Mr. sc. Boris Sviličić
Dr. sc. Antun Kraš
Pomorski fakultet u Rijeci
Rijeka, Studentska 2

Pregledni članak
UDK: 004.451.64
004.738
Primljeno: 07. lipnja 2005.
Prihvaćeno: 19. srpnja 2005.

ZAŠTITA PRIVATNOSTI RAČUNALNOG SUSTAVA

Sigurnost je najkritičnije područje računalne tehnologije te počinje zauzimati izuzetno važnu poziciju u današnjem okružju računalnih sustava. Ovim radom predstavljen je princip rada vatrozida, uređaja koji omogućuje razne metode kontrole i upravljanja prometom podataka između dviju računalnih mreža, s ciljem zaštite sigurnosti privatnog dijela mreže od sigurnosnih rizika javnog dijela mreže. Predstavljene su i razrađene osnovne funkcije vatrozida: paketno filtriranje, maskiranje mrežnih adresa, posredne usluge i virtualna privatna mreža. Objašnjene su uloge pojedinih osnovnih funkcija vatrozida te su razmotrene prednosti i nedostaci njihova korištenja. Ovim radom su ponuđene smjernice za rješavanje problema zaštite privatnosti računalnih sustava.

Ključne riječi: vatrozid, paketno filtriranje, maskiranje mrežnih adresa, posredne usluge, virtualna privatna mreža

1. UVOD

Sve većim oslanjanjem društva na računalne sustave, raste svijest o njihovoj važnosti. Sigurnost računalnog sustava je jedan od najvažnijih vidova poslovanja organizacija koje svoje poslovanje zasnivaju na računalnim sustavima. Sveprisutnost Interneta u većini tvrtki, ali i domova građana, stvorila je potrebu za zaštitom od neovlaštenih udaljenih zlonamjernih korisnika.

S ciljem očuvanja sigurnosti unutar privatne računalne mreže, ponekad se ne želi dopustiti pristup računalima s dijela mreže koji ne možemo direktno kontrolirati. Konkretno, to znači želimo dopustiti pristup korisnicima privatne mreže na Internet, ali ne i pristup s Interneta na privatnu mrežu. U takvim se slučajevima koriste razne hardverske i softverske metode kontrole pristupa, koje se jednim imenom nazivaju vatrozid (eng. *firewall).*

1. VATROZID

U svijetu računala, vatrozid je uređaj kojim štitimo privatni dio mreže od javnog dijela. Primarna mu je funkcija omogućivanje kontroliranog pristupa iz privatnog, unutrašnjeg dijela mreže na javni, vanjski dio mreže (npr. Internet) i obratno. Na vatrozid se može gledati kao na skup veoma različitih mehanizama koji se mogu podijeliti na dva osnovna principa; jedan koji služi sprječavanju prometa paketa u mreži i drugi koji služi omogućavanju prometa u mreži. Napredni vatrozidi osiguravaju spajanje unutrašnje i vanjske mreže na svim programskim slojevima, od podatkovnog sve do aplikacijskog.

Vatrozidi se postavljaju na granici mreže te omogućuju pristup drugim mrežama. Ovaj koncept je bitan jer bez njega bi svako računalo na mreži trebalo obavljati iste funkcije kao i vatrozidi, trošeći na taj način vlastite resurse. Korištenjem vatrozida omogućena je centralizacija svih sigurnosnih servisa na jednom uređaju optimiziranom za izvršavanje tih zadataka.

Vatrozidi stvaraju "uska grla" (eng. bottlenecks) između unutarnjih i vanjskih mreža jer cijeli promet među mrežama prolazi kroz jednu kontrolnu točku. Pored toga, ovo je mala cijena za postizanje sigurnosti. Također, dok je brzina vanjske veze relativno mala u odnosu na brzinu današnjih računala, kašnjenje prouzročeno vatrozidom može biti zanemareno.

