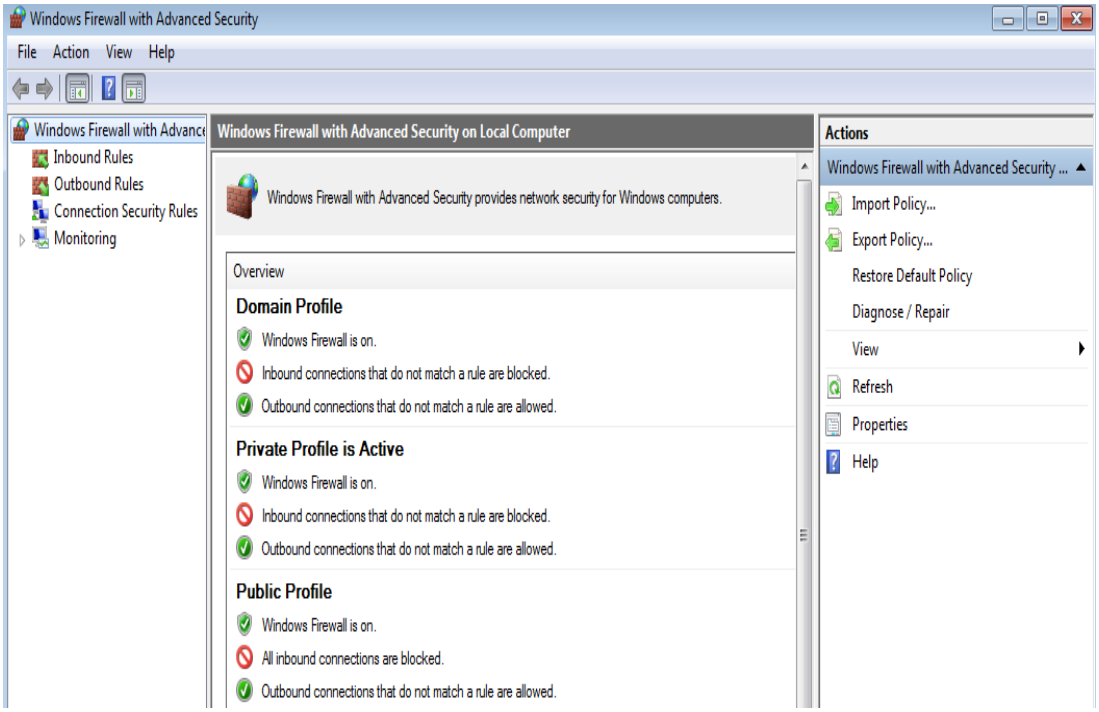
6.5. Zaključak poglavlja

Vatrozidi prema zaštitnim funkcijama koje omogućuju mogu biti vatrozidi sa filtriranjem paketa, vatrozidi sa proxy servisom, te vatrozidi sa translatiranjem mrežnih adresa. U radu je prezentirana konfiguracija postavki Windows vatrozida koji omogućuje filtriranje paketa. Nakon upoznavanja sa sustavom ECDIS, sa vrstom

internetske veze koju omogućuje INMARSAT, definiranja protokola, te upoznavanja sa tehnikama napada na te protokole, moguće je izraditi konfiguraciju postavki vatrozida. Sedmo poglavlje donosi izrađenu konfiguraciju postavki Windows vatrozida za sustav ECDIS temeljenu na ICMP, TCP i UDP protokolu.

7. Konfiguracija postavki vatrozida

Windows vatrozid je izveden sa praćenjem veze (engl. stateful firewall) što znači da ima mogućnost filtriranja paketa IPv4 i IPv6 verzije. Filtriranje paketa se obavlja s obzirom na unaprijed podešene parametre. Budući da se radi o vatrozidu sa praćenjem veze, početne postavke su podešene tako da je dolazni promet blokiran, osim ako su dolazni paketi odgovor na unaprijed inicirani poziv sa strane nekog od računala štićene mreže. Windows vatrozid je softverskog tipa, pa je moguće podešavati parametre za promet s obzirom na broj porta, izvorišnu i odredišnu IP adresu, ali i s obzirom na aplikaciju koja želi vezu na Internet.



Slika 22. Početni ekran „Windows Firewall with Advanced Security“

Na slici 22 prikazan je početni zaslon Windowsovog vatrozida koji će se koristiti prilikom izrade modela zaštite za sustav ECDIS.

Windows vatrozid podržava tri vrste pravila za definiranje parametara:

- Dopusti vezu
- Dopusti vezu samo ako je zaštićena IPsec protokolom
- Blokiraj vezu

Glavni zaslon prikazuje:

„Inbound rules“ – pravila koja se tiču dolaznog prometa. Po početnim postavkama, dolazni promet je zabranjen. Moguće je dakle, dozvoliti ili zabraniti dolazni promet s obzirom na izvorišnu IP adresu, protokol i druge parametre.

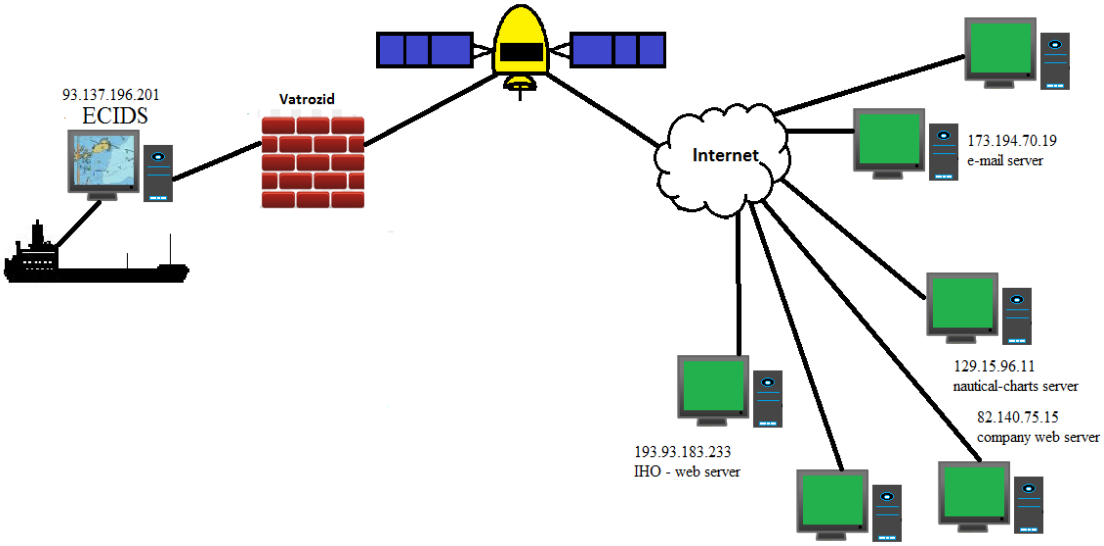
„Outbound rules“ – odnosi se na pravila koja se tiču odlaznog prometa. Dakle, pravila koja definiraju dozvoljava li vatrozid ili ne dozvoljava promet prema van. Po početnim postavkama, izlazni promet je dozvoljen, a moguće ga je i zabraniti s obzirom na IP adresu, port i druge parametre.

„Connection Security Rules“ – pravila kojima je moguće ostvariti provjeru autentičnosti između dva računala u vezi, primjerice razmjenom ključeva. Podaci koji se šalju putem veze su sačuvani uporabom IPsec protokola. Moguća je enkripcija podataka. Da bi se ova pravila mogla koristiti, oba računala u vezi moraju imati definirana sigurnosna pravila (Connection Security Rules).

„Monitoring“ – praćenje postojećih aktivnih pravila vatrozida na računalu. Prikaz trenutno aktivnog profila.

Profili – koriste se za grupiranje pravila. Administrator može željeti postaviti različita pravila, s obzirom na mjesto gdje vatrozid spaja. Tako postoje tri različita profila:

- „Domain profile“ – pravila se primjenjuju na Windows domenu
- „Private profile“ – pravila se primjenjuju kada je računalo spojeno na privatnu mrežu koja nije direktno spojena na Internet, već ju štiti neki zaštitni uređaj npr. vatrozid.
- „Public profile“ – pravila se primjenjuju kada je računalo spojeno na javnu mrežu putem Interneta. Budući da je nepoznata sigurnost javne mreže, uobičajeno je da pravila budu stroža na ovom profilu. Definiranje pravila kod ovog profila ključno je za obranu uređaja ECDIS, budući da se spaja satelitskim Internetom na javnu mrežu.
- Budući da je ovaj model konfiguracije vatrozida temeljen na pretpostavkama, treba prikazati kako izgleda pretpostavljeno spajanje sustava ECDIS na Internet putem INMARSAT satelita.



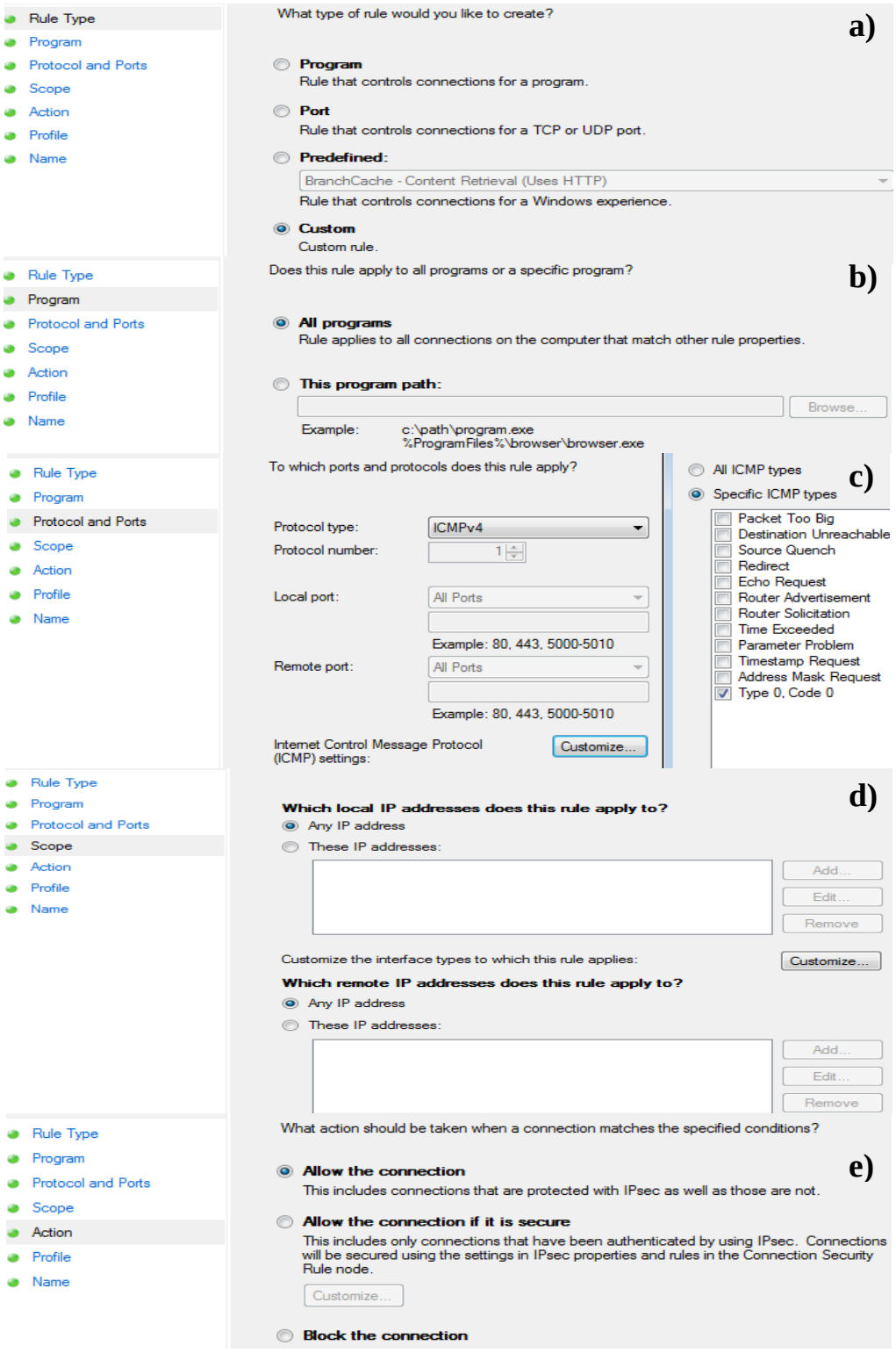
Slika 23. Prikaz pretpostavljene konfiguracije spajanja sustava ECDIS na Internet

Slika 23 prikazuje sustav ECDIS na brodu štićen Windows vatrozidom. Spaja se na Internet putem INMARSAT satelita. Korisnicima sustava ECDIS omogućiti će se spajanje na web poslužitelj IHO organizacije, web poslužitelj vlastite brodarske kompanije i na poslužitelj sa nautičkim kartama.

