FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA
ZAGREB

Zavod za elektroničke sustave i obradbu informacija

Sustavi za praćenje i vođenje procesa

STATEFUL INSPECTION FIREWALL

Sanja Žonja
0036381544

Zagreb, 05.06.2005.

Sadržaj:

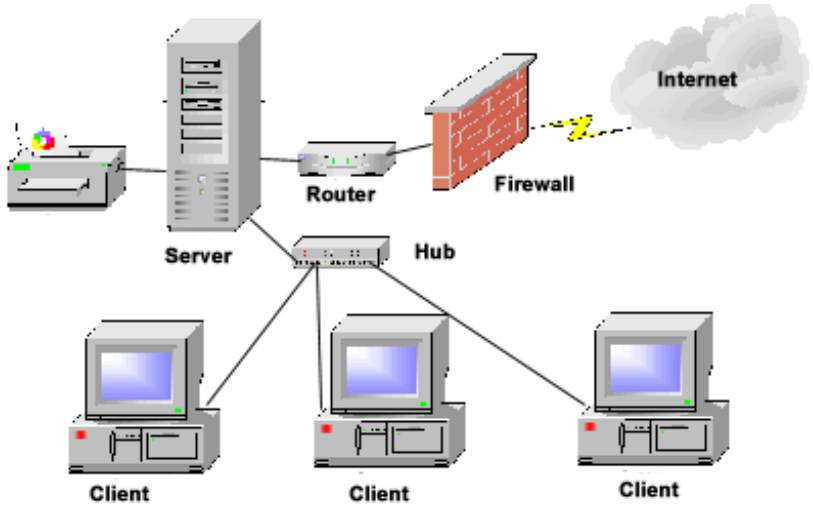
1. Općenito o vatrozidu

Termin *firewall* (ili hrvatski *vatrozid*) originalno označava granicu ili zid stvoren sa svrhom sprječavanja širenja vatre s jednog kraja zgrade ili strukture na drugi kraj. U domeni Interneta, vatrozidi su prvenstveno bili konstruirani u vojne svrhe, ali u novije vrijeme razvijaju se primarno da bi se zaštitila privatna računala.

Vatrozid označava sredstvo sigurnosti mreže kome je osnovna zadaća kontrola i filtriranje paketa koji putuju s zaštićene mreže na Internet i/ili s Interneta na zaštićenu mrežu. Oni prate i kontroliraju komunikaciju, te odlučuju da li će propustiti ili ne podatke prispjele na njih. Odluke o propuštanju pojedinih paketa donose se na temelju zaglavlja paketa u kojem se nalaze osnovni podaci o paketu i stanju konekcije: odredišna i izvorišna IP adresa, odredišni i izvorišni port, tip paketa, itd... Osim zaglavlja paket sadrži i tijelo paketa u kojem se nalaze podaci.

Nakon što paket stigne na vatrozid posebni programi analiziraju sadržaj zaglavlja paketa te ga uspoređuju s prethodno definiranim skupom pravila. Pravila se slijedno, u lancu (*chains*), primjenjuju na paket dok se ne odredi što s tim paketom treba učiniti. Paket se može odbaciti, prihvatiti, preusmjeriti na dio lanca za dodatnu analizu i sl.

Slika 1.1. prikazuje ilustraciju vatrozida.



Slika 1.1.

Glavna zabluda vezana uz vatrozida je da oni garantiraju sigurnost mreže, no vatrozid ne može, i samim time ne garantira da je naša mreža 100% sigurna. Isto tako ne mogu pružiti zaštitu od vanjskih napada. Da bi vatrozid bio učinkovit, sav promet mora proći kroz njega. Korisnik koji se nalazi sa pod žaštićenom mrežom najčešće ima pristup zaštićenim servisima bez prolaska kroz vatrozid. No, veliki postotak sigurnosnih incidenata dolazi baš sa strane unutarnje zaštićene mreže. Također, u večini slučajeva, ne mogu pružiti zaštitu od vriusa i malicioznih kodova. Kako većina vatrozida ne provjerava sadžaja paketa koji dolazi, nisu svjesni prijetnje koja se može skrivati unutra. A i samim time, kad prestane djelovati naša pretplata (šifra) vatrozida, to je adekvatno njegovom nepostojanju.