Osnovne funkcije vatrozida koriste četiri osnovne metode:

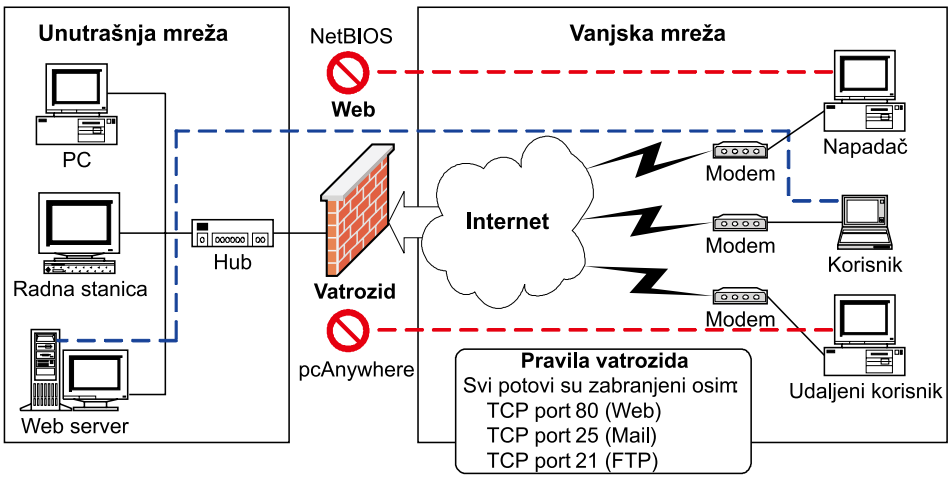
- Paketno filtriranje (eng. *packet filtering)*
  Paketnim filtriranjem odbacuju se neželjeni mrežni paketi s obzirom na izvorišnu adresu računala, odredišnu adresu ili vrstu podataka koji se prenose mrežom.
- Maskiranje mrežnih adresa (eng. *network address translation, NAT)*
  Maskiranje mrežnih adresa vrši se pretvorbom mrežnih adresa unutrašnje, privatne mreže s ciljem zaštite tajnosti mrežne konfiguracije.
- Posredna usluga (eng. *proxy service)*
  Posredna usluga je specijalizirana aplikacija ili serverski program koji služi kao posrednik pri ostvarivanju veze između klijentskog i serverskog računala, radi skrivanja identiteta korisnika unutrašnje, privatne mreže.
- Virtualne privatne mreže (eng. *virtual private network, VPN)*
  Virtualne privatne mreže su način implementacije kriptografske zaštite podataka s ciljem korištenja javne mreže kao da je privatna.

Naravno, moguće je korištenje uređaja ili servera koji pružaju samo jednu od navedenih funkcija, primjerice, postavljanjem usmjerivača (eng. router) koji pruža filtriranje paketa te proxy servera na drugom uređaju. Ovakva situacija je manje sigurna od slučaja kad se koristi jedan vatrozid koji pruža obje funkcije, jer usmjerivač mora propustiti promet do proxy servera ili se proxy server mora smjestiti izvan mreže bez zaštite paketnog filtriranja. Oba slučaja su manje sigurna od korištenja jednog vatrozida koji pruža sve sigurnosne funkcije.

PAKETNO FILTRIRANJE

Prvi vatrozidi su bili samo paketni filteri. Oni uspoređuju pakete mrežnih (npr. IP protokol) i transportnih protokola (npr. TCP protokol) s pravilima zapisanih bazom pravila te prosljeđuju samo one pakete koji se poklapaju s kriterijima specificiranim u bazi pravila. Dakle, paketni filteri su uređaji koji odbacuju neželjene pakete s obzirom na izvorišnu adresu, odredišnu adresu ili vrstu podataka specificiranu brojem TCP porta. Filteri mogu biti implementirani unutar usmjerivača ili u TCP/IP *stackovima* servera.

Sljedećom slikom prikazan je princip rada paketnog filtriranja. Prema pravilima definiranim na vatrozidu, dozvoljen je prolaz samo TCP paketima na portovima 80 (web), 25 (email) i 21 (FTP), dok je promet na svim ostalim portovima zabranjen. Na primjer, udaljenom korisniku nije dozvoljen pristup unutrašnjoj mreži korištenjem NetBIOS protokola.