7.1. ICMP protokol

7.1.1. ICMP „Echo“

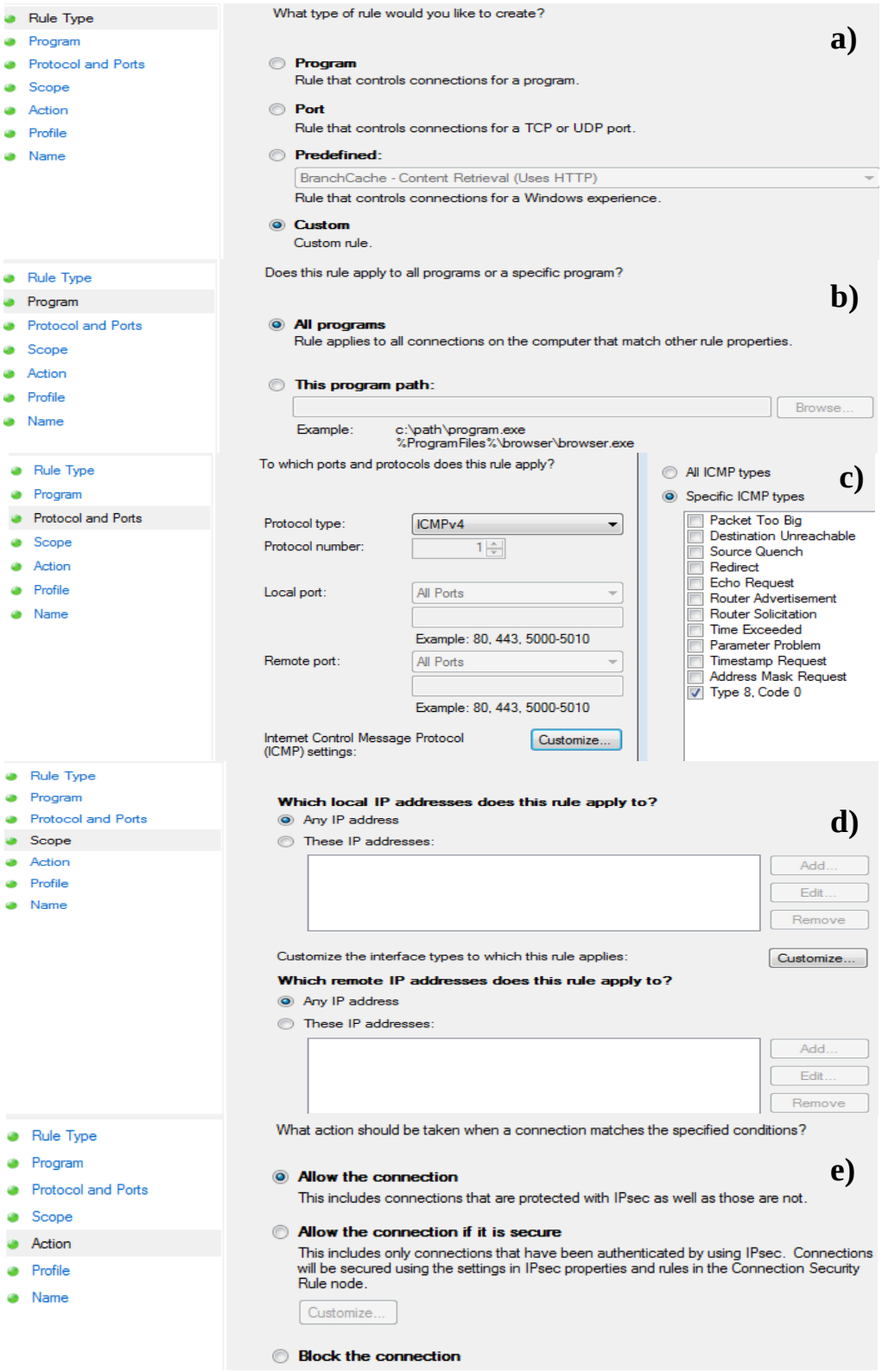
ICMP protokol važan je za dijagnosticiranje različitih problema mreže, pa ga nije uvijek poželjno cijelog blokirati. Vrlo je koristan, ali kompleksan, pa za podešavanje konfiguracije ICMP postavki kod vatrozida ima mnogo različitih mišljenja. Međutim, taj se protokol može zlorabiti pa je potrebno postaviti određene restrikcije na njega. Obrana od ICMP napada na raspoloživost računala ECDIS može se izvesti na više načina. Na slici 23 je prikazana pretpostavljena konfiguracija spajanja na Internet, iz koje se vidi da je ECDIS jedino računalo u unutarnjoj štićenoj mreži. Napad ICMP protokolom koji bi koristio brodsku LAN mrežu kao „pojačalo“ mogao bi se izvesti ako bi uz ECDIS u lokalnoj mreži bilo spojeno još računala. Budući da prema pretpostavljenoj konfiguraciji nema drugih računala u unutarnjoj mreži, DOS napad se ne može izvesti uz pomoć lokalnih računala. Protokol ICMP može napadaču otkriti dosta važnih informacija o konfiguraciji mreže koju napada. S obzirom na sve navedeno slijedi konfiguracija postavki vatrozida.



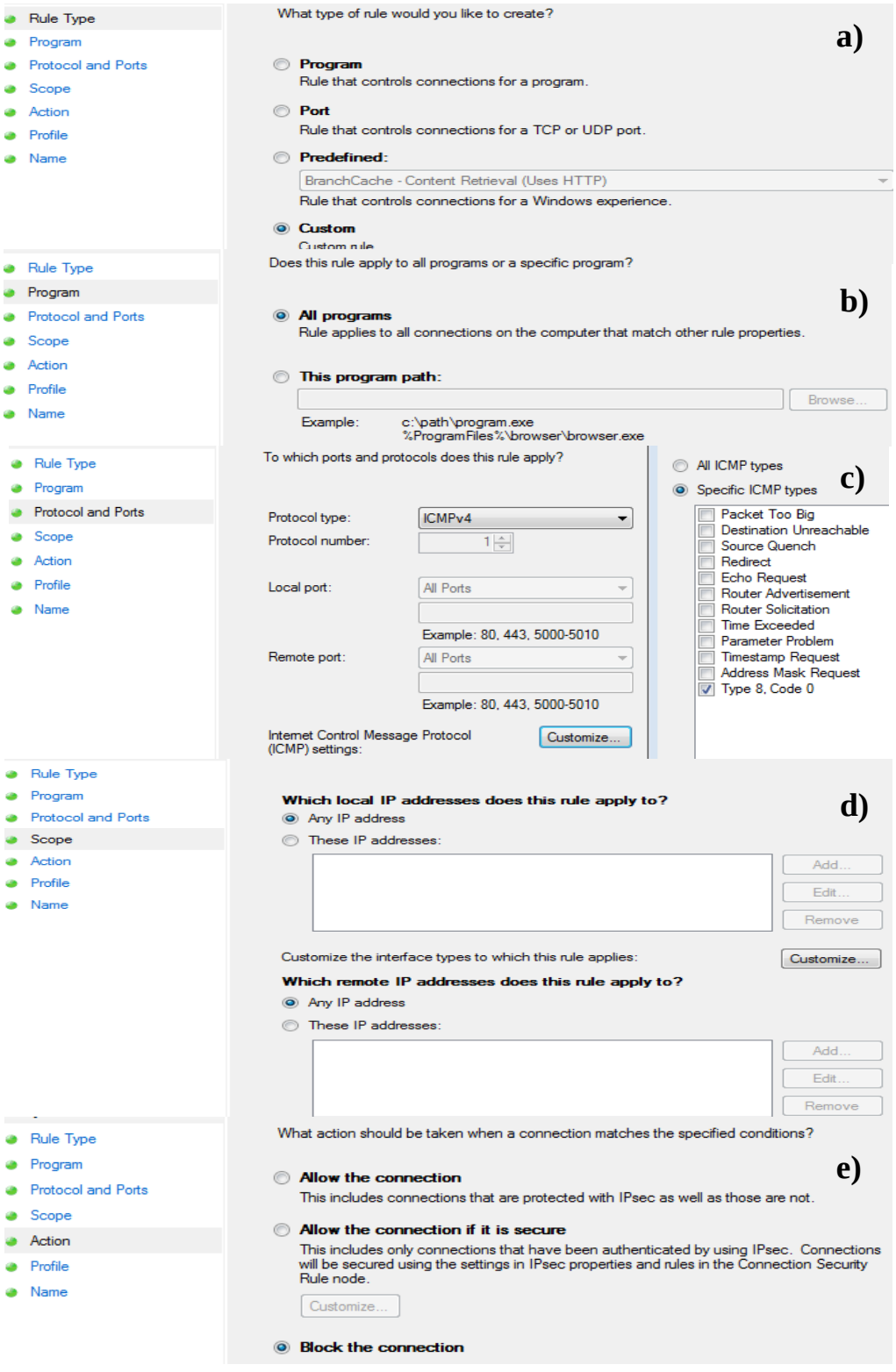
Slika 24. Dolazni „Echo“ odgovor: a) Prikaz odabira tipa pravila b) Prikaz programa na kojeg se odnosi pravilo, c) Prikaz ICMP tipa na kojeg se odnosi pravilo, d) Prikaz IP adresa na koje se primjenjuje akcija, e) Prikaz akcije koja se primjenjuje u pravilu

Slika 24 prikazuje kako je definirano pravilo za dolazni „Echo“ odgovor. Budući da se postavke u ovom pravilu odnose na dolazni promet definiraju se u kartici „Inbound Rules“ glavnog prozora vatrozida. Za tip pravila, odabrana je funkcija „Custom“ koja se koristiti kad je nepoželjno primijeniti neko unaprijed ponuđeno pravilo, već ga se želi proizvoljno definirati (slika a). Pravilo se primjenjuje na sve programe (slika b). Odnosi se na ICMP protokol tipa 0 i koda 0, što označava „Echo“ odgovor (slika c). Akcija koja se primjenjuje u pravilu odnosi se na sve udaljene (engl. remote) i lokalne IP adrese (slika d). Dolazne „Echo“ odgovore vatrozid propušta prema štićenom računalu (slika e). Ovaj tip ICMP protokola je propušten iz razloga što se DOS napad uglavnom provodi na računala koja imaju svojstva poslužitelja i na taj način se pokuša onemogućiti udaljenim korisnicima pristup. Budući da ECDIS nije server, već udaljeno klijentsko računalo koje se spaja na server, nije realno očekivati ovakvu vrstu napada na ECDIS, međutim određeni sigurnosni rizik postoji. Upravo zbog toga, vatrozid će propuštati dolazne „Echo“ odgovore, dok će blokirati dolazne upite. Nema razloga da netko provjerava dostupnost računala ECDIS „pinganjem“, već postoji potreba da se testira dostupnost poslužitelja.

S druge strane, postoje odlazni „Echo“ upiti koje može primjerice upotrijebiti korisnik sustava ECDIS da ustvrdi je li poslužitelj sa navigacijskim kartama dostupan. Slika 25 prikazuje kako je definirano pravilo za odlazne „Echo“ upite. Isto kao i kod prethodnog pravila, odabrana je funkcija „Custom“ (slika a) što znači da se neće koristiti neki unaprijed definirani tip pravila, već će se proizvoljno definirati. Ovo pravilo primjenjuje se na sve programe (slika b). Budući da se postavke u ovom pravilu odnose na odlazni promet, definiraju se u kartici „Outbound Rules“ glavnog prozora vatrozida. Pravilo je definirano za ICMP protokol tipa 8 koda 0, što označava odlazni „Echo“ upit (slika c). Raspon (engl. scope) IP adresa je definiran tako da pravilo vrijedi za sve udaljene i lokalne adrese (slika d). Odlazni „Echo“ upiti su dozvoljeni (slika e).



