

ZAŠTITA MAIL SERVERA NA NIVOU MREŽNE INFRASTRUKTURE

dipl. ing. Jelena Milojković¹, *Repub.zavod za statistiku Srbije,*
mima@statserb.sr.gov.yu

dipl. ing. Rastko Šoškić², *Repub.zavod za statistiku Srbije,*
rsoskic@statserb.sr.gov.yu

Apstrakt: *Ovaj rad se bavi pregledom nekih od mogućih napada na mail server, i mogućnošću zaštite mail servera od tih napada, na nivou mrežne infrastrukture.*

Ključne reči: *zaštita, mail, server, Internet, mreža.*

IMPLEMENTING A SECURE NETWORK FOR MAIL SERVER

Abstract: *This paper gives the overview of some attacks and defences for the mail server. Defences that are described are implemented on the network infrastructure level.*

Key words: *protection, mail, server, Internet, network.*

UVOD

Mrežna infrastruktura igra veoma važnu ulogu u zaštiti mail servera, zato što je to prva linija odbrane između Interneta i mail servera. Na nivou mrežne infrastrukture se prvenstveno obezbeđuje raspoloživost i kontrola pristupa mail serveru. Treba napomenuti da se apsolutna zaštita ne može ostvariti. Doslednom primenom metoda i postupaka zaštite može se znatno otežati njeno narušavanje, što i jeste glavni cilj svakog sistema primenjene zaštite. Ovaj rad se ograničava na mogućnost zaštite mail servera na nivou mrežne infrastrukture.

1 VRSTE NAPADA

Napadi mogu biti izvedeni izuzetno jednostavnom tehnologijom (npr. lažnim predstavljanjem službeniku kompanije u telefonskom razgovoru) ili korišćenjem visoke tehnologije (npr. prebacivanje adrese web sajta na drugi server). U daljem tekstu biće opisane neke od vrsta napada koje se mogu sprečiti ili otežati na nivou mrežne infrastrukture.

Peslikavanje – skeniranje sistema. Svrha skeniranja sistema je da se što više sazna o meti pre napada jer time napadač smanjuje verovatnoću da će biti uhvaćen, i ima veće izglede za uspeh napada koji sledi. Program kao što je ping može da se upotrebi da bi se utvrdile IP adrese mašina u mreži jednostavnim posmatranjem koje adrese odgovaraju na poruku ping. Skeniranje portova odnosi se na tehniku skvencijalnog kontaktiranja (preko zahteva za TCP konekciju, ili preko jednostavnog UDP dijagrama) brojeva portova na mašini i gledanja šta se dešava kao odgovor. Skeniranjem portova napadač može otkriti propuste u zaštiti i kroz neki nepotrebno otvoreni port ugroziti sistem.

IP varanje – IP spoofing. Svaki uređaj povezan sa Internetom obavezno šalje IP datagrame u mrežu. Ti datagrami nose adresu pošilaoa (i primaoca), kao i podatke iz višeg sloja. Korisnik sa potpunom kontrolom nad softverom uređaja (posebno njegovim operativnim sistemom) može lako da promeni protokole uređaja tako da postave proizvoljnu IP adresu u polje datagrama rezervisano za IP adresu izvora. To se zove IP varanje (IP spoofing). Korisnik – napadač na taj način može da napravi IP paket koji po želji sadrži bilo kakve podatke (iz višeg sloja) u korisnom teretu sa proizvoljnog računara. IP varanje se često koristi u napadima odbijanja usluge da bi se sakrio organizator napada. Sa lažnom IP adresom izvora u datagramu, teško je pronaći računar koji je stvarno poslao datagram.