Slika 1. Paketno filtriranje

Prednosti korištenja paketnog filtriranja su sljedeće:

- Jedan uređaj štiti cijelu mrežu
  Jedna od najvažnijih značajki paketnog filtriranja je u tome što jedan strateški dobro konfiguriran usmjerivač za filtriranje paketa štiti cijelu mrežu. Ukoliko se lokalna mreža spaja na Internet preko samo jednog usmjerivača, postavljajući na njemu sustav paketnog filtriranja, znatno se povećava sigurnost mreže.
- Velika efikasnost
  Jednostavno filtriranje paketa je vrlo efikasno. Budući da filtriranje paketa zahtjeva pregledavanje samo nekoliko zaglavlja paketa, cijeli proces se odvija s vrlo malim zakašnjenjem.
- Široka dostupnost
  Produkti za implementaciju paketnog filtriranja su široko dostupni u mnogobrojnim hardverskim i softverskim proizvodima, komercijalnim ili besplatnim. Mnogi komercijalni routerski produkti standardno uključuju mogućnost paketnog filtriranja.

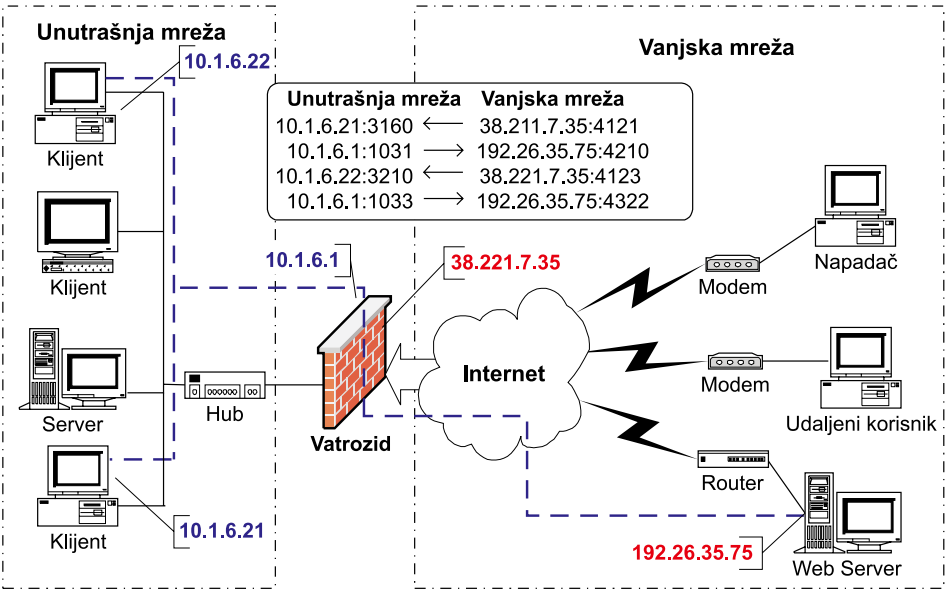
Nedostaci korištenja paketnog filtriranja su sljedeći:

- Alati za filtriranje nisu savršeni
  Pored toga što su alati za paketno filtriranje široko rasprostranjeni i dostupni u različitim hardverskim i softverskim proizvodima, paketno filtriranje još uvijek nije savršeno. Postoje ograničenja pri razvoju i implementaciji alata za filtriranje, kao što su; zahtjevno konfiguriranje pravila za filtriranje, jednom konfigurirana pravila teško je testirati, propusti i neispravnosti alata za filtriranje itd.
- Nemogućnost implementacije neke od zabrana
  Neke od željenih pravila kontrole mrežnog prometa nije moguće implementirati. Na primjer, paketi koji se provjeravaju paketnim filtriranjem sadrže informacije kojem računalu su namijenjeni, ali ne i kojem korisniku. Dakle, zabrane na nivou korisnika nisu moguće. Slična je i situacija kada paketi nose informaciju na koji se port prenose, ali ne i koja je aplikacija u pitanju. Prema tome, zabrane na višem nivou protokola vrše se preko brojeva portova, nadajući se da se ništa drugo ne izvršava na tom portu.