Slika 25. Odlazni „Echo“ upit: a) Prikaz odabira tipa pravila b) Prikaz programa na kojeg se odnosi pravilo, c) Prikaz ICMP tipa na kojeg se odnosi pravilo, d) Prikaz IP adresa na koje se primjenjuje akcija, e) Prikaz akcije koja se primjenjuje u pravilu



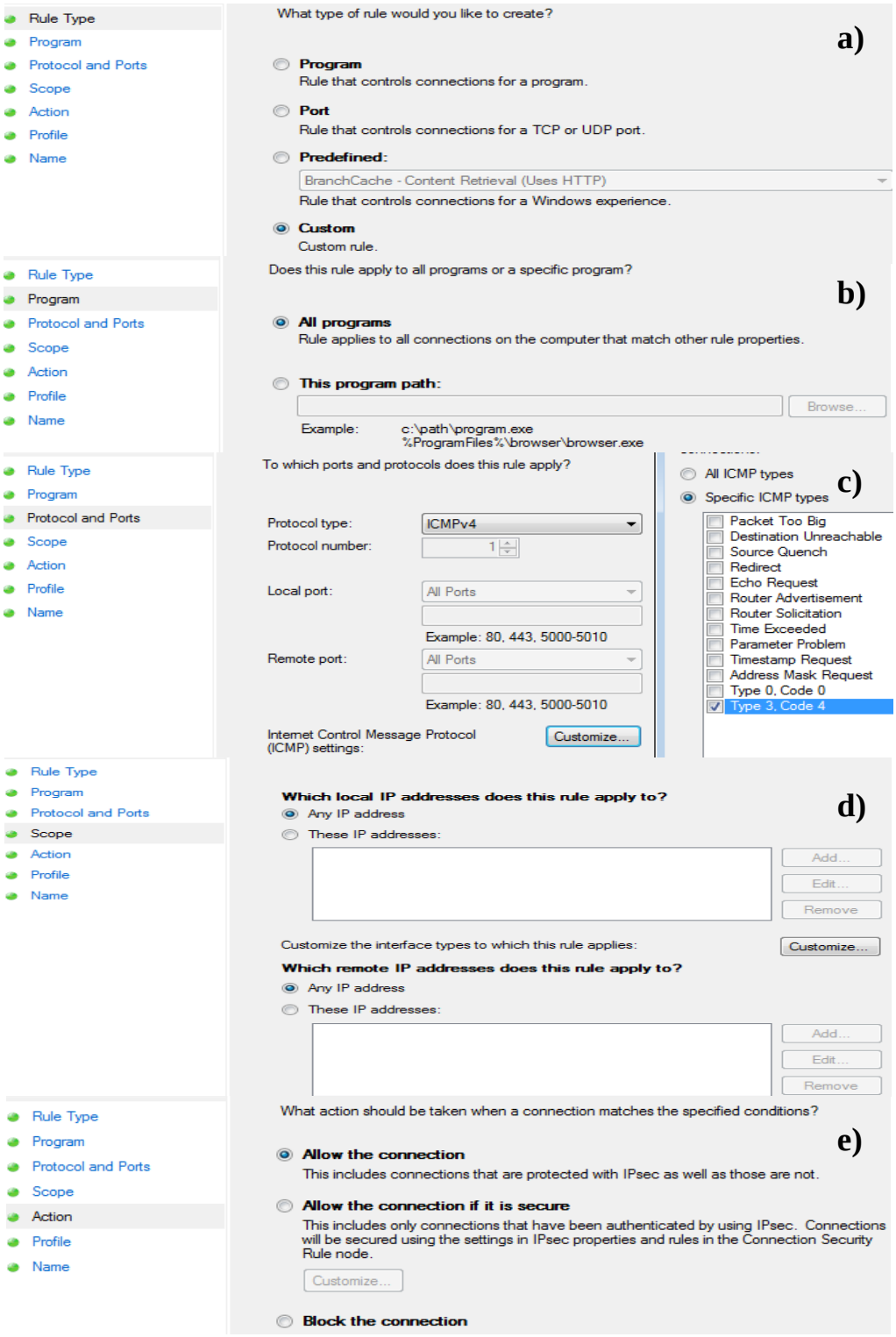
Slika 26. Dolazni „Echo“ upit: a) Prikaz odabira tipa pravila b) Prikaz programa na kojeg se odnosi pravilo, c) Prikaz ICMP tipa na kojeg se odnosi pravilo, d) Prikaz IP adresa na koje se primjenjuje akcija, e) Prikaz akcije koja se primjenjuje u pravilu

Slika 26 prikazuje pravilo definirano za dolazne „Echo“ upite. Tip pravila je „Custom“ što znači da je pravilo proizvoljno definirano, a nije korišteno neko od prethodno ponuđenih (slika a). Primjenjuje se na svaki program (slika b). Odnosi se na ICMP protokol tipa 8 koda 0, što označava „Echo“ upit (slika c). Rang IP adresa na koje se odnosi pravilo je podešen tako da vrijedi za sve vanjske i lokalne adrese (slika d). Dolazni „Echo“ upiti su blokirani (slika e), budući da nema potrebe za „pinganjem“ sustava ECDIS. Kako su dolazni „Echo“ upiti blokirani, postavke za odlazne „Echo“ odgovore nije potrebno postavljati.

7.1.2. ICMP „Destination Unreachable“

Konfiguracija postavki vatrozida za ICMP protokol tipa 3 (Destination Unreachable) složena je iz razloga što postoji više od 11 kodova sa različitim značenjima. U radu je već spomenuto 8 najvažnijih poruka, međutim Windows vatrozid u ponudi daje izbor od 11. Prilikom slanja paketa putem vanjske internetske mreže može se dogoditi da neki od „gateway-a“ putem kojih se paket prosljeđuje nema zadanu rutu i nema mogućnost daljnjeg prosljeđivanja paketa. U takvom slučaju taj će „gateway“ vratiti poruku izvoru da mu je odredišna mreža nedostižna (engl. net unreachable). Analogno vrijedi i ukoliko taj „gateway“ ne podržava protokol kojim se šalje paket, pa vraća izvoru poruku nedostižni protokol (engl. protocol unreachable). Primjerice, kada paket koji se šalje stigne do odredišta, ali port putem kojeg se pokušava uspostaviti veza nije otvoren, vraća se poruka da je port nedostižan (engl. port unreachable).

Pored svih kodova tipa 3 ICMP protokola, kod 4 (enlg. Fragmentation needed and DF set) je najvažniji za uspješan prijenos podataka. Paketi se pokušavaju slati na način da budu što veći bez potrebe za fragmentacijom, jer se takvim prijenosom postiže visoka efikasnost transfera. Ako se dogodi da neki od posrednog usmjernika koji je sastavni dio rute ima niži kapacitet za prijenos paketa, javlja se potreba za fragmentacijom. Tada usmjernik šalje povratnu poruku sa kodom 4, pa će se s izvora slati manji paket kojega posredni usmjernik može proslijediti. Maksimalna veličina paketa određena je MTU jedinicom (engl. maximum transmission unit), koja se smanjuje nakon poruke s kodom 4. Poruke tipa 3 koda 4 su nužne za prijenos paketa, te će se iz tog razloga propustiti.

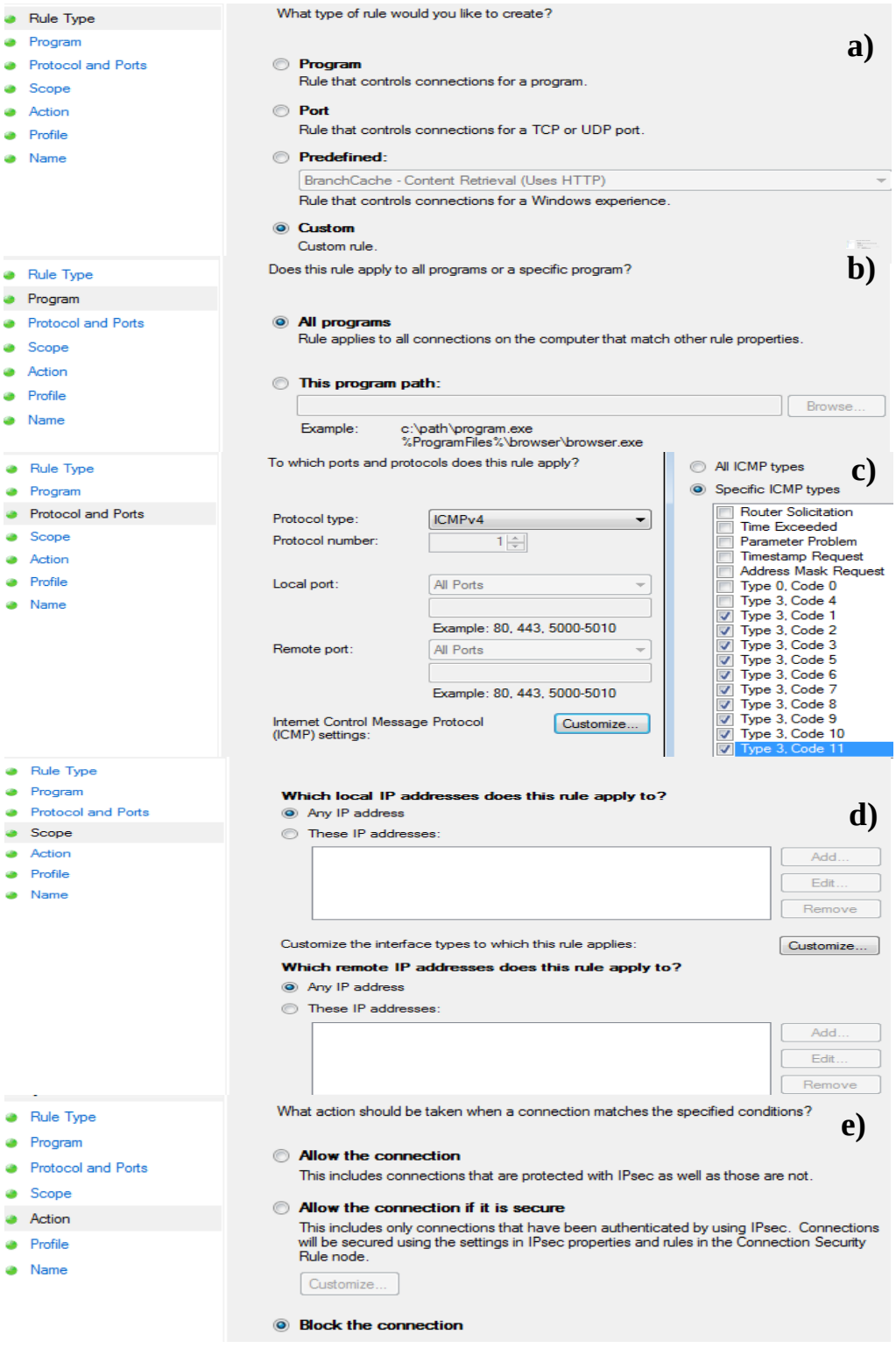


Slika 27. Dolazne „Destination Unreachable“ poruke koda 4: a) Prikaz odabira tipa pravila b) Prikaz programa na kojeg se odnosi pravilo, c) Prikaz ICMP tipa na kojeg se odnosi pravilo, d) Prikaz IP adresa na koje se primjenjuje akcija, e) Prikaz akcije koja se primjenjuje u pravilu

Slika 27 prikazuje kako je definirano pravilo za ICMP protokol tipa „Destination Unreachable“ koda 4. Tip pravila je „Custom“ što znači da je pravilo proizvoljno definirano, a nije korišteno neko od prethodno ponuđenih (slika a). Odnosi se na sve programe (slika b), te na ICMP protokol tipa 3 koda 4 što označava „Destination Unreachable“ poruke koda 4 (slika c). Rang IP adresa je isti kao i kod svih definiranih pravila do sada, što znači da pravilo vrijedi za sve udaljene i lokalne adrese (slika d). Akcija koju pravilo primjenjuje na dolazni promet dopušta „Destination Unreachable“ poruke koda 4 (slika e).

Ostale poruke tipa 3 su zabranjene budući da se mogu zlorabiti za izvođenje DOS napada, ili slijepog napada za prekidanje veze. Isto tako, mogu se zlorabiti za napad na propusnost. Obrana od DOS napada postiže se zabranom učestalog slanja poruka tipa 3 (engl. rate limiting). Takvu mogućnost ima svaki bolji hardverski vatrozid, dok je Windows 7 nema. Konfiguracija postavki za izlazne ICMP poruke tipa 3 iste su kao i za dolazne. Ovdje je važno blokirati poruke koda 3, koje se mogu zlorabiti za prikupljanje informacija o portovima. Budući da je namještanje odlaznih postavki isto kao i za dolazne poruke, konfiguracija se neće posebno prikazivati.

Slika 28 prikazuje kako je definirano pravilo za ostale dolazne ICMP poruke tipa 3. Budući da se postavke u ovom pravilu odnose na dolazni promet definiraju se u kartici „Inbound Rules“ glavnog prozora vatrozida. Tip pravila je „Custom“ što znači da je pravilo proizvoljno definirano, a nije korišteno neko od prethodno ponuđenih (slika a). Pravilo se odnosi na sve programe (slika b). Također, odnosi se na ICMP poruke tipa 3 sa kodovima od 1 do 3 te kodovima od 5 do 11 (slika c). Rang IP adresa je neodređen (slika d), a akcija koju primjenjuje ovo pravilo blokira sve ICMP poruke koje nisu koda 4 (slika e).