Napadi odbijanja usluge – denial of service DoS. Široku klasu bezbednosnih pretnji čine napadi odbijanja usluge – DoS napadi. Kao što im ime nagoveštava, DoS napadi čine mrežu, računar ili neki deo mrežne infrastrukture neupotrebljivim za legitime korisnike. DoS napad obično deluje tako što stvara toliko mnogo posla za infrastrukturu koja mu je izložena, da legitimni rad ne može da se obavi. Postoji više vrsta DoS napada, neki od njih su:

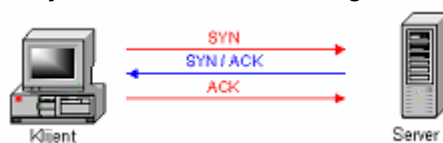
Ping of Death. Program ping spada u pomoćne programe, kojim se proverava da li između neka dva uređaja u mreži uopšte postoji veza. Kada jedan uređaj pošalje jedan ili više ping paketa drugom uređaju, ovaj ukoliko ih dobije, automatski odgovara na njih. Ping paket ima strogo definisan format i operativni sistemi i njihovi programi za podršku TCP/IP protokolima to rutinski podržavaju. Ukoliko se nekoj mašini namerno pošalje ping paket suviše velike dužine, u zavisnosti od tipa operativnog sistema, uređaj može jednostavno da se blokira i prestane da radi. Da bi se uređaj povratio, potrebno ga je restartovati, što, kad je server u pitanju, može da bude prilično neprijatna

stvar. Ping of Death je, veoma jednostavan i efikasan DoS napad, pošto se dešava da jedan jedini poslati paket blokira radnu stanicu ili server. Pozitivno je, da je ovaj problem kod većine savremenih operativnih sistema ipak rešen, ali su starije verzije, ukoliko nisu "zakrpljene", i dalje izložene opasnosti.

Smurf napad – napad “štrumfova”. Smurf napad radi tako što veliki broj nevinih računara odgovara na pakete zahteva ICMP eho (ping) koji sadrže lažnu IP adresu izvora. Kao IP adresa izvora stavlja se IP adresa uređaja (računar, ruter, firewall) koji se želi napasti. Rezultat je veliki broj paketa odgovora na komandu ping koja se šalje na IP adresu koja je navedena kao izvorišna IP adresa.

Fraggle. Fraggle DoS napad je sličan Smurf napadu, izuzev što Fraggle koristi UDP echo i UDP echo reply poruke umesto ICMP poruka. Pošto se UDP echo poruke inače filtriraju, manja je verovatnoća da će ovaj tip napada imati uticaja na rad sistema kao što to ima Smurf napad.

SYN poplava – SYN flood. SYN napad koristi rupu u TCP/IP pri autentifikaciji server-klijent, koja se naziva three-way handshake (tri načina rukovanja). Da bi se shvatio ovaj način napada mora se znati prvo na koji način Windows autentifikuje klijente koji mu pristupaju. Kada računar pristupa drugom računaru njihov dogovor se odvija u tri koraka (slika 1.): prvo klijentski računar šalje paket računaru kome pristupa (recimo serveru) i taj paket se zove SYN, potom server odgovara klijentu SYN/ACK paketom, i na kraju, klijent šalje paket ACK (acknowledgement) da prihvata dogovorenu komunikaciju. U prvom paketu koji šalje klijent nalazi se zahtev za uspostavljanje komunikacije, IP adresa klijenta, da bi server mogao da mu odgovori, i ISN (initial sequence number), koji je potreban serveru da bi pravilno sastavio pakete koje mu šalje klijent. U paketu koji server šalje klijentu nalaze se isti podaci, samo sada idu od strane servera. Pri SYN napadu, napadač potapa server paketima TCP SYN, od kojih svaki ima lažnu IP adresu izvora. Server, nemoćan da napravi razliku između legitimnog i lažnog SYN-a, završava drugi korak TCP potvrđivanja spremnosti za prenos za lažni SYN, dodeljujući strukturu i stanje podataka. Napadač nikad ne izvrši treći korak trosrke sinhronizacije, ostavljajući za sobom delimično otvorene konekcije čiji se broj stalno povećava. Opterećenje SYN paketima koji treba da se obrade i iscrpljivanje slobodne memorije na kraju baca server na kolena. SYN Flood napad, u zavisnosti od operativnog sistema i njegove konfiguracije, može da izazove potpuno zagušenje komunikacija ili čak totalno obaranje sistema. Pošto je ova vrsta napada bazirana na samom TCP protokolu, SYN Flood je veoma teško otkloniti. Odgovarajućim podešavanjem rutera ili firewall-a može se samo zaustaviti obaranje sistema, ali ne i zagušenje. Iako pojedini operativni sistemi uvode neke mere za otklanjanje mogućnosti ovog napada, većim hakerskim manipulacijama se i ove mere mogu izbesci.



