

SEMINARSKI RAD

Zaštita RM(Firewalls)

<http://www.MATURSKIRADOVI.NET/>

SADRŽAJ

POGLAVLJE I

1.	Šta su firewall-oli.....	1
----	--------------------------	---

POGLAVLJE II

2.	Podjela potencijalnih napadača.....	3
2.1	Zaštita lokalne mreže od štetnog djelovanja 'napadača'.....	3
2.2	Zaštita od štetnog djelovanja lokalnih korisnika.....	4
2.3	Naplatna rampa	5
2.4	Osnovne koncepcije firewall skeniranja paketa	7
2.4.1	Statičko filtriranje paketa (eng. stateless inspection)	7
2.4.2	Filtriranje paketa zavisno o vrsti protkola.....	7
2.4.3	Filtriranje paketa zavisno o IP adresama odredišta tj izvorišta	7
2.4.4	Filtriranje paketa zavisno o odredišnim tj izvorišnim portovima	7
2.4.5	Filtriranje paketa zavisno o ruti usmjeravanja paketa (Eng.Source routing) ..	8
2.4.6	Filtriranje paketa zavisno o broju fragmentiranog paketa.....	8
2.5	Osnovne firewall konfiguracije	9
2.5.1	Dual-Homed gateway	9
2.5.2	Screened host gateway	10
2.5.3	Virtualne privatne mreže (VPN-Virtual private networks).....	11
2.5.4	Konfiguracija mreže bez servera	12
2.5.5	Konfiguracija mreže sa jednim serverom i jednim firewallom	12
2.5.6	Konfiguracija mreže sa serverima i dva firewall-a	14
2.5.7	Konfiguracija mreže sa demilitarizovanom zonom	15
2.5.8	Firewall-i zasnovani na hostu	16
2.5.9	Izolacijske mreže	17

POGLAVLJE III

3.1	Praktičan primjer realne konfiguracije firewall-a	18
3.2	Halted firewall-i	20
3.2.1	Uopšteno o halted firewallu	21
3.2.2	Prednost halted firewall-a	22

3.2.3	Nedostaci halted firewall-a	23
3.3	Firewall programi za personalne računare	24
3.4	Zaključak.....	26
	Literatura	27

POGLAVLJE I

1. UVOD

1.1.ŠTA SU FIREWALL-OLI?

Firewall je sigurnosni element smješten između neke lokalne mreže i javne mreže (Interneta), a koji je dizajniran kako bi zaštitio povjerljive, korporativne i korisničke podatke od neautoriziranih korisnika, (blokiranjem i zabranom prometa po pravilima koje definira usvojena sigurnosna politika). Nije nužno da svi korisnici u LAN-u imaju jednaka prava pristupa Internet mreži. Postavljanjem Firewall uređaja između dva ili više mrežnih segmenata može se kontrolirati i prava pristupa pojedinih korisnika pojedinim djelovima mreže. U takvom slučaju Firewall je dizajniran da dopušta pristup valjanim zahtjevima, a blokira sve ostale. Firewall ujedno predstavlja idealno rješenje za kreiranje Virtualne Privatne mreže jer stvarajući virtualni tunel kroz koji putuju kriptirani podaci.(omogućuje sigurnu razmjenu osjetljivih podataka među dislociranim korisnici) Firewall je servis (koji se tipično sastoji od firewall uređaja i Policy-a (pravilnika o zaštiti), koji omogućuje korisniku filtriranje određenih tipova mrežnog prometa sa ciljem da poveća sigurnost i pruži određeni nivo zaštite od provale.

Osnovna namjena Firewall-a je da spreči neautorizovani pristup sa jedne mreže na drugu. U suštini, ovo znači zaštitu unutrašnje mreže od Internet-a. Ako vaš sistem raspolaže Firewall-om, to znači da je odluka o tome šta je dozvoljeno, a šta nije - već donijeta. Ove odluke su u direktnoj vezi sa politikom sigurnosti vašeg informacionog sistema. Pri planiranju ponude informacionih servisa, politika sigurnosti određuje opcije konfiguracije servisa. Osnova rada Firewall-a je u ispitivanju IP paketa koji putuju između klijenta i servera, čime se ostvaruje kontrola toka informacija za svaki servis po IP adresi i portu u oba smjera. Za Firewall je tipičan i kompromis između sigurnosti i lake upotrebe. Stav da "sve što nije dozvoljeno je zabranjeno" zahteva da se svaki novi servis individualno omogućava.