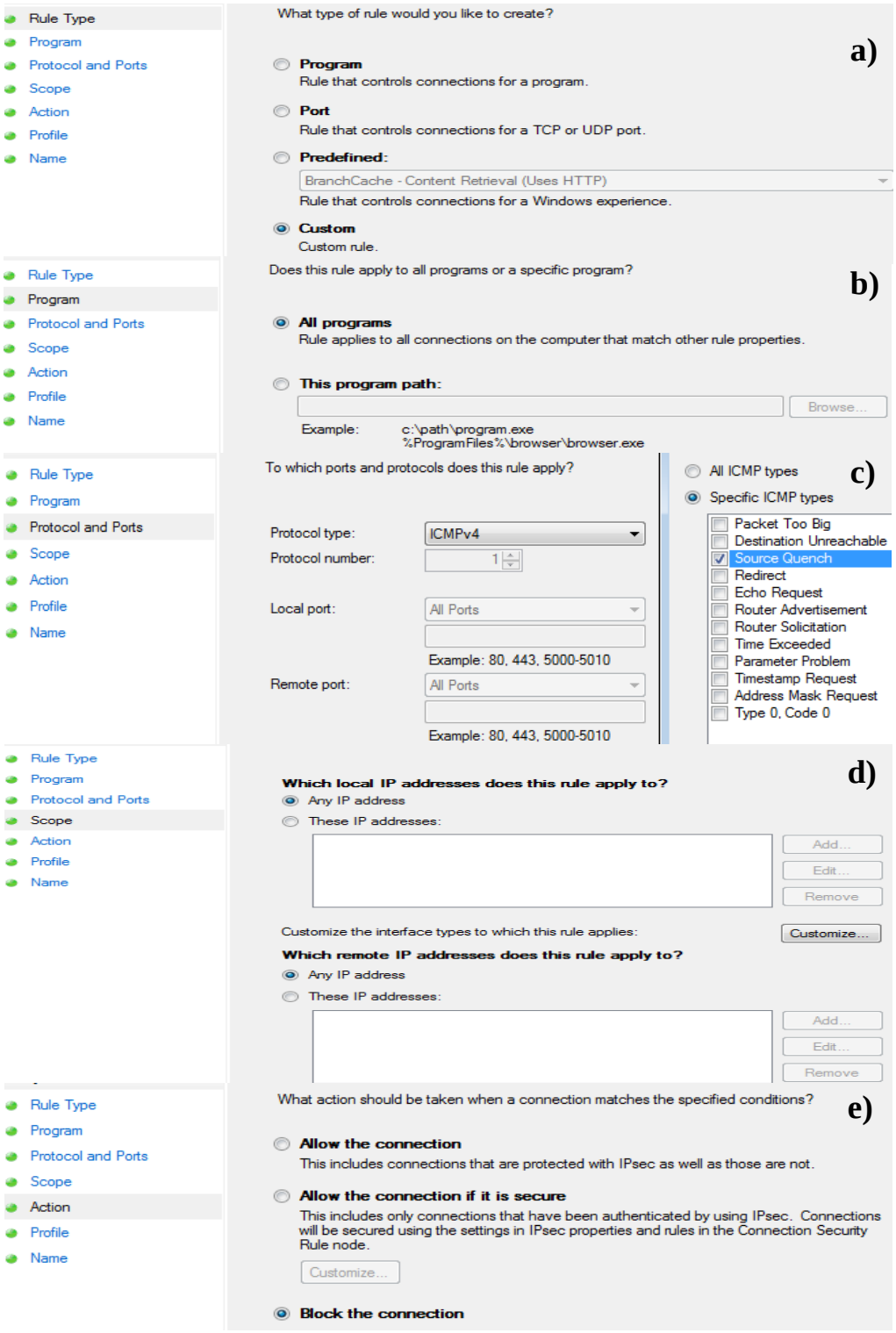


Slika 28. Ostale dolazne „Destination Unreachable“ poruke: a) Prikaz odabira tipa pravila b) Prikaz programa na kojeg se odnosi pravilo, c) Prikaz ICMP tipa na kojeg se odnosi pravilo, d) Prikaz IP adresa na koje se primjenjuje akcija, e) Prikaz akcije koja se primjenjuje u pravilu

7.1.3. ICMP „Source Quench“

Poruke tipa 4 (engl. Source Quench) se blokiraju iz razloga što TCP ima svoj mehanizam za definiranje propusnosti koji ne koristi ICMP protokol. Računalo koje koristi ovaj tip ICMP poruka podložno je slijepim napadima na propusnost, pa nije potrebno riskirati sa dopuštanjem ove poruke. Slika 29 prikazuje konfiguraciju postavki za „Source Quench“ poruke. Postavke vatrozida za izlazne ICMP „Source Quench“ poruke su iste kao i za dolazne pa se neće posebno prikazivati.

Pravilo definirano za dolazne „Source Quench“ poruke vrijedi za sve programe (slika b), a tip pravila je „Custom“ (slika a). Odnosi se na dolazne „Source Quench“ poruke ICMP protokola (slika c). Rang IP adresa je neodređen, što znači da se pravilo odnosi na sve udaljene i lokalne IP adrese (slika d). Konačna akcija koju pravilo poduzima kada se vatrozid susretne sa dolaznim „Source Quench“ porukama je blokiranje tog prometa (slika e).

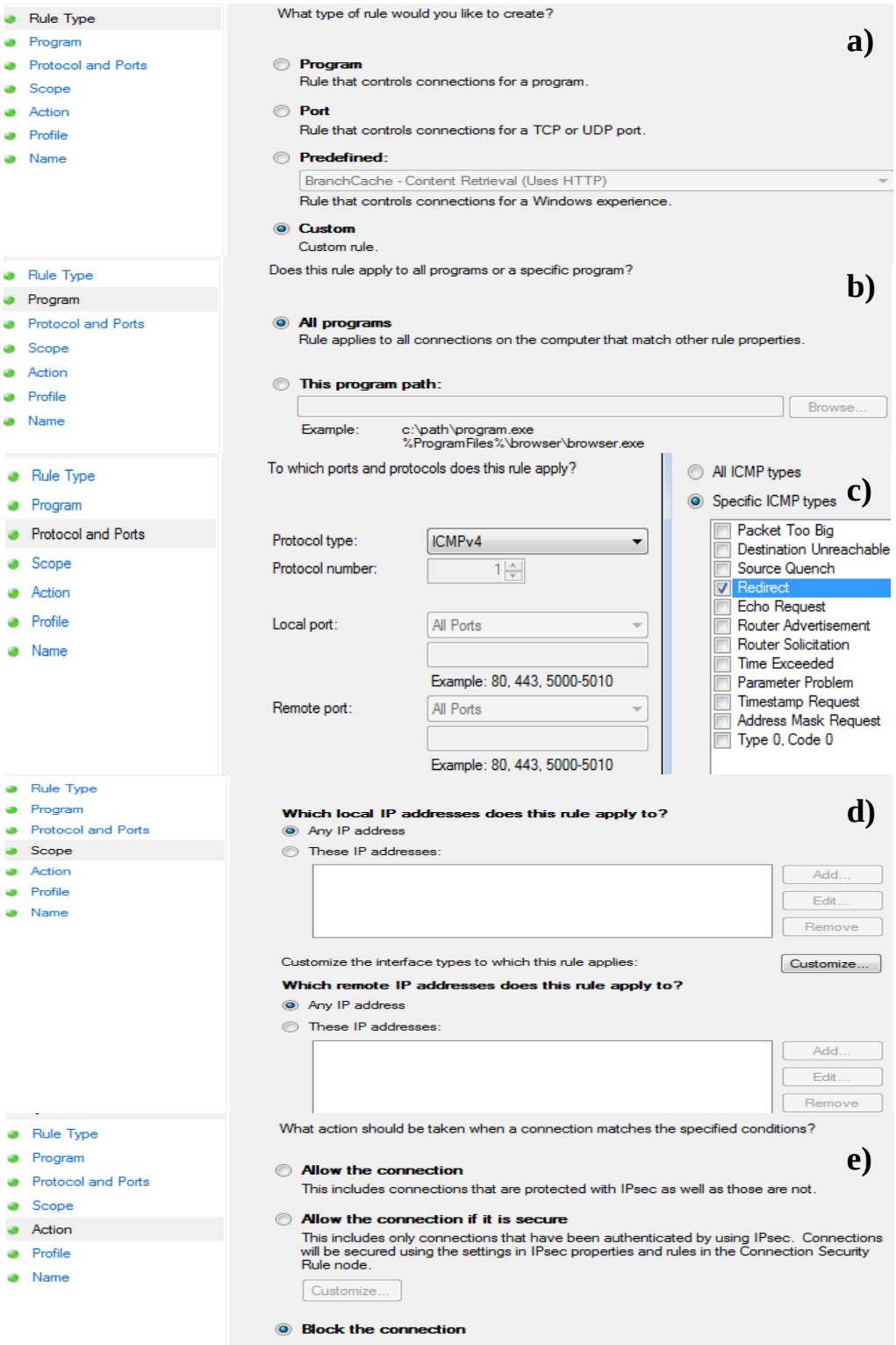


Slika 29. Dolazne „Source Quench“ poruke : a) Prikaz odabira tipa pravila b) Prikaz programa na kojeg se odnosi pravilo, c) Prikaz ICMP tipa na kojeg se odnosi pravilo, d) Prikaz IP adresa na koje se primjenjuje akcija, e) Prikaz akcije koja se primjenjuje u pravilu

7.1.4. ICMP „Redirect“

Poruke tipa 5 odnose se na preusmjeravanje rute kojom paket putuje. Koristi se za obavijesti o boljim rutama za prijenos paketa, pa se upravo zbog tog principa mogu zlorabiti. Primjerice, sposoban napadač može prikazati kao najbolju rutu onu koja će prosljeđivati promet do njega. Poruke ovog tipa se mogu blokirati jer to nema značajnog negativnog utjecaja na transfer podataka.

Slika 30 prikazuje postavke dolaznog prometa za „Redirect“ poruke ICMP protokola. Tip pravila je „Custom“ (slika a) i odnosi se na sve programe (slika b). Protokol na koji se pravilo odnosi je ICMP tipa „Redirect“ (slika c). Rang IP adresa je neograničen, što znači da se pravilo odnosi na sve udaljene i unutarnje IP adrese (slika d). Konačna akcija koja se poduzima blokira dolazni „Redirect“ promet (slika e). Postavke za izlazni promet postavljaju se na jednak način pa neće biti posebno prikazane.