Slika 1. TCP sinhronizacija u tri koraka: razmena segmenata

Distribuirani napadi odbijanja usluge – Distributed Denial of Service DDoS. U napadu distribuiranog odbijanja usluge DDoS. Napadač najpre treba da dobi je pristup korisničkim nalogima na brojnim računarima na Internetu (npr., uhođenjem lozinki ili drugim vrstama prodora u korisnikov nalog. Napadač onda instalira i pušta u rad program-slugu na svakoj od lokacija, koji tiho čeka komandu od programa-gospodara. Sa velikim brojem takvih programa-slugu koji se izvršavaju, program-gospodar onda uspostavlja kontakt i nalaže svakom od njih da započne napad odbijanja usluge usmeren na isti ciljni računar – žrtvu. Rezultujući koordinirani napad je posebno razoran, zato što dolazi sa velikog broja napadačkih računara u isto vreme.

2. MREŽNA LOKACIJA MAIL SERVERA

Prva i, u većini slučajeva, najvažnija odluka kada je u pitanju zaštita na nivou mrežne infrastrukture je smještanje mail servera na određenu lokaciju u mreži. Lokacija je važna zato što time određujemo koje komponente mrežne infrastrukture možemo iskoristiti za zaštitu mail servera na mrežnom nivou i koji će delovi mreže još biti ranjivi u slučaju napada na mail server.

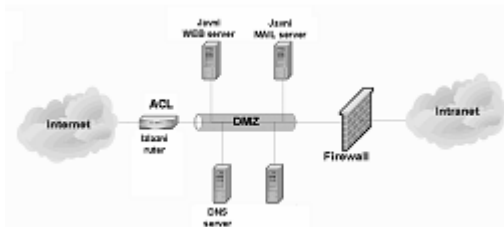
2.1 Primeri loše lokacije za mail server

Loš primer postavljanja javnog mail servera, je postavljanje unutar lokalne mreže tj. postavljanje mail servera u mrežu u kojoj se nalaze interni korisnici i serveri. Glavna slabost ovakvog sistema je u tome što se zbog potrebe pristupa mail serveru sa strane Interneta moraju na aktivnoj mrežnoj opremi ostaviti odgovarajući prolazi i na taj način korisnici iz spoljašnjeg sveta su u mogućnosti da ugroze osim mail servera i lokalnu računarsku mrežu. U ovom slučaju se lokalna mreža izlaže potpuno nepotrebnom riziku.

Druga mrežna lokacija koja se ne preporučuje je postavljanje mail servera ispred firewall-a ili rutera koji štiti lokalnu mrežu (LAN) putem filtriranja saobraćaja na mrežnom sloju (filtriranje IP paketa). U ovom slučaju mail server ne ugrožava lokalnu mrežu ali je sam ostao bez ikakve zaštite koju mu mogu pružiti uređaji kao što su ruter i firewall. Jedina zaštita koju ima mail server u ovom slučaju je zaštita koju sam sebi može pružiti na nivou operativnog sistema i na nivou aplikacije što nije dovoljno.

2.2 Demilitarizovana zona (DMZ)

Demilitarizovana zona je segment mreže koji se može opisati kao "neutralna zona" umetnuta između lokalne mreže (intraneta) i spoljašnje mreže (Interneta). Smještanjem mail servera u demilitarizovanu zonu sprečavamo spoljašnje korisnike mail servisa, da pristupe lokalnoj mreži organizacije koja je vlasnik tog mail servera. Demilitarizovana zona omogućava pristup mail serveru i korisnicima iz lokalne mreže i korisnicima sa Interneta. U daljem tekstu biće opisane neke moguće konfiguracije demilitarizovane zone.