MASKIRANJE MREŽNIH ADRESA

Maskiranje mrežnih adresa vrši se pretvorbom mrežnih adresa unutrašnje mreže s ciljem predstavljanja situacije u kojoj izgleda da sav mrežni promet proizlazi iz jedne točke. Na taj način omogućuje se korištenje jedne skupine mrežnih adresa interno i druge skupine za rad s vanjskim mrežama, tj. omogućeno je skrivanje identiteta klijenata unutrašnje mreže. Maskiranje mrežnih adresa ne pruža direktnu sigurnost sustavu, ali omogućuje očuvanje tajnosti konfiguracije unutrašnje mreže, što predstavlja značajnu sigurnosnu mjeru.

Princip rada maskiranja mrežnih adresa prikazan je na slici 2. Iz slike je vidljivo, kada se gleda sa strane vanjske mreže, kao da cijeli promet proizlazi iz jedne točke te da se sustav za maskiranje adresa koristi TCP portovima, kako bi sačuvao put spajanja vanjskog i unutrašnjeg računala.



Slika 2. Maskiranje mrežnih adresa

Razlog korištenja maskiranja mrežnih adresa je zaštita tajnosti mrežne konfiguracije, ali i sljedeće sigurnosne značajke:

- Prisila korištenja vatrozida
  Ukoliko su na pojedinim računalima postavljene mrežne adrese koje ne mogu biti korištene na vanjskoj mreži, nužno je korištenje sustava za pretvorbu mrežnih adresa. Ako računalo i pronađe put za spajanje na vanjsku mrežu zaobilazeći sustav za pretvorbu mrežnih adresa, veza neće raditi. Na taj način postiže se prisilno uspostavljanje veze kroz jednu kontrolnu točku, vatrozid.
- Dodatna restrikcija ulaznog prometa
  U ovisnosti o konfiguraciji sustava maskiranja mrežnih adresa, moguće je postavljanje dodatnih restrikcija na ulazni promet u odnosu na paketno filtriranje. Sustavi koji koriste dinamičku pretvorbu adresa dozvoljavaju prolaz unutra samo paketima koji su dio trenutne interakcije, tj. postavljeni su veći vremenski zahtjevi za napadače. U ovom slučaju,ukoliko napadač prilikom neovlaštenog upada ne reagira neko vrijeme, sustav za pretvorbu mrežnih adresa poništava adresu ili je dodjeljuje nekom drugom računalu.

Pri korištenju maskiranja mrežnih adresa prisutni su sljedeći nedostaci:

- Prepoznavanje mrežnih adresa
  Sustav za pretvorbu mrežnih adresa vrše pretvorbu adresa koje se nalaze u zaglavljima paketa. Pojedini protokoli skrivaju adrese te je nužno da sustav za pretvorbu mrežnih adresa poznaje protokol dovoljno dobro, kako bi uspio promijeniti adresu. Većina sustava za pretvorbu mrežnih adresa je u mogućnosti to napraviti barem za nekoliko protokola, ali ne za sve.
- Čuvanje statusa veze kod pretvorbe adrese