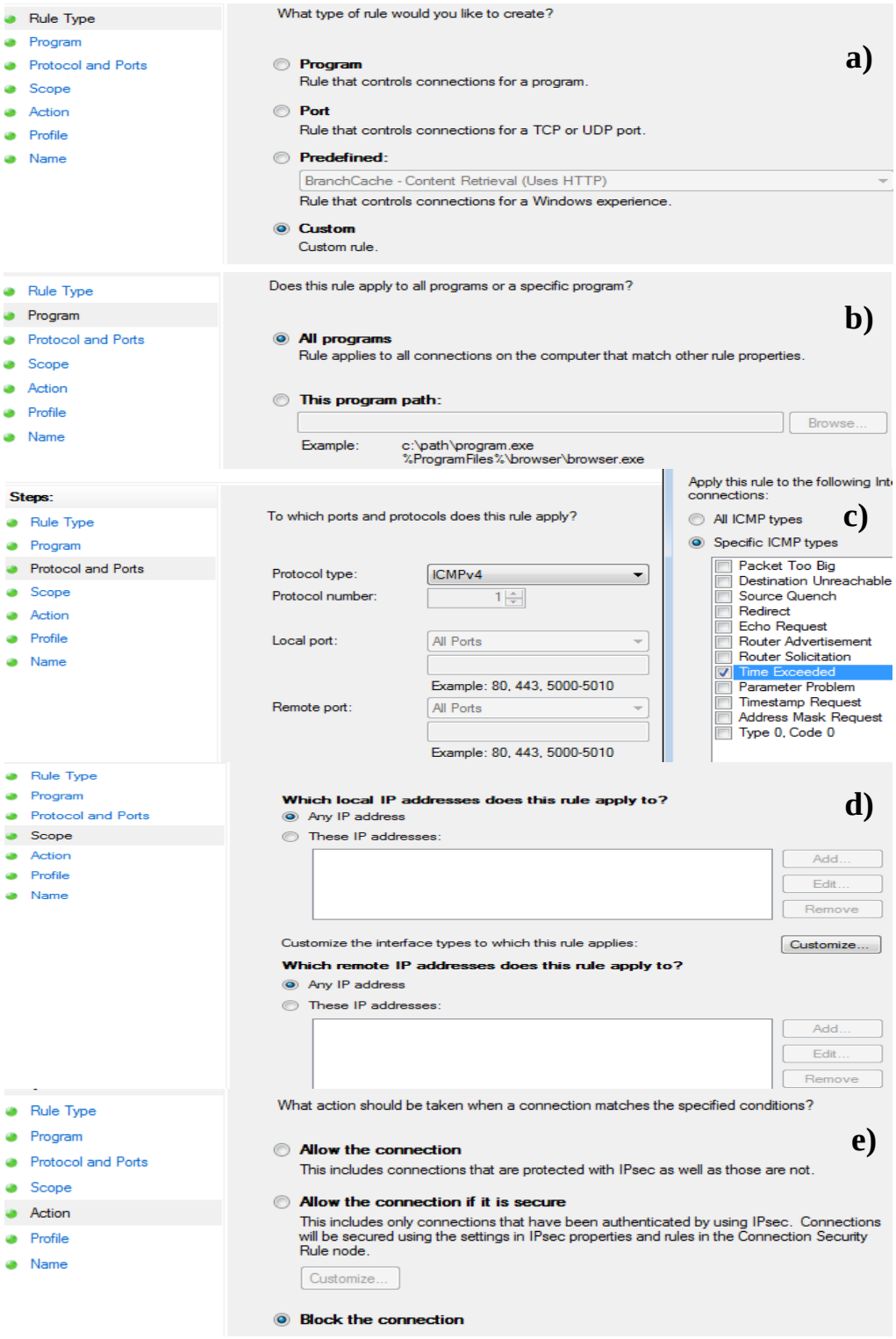


Slika 30. Dolazne „Redirect“ poruke : a) Prikaz odabira tipa pravila b) Prikaz programa na kojeg se odnosi pravilo, c) Prikaz ICMP tipa na kojeg se odnosi pravilo, d) Prikaz IP adresa na koje se primjenjuje akcija, e) Prikaz akcije koja se primjenjuje u pravilu

7.1.5. ICMP TTL “Exceeded“

Ovaj tip ICMP poruke vrlo je koristan za određivanje problema u mreži. Zaglavlje IP paketa sadrži polje TTL. Nakon svakog prolaska paketa kroz neki od posrednih usmjernika prilikom transfera, TTL vrijednost padne za jedan. Ako je broj usmjernika u ruti veći od TTL vrijednosti, ruter gdje se javi vrijednost 0 vraća poruku tipa 3 koja označava da je vrijeme za prijenos paketa isteklo. Na taj se način onemogućuje paketu da „beskonačno“ kruži mrežom. Iako je ova poruka jako korisna, prilikom konfiguracije Windows vatrozida koji je implementiran unutar računala, nema smisla dopuštati ovu poruku. Ako je paket već došao do računala znači da TTL još nije nula. Ovu je poruku korisno propuštati kod vatrozida koji se smatraju posredničkima pri slanju paketa, a sustav ECDIS je odredišno, ne posredničko računalo.

Slika 31 prikazuje kako je definirano pravilo za dolazne „Time Exceeded“ poruke ICMP protokola. Tip pravila je „Custom“ što označava da se nije koristilo neko od ponuđenih pravila, već ga korisnik sam definira (slika a). Pravilo se odnosi na sve programe (slika b), te na ICMP protokol tipa „Time Exceeded“ (slika c). Rang IP adresa je neodređen, pa se pravilo primjenjuje na sve lokalne i udaljene adrese (slika d). Akcija koja se poduzima kada na vatrozid dođe „Time Exceeded“ poruka blokira taj promet (slika e).

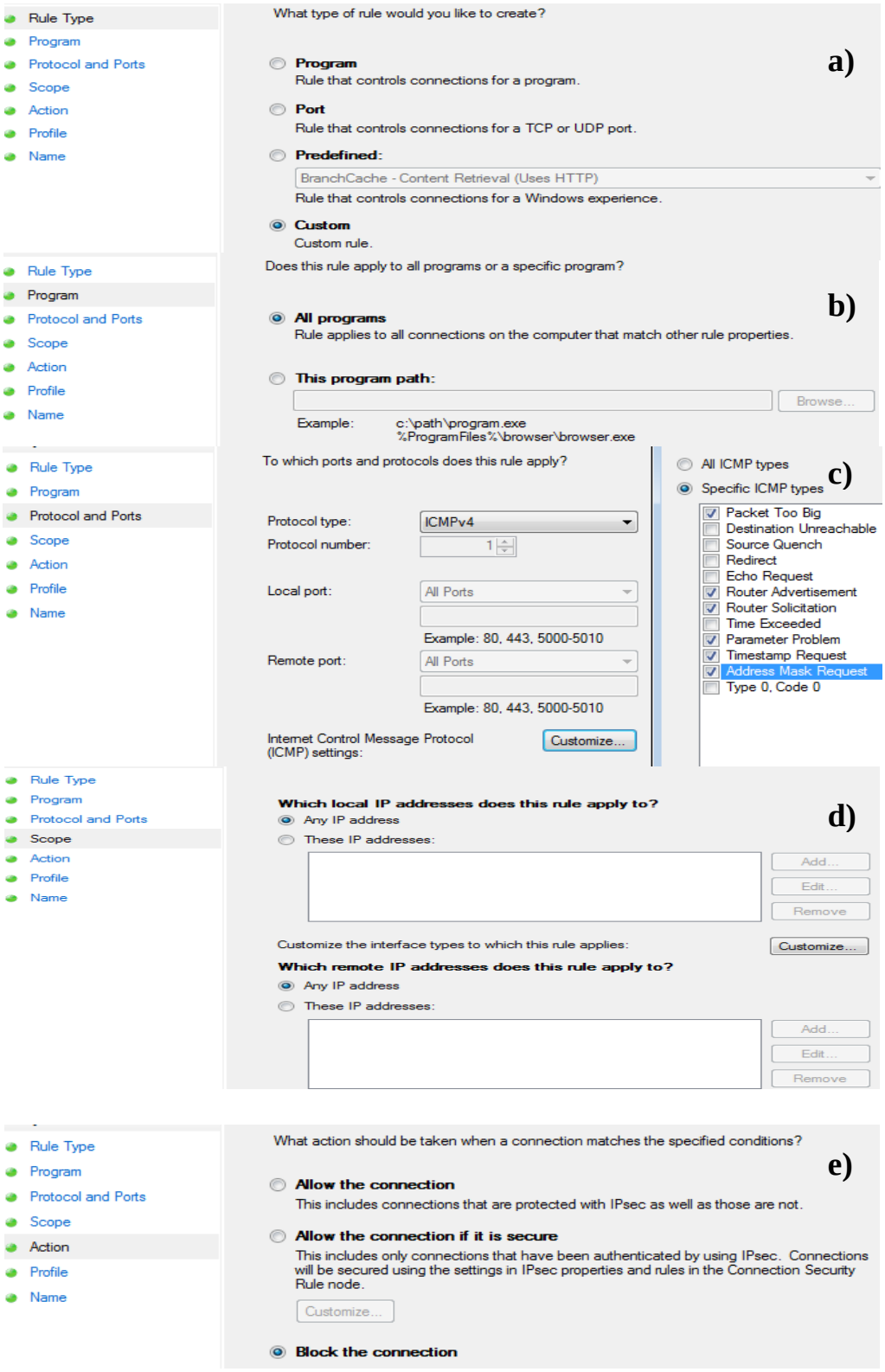


Slika 31. Dolazne „Time Exceeded“ poruke: a) Prikaz odabira tipa pravila b) Prikaz programa na kojeg se odnosi pravilo, c) Prikaz ICMP tipa na kojeg se odnosi pravilo, d) Prikaz IP adresa na koje se primjenjuje akcija, e) Prikaz akcije koja se primjenjuje u pravilu

7.1.6. Ostale ICMP poruke

Preostali tipovi ICMP poruka mogu se blokirati, budući da odaju određene informacije o sistemu kojega se nastoji zaštititi, a nemaju negativnog utjecaja na mrežu ako su blokirane.

Slika 32 prikazuje kako je definirano pravilo za ostale dolazne poruke ICMP protokola. Budući da se postavke u ovom pravilu odnose na dolazni promet, definiraju se u kartici „Inbound Rules“ glavnog prozora vatrozida. Za tip pravila proizvoljno je definiran „Custom“ (slika a). Pravilo se odnosi na sve programe (slika b), te na sve ICMP tipove za koje do sada nema definiranih postavki (slika c). Rang IP adresa je neodređen, pa se pravilo primjenjuje na sve lokalne i udaljene adrese (slika d). Akcijom koja se poduzima kada na vatrozid dođe neka od ostalih ICMP poruka blokira se promet (slika e).

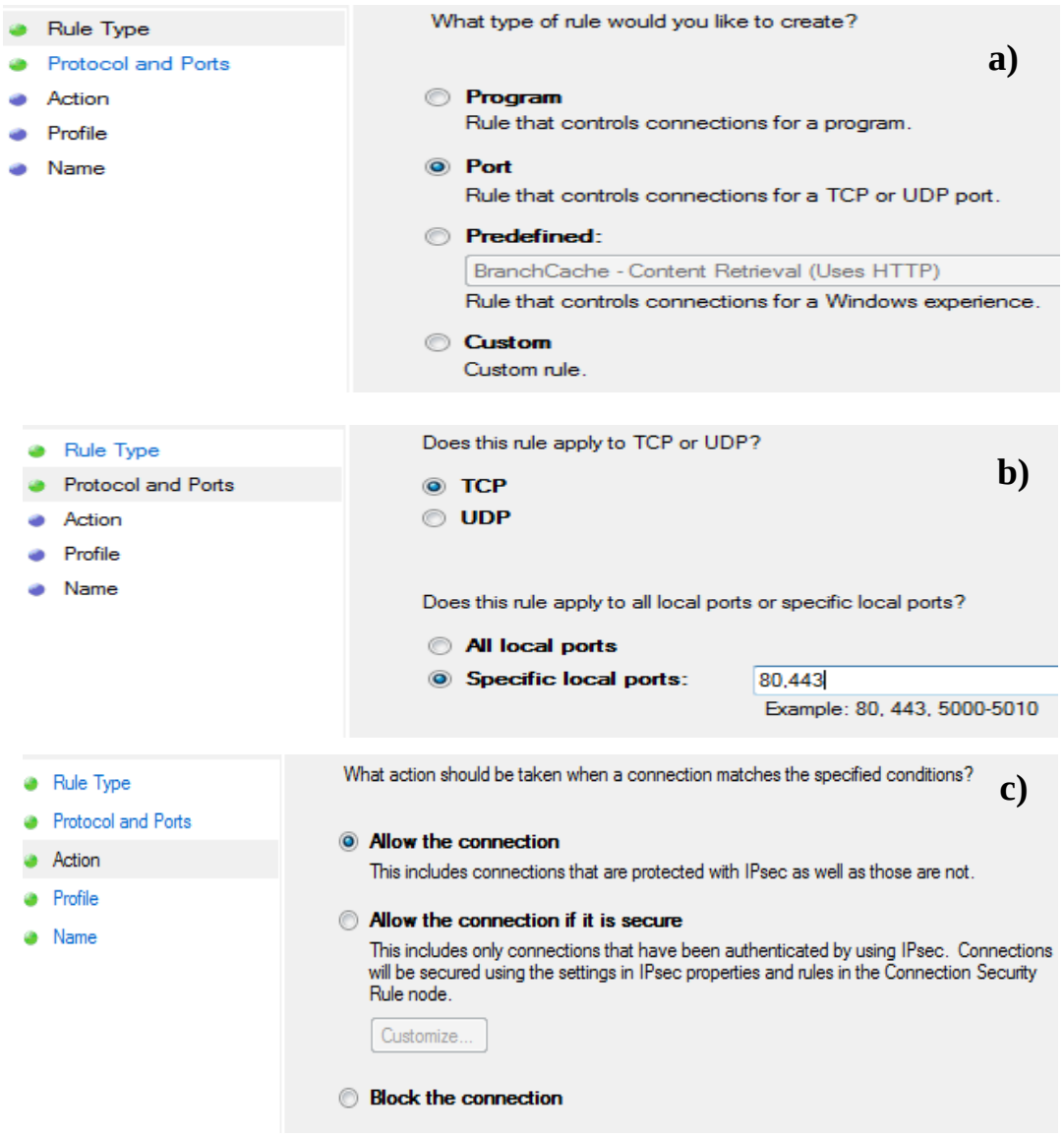


Slika 32. Ostale ICMP poruke: a) Prikaz odabira tipa pravila b) Prikaz programa na kojeg se odnosi pravilo, c) Prikaz ICMP tipa na kojeg se odnosi pravilo, d) Prikaz IP adresa na koje se primjenjuje akcija, e) Prikaz akcije koja se primjenjuje u pravilu