Svako umreženo računalo ima jedinstvenu IP adresu pridruženu mrežnom sučelju pomoću kojeg je povezano s ostalim računalima. Ukoliko računalo obavlja funkciju usmjerivača (engl. *router*) ono će biti spojeno na dvije ili više računalnih mreža te će imati više mrežnih sučelja s različitim IP adresama.

Osim IP adrese svako umreženo računalo posjeduje i svoju Ethernet MAC (engl. *Medium Access Control*) adresu koja jedinstveno identificira svaku Ethernet mrežnu karticu. Za razliku od IP adrese koja ima 32 bita, MAC adresa ima 48 bitova.

ARP (engl. *Address Resolution Protocol*) je protokol koji omogućava povezivanje MAC adresa s IP adresom. Klijent koji traži MAC adresu drugog računala provjerava svoju ARP tablicu, i ako njoj nema traženih podataka, odašilje ARP upit prema svim računalima u mreži (*broadcast*). Taj upit dolazi i od odredišnog računala. Odredišno računalo s traženom IP adresom šalje odgovor računalu koje je postavilo upit sa svojom MAC adresom. Zahvaljujući tom odgovoru računalo koje je postavilo upit zna kome treba poslati pakete.

Postoji vise vrste mehanizama prema kojima vatrozidi rade, prva vrsta radi na principu preskakanja podataka koja razmjenjuju računala koje vatrozid štiti i neka druga računala.

Druga skupina se zasniva na principu *proxy*a, odnosno postajanju međuaplikacije koja ne dopusta direktnu IP vezu, vec se ponaša kao posrednik za zahtjeve korisnika i stvara novu vezu do željenih resursa.
Također nas ocekuju Mehanizmi za filtriranje paketa ili na engleskom packet-filter naprednija verzija mehanizma za filtriranje se naziva stateful inspection.

Mehanizmi za filtriranje podataka rade na prncipu izvlačenja potrebnih podataka iz samih zaglavlja IP paketa. Polja zaglavlja paketa koje filtar najčešće ima na raspolaganju su tip paketa (TCP, UDP,..), izvorišna IP adresa te izvorišni i odredišni TCP/UDP port.

Iako postoje i druge tehnike pristupa poslužiteljima, radi jednostavnosti osvrćemo se samo *Proxy ARP* metodu.

Proxy ARP koristi se u slučajevima kada postoji jedno ili grupa računala koje su na neki način odvojene od ostataka mreže (npr. pomoću vatrozida ili usmjerivača). Kada vanjsko računalo zatraži da mu se javi računalo koje se nalazi iza vatrozida, na njegov upit javit će se sam vatrozid i poslati mu svoju MAC adresu. Nakon toga će računalo koje je poslalo upit slati mrežne pakete na vatrozid koji će pakete u pravilu provjeravati i prosljeđivati dalje na zaštičenu mrežu.

Da bi se ubrzao rad vatrozida obično se računala u zaštićenoj mreži grupiraju u podmreže. Za primjer uzmimo podmrežu 161.53.64.128 s mrežnom maskom 255.255.255.192, i *broadcast* adresom 161.53.64.191. To znači da se u toj mreži nalaze računala s IP adresama od 161.53.64.129 do 161.53.64.190, a adrese 161.53.64.128 i 161.53.64.191 rezervirane su za adresu mreže i *broadcast* adresu. Kada neko vanjsko računalo zatraži MAC adresu od zaštićenog računala vatrozid uz pomoć AND logičke operacije između odredišne IP adrese i podmrežne maske provjerava da li se odredišna adresa nalazi na podmreži.

Osim ARP protokola postoji i RARP protokol (engl. *Reverse Address Resolution Protocol*) koji omogućava da se uz poznavanje fizičke MAC adrese računala sazna i njegova IP adresa. RARP protokola se primjenjuje kod sustava bez diska koji prilikom pokretanja ne znaju vlastitu IP adresu i saznaju je pomoću RARP upita. Glavna razlika u odnosu na ARP protokol je što na RARP upit

odgovara posebni RARP poslužitelj koji održava bazu podataka fizičkih MAC i logičkih IP adresa.

Povijesno, tri različite tehnologije uporebljavane su za implementaciju vatrozida: Packet Filters, Application-Layer Gateways i Stateful Inspection Firewalls. U ovom dokumentu osvrnuti ćemo se samo na zadnju tehologiju.