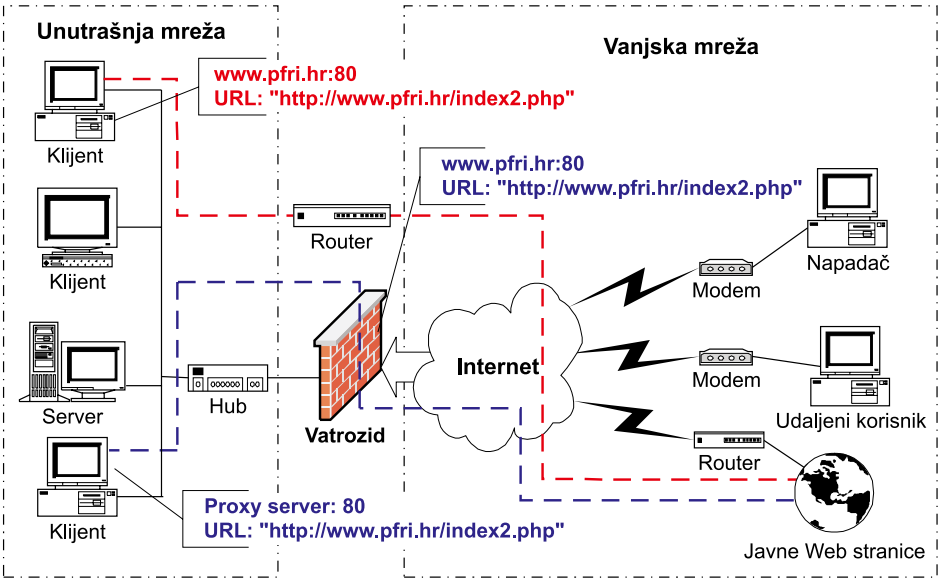
Sustavom za pretvorbu mrežnih adresa jednostavno je saznati je li računalo prekinulo TCP vezu. Međutim, ne postoji način kojim bi se saznalo, na nivou zaglavlja paketa, je li UDP paket dio procesa konverzije ili je izolirani događaj, tj. je li prekinuta UDP veza. To znači da u sustavu za pretvorbu mrežnih adresa mora biti definirano koliko dugo će se čuvati trenutna pretvorba jer postoji opasnost gubitka odgovora ili dostavljanja odgovara pogrešnom računalu.

- Dinamičko alociranje portova preklapa se s paketnim filtriranjem
  Sustavi za paketno filtriranje pregledavaju izvorišni i odredišni broj porta s ciljem saznanja koji je protokol korišten. Promjenom izvorišnog porta može doći do promjene paketa. U većini slučajeva ovo nije problem jer sustavi za pretvorbu mrežnih adresa vrše pretvorbu za klijente koji su obično ovlašteni za korištenje bilo kojeg porta poviše 1023. Međutim, ukoliko su portovi poviše 1023 translatirani u portove ispod 1023, moguće je da promet bude odbačen.
- Mogući problemi sa sustavima za kriptiranje podataka
  Sustavi za kriptiranje podataka osiguravaju integritet podataka tako da sustavi koji komuniciraju znaju da su podaci sigurno preneseni. Ovaj nedostatak dolazi do izražaja ukoliko korišteni protokol zaštićuje podatke koje mijenjaju sustavi za pretvorbu mrežnih adresa. U tom slučaju provjera integriteta neće biti uspješna i veza će biti prekinuta. Kod većine protokola, zaglavlja paketa nisu u dijelu zaštićenih podataka protokola. Glavna iznimka za ovo pravilo je IPsec protokol koji zaštićuje sve pakete, uključujući i zaglavlja.

POSREDNA USLUGA

Posredna usluga (eng. *proxy service*) je specijalizirana aplikacija ili serverski program koji prvotno prima zahtjev za određenom uslugom (npr. web pretraživanje) od strane korisnika te isti zahtjev prosljeđuje aktualnim servisima smještenim u vanjskoj mreži. Na taj način postiže se situacija u kojoj, na strani odredišnog servera, izgleda kao da su svi upiti postavljeni od strane proxy servera, odnosno postiže se skrivanje identiteta unutrašnjih korisnika. Zbog načina rada proxy serveri se nazivaju i aplikacijskim usmjerivačima (eng. *application – level gateway*).

Sljedećom slikom prikazan je princip rada proxy servisa.



Slika 3. Proxy servis

Osim skrivanja identiteta računala unutrašnje mreže, prednosti korištenja proxy servisa su sljedeće:

- Pohrana upita
  Budući da svi upiti moraju proći kroz proxy servis moguće je da proxy vrši spremanje (eng. *cashing*) čestih upita na proxyu, tj. lokalno pohranjivanje kopija podataka. Ukoliko je broj ponovljenih upita velik, *cashiranjem* se znatno povećavaju performanse sustava.
- Inteligentno pročišćavanje sadržaja
  Proxy servis omogućuje inteligentno pročišćavanje sadržaja podataka (eng. *content scaning*) s ciljem detektiranja i uklanjanja potencijalno zlonamjernog programskog koda, primjerice računalnih virusa.
- Kontrola pristupa na nivou korisnika
  Budući da je proxy sustav aktivno uključen u konekciju, moguće je vršiti kontrolu pristupa na nivou korisnika i poduzeti određenu akciju u ovisnosti o radnjama samog korisnika. Naravno, ovo je mnogo teže postići korištenjem paketnog filtera.