7.2. TCP protokol

Izlazne postavke:

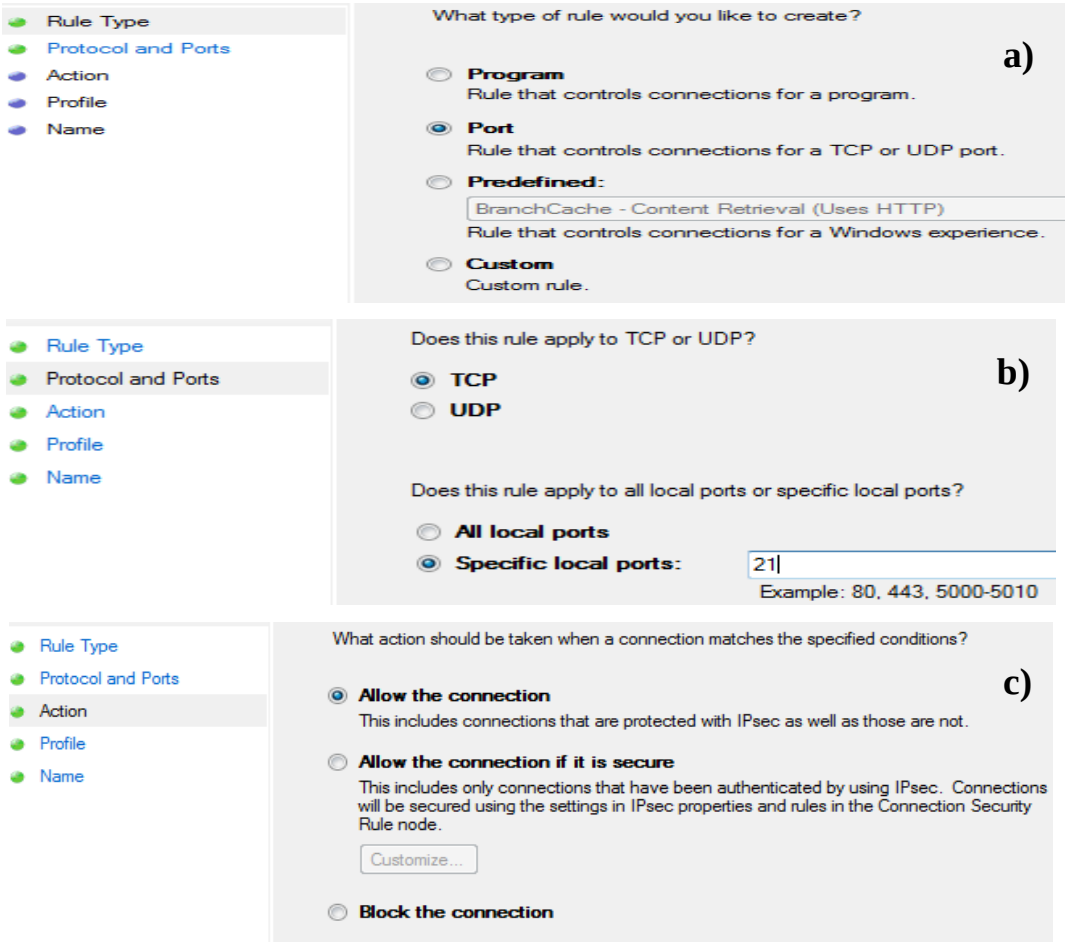
Portovi 80 i 443 se koriste za izlazak na Internet. Port 80 je glavni port za pristup web serveru, dok je port 443 vezan za https web stranice. Vatrozid propušta oba porta kako bi računalo sustava ECDIS imalo pristup http i https web stranicama na Internetu.



Slika 33. Prikaz postavki za TCP portove 80 i 443: a) Prikaz odabira tipa pravila b) Prikaz protokola i portova na koje se pravilo odnosi, c) Akcija koju pravilo primjenjuje

Slika 33 prikazuje postavke za TCP portove 80 i 443 kod odlaznog prometa. Budući da se ovo pravilo definira za izlazne postavke, namješta se u kartici „Outbound Rules“ glavnog prozora vatrozida. Za razliku od do sada prezentiranih, ovaj tip pravila odnosi se na TCP ili UDP port/ove (slika a). Slijedećim korakom definirano je da se pravilo odnosi na TCP protokol i na portove 80 i 443 (slika b). Odlazni TCP promet koji koristi portove 443 i 80 je dopušten (slika c).

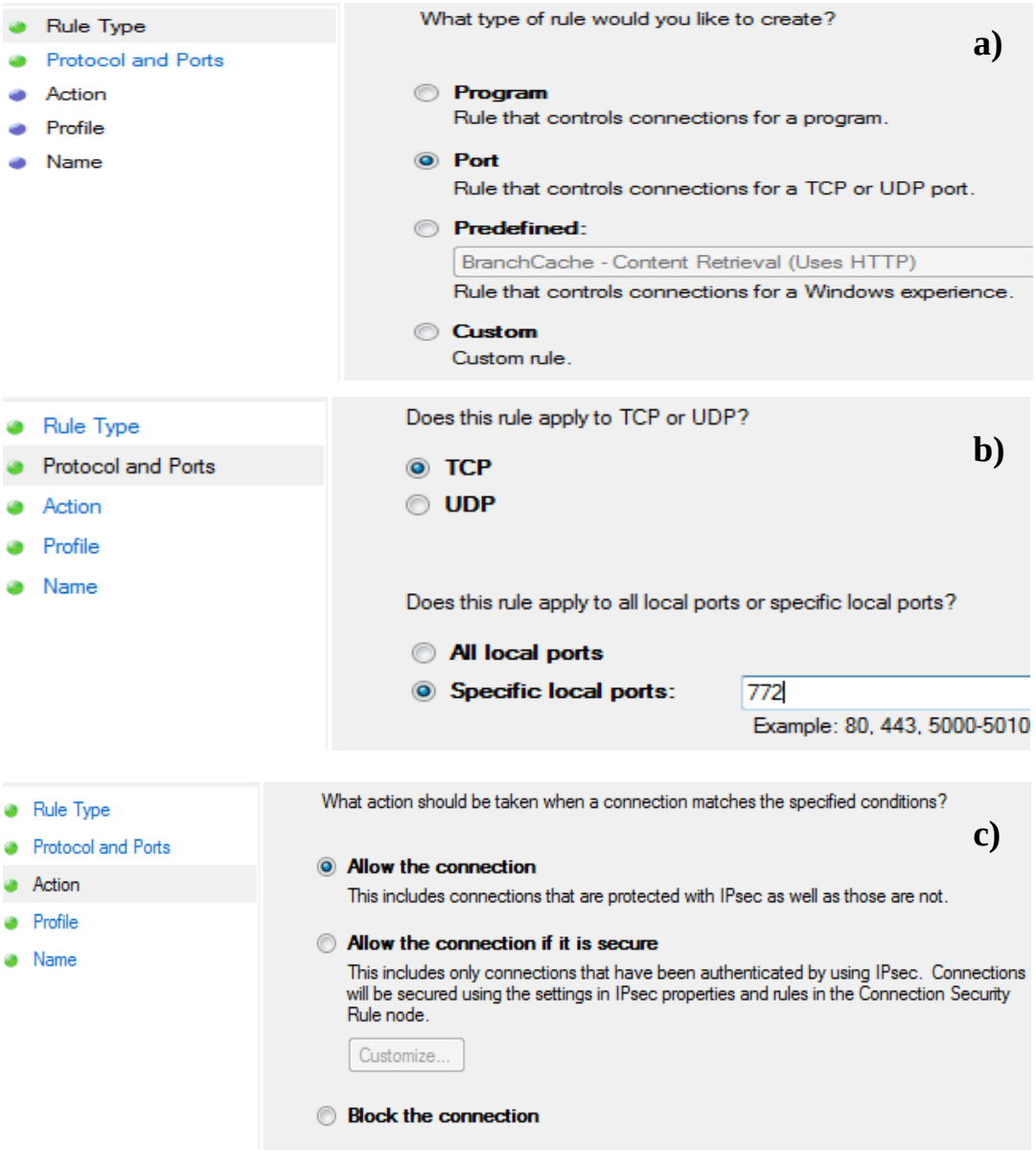
Slika 34 prikazuje konfiguraciju odlaznog pravila za TCP port 21 koji je glavni port kod FTP veze. Kada je port 21 otvoren, računalu sustava ECDIS omogućena je veza prema serveru FTP.



Slika 34. Prikaz pravila za TCP port 21: a) Prikaz odabira tipa pravila b) Prikaz protokola i portova na koje se pravilo odnosi, c) Akcija koju pravilo primjenjuje

Pravilo sa slike 34 definira postavke za izlazni promet u kartici „Outbound Rules“ glavnog prozora vatrozida (slika 22). Tip pravila odnosi se na neki od portova TCP ili UDP protokola (slika a). Drugim korakom, definira se da pravilo vrijedi za TCP protokol i port 21 (slika b). Akcijom koja se primjenjuje na TCP protokol i port 21 propušta se odlazni promet (slika c).

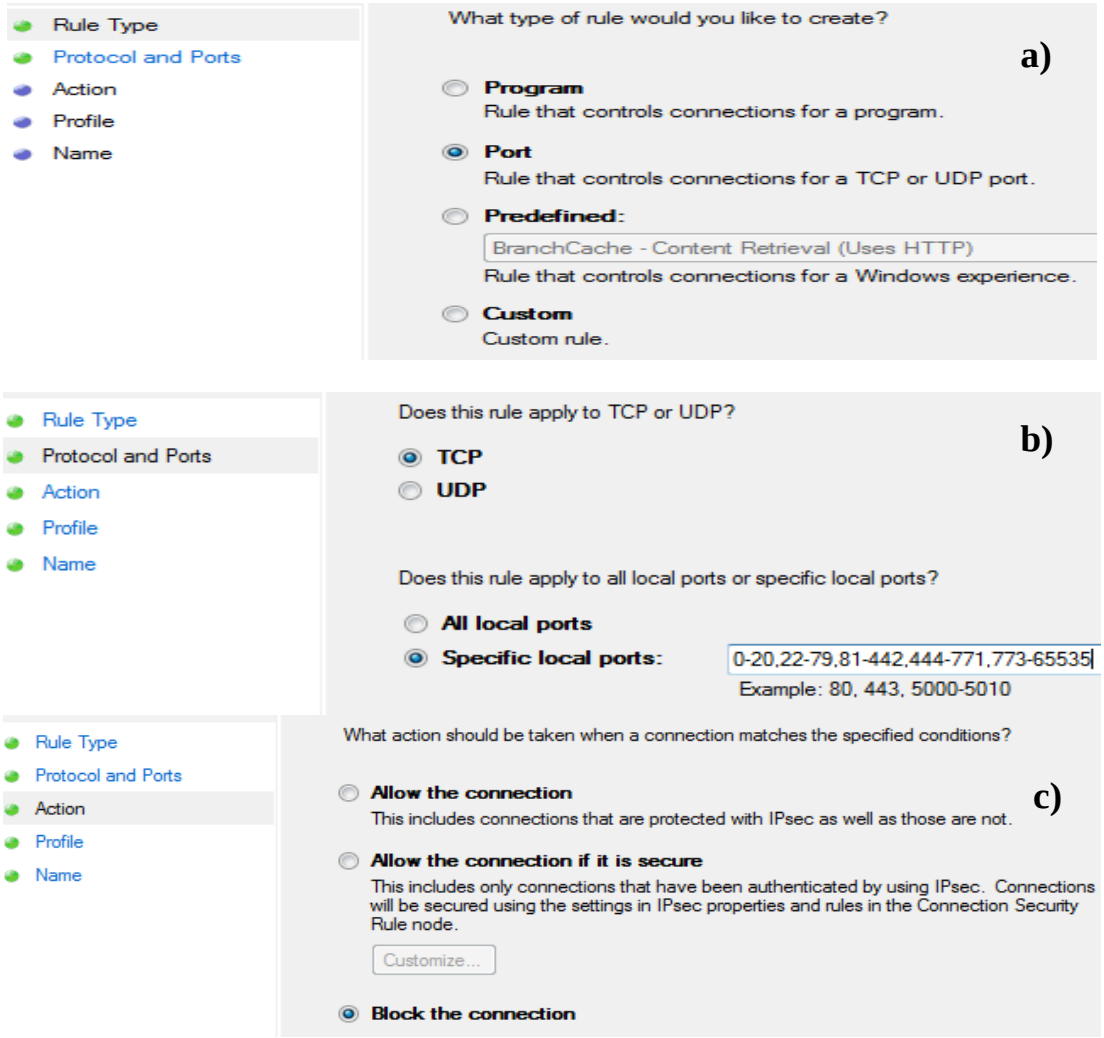
Slika 35 prikazuje konfiguraciju pravila za port 772 preko kojega se izvršava ICMP poruka tipa 3 koda 4 (odlazni promet).