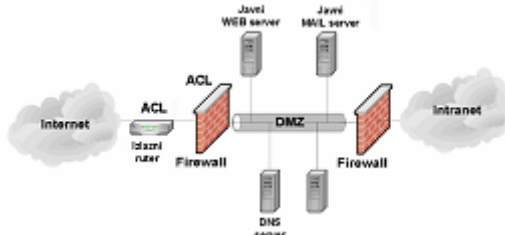


Slika 2. Jednostavan DMZ sa jednim firewallom

Jedan od najjednostavnijih načina kreiranja demilitarizovane zone je postavljanje firewalla između izlaznog rutera i unutrašnje mreže (Slika 2.). Tako se stvara novi segment mreže (između izlaznog rutera i firewall-a) gdje se može postaviti mail server

(i svi ostali serveri potrebni za pružanje usluga javnih servisa). U ovom primeru zaštita mail servera se vrši pomoću liste za kontrolu pristupa ACL (access control lists) koja se postavlja na izlaznom ruteru i kojom se ograničava određeni tip saobraćaja u i iz DMZ-a.

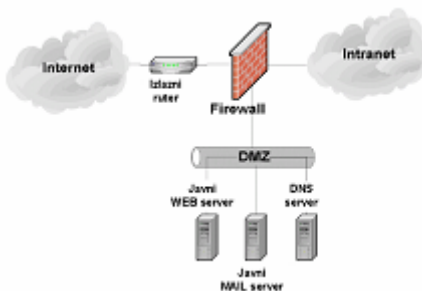
Ova konfiguracija DMZ je jednostavno i jeftino rješenje, a prisutna je i zaštita mail servera od strane izlaznog ruter-a. Ovo rešenje može biti odgovarajuće za male organizacije koje su izložene minimalnim pretnjama. Glavni nedostatak konfiguracije je u tome što izlazni ruter nije "svestan" mail protokola na aplikacionom sloju (SMTP, POP3, IMAP) tako da on nije u stanju da spreči napade takvog tipa na mail server. Pored toga ruter nije u stanju da pruži anti-virusnu zaštitu i da skenira dolaznu e-poštu. Poboljšanje konfiguracije postiže se postavljanjem još jednog firewall-a između izlaznog ruter-a i DMZ-a. Konfiguracija je prikazana na Slici 3.



Slika 3. DMZ sa dva firewall-a

Konfiguracija DMZ-a pomoću dva firewall-a pruža veoma dobru zaštitu mail servera. Sigurnosna pravila koja se mogu podesiti na firewall-u su mnogo efikasnija i složenija nego ona koja se mogu dobiti sa ruter-om. Osim toga firewall-ovi su često sposobni da analiziraju ulazni i izlazni saobraćaj e-pošte, mogu registrovati i sprečiti napade na aplikacijskom sloju. Mana ovakve konfiguracije DMZ je u tome što u zavisnosti od konfiguracije firewall-ova i sa velikom količinom saobraćaja dolazi do značajnijeg gubitka performansi sistema.

Za organizacije koje žele nivo zaštite koju pruža konfiguracija sa dva firewall-a, ali nemaju materijalne mogućnosti i da ih nabave, postoji rešenje sa jednim firewall-om koji poseduje tri (ili više) mrežnih adaptera. Jedan mrežni adapter se povezuje sa lokalnom mrežom (inside interface), drugi adapter se povezuje sa izlaznim ruter-om (outside interface), a treći adapter se povezuje sa DMZ-om. Ako postoji više od tri mrežna adaptera moguće je formirati konfiguraciju sa više demilitarizovanih zona. Konfiguracija DMZ-a sa jednim firewall-om sa tri mrežna adaptera prikazana je na slici 4.



Slika 4. DMZ sa jednim firewall-om sa tri mrežna adaptera

3. AKTIVNA MREŽNA OPREMA

Kada se mail server postavi na izabranu lokaciju u mreži potrebno je aktivne elemente mrežne infrastrukture podesiti da podržavaju i štite mail server. Najčešće korišćeni elementi mrežne infrastrukture koji imaju uticaja na bezbednost mail servera su: ruteri i firewall-ovi. Svaki od ovih uređaja ima svoju ulogu u cilju zaštite mail servera. Pojedinačno oni nisu u stanju zaštititi mail server od svih vrsta pretnji i napada.

