

Sigurnosna stijena - firewall

Vrsta: Seminarski | Broj strana: 48

Sadržaj

1. Uvod.....	1	2. Osnovne funkcije, vrste i izvedbe sigurnosne stijene.....	2	1.2. Osnovne funkcije.....	2.2.2.
2.1. Osnovne funkcije.....		Vrste sigurnosnih stijena.....	3	2.2.1. Mosni filter.....	
2.2.1. Mosni filter.....		2.2.2. Filtri paketa.....		2.2.3. Intelligentni filtri paketa.....	
2.2.2. Filtri paketa.....		2.2.4. Aplikacijski posrednik.....	3 3 3	2.2.4. Aplikacijski posrednik.....	
2.2.3. Intelligentni filtri paketa.....		3. Izvedbe.....	4	3. Arhitekture sigurnosnih stijena i njihova prometna pravila.....	5
2.2.4. Aplikacijski posrednik.....		3.1. Računalo izvan zaštićenog područja.....	5 3.2.	3.1. Računalo izvan zaštićenog područja.....	5 3.2.
3. Vrste sigurnosnih stijena.....	3	Računalo unutar zaštićenog područja.....	6 3.3.	Računalo unutar zaštićenog područja.....	6 3.3.
4.2.2.1. Mosni filter.....		Demilitarizirana zona.....	7 3.4.	Demilitarizirana zona.....	7 3.4.
4.2.2.2. Filtri paketa.....		Demilitarizirana zona s dvije sigurnosne stijene.....	8	Demilitarizirana zona s dvije sigurnosne stijene.....	8
4.2.2.3. Intelligentni filtri paketa.....		4. Ostvarenje sigurnosne stijene.....	9	4.1. Preporučene mjere zaštite.....	9 4.2.
4.2.2.4. Aplikacijski posrednik.....		Osobna sigurnosna stijena.....	10 4.3.	Osobna sigurnosna stijena.....	10 4.3.
4.3. Računalo unutar zaštićenog područja.....		Komercijalna ostvarenja.....	11	4.3.1. Cisco PIX.....	11
4.3.1. Demilitarizirana zona.....		4.3.2. Check Point Firewall-1.....	11	4.3.2. Check Point Firewall-1.....	11
4.3.2. Demilitarizirana zona s dvije sigurnosne stijene.....		4.4. Netfilter/iptables.....	11 4.5.	4.4. Netfilter/iptables.....	11 4.5.
4.3.3. Računalo unutar zaštićenog područja.....		OpenBSD PF.....	12 4.6.	OpenBSD PF.....	12 4.6.
4.3.4. Demilitarizirana zona.....		Ispitivanje sigurnosne stijene.....	13 4.7. Ostali tipovi zaštite.....	Ispitivanje sigurnosne stijene.....	13 4.7. Ostali tipovi zaštite.....
4.3.5. Demilitarizirana zona s dvije sigurnosne stijene.....		4.7.1. Sustavi detekcije upada.....	13	4.7.1. Sustavi detekcije upada.....	13
4.3.6. Računalo unutar zaštićenog područja.....		Honey – Pot, Net, Wall.....	14	Honey – Pot, Net, Wall.....	14
4.3.7. Demilitarizirana zona.....		Virtualne privatne mreže.....	15	Virtualne privatne mreže.....	15
4.3.8. Računalo unutar zaštićenog područja.....		Budućnost – DPI.....	16	Budućnost – DPI.....	16
4.4. Komercijalna ostvarenja.....		5. Praktični dio.....	17	5. Praktični dio.....	17
4.4.1. Demilitarizirana zona.....		5.1. Teorijski uvod - IPsec.....	17	5.1. Teorijski uvod - IPsec.....	17
4.4.2. Demilitarizirana zona s dvije sigurnosne stijene.....		5.1.1. AH protokol.....	18	5.1.1. AH protokol.....	18
4.4.3. Računalo unutar zaštićenog područja.....		5.1.2. ESP protokol.....	19	5.1.2. ESP protokol.....	19
4.4.4. Demilitarizirana zona.....		5.1.3. IKE protokol.....	20	5.1.3. IKE protokol.....	20
4.4.5. Demilitarizirana zona s dvije sigurnosne stijene.....		Zaobilaznje utjecaja NAT-a.....	20	Zaobilaznje utjecaja NAT-a.....	20
4.4.6. Računalo unutar zaštićenog područja.....		5.2. IPsec-Tools.....	21	5.2. IPsec-Tools.....	21
4.4.7. Demilitarizirana zona.....		5.2.1. Alat setkey.....	21	5.2.1. Alat setkey.....	21
4.4.8. Računalo unutar zaštićenog područja.....		5.2.2. Alat racoon.....	22	5.2.2. Alat racoon.....	22
4.4.9. Demilitarizirana zona.....		5.2.3. Alat racoonctl.....	23	5.2.3. Alat racoonctl.....	23
4.4.10. Računalo unutar zaštićenog područja.....		5.3. Roadwarrior scenarij.....	24	5.3. Roadwarrior scenarij.....	24
4.4.11. Demilitarizirana zona.....		5.3.1. Konfiguracija mreže.....	25	5.3.1. Konfiguracija mreže.....	25
4.4.12. Računalo unutar zaštićenog područja.....		5.3.2. Konfiguracija poslužitelja.....	25	5.3.2. Konfiguracija poslužitelja.....	25
4.4.13. Demilitarizirana zona.....		5.3.3. Konfiguracija roadwarrior klijenta.....	27	5.3.3. Konfiguracija roadwarrior klijenta.....	27
4.4.14. Računalo unutar zaštićenog područja.....		5.3.4. Uspostava veze.....	30	5.3.4. Uspostava veze.....	30
4.4.15. Demilitarizirana zona.....		5.3.5. Windows XP klijent – ShrewSoft VPN Client.....	34	5.3.5. Windows XP klijent – ShrewSoft VPN Client.....	34