Nedostaci korištenja proxy servisa su sljedeći:

- Dostupan samo za određene usluge
  Proxy programski paketi su široko dostupni za starije i jednostavnije usluge (npr. web, email), dok je provjerene programske pakete za novije i manje rasprostranjene servise teško nabaviti.
- Proxy servis za svaki pojedini protokol
  Moguća je situacija u kojoj je potrebno postaviti različite proxy servere za svaki pojedini protokol. Razlog tome je taj što proxy server mora u potpunosti poznavati protokol, kako bi uspješno izvršio svoju funkciju. Skupljanje, instalacija i konfiguracija

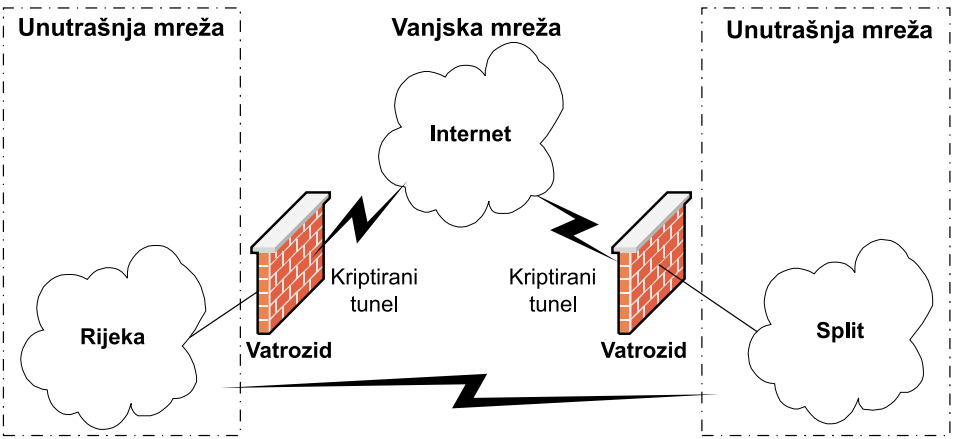
svih različitih proxy servisa može biti vrlo zahtjevna.

- Izmjena postavki klijenata, korisničkih programa i/ili procedura
  Pored uvođenja servisa dizajniranih za obavljanje *proxinga*, potrebna je i izmjena postavki klijenata, korisničkih programa i/ili procedura. Na primjer, korisnici nisu uvijek u mogućnosti koristiti neke od alata prema njihovim standardnim uputama, proxy programi ne rade uvijek jednako kao i neproxy programi itd.

VIRTUALNE PRIVATNE MREŽE

Kriptirani tuneli se često nazivaju i virtualnim privatnim mrežama. Njima je omogućeno sigurno spajanje dviju fizički odvojenih privatnih mreža preko javne mreže (npr. Internet), bez izlaganja podataka monitoriranju od strane zlonamjernih napadača. Sami kriptirani tuneli mogu biti uspješno napadnuti raznim alatima, prilikom uspostavljanja kriptirane veze. Međutim, ukoliko su implementirani kao integrirani dio vatrozida, autentikacija preko vatrozida i sigurnosni servisi omogućuju sigurno uspostavljanje kriptiranog tunela.

Virtualne privatne mreže su način implementacije kriptografske zaštite podataka s ciljem korištenja javne mreže kao da je privatna mreža. Radi osiguranja privatnosti, brze veze na velikim udaljenostima između dviju domena mnogo su skuplje od spajanja istih domena preko javne mreže, ali i mnogo sigurnije. Virtualna privatna mreža je kombinacija korištenja prednosti javne mreže (manja cijena i široka dostupnost) i privatne mreže (sigurnost).