3.1 Ruter

Ruteri (routers – usmerivači) rade tačno ono što im i ime kaže: usmeravaju podatke između mreža. Na putu između dve mreže može postojati veoma veliki broj rutera i njihova namena je da proslede paket na željeno odredište. Pomoću rutera se lokalna mreža povezuje sa telekomunikacionom mrežom i na taj način se ostvaruje komunikacija između LAN-a i Interneta.

Ruter takođe može da radi i kao regulator saobraćaja, filtriranjem. Zbog ove osobine ruter se može koristiti i u cilju zaštite resursa koji se štite kao što je mail server. Zapravo ruter funkcioniše kao firewall mrežnog sloja (familije internet protokola) i može da pruži filtriranje paketa na osnovu:

- IP adrese izvora
- IP adrese odredišta
- Tipa ICMP poruke. ICMP – Internet Control Message Protokol je protokol koji koriste računari i ruteri za međusobno prenošenje informacija o mrežnom sloju. Naredbom ping šalje se navedenom računaru ICMP poruka tipa 8 sa šifrom 0, odgovor računara na ping je ICMP poruka tipa 0 šifre 0.
- TCP/UDP broja porta (samo neki ruteri)

3.2 Firewall

Firewall je uređaji koji se koristi za kreiranje kontrolnih tačaka bezbednosti (checkpoints), na granicama privatnih mreža. Na ovim kontrolnim tačkama firewall-ovi ispituju sve pakete koji prolaze između privatne mreže i Interneta. U zavisnosti od toga da li paket odgovara ili ne pravilima politike programirane na firewall-u, paket se propušta ili odbacuje.

Postoje na stotine raspoloživih firewall proizvoda kao i mnoštvo različitih teorija stručnjaka za bezbednost o tome kako treba koristiti firewall-ove u cilju zaštite resursa. Grubo se mogu podeliti na:

- firewall-ove mrežnog sloja koji mogu filtrirati pakete na osnovu IP adrese izvora/odredišta, i na osnovu TCP/UDP broja porta.
- firewall-ove aplikacionog sloja još se nazivaju i proxy firewall-ovi. U stanju su da “razumeju” i filtriraju saobraćaj elektronske pošte na osnovu njenog sadržaja i na osnovu komandi protokola e-pošte.

Firewall se nalazi na granici mreže i povezan je direktno na ruter koji omogućava pristup drugim mrežama. Iz tog razloga firewall-ovi su poznati kao pogranično obezbeđenje. Ovakav koncept pograničnog obezbeđenja veoma je bitan – bez njega svaki host (domaćin) na mreži morao bi sam da obavlja funkciju firewall-a, bespotrebno trošeći svoje resurse i povećavajući vreme potrebno za povezivanje, autentifikaciju i šifrovanje podataka. Firewall-ovi omogućavaju centralizaciju svih bezbednosnih servisa na spoljnim uređajima koji su optimizovani i posvećeni zadatku zaštite.

Firewall-ovi primarno funkcionišu koristeći tri osnovna metoda:

- **Filtriranje paketa.** Prihvatanje ili odbijanje paketa u zavisnosti od IP adresa izvora – odredišta i TCP-UDP broja porta a na osnovu definisane liste za kontrolu pristupa ACL (access control lists).

- **Prevođenje mrežnih adresa** (Network Address Translation **NAT**). IP adrese unutrašnjih hostova se prevode u spoljnu ili spolje adrese i tako skrivaju od spoljnog praćenja.

3.3 Filtriranje paketa za pristup mail serveru u DMZ

Postoje dva osnovna pristupa podešavanja bezbednosti. Prvi, pesimistički, gde se zabranjuje sav saobraćaj osim onog koji je neophodan i drugi, optimistički, gde se dozoljava sav saobraćaj osim onog za koji se zna da je štetan. U svrhu bezbednosti, trebalo bi uvek imati pesimistički pristup, jer optimistički pristup podrazumeva da je unapred poznata svaka moguća pretnja, što je nemoguće. Filtriranje paketa na ruterima i firewall-ovima vrši se pomoću listi za kontrolu pristupa ACL (access control lists) koje se mogu postaviti na svakom od interfejsa ovih uređaja. ACL na interfejsu mogu biti ulazne i izlazne.