6. Zaključak..... 42 7.

Literatura..... 43

1. Uvod

Pojava širokopojasnog pristupa Internetu stvorila je izuzetno iskustvo administratora u računalnim mrežama. Brzi pristup je otvorio prostor mnogim inovacijama na području razmjene podataka, pristupa uređajima i drugim naprednim računalnim tehnologijama. Nažalost, ta tehnologija je također stvorila i lako dostupni put prema unutrašnjosti svake mreže, pa i svakog računala. Kako mreže postaju sve kompleksnije, postaju i napadači koji se pokušavaju infiltrirati u njih. Mrežna sigurnost više nije samo zaštita poslužitelja i radnih stanica. Danas ona zahtijeva detaljno razumijevanje mreže i spoznaju o ranjivostima mreže, kako u njenoj jezgri, tako i na njenim rubnim dijelovima. Kako su napadači postali sofisticiraniji, tako su se poboljšali i alati koje napadači koriste da bi se infiltrirali u mreže. Ti alati, većinom besplatni, dostupni su na različitim Web stranicama, te omogućuju i manje educiranim korisnicima da napadnu mreže. Danas napade na mreže izvode računalni početnici, lјuti kupci, bivši zaposlenici ili pak oni koji samo žele vidjeti što se sve može učiniti. Sve ove promjene su uzrokovale znatno otežavanje posla osiguranja mreža od napada. Čak je i broj uređaja koji se moraju štititi narastao. Administratori sigurnosti danas moraju odrediti da li se uopće radi o stvarnom napadu nekoga tko zna što radi, ili neki školarac isprobava novu programsku podršku za DoS (engl. denia

----- OSTATAK TEKSTA NIJE PRIKAZAN. CEO RAD MOŽETE PREUZETI NA SAJTU. -----

www.maturskiradovi.net

MOŽETE NAS KONTAKTIRATI NA E-MAIL: maturskiradovi.net@gmail.com