2. Stateful inspection firewall (vatrozid)

2.1. Način rada

Stateful inspection je u sredinom devedesetih godina prošlog stoljeća kao novu tehnologiju uvela tvrtka Check Point Software Technologies u upotrebi svog FireWall-1. Stateful inspection revolucionizirala je tehnologiju vatrozida te postala de facto industrijski sandard.

Uobičajeni način provjere mrežnih paketa od strane vatrozida, tzv. *stateless inspection*, sadrži velik broj propusta i sigurnosnih rupa. Tim načinom provjere paketi se analiziraju kao jedinke i nije moguće utvrditi da li oni pripadaju nekoj postojećoj vezi ili su to inicijalni paketi konekcije. Nasuprot tome, tzv. *stateful inspection* način provjere mrežnih paketa omogućava detaljniju analizu paketa. Moguće je utvrditi da li su paketi dijelovi neke uspostavljene veze ili ne. Za razliku od statičkog filtriranja paketa, koje analizira pakete samo na temelju njihovih zaglavlja, *stateful inspection* način rada registrira sve uspostavljene konekcije između pojedinih mrežnih sučelja te na temelju njihovih stanja obavlja provjere.

Stateful inspection vatrozid zbog toga mora održavati tablice stanja u kojima su određenim vezama pridružene određena stanja. Zbog toga se odluke o filtriranju ne donose samo na temelju definiranih pravila (tzv. statičko filtriranje), već i na temelju sadržaja prethodno proslijeđenih paketa (tzv. dinamičko filtriranje). Upravo zato se i stateful inspection vatrozid naziva još i dinamičkim filtriranjem paketa.

Prilikom uspostavljanja veze između dva računala bitno je znati da se paketi koji putuju između ta dva računala sastoje od 7 slojeva (fizički, podatkovni, mrežni, prijenosni, sjednički, prezentacijski i aplikacijski sloj). Nama su važni podatkovni, mrežni, prijenosni i aplikacijski sloj. Zadatak podatkovnog sloja je ostvarivanje pouzdanog prijenosnog kanala između dvije ili više točaka. Više jedinica podataka grupira se u “okvire”, dodaje im se zaglavlje i glava te informacije potrebne za otkrivanje greške u prijenosu. Mrežni sloj se bavi pitanjima važnim za rad cijele podmreže i suradnjom s drugim mrežama. Sadrži

izvorišnu i odredišnu IP adresu te još neke postavke kao što su zaštitna suma i sl.. Prijenosni sloj sadrži informacije potrebne za razlučivanje koji paket pripada kojem procesu (izvorišni i odredišni port..). Aplikacijski se odnosi na vrstu programa koji se koristi i on prenosi dio tijela poruke, kriptirano ili ne, kakvo je odašiljatelj poslao. To može biti naredba ili dio naredbe, datoteka ili dio datoteke i slično.

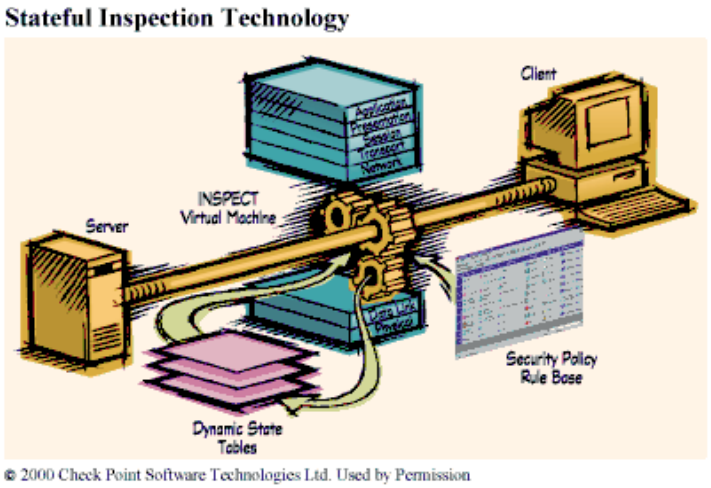
Ideja stateful inspection mehanizma je da je ispitivanje paketa izoliranih od ostatka komunikacije nedovoljno te da se mora obavljati u širem kontekstu kako bi se mogle donijeti kritične sigurnosne odluke. Ispitivanje šireg konteksta se odnosi na na:

a) analiziranje svih komunikacijskih razina iz kojih se izvlače važni podaci o vezi, komunikacijskom stanju i aplikaciji.

b) Informacije dobivene od prijašnjih komunikacijskih veza, npr. PORT izlazna naredba FTP komunikacije se moze pohraniti kako bi se ulazna FTP podatkovna veza mogla verficirati.

c) Informacije dobivene od drugih aplikacija, npr. propušta se predefinirana vrsta prometa za korisnike, čiji je identitet prethodno provjeren ovisno o njihovim predefiniranim pravilima

d) Manipuliranje informacija dobivenim od prethodna tri načina.