Osnovni principi pri korišćenju filtriranja paketa su:

- zabrana svih protokola i adresa osim onih koji su neophodni
- odbacivanje ICMP poruka za redirekciju i eho (ping).
- odbacivanje svih spoljnih ažuriranja protokola rutiranja (RIP, OSPF) za rutere na mreži koja se štiti (u DMZ najverovatnije uopšte nema rutera ali to je stvar konfiguracije mrežne infrastrukture organizacije)
- u zaštiti mreže ne oslanjati se samo na filtriranje paketa.

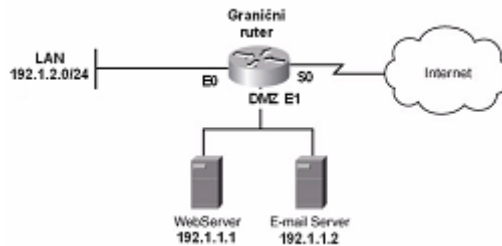
Filtriranjem paketa možemo odbaciti sve pakete zahteva ICMP eho (ping) i time zaštititi mail server od napada kao što su *Smurf*, *Fraggle* i *Ping of death*.

3.4 Prevođenje mrežnih adresa (Network Address Translation NAT).

Prevođenje adresa iz mreže rešava problem skrivanja IP adresa unutrašnjih uređaja. NAT je zapravo proxy mrežnog sloja: jedan host čini zahteve u ime svih unutrašnjih hostova. Na taj način on skriva njihov identitet na javnoj mreži. NAT skriva adrese unutrašnjih uređaja, konvertujući ih u adresu firewall-a. Gledano sa Interneta, sav saobraćaj sa Vaše mreže izgleda kao da dolazi sa jednog, ekstremno zaposlenog računara. NAT efikasno skriva sve TCP/IP informacije unutrašnjih hostova od očiju Interneta. Ovim se otežava napad skeniranja sistema.

3.5 Primer zaštite mail servera od DoS napada

U ovom primeru biće prikazana osnovna pravila filtriranja paketa koja treba postaviti u ACL u cilju zaštite mail servera (i ostatka mreže) od DoS napada. U ovom slučaju izabran je ruter kao uređaj za filtriranje ali se pravila takođe mogu postaviti i na firewallu. Mrežna konfiguracija prikazana je na slici 5.



apada

Osnovna pravila:

- (1a) Router(config)# access-list 100 deny ip any 192.1.1.0 0.0.0.0
- (1b) Router(config)# access-list 100 deny ip any 192.1.1.255 0.0.0.0
- (1c) Router(config)# access-list 100 deny ip any 192.1.2.0 0.0.0.0
- (1d) Router(config)# access-list 100 deny ip any 192.1.2.255 0.0.0.0
- (2) Router(config)# access-list 100 permit icmp any host 192.1.2.9 echo-reply
- (3) Router(config)# access-list 100 deny icmp any any echo
- (4) Router(config)# access-list 100 deny icmp any any echo-reply
- (5) Router(config)# access-list 100 deny udp any any eq echo
- (6) Router(config)# access-list 100 deny udp any eq echo any
- (7) Router(config)# access-list 100 permit tcp any host 192.1.1.1 eq 80 established
- (8) Router(config)# access-list 100 permit tcp any host 192.1.1.1 eq 80
- (9) Router(config)# access-list 100 permit tcp any host 192.1.1.2 eq 25 established
- (10) Router(config)# access-list 100 permit tcp any host 192.1.1.2 eq 25
- (11) Router(config)# access-list 100 deny ip any any

Access lista 100 pridružuje se interfejsu S0 kao ulazna ACL.