Slika 35. Prikaz pravila za TCP port 772: a) Prikaz odabira tipa pravila b) Prikaz protokola i portova na koje se pravilo odnosi, c) Akcija koju pravilo primjenjuje

Pravilo se odnosi na izlazni promet, stoga se definira u kartici „Outbound Rules“ glavnog prozora vatrozida. Tip pravila prikazuje da se radi o pravilu vezanom za TCP ili UDP protokol (slika a). Konkretno, odnosi se na TCP protokol i port 772 (slika b). Kroz port 772 propušta se izlazni promet kada se ispune kriteriji vezani za ovo pravilo (slika c).

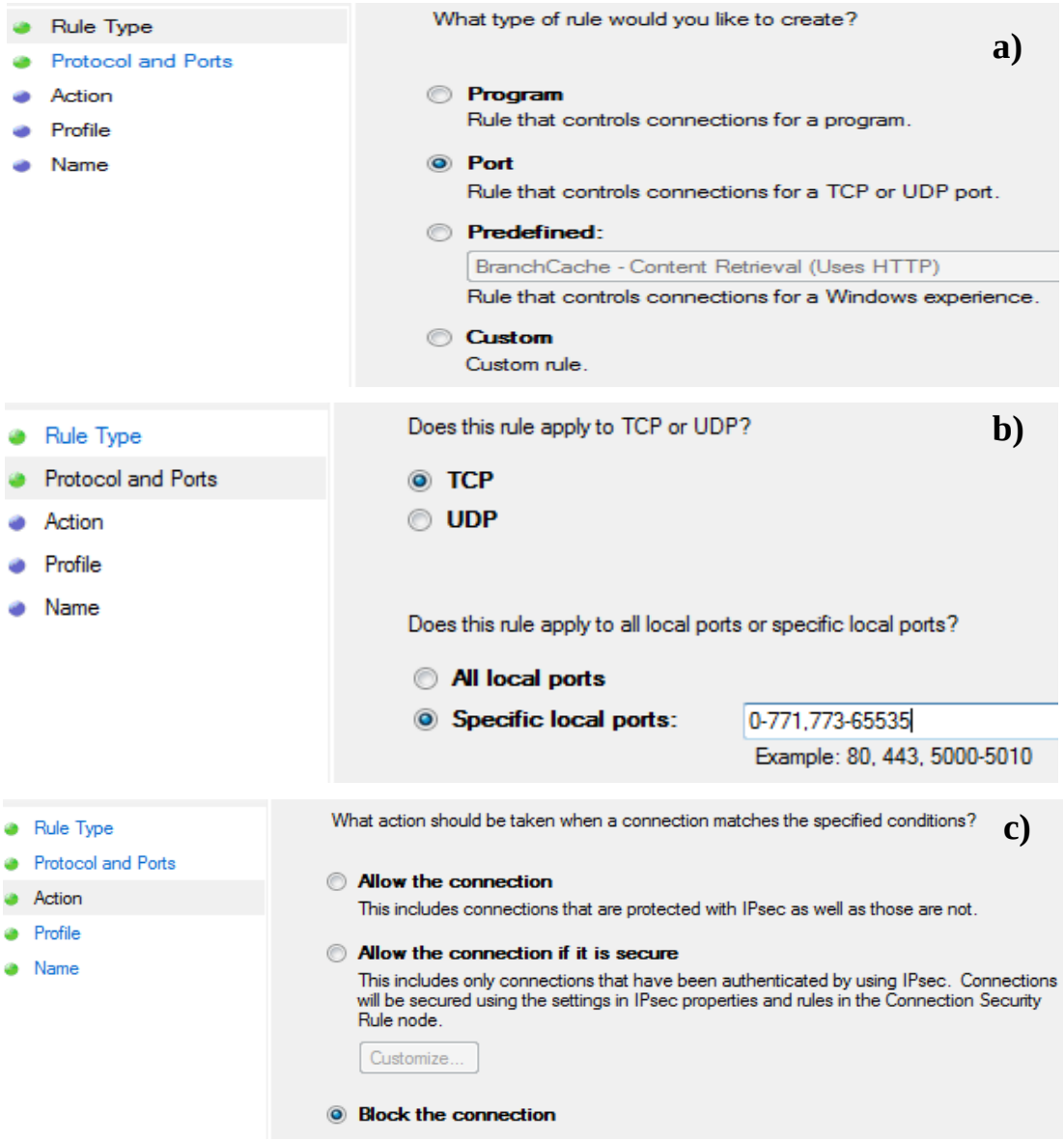
Slika 36 prikazuje konfiguraciju pravila za preostale portove. Tip pravila prikazuje da se radio o pravilu vezanom za TCP ili UDP protokol (slika a). Odnosi se na TCP protokol i sve preostale portove za koje do sada nema definiranih pravila (slika b). Vatrozid blokira te portove (slika c).



Slika 36. Prikaz pravila za ostale portove: a) Prikaz odabira tipa pravila b) Prikaz protokola i portova na koje se pravilo odnosi, c) Akcija koju pravilo primjenjuje

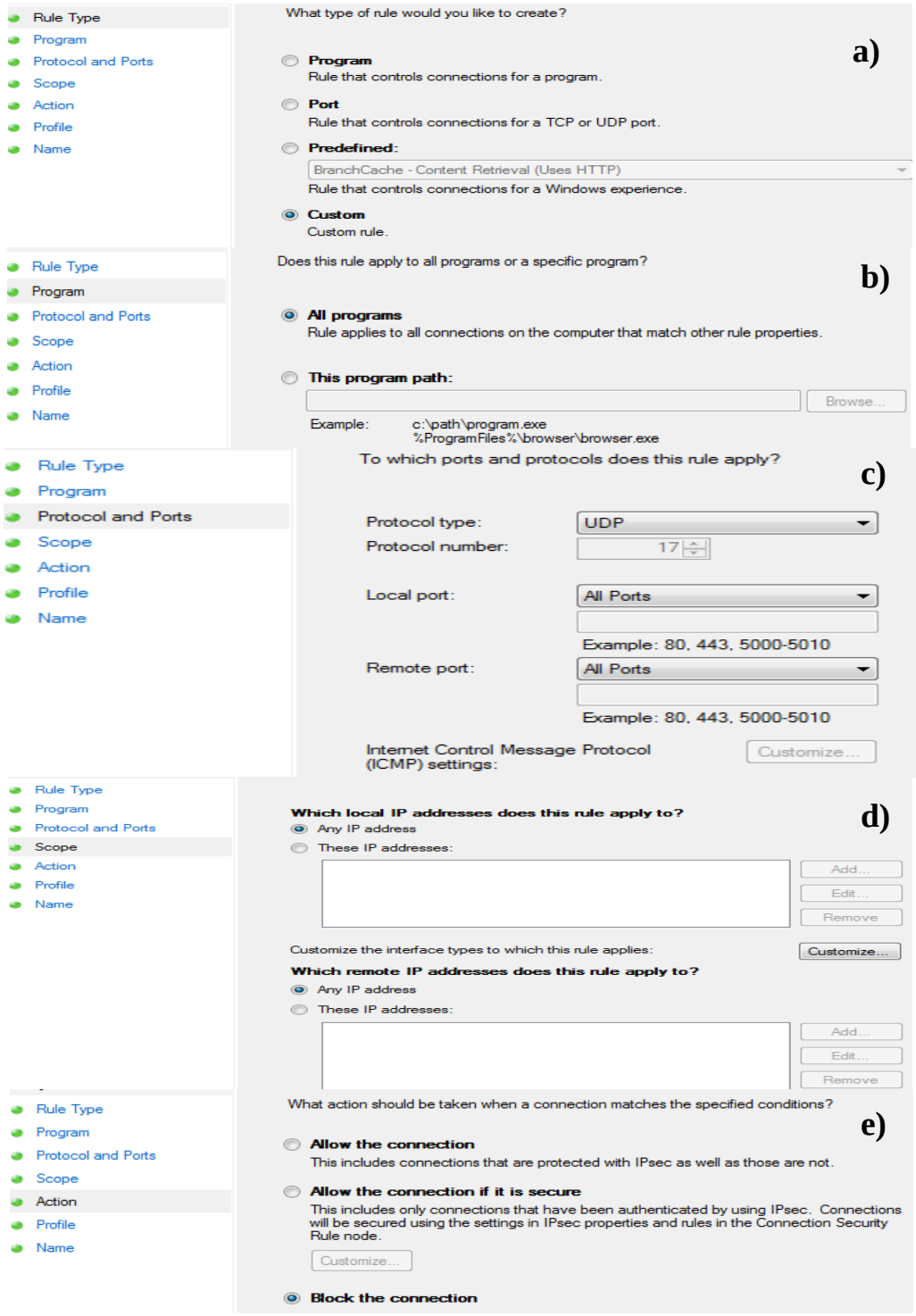
Dolazni promet:

Slika 37 prikazuje konfiguraciju pravila vatrozida za ostale portove prilikom dolaznog prometa, gdje su svi portovi osim 772 blokirani. Pravilo se definira u kartici „Inbound Rules“ glavnog prozora vatrozida. Tip pravila odnosi se na port (slika a). Pravilo se odnosi na TCP protokol i portove 0-771, 773-65535 (slika b). Pri dolaznom prometu, moguće je ostvariti konekciju jedino preko porta 772 budući da su svi ostali portovi blokirani (slika c).



Slika 37. Prikaz pravila za ostale portove: a) Prikaz odabira tipa pravila b) Prikaz protokola i portova na koje se pravilo odnosi, c) Akcija koju pravilo primjenjuje

7.3. UDP protokol

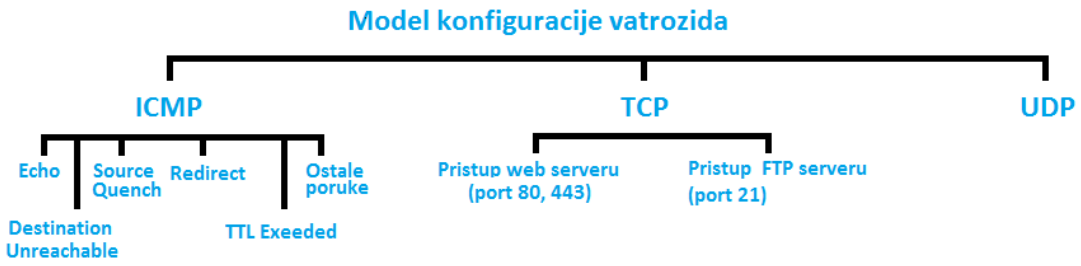


Slika 38. Prikaz pravila za UDP protokol: a) Prikaz odabira tipa pravila b) Prikaz programa na kojeg se odnosi pravilo, c) Prikaz ICMP tipa na kojeg se odnosi pravilo, d) Prikaz IP adresa na koje se primjenjuje akcija, e) Prikaz akcije koja se primjenjuje u pravilu

Slika 38 prikazuje kako je definirano pravilo za UDP protokol. Tip pravila je „Custom“ što znači da je proizvoljno definirano (slika a). Odnosi se na sve programe (slika b), te na UDP protokol na svim portovima (slika c). Rang IP adresa je neodređen, što znači da se pravilo primjenjuje na sve lokalne i vanjske adrese (slika d). Sav promet koji koristi UDP protokol, bez obzira na port, blokiran je (slika e).

7.4. Model konfiguracije vatrozida za ECDIS

Model konfiguracije vatrozida predstavljen u sedmom poglavlju temelji se na ICMP, TCP i UDP protokolima. U razmatranje su uzeta ova tri protokola, budući da vatrozid sa paketnim filtriranjem radi na trećem i četvrtom sloju OSI referentnog modela. Postavke su izrađene prema pretpostavljenoj mrežnoj konfiguraciji (slika 23).