Slika 2.1.

Slika 2.1. prikazuje stateful inspection tehnologiju. Na temelju OSI slojeva i sigurnosnih pravila formiraju se tablice dinamičkog stanja koje nam govore o povezanosti paketa koji pristižu na vatrozid.

Stateful inspection može riješiti probleme poput filtriranja UDP i RPC protokola. UDP protokol je težak za filtriranje jer nema razlike izmedu zahtjeva i odgovora odnosno ne uspostavlja se veza. Kako je svaki UDP paketa zapravo sam za sebe, prije stateful inspection mehanizma problem sa UDP paketima se uglavnom riješavao tako da se puste svi UDP paketi ili da se odbace svi paketi po načelu svi za jednog jedan za sve.

Komplikacija sa RPC-om je u tome da se ne koriste predefinirani portovi vec se dinamički alociraju. Stateful inspection može i RPC bazirane usluge osiguravati pohranjivanjem konteksta iz prethodne komunikacije.

Korisnik koji odašilje paket, svjesno ili nesvjesno šalje taj paket na određeni port na odredišnom računalu, s određenog izvorišnog porta. Ukupni broj raspoloživih portova je 65536. Portovi do 1024 rezervirani su za neke standardne protokole, odnosno aplikacije i nije ih moguće prenamijeniti (npr FTP, Telnet, SMTP, HTTP, …). Portovi iznad 1024 namijenjeni su za različite svrhe. S njih se uspostavlja veza s drugim odredišnim računalima, a na njih je moguće i prihvatiti odgovore ili zahtjeve za određenim uslugama.

Problem kod vatrozida koji obavljaju statičko filtriranje je u tome što većina njih ostavlja otvorene sve pristupne mrežne portove iznad porta 1024. Ti portovi su ostavljeni otvorenima jer se paketi-odgovori šalju na njih. Ostavljanje tih portova otvorenima predstavlja veliki sigurnosni nedostatak za vatrozid. Moguće je da napadač ubaci maliciozno prilagođeni mrežni paket prema određenom računalu koje na otvorenom portu očekuje neki drugi paket, ali od nekog drugog pošiljatelja.

Vatrozid s podržanim *stateful inspection*-om radi na drugačijem principu. On ne dozvoljava promet nikakvih paketa s nezaštićene mreže osim onih koji pristupaju otvorenim portovima. Za razliku od statičkog filtriranja, portovi iznad 1024 su zatvoreni, a otvaraju se samo kada postoji uspostavljena dozvoljena

konekcija. Ukoliko zaštićena mreža ne posjeduje poslužitelje obično su dozvoljene samo konekcije inicirane iz zaštićene mreže.

*Linux*ov *IP Tables* programski paket podržava *stateful inspection* način rada i pri tome pojedinim vezama dodjeljuju određena stanja. Stanja ključna za filtriranje prometa baziranog na *IP Tables* programskom paketu su NEW, ESTABLISHED i RELATED. NEW stanje označava pakete koji nisu dio uspostavljene konekcije i to su obično paketi koji pokušavaju uspostaviti konekciju. Nakon što se uspostavi konekcija prelazi se u ESTABLISHED stanje. Ukoliko je neka konekcija povezana s drugom vezom onda je ta konekcija označena RELATED stanjem. Primjer za takvu vezu je FTP podatkovna veza koja je povezana s FTP kontrolnom vezom. Osim spomenutih postoji i INVALID stanje koje označava sve pakete koji se ne mogu identificirati, ili im nije pridruženo ni jedno drugo stanje. Da bi IP Tables za određeni mrežni paket znao u kojem se stanju nalazi, analiziraju se izvorišne i odredišne IP adrese, TCP portovi, brojevi TCP sekvenci, te dodatno TCP zastavice mrežnih paketa.