Router(config)# interface serial0

Router(config-if)# ip access-group 100 in

U primeru ove ACL osim pravila pomoću kojih se filtrira saobraćaj postoje i dodatna pravila koja služe za detektovanje nekog od DoS napada: direktni broadcast napad (redovi 1a – 1d), koji se koristi u okviru mnogih DoS napada; Smurf napad (redovi 2, 3, i 4); Fraggle napad (redovi 5 i 6); i TCO SYN poplava (redovi 7 i 8):

- U slučaju Smurf napada, broj pogodaka za redove 2 i 4 naglo raste, to je indikacija da ste direktna žrtva smurf napada. U slučaju da napadač pokušava da vaše resurse iskoristi za reflektovanje napada na nekog drugog, broj pogodaka u redu 3 naglo raste. Potrebno je još omogućiti beleženje događaja (logging) na ruteru.
- Za Fraggle, napad, ako broj pogodaka za red 5 naglo poraste to je indikacija da ste žrtva, veliki broj pogodaka za red 6 indicira da ste reflektor napada.
- U slučaju TCP SYN napada, prikazaće se broj pogodaka za redove 8 i 10 mnogo puta veći od očekivanog za normalan saobraćaj. Treba primetiti da redovi 7, 8, 9 i 10 propuštaju a ne blokiraju saobraćaj ka mail serveru (i web serveru) jer bi inače i legalan saobraćaj bio blokiran. Ipak na ovaj način ako dođe do napada to će moći da se primeti, prati i da se reaguje. Pošto postoji mnogo oblika napada TCP poplave (flood), koji koriste različite TCP zastavice (flags), redovima 7 i 9 se prate TCP paketi sa drugačijim vrednostima zastavica (delovi TCP segmenta koji nose određene informacije).
- Takođe, redovi od 1a – 1d blokiraju saobraćaj na mrežnu adresu i na adresu direktnog broadcast-a za oba segmenta unutrašnjih mreža (DMZ i LAN). Ove adrese se često koriste za DoS napad.

Firma CISCO, napravila je softverski paket kojim je moguće nadgraditi CISCO operativni sistem rutera čime ruter dobija neke mogućnosti kontrole saobraćaja na aplikacionom nivou. Naziv tog sigurnosnog softverskog paketa je **Cisco Secure Integrated Firewall Software**.

Da bi se dodatno zaštitio mail server od napada tipa TCP SYN poplave, Smurf i Fraggle potrebno je osim kreiranja ACL podesiti još neke parametre na ruteru. U okviru dodatnog softverskog paketa postoji set komandi pomoću kojih se može definisati i ograničiti vreme za koje treba da se uspostavi konekcija, koliko dugo konekcija može biti neaktivna i sl. Na ovaj način ruter je u stanju da prekine sesiju koja se na osnovu postavljenih parametara može smatrati sumnjivom.

Neke od komandi koje se mogu iskoristiti za zaštitu mail server od DoS napada su:

- **ip inspect tcp synwait-time seconds** – definiše koliko dugo će softver čekati da TCP konekcija bude uspostavljena (završen treći korak sinhronizacije) pre nego što je odbaci i prekine. Unapred određena vrednost je 30 s.
- **ip inspect tcp finwait-time seconds** – definiše koliko dugo će se opsluživati TCP konekcija od trenutka kada ruter ili firewall detektuju signal spremnosti da se TCP konekcija zatvori FIN-exchange. Unapred određena vrednost je 5 s.
- **ip inspect tcp idle-time seconds** – definiše koliko će se dugo opsluživati TCP sesija koja ne pokazuje znake aktivnosti. Unapred određena vrednost je 3600 s - 1 sat.
- **ip inspect udp idle-time seconds** – definiše koliko će se dugo opsluživati UDP sesija koja ne pokazuje znake aktivnosti. Unapred određena vrednost je 30 s.
- **ip inspect dns-timeout seconds** – definiše koliko će se dugo opsluživati sesija za razrešenje DNS imena koja ne pokazuje znake aktivnosti. Unapred određena vrednost je 5 s.
- **ip inspect max-incomplete high number** - definiše broj postojećih napola otvorenih sesija koji će uticati na softver da počne da briše te napola otvorene sesije. Unapred određena vrednost je 500.
- **ip inspect max-incomplete low number** - definiše broj postojećih napola otvorenih sesija koji će uticati na softver da prestane da briše te napola otvorene sesije. Unapred određena vrednost je 400.
- **ip inspect one-minute high number** - definiše broj novih neuspostavljenih sesija u vremenskom periodu od 1 minuta koji će uticati na softver da počne da briše napola otvorene sesije. Unapred određena vrednost je 500.
- **ip inspect one-minute low number** - definiše broj novih neuspostavljenih sesija u vremenskom periodu od 1 minuta koji će uticati na softver da prestane da briše napola otvorene sesije. Unapred određena vrednost je 400.
- **ip inspect tcp max-incomplete host number block-time minutes** – u ovoj komandi postoje dva parametra. Parametar *number* definiše koliko poluotvorenih TCP sesija sa iste IP adrese je dozvoljeno pre nego što softver počne da ih briše, početna vrednost je 50. Dugi parametar *minutes* određuje koliko dugo će se odbijati novi zahtevi za konekcijom sa te IP adrese (od trenutka kada su počeli da se brišu), početna vrednost je 0 minuta.