Firewall je odgovoran za više važnih stvari unutar informacionog sistema:

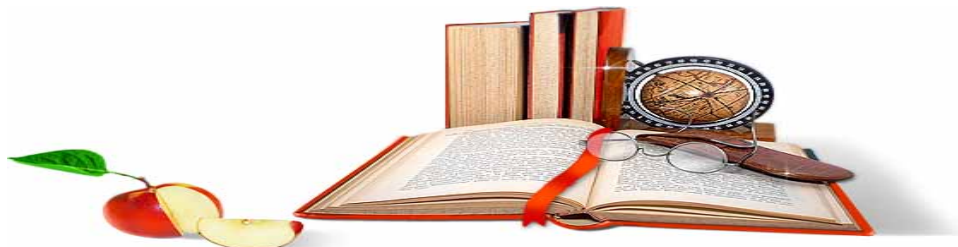
- Mora da implementira politiku sigurnosti. Ako određeno svojstvo nije dozvoljeno, Firewall mora da onemogući rad u tom smislu.
- Firewall treba da beleži sumnjive događaje.
- Firewall treba da upozori administratora na pokušaje proboja i kompromitovanja politike sigurnosti.
- U nekim slučajevima Firewall može da obezbedi statistiku korišćenja.

Firewall može biti softverski ili hardverski. Softverski firewall omogućuje zaštitu jednog računara , osim u slučaju kada je isti računar predodređen za zaštitu čitave mreže. Hardverski firewall omogućuje zaštitu čitave mreže ili određenog broja računara. Za ispravan rad firewall-a, potrebno je precizno odrediti niz pravila koja definiraju kakav mrežni promet je dopušten u pojedinom mrežnom segmentu. Takvom politikom se

**---- OSTATAK TEKSTA NIJE PRIKAZAN. CEO RAD MOŽETE
PREUZETI NA SAJTU WWW.MATURSKI.NET ----**

**[BESPLATNI GOTOVI SEMINARSKI, DIPLOMSKI I MATURSKI TEKST](http://WWW.SEMINARSKIRAD.ORG)
RAZMENA LINKOVA - RAZMENA RADOVA
RADOVI IZ SVIH OBLASTI, POWERPOINT PREZENTACIJE I DRUGI EDUKATIVNI MATERIJALI.**

**WWW.SEMINARSKIRAD.ORG
WWW.MAGISTARSKI.COM
WWW.MATURSKIRADOVI.NET**



NA NAŠIM SAJTOVIMA MOŽETE PRONAĆI SVE, BILO DA JE TO **[SEMINARSKI](#)**, **[DIPLOMSKI](#)** ILI **[MATURSKI](#)** RAD, POWERPOINT PREZENTACIJA I DRUGI EDUKATIVNI MATERIJAL. ZA RAZLIKU OD OSTALIH MI VAM PRUŽAMO DA POGLEDATE SVAKI RAD, NJEGOV SADRŽAJ I PRVE TRI STRANE TAKO DA MOŽETE TAČNO DA ODABERETE ONO ŠTO VAM U POTPUNOSTI ODGOVARA. U BAZI SE NALAZE **[GOTOVI SEMINARSKI, DIPLOMSKI I MATURSKI RADOVI](#)** KOJE MOŽETE SKINUTI I UZ NJIHOVU POMOĆ NAPRAVITI JEDINSTVEN I UNIKATAN RAD. AKO U **[BAZI](#)** NE NAĐETE RAD KOJI VAM JE POTREBAN, U SVAKOM MOMENTU MOŽETE NARUČITI DA VAM SE IZRADI NOVI, UNIKATAN SEMINARSKI ILI NEKI DRUGI RAD RAD NA LINKU **[IZRADA RADOVA](#)**. PITANJA I ODGOVORE MOŽETE DOBITI NA NAŠEM **[FORUMU](#)** ILI NA

maturskiradovi.net@gmail.com