Vatrozid ugrađen npr. u WinXP će propustiti sve odlazeće pakete, ali će dopustiti prolaz samo onim paketima koji su dio ESTABLISHED veze, sprječavjući na taj način bilo kakav upad na zaštičen stroj od strane hakera.

Svi paketi koji dolaze s mreže koja nije povjerljiva analiziraju se, a pomoću internih tablica utvrđuje se koje stanje je pridruženo kojem paketu. Ukoliko je paket dio ESTABLISHED ili RELATED konekcije, paket se prosljeđuje. Zahtjevi za uspostavom nove konekcije u pravilu se prihvaćaju samo s mreža koje se štite i ukoliko su usmjereni prema poslužiteljima u DMZ-u (De-militarizirana zona). Takvim paketima se pridjeljuje stanje NEW. DMZ je mreža odvojena od interne mreže i u njoj se nalaze poslužitelji kojima korisnici javne mreže smiju pristupati (Web, Mail, FTP, ...).

Primjer za rad *stateful inspection*-a je sljedeći: ukoliko se korisnik iz zaštićene mreže odluči spojiti na vanjsku nezaštićenu mrežu vatrozid će mu to dozvoliti. Svi paketi koje korisnik sa svog računala šalje na mrežu dio su uspostavljene (engl. ESTABLISHED) veze. Također, svi paketi koje korisnik prima na svoje računalo s nezaštićene mreže dio su uspostavljene veze i

vatrozid ih propušta na određeni port. Ukoliko neko računalo iz nezaštićene mreže pokuša poslati paket na računalo na zaštićenoj mreži, taj paket biti će dio nove (engl. NEW) veze i vatrozid neće dozvoliti prosljeđivanje.

2.2. Prednosti

- Stateful inspection vatrozidi imaju jako malo utjecaja na ponašanje mreže, mogu se lako transparentno implementirati te su aplikacijski neovisni.

- Stateful inspection vatrozidi su prilično sigurni, ako ih usporedđujemo sa njihovim pretečama. Prodiru dublje u zaglavlje samog paketa da bi definirali vezu sa prethodnim paketima, te su tako bolje opremljeni za čuvanje protiv neželjenih ili neovlaštenih pristupa zaštićenoj mreži.

- Stateful inspection pruža svjesnost o protokolima aplikacijskog sloja. Ova metoda može potvrditi da se protokoli aplikacijskog sloja ponašaju kako se i očekuje od njih.

- Vatrozidi ove vrste često imaju određene sposobnosti zabilježavanja prometa (na taj način možemo identificirati i pratiti promet koji prolazi kroz vatrozid).

2.3. Nedostaci

- Stateful inspection vatrozid dozvoljava uspostavu direktne veze između dvije krajnje točke komunikacijskog kanala**.**

- Pravila i filtri ovog paketa mogu postati prilično složeni, teški za rukovanje, skloni pogreškama i te nezgodni za testiranje.

- Stateful inspection ne pruža veći stupanj sigurnosti motrenjem informacije o stanju veze.

3. Zaključak

Stateful inspection vatrozidi danas štite oko 80% mreža raznih poduzeća. No sama raširenost na tržištu ne kaže ništa o kavliteti. (Kad bi to bilo tako, lako bi bilo za zaključiti da su npr. Windowsi najbolji i najkvalitetniji OS koji je ikad postojao.)

Stateful inspection vatrozidi su prikladno sredstvo pružanja sigurnosti za mnoge svrhe. Dovoljno su dobri da bi se mnoga poduzeća pod njihovom zaštitom osjećala sigurno sa rijetkim probojima vatrozida. Nažalost, trojani i spyware programi nam demonstriraju kako nesputan transparentan pristup nije komatibilan s visokom sigurnošću.

Usporedno s razvojem vatrozida, razvijali su se i hakerski napadi. Hakeri više nisu mogli očekivati da će samo salanjem nepovezanog paketa uspjeti probiti ranjivi vatrozid. Njihovi novij i podmukliji pokušaji naveli su na razvoj Deep inspection firewalla kao snažnijeg, tehnološki naprednijeg potomka Stateful inspection firewalla. Za očekivati je da će se i ova tehnologija dalje razvijati.

Literatura:

- Skripte s predavanja kolegija «Sustavi za praćenje i vođenje procesa»
- Internet
  - www.carnet.hr
  - www.more.net/technical/netserv/tcpip/firewalls
  - www.checkpoint.com