Slika 4. Virtualna privatna mreža

Najvažniji razlog korištenja virtualnih privatnih mreža je ekonomski, ali virtualne privatne mreže pružaju i sljedeće sigurnosne značajke:

- Omogućena je sveukupna kriptografija podataka
  Virtualne privatne mreže obuhvaćaju cijeli promet koji se koristi, odnosno svi mrežni podaci koji se prenose su kriptirani. Na taj se način osigurava mrežni promet, tako da neovlaštene osobe nisu u mogućnosti doći do informacije koje se unutrašnje računalo koristi, koji je korišteni protokol itd.

- Mogućnost udaljenog korištenja protokola koje je teško osigurati na drugi način
  Pojedine protokole je zbog svoje funkcionalnost vrlo teško koristiti u sigurnom okruženju koje se postiže korištenjem paketnog filtriranja i proxy servisa. Virtualne privatne mreže omogućuju kriptiranjem podataka siguran udaljen pristup korištenjem ovih protokola.

Iako su virtualne privatne mreže važan sigurnosni alat, prisutni su sljedeći nedostaci:

- Opasnost za računala spojena na javnu mrežu
  Virtualna privatna mreža koristi aktualnu mrežu koja nije privatna, odnosno sigurna mreža. Računala priključena u virtualnim privatnim mrežama moraju biti spojena na tu aktualnu mrežu te su u opasnosti od neovlaštenih upada. Na primjer, ukoliko koristimo virtualne privatne mreže za spajanje unutrašnje mreže s mobilnim korisnicima koji su spojeni na Internet, njihova računala mogu biti napadnuta s Interneta.
- Opasnost od neovlaštenih upada u unutrašnju mrežu
  Priključenjem računala u virtualnu privatnu mrežu, to računalo postaje legitimni član unutrašnje, privatne mreže. Ukoliko je na računalu virtualne privatne mreže napravljen neovlašteni upad, napadač je u mogućnosti preko virtualne privatne mreže ugroziti sigurnost ostalih računala unutrašnje mreže. Virtualne privatne mreže se koriste za pružanje pristupa računalima koja su manje sigurna od računala unutrašnje mreže. Na primjer, kod prijenosnih računala postoji opasnost od krađe, kućnim računalima djeca imaju pristup itd.

3. ZAKLJUČAK

U današnje vrijeme, kada je Internet nezaobilazan alat u svim organizacijama, potrebno je posvetiti posebnu pozornost računalnoj sigurnosti. Vatrozidi imaju veliku ulogu u očuvanju sigurnosti računalnog sustava jer omogućuju naprednu kontrolu i upravljanje mrežnim prometom, zaštićuju tajnost konfiguracije privatne mreže, skrivaju identitet unutrašnjih korisnika te omogućuju sigurno spajanje s privatnom mrežom putem javne mreže. Pored brojnih i raznolikih sigurnosnih mjera i mehanizama, vatrozidi omogućuju centralizaciju svih sigurnosnih servisa u jednoj kontrolnoj točki te na taj način olakšavaju njihovo implementiranje i održavanje.

LITERATURA

[1] Cheswick, W.R., Bellovin, S.M., Rubin, A.D., Firewalls and Internet Security, 2003., Addison-Wesley
[2] Deal, R.A., Cisco PIX Firewalls, 2002., Syngress
[3] Luotonen, A., Web Proxy Servers, 1997., Prentice Hall PTR
[4] Maxwell, D., Amon, C., Noble, J., Check Point NG VPN-1/Firewall, 2003., Syngress
[5] Zwicky, E.D., Cooper, S., Chapman, D.B., Building Internet Firewalls, 2000., O'Reilly

Summary

COMPUTER SYSTEMS PRIVACY PROTECTION

Being the most critical area of computer technology, security assumes growing importance in today's computer systems environment. This paper presents working principles of "firewall", a device that enables different methods of control and management of data traffic between two computer networks, with the purpose of protecting private network security from public network security risks. Basic "firewall" functions are presented and devised: packet filtering, network address masking, proxy service and virtual private network. Main roles of the basic "firewall" functions are explained and advantages and disadvantages of their use are examined. This paper provides guidelines for protecting computer systems privacy.

Key words: "firewall", packet filtering, network address masking, proxy service, virtual private network.

Faculty of Maritime Studies Rijeka
Studentska 2, 51000 Rijeka
Croatia