Sa podešavanjem ovih vrednosti na ruteru mora se biti pažljiv jer ako se stavi previše kratko vreme ili premali broj napola otvorenih sesija može se desiti da u vreme povećanog legitimnog saobraćaja ruter ometa normalan rad i saobraćaj.

Primer vrednosti koje bi se mogle preporučiti za manju mrežu (~250 računara) su:

```
# ip inspect tcp synwait-time 20
# ip inspect tcp idle-time 60
# ip inspect udp idle-time 20
# ip inspect max-incomplete high 400
# ip inspect max-incomplete low 300
# ip inspect one-minute high 600
# ip inspect one-minute low 500
# ip inspect tcp max-incomplete host 300
lock-time 0
```

4. ZAKLJUČAK

Mrežna infrastruktura igra veoma važnu ulogu u zaštiti mail servera, zato što je to prva linija odbrane između Interneta i mail servera. Kakva će biti mrežna infrastruktura koja podržava mail server zavisi ne samo od potrebe za zaštitom već i od materijalnih mogućnosti organizacije, potrebnih performansi i pouzdanosti sistema. Mrežna infrastruktura, ne može sama zaštititi mail server, jer frekvencija, sofisticiranost i različitost današnjih "napada" na mail sisteme utiču na to da zaštita mora biti implementirana na različitim segmentima sistema i na različitim slojevima familije Internet protokola. Sprovođenjem zaštite mail servera, na nivou mrežne infrastrukture smanjuje se mogućnost neželjenih upada u sistem i DoS (Denial Of Service) napada na mail servis, a time se povećava dostupnost podataka na mail serveru. Zaštitom na mrežnom nivou mail server nije zaštićen od napada na SMTP, POP3 i IMAP aplikacije, neželjene pošte (spam-a) i virusa. Zaštita mail servera je neprestani proces koji zahteva konstantno prisustvo truda, sredstava i budnosti.

5. LITERATURA

1. James F. Kurose, Keith W. Ross (2005); *"Umrežavanje računara – od vrha ka dnu"*, Pearson Education, Inc. 2005, prevod CET Beograd
2. Miles Tracey, Wayne Jansen and Scott Bisker (2002); *"NIST Special publication 800-45 Guidelines on Eletronic Mail Security"*, Gaithersburg
3. Richard A. Deal (2004); *"Cisco Router Firewall Security"*, Cisco Press
4. Matthew Strebe, Charles Perkins (2003); *"Firewalls zaštita od hakera"*, SYBEX 2002, prevod Kompjuter biblioteka
5. Stuart McClure, Joel Scambray, George Kurtz (2002); *"Hakerske tajne zaštita mrežnih sistema"*, The McGraw-Hill Companies 2001, prevod Mikro knjiga 2002.
6. Steve McQuerry, *"Povezivanje Cisco mrežnih uređaja"*, Cisco Press 2000, prevod CET 2001.
7. J. F. DiMarzio, *"Rutiranje"*, SAMS Publising 2002, prevod Kompjuter biblioteka 2002.
8. Mark Tripod, *"Cisco ruteri Konfigurisanje i rešavanje problema"*, New Readers Publishing 2000, prevod CET 2000.
9. Kris Brenton, Bob Abuhof, *"Cisco Ruteri"*, Sybex 2002, prevod Kompjuter biblioteka 2003.
10. Toby J. Velte, Anthony T. Velte, *"Osnove Cisco tehnologija"*, Osborne 2001, prevod Kompjuter biblioteka 2002.