iptables – brzi pregled osnovnih funkcija

Lanac (CHAIN):	Opis:
INPUT	Promet koji poslužitelj prima
FORWARD	Promet koji poslužitelj usmjerava
OUTPUT	Promet koji poslužitelj šalje

Naredba:	Učinak
iptables -L	Ispisuje sadržaj iptablesa
iptables -A CHAIN [PRAVILO]	Dodaje pravilo u lanac (chain)
iptables -D CHAIN N	Briše pravilo rednog broja N iz lanca (N=1,2,3,4...)
iptables -F	Brisanje svih pravila u svim lancima
iptables -F CHAIN	Brisanje svih pravila u lancu
iptables-save > datoteka	Snimanje konfiguracije vatrozida u datoteku
iptables-restore < datoteka	Postavljanje konfiguracije vatrozida iz datoteke

Mete (TARGET):	Opis:
ACCEPT	Prihvati promet i završi prolaz kroz lanac
REJECT	Spriječi promet i završi prolaz kroz lanac
DROP	Odbaci promet bez javljanja greške i završi prolaz
LOG	Zabilježi okidanje pravila i nastavi prolaz

Parametri:	Opis:
-p PROTO	Odabir protokola (PROTO = tcp, udp, icmp, all)
-p PROTO -h	Ispiši moguća pravila za podudaranje za zadani protokol
-d DESTINATION	Odabir odredišta (IP, CIDR ili HOST)
-s SOURCE	Odabir izvora (IP, CIDR ili HOST)
-j TARGET	Skakanje na neku metu (Krajnji parametar)

Podudaranja:	Opis:
--dport PORT	Po ciljnom portu / protokolu (PORT= 22,23... www,smtp,pop3,telnet...)
--sport PORT	Po izvornom portu / protokolu (PORT= 22,23... www,smtp,pop3...)
-m mac --mac-source MAC	Podudaranje po MAC adresi
-m multiport	Podudaranje po više portova (--ports --sports)

Tonimir Kišasondi v.0.1

Primjer pravila:	Opis:
iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT iptables -A INPUT -j REJECT	Odbijanje svog ulaznog prometa osim naših uspostavljenih veza
iptables -A OUTPUT -p tcp --dport www -j REJECT	Blokiranje izlaznog WWW prometa
iptables -A OUTPUT -p tcp --dport smtp -j REJECT	Blokiranje izlaznog SMTP prometa
iptables -A OUTPUT -p tcp -d 64.58.76.0/24 --dport www -j REJECT	Blokiranje WWW prometa prema subnetu sa CIDR maskom
iptables -A OUTPUT -d www.net.hr --dport www -j REJECT	Blokiranje WWW prometa prema hostu
iptables -A INPUT -i lo -j ACCEPT	Prihvačanje prometa sa lokalnog računala
iptables -A INPUT -i lo -j ACCEPT iptables -A INPUT -m mac --mac-source 11:22:33:44:55:66 -j ACCEPT iptables -A INPUT -j REJECT	Prihvačanje prometa samo od računala sa određenom MAC adresom
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP	Odbacivanje ping-ova (ICMP echo)
iptables -A INPUT -i lo -j ACCEPT iptables -A INPUT -m multiport -p tcp --dport www,ssh,smtp -j ACCEPT iptables -A INPUT -j LOG iptables -A INPUT -j REJECT	Primanje WWW, SSH i SMTP prometa po tcp protokolu prema našem poslužitelju, sve ostale pokušaje bilježimo (LOG) te zabranjujemo
iptables -A INPUT -s 209.85.137.0/24 -j REJECT	Blokiranje prometa prema našem poslužitelju pomoću CIDR maske