Slika 39. Model vatrozida temeljen na ICMP, TCP, UDP protokolima

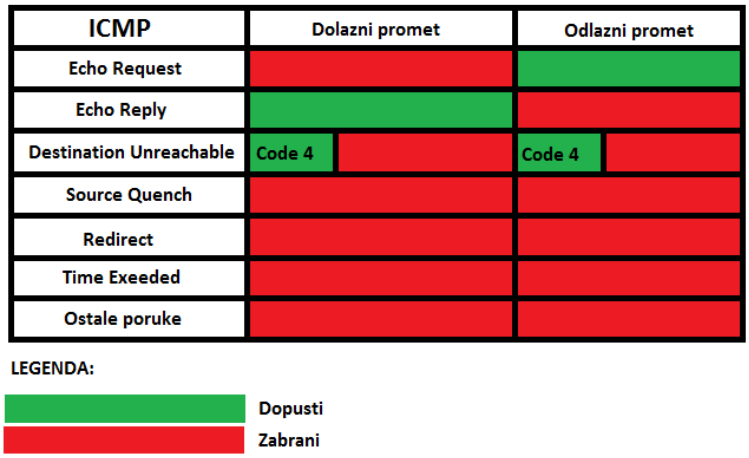
Model konfiguracije postavki vatrozida prikazan je na slici 39. TCP i UDP protokoli se nalaze na četvrtom, prijenosnom sloju OSI referentnog modela, dok je ICMP sastavni dio mrežnog OSI referentnog modela. Protokol TCP sudjeluje u stvaranju veze za prijenos podataka, a ICMP služi za izvješćivanje o greškama pri prijenosu.

7.5. Zaključak poglavlja:

U ovom poglavlju je prezentiran model konfiguracije vatrozida s obzirom na ICMP, TCP i UDP protokole. Postavke su izrađene prema pretpostavljenoj mrežnoj

konfiguraciji spajanja. Analizirajući ICMP protokol razmatrano je jedanaest vrsta poruka, s obzirom na dolazni i odlazni promet.

Slika 40 prikazuje postavke vatrozida s obzirom na ICMP protokol. Završna konfiguracija vatrozida dopušta „Echo“ upit samo za odlazni promet, dok dolazne upite zabranjuje. Nadalje, dolazne „Echo“ odgovore propušta budući da su inicirani od strane računala ECDIS, a odlazne odgovore na upit zabranjuje. Pri ovakvoj konfiguraciji postoji mogućnost da se na računalo ECDIS izvede napad DOS, međutim puno je veća opasnost od takve vrste napada na računala koja se koriste kao poslužitelji.

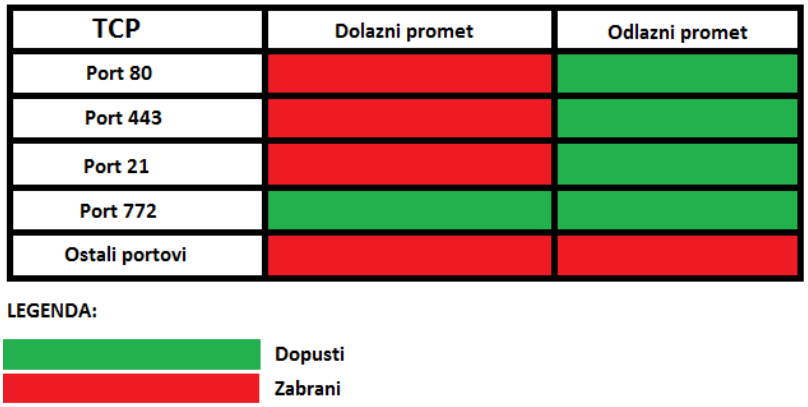


Slika 40. Tablica modela vatrozida s obzirom na ICMP protokol

Sve poruke tipa 3 (Destionation Unreachable) su blokirane, osim onih sa kodom 4 koje imaju nezamjenjivu ulogu u povećanju efikasnosti transfera podataka prilikom smanjenja kapaciteta nekog od posrednih usmjernika. ICMP poruke tipa „Source Quench“ blokirane su budući da su podložne slijepim napadima na propusnost. Obavijesti tipa 5 (Redirect) su također blokirane, jer se mogu zlorabiti, a „Time Exeeded“ poruke nisu potrebne u slučaju veze između sustava ECDIS i poslužitelja budući da je ECDIS u takvoj vezi odredišno računalo. Ostali tipovi ICMP poruka su blokirani budući da mogu potencijalnim napadačima otkriti neke informacije o štićenoj unutarnjoj mreži.

Slika 41 prikazuje postavke za TCP protokol. Pretpostavljena konfiguracija spajanja sustava ECDIS na vanjske web lokacije zahtjeva mogućnost povezivanja sa web serverima i serverom FTP. Prema tome, s obzirom na protokol TCP propuštaju se

portovi 80 i 443 za web servere, i port 21 za pristup serveru FTP (odlazni promet). Također, budući da su ICMP poruke tipa 3 koda 4 dopuštene, port 772 mora biti otvoren (odlazni promet). Ostali portovi se ne koriste i trebaju biti zatvoreni. Dolazni TCP promet je blokiran, osim na portu 772 koji se koristi za ICMP poruke tipa „Destination Unreachable“.



Slika 41. Tablica modela vatrozida s obzirom na TCP protokol

Slika 42 prikazuje tablicu modela vatrozida s obzirom na UDP protokol. UDP protokol nema sigurnosnog mehanizma za prijenos podataka, te zbog toga daje veću brzinu prijenosa od TCP protokola. Zato se najčešće koristi za „streaming“ ili primjerice za „video“ pozive. Nije povoljan za korištenje u primjenama gdje je nužno osigurati siguran prijenos podataka kao što je u slučaju osvježavanja sustava ECDIS kartama. Protokol UDP je podložan primjerice „flood“ napadima na raspoloživost, kod kojih se računalu kojeg se želi onesposobit šalje veliki broj UDP datagrama u IP paketu na otvorene portove. Na taj način se smanjuje raspoloživost napadnutog računala. Iz razloga što je podložan napadima, a nije povoljan za korištenje kod sustava ECDIS protokol UDP je u konfiguraciji vatrozida blokiran.

Slika 42. Tablica modela vatrozida s obzirom na UDP protokol

8. Zaključak ovog rada

U radu je prezentirana konfiguracija postavki vatrozida s obzirom na ICMP, TCP i UDP protokole, iz razloga što Windows vatrozid može uspješno upravljati specifičnim sigurnosnim rizicima sustava ECDIS. Radi na mrežnom i transportnom sloju OSI referentnog modela. Također, prezentirane su i postavke za FTP, koji je protokol aplikacijskog (korisničkog) nivoa. Kada se želi ostvariti transfer podataka preko FTP klijent – server sistema, pokreće se najčešće zahtjev za TCP vezom na portu 21. Kako bi sustav ECDIS mogao pristupiti serveru FTP, mora imati otvoren port 21 za izlazni promet. Isto tako, da bi ECDIS imao pristup web servisima mora imati otvorene portove 80 i 443 za odlazni promet.

Windows vatrozid, budući je sastavni dio operativnog sustava i stoga besplatan, jednostavan je za korištenje (engl. user friendly). Vrlo je popularan, pa pored službenih Microsoftovih web stranica ima i puno drugih web lokacija na kojima se mogu pronaći upute za korištenje. Pokazalo se da Windows vatrozid može biti prihvatljivo rješenje za obranu sustava ECDIS u slučaju da ima više računala u lokalnoj brodskoj mreži, ali u smislu zaštite od ostalih računala u mreži. U radu je prikazano da se koristi za zaštitu računala na kojem se nalazi, te ne može zaštititi ostala računala u lokalnoj brodskoj mreži. U slučaju kada je potrebno jednim vatrozidom štititi cijelu brodsku mrežu koriste se hardverski vatrozidi kao što su Transocean-ov TFAP ili Stratos-ov Trench. Radom se pokazalo da korištenje Windows vatrozida, uz pretpostavku da je računalo sustava ECDIS jedino u unutarnjoj brodskoj mreži, može biti prihvatljivo rješenje u slučajevima kada je potrebno brzo i jeftino „low-cost“ rješenje. Međutim, bolju zaštitu pružaju hardverski vatrozidi budući da imaju neke dodatne mogućnosti koje Microsoft ne omogućuje. Primjerice, Windows vatrozid nema mogućnost translatiranja mrežnih adresa, što je izuzetno korisno ako se želi sakriti unutarnja konfiguracija brodske mreže. Treba napomenuti da je sakrivanje unutarnje konfiguracije brodske mreže pogodno i u slučaju kada je računalo sustava ECDIS jedino u unutarnjoj mreži. Bolji hardverski vatrozidi daju mogućnost definiranja pristupnih kontrolnih listi.

Sam vatrozid je tek jedan element u ukupnom sigurnosnom aspektu informacijskog sustava. Primjerice, i najbolje postavljeni vatrozid ne može zaštiti od e-pošte koja u

svom privitku ima zlonamjerni kod. Pored dobro konfiguriranog vatrozida, potrebno je imati i druge zaštitne mehanizme poput enkripcije podataka, filtriranja web prometa, IDS programa (engl. intrusion detection system) i slično. Antivirusna zaštita je danas također nužna i nezaobilazna. Prema tome, dobra konfiguracija vatrozid postavki, uz ostale alate za minimiziranje sigurnosnih rizika, može uvelike doprinijeti očuvanju stabilnosti i sigurnosti informacijskog sustava.

Ovim radom je predstavljeno besplatno, jednostavno i efikasno rješenje za vatrozid, te su ponuđene smjernice prema kojima bi softverski vatrozid mogao biti konfiguriran s obzirom na sigurnosne rizike koji su specifični za sustav ECDIS.

Literatura

[1] Microsoft, „*Što je vatrozid*“, Web stranica: http://windows.microsoft.com/hr-hr/windows/what-is-firewall#1TC=windows-7 (Pristupljeno: svibanj 2014).

[2] International Hydrographic Organization 1996, „*Guidance on updating the electronic navigational chart*“ 3rd Edition, Monaco.

[3] International Hydrographic Bureau 2004, „*Specifications for Chart Content and Dipslay Aspects of ECDIS*“, 6th Edition, Monaco.

[4] Maritime Safety Service 2013, „SafetyNET Users Handbook“, 5th Edition, London.

[5] Inmarsat, „*FleetBroadband 250*“, Web stranica: http://www.INMARSAT.com/service/fleetbroadband-250/ (Pristupljeno: 25. svibanj 2014)

[6] Carroll B. J. 2007, „*CCSP SND Quick Reference*“, Cisco Press.

[7] Transas Marine 2011, „*Navi Sailor 4000 Pilot*“, Transas Marine Limited.

[8] International Hydrographic Office „ *Impact Analysis of S-63 (Encryption) and S-58 (Validation) on ECDIS*“, Web stranica: http://www.iho.int/mtg_docs/com_wg/TSMAD/TSMAD20/TSMAD20_DIPWG2-24.2A_S-58_Impact_Analysis_on_ECDIS.pdf (Pristupljeno: svibanj 2014)

[9] Maral G., Bousquet M. 2009, „*Satellite communications systems*“, Fifth edition, Wiely publication.

[10] Inmarsat 2009, „*Fleet Broadband Best Practice Manual*“, Version 1.0.

[11] Sun Z. 2005, „*Satellite networking – Principles and protocols*“, University of Surrey, UK, Wiely Publication.

[12] Ožegović J. 1990, „*Računalne mreže radni materijal*“, Split.

[13] Postel J. 1981, „*Internet Control Message protocol, Darpa Internet Program Protocol Specification*“.

Popis slika

Izvori slika

[1.1] Kongsberg Maritime, „*ECDIS Electronic Chart Display and Information System*“ http://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/39DAD27FC6D37518C1256E150038656C?OpenDocument (Pristupljeno: srpanj, 2014.)

[2.1] Pomorski Fakultet u Rijeci, autorizirana predavanja dr.sc. Boris Sviličić

[3.1] International Hydrographic Organization 1996, „*Guidance on updating the electronic navigational chart*“, 3rd Edition, Monaco.

[4.1] Spinaker d.o.o., „*Inmarsat C Communication*“ http://www.egmdss.com/gmdss-courses/mod/resource/view.php?id=2288 (Pristupljeno: srpanj, 2014.)

[14.1] Pomorski Fakultet u Rijeci, Sigurnost informacijskih sustava, autorizirana predavanja prof.dr.sc. Boris Sviličić

[16.1] Pomorski Fakultet u Rijeci, Sigurnost informacijskih sustava, autorizirana predavanja prof.dr.sc. Boris Sviličić

[18.1] Pomorski Fakultet u Rijeci, Sigurnost informacijskih sustava, autorizirana predavanja prof.dr.sc. Boris Sviličić

[19.1] Pomorski Fakultet u Rijeci, Sigurnost informacijskih sustava, autorizirana predavanja prof.dr.sc. Boris